Rocznik Bezpieczeństwa Morskiego

PRZESTĘPCZOŚĆ TELEINFORMATYCZNA 2022

Pod redakcją:

Jerzego Kosińskiego
Roberta Janczewskiego

Gdynia 2023

Recenzenci:
prof. dr hab. Krzysztof FICOŃ
dr hab. Bartłomiej PĄCZEK

© Copyright by:
Wydawca

Wszystkie prawa zastrzeżone. Książka ani żadna jej część nie może być powielana ani rozpowszechniana za pomocą urządzeń elektronicznych i mechanicznych bez pisemnej zgody posiadaczy praw autorskich.

Wydawca:
WYDAWNICTWO BP
ul. Modrzewiowa 2c/22, 81-074 Gdynia
bartlomiej@paczek.eu

Współwydawca:
Wydział Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej
im. Bohaterów Westerplatte w Gdyni

ISSN 1898-3189

Poglądy wyrażone w rozdziałach nie zawsze są zgodne z poglądami redaktorów.
Publikowane referaty nie były poddane pracom korektorskim w Wydawnictwie
i są publikowane w postaci dostarczonej przez autorów.

SPIS TREŚCI

Wstęp

Najnowsze techniczne i technologiczne rozwiązania w dziedzinie teleinformatyki stwarzają warunki do wygodnego życia. Niestety, są również wykorzystywane przez przestępców do wielu, różnych działań przestępczych. Działania nieuczciwych i wrogich podmiotów zarówno indywidualnych jak i zespołowych; państwowych lub niepaństwowych; krajowych lub zagranicznych mają różne podłoża. Ich motywacje mogą pozostać nieznane, tożsamość nieustalona, a to może skutkować uniknięciem wykrycia i odpowiedzialności karnej. Szybki rozwój teleinformatyki utworzył specyficzną sferę swoistej walki. Przestępcy w coraz bardziej złożony, czasem dyskretny i wręcz niezauważalny sposób wykorzystują cyberprzestrzeń do uzyskania swoich sprzecznych z prawem korzyści. Podmioty zaatakowane dążą do opracowania skutecznych narzędzi na wielu poziomach: technicznym, prawnym, ekonomicznym, proceduralnym czy organizacyjnym.

Wychodząc naprzeciw potrzebom stworzenia warunków do dyskusji, dzielenia się doświadczeniami, prezentowania i omawiania najnowszych rozwiązań przeciwdziałania przestępczości teleinformatycznej, wypracowywania wspólnego punktu widzenia podmiotom zajmującym się lub zainteresowanym zwalczaniem negatywnych, niezgodnych z prawem działań wykorzystujących cyberprzestrzeń tradycyjne, w murach Akademii Marynarki Wojennej, w 2022 roku zorganizowana została doroczna, kolejna edycja Konferencji Naukowej Przestępczość Teleinformatyczna XXI (PTXXI). Zgromadziła ona bardzo liczne grono (ok. 300) uczestników, którzy uczestniczyli w wielu tematycznych, poświęconym różnym aspektom cyberprzestępczości sesjach. Ta edycja konferencji poświęcona została tematyce trendów cyberprzestępczości, monitorowaniu zagrożeń w Internecie, dowodów cyfrowych oraz zwalczaniu cyberprzestępczości.

Konferencję otworzył poprzez wygłoszenie przemówienia powitalnego kontradmirał prof. dr hab. Tomasz Szubrycht - Rektor-Komendant Akademii Marynarki Wojennej. Przemówienia powitalne wygłosili także Bogna Niklasiewicz - Dyrektor Działu Trust and Safety, Allegro.pl, Tomasz Zdzikot - Przewodniczący Zespołu Doradców Społecznych Ministra Obrony Narodowej ds. Cyberbezpieczeństwa oraz mł. insp. Michał Pudło - Zastępca Komendanta CBZC. W trakcie tego trzydniowego spotkania naukowego wystąpiło 75 prelegentów w wielu zarówno w polskojęzycznych jak i anglojęzycznych sesjach tematycznych. W trakcie konferencji odbywały się także warsztaty.

W pierwszym dniu (poniedziałek, 13.06.2022 r.) w dwóch równoległych ścieżkach tematycznych wygłoszono następujące referaty:

- Obserwacje i doświadczenia Działu Bezpieczeństwa Allegro – Jakub Kalinowski, Allegro.pl;
- 3 ciekawe techniki OSINT-u – Piotr Konieczny, niebezpiecznik.pl;
- Rosyjskie cyberataki na Ukrainę – Robert Kośla, Microsoft;
- Współpraca organów ochrony danych i organów ścigania – Wojciech Wiewiórowski, Europejski Inspektor Ochrony Danych;
- Ukraińska cyberobrona obywatelska – Jan Ukraiński, Civil Network OPORA;
- Czy polski ekosystem prawny jest przyjazny dla stworzeń mitycznych i bytów nadprzyrodzonych – Wojciech Pilszak, e-Detektywi sp. z o.o.;
- The Real Ransomware Heroes – Anna Krakowska, Sekurak
- Przyszłość kontroli operacyjnej – Aleksander Goszczycki, Matic S.A.;
- Why your cyber practice needs proactive cyber threat intelligence – Sean Cooper, Team Cymru;
- Digital Twins in operational Areas Mathias Fanning – Hexagon/Leica Swiss;
- Forensic analysis of Flash memory using X-ray and Logic analyzer – Alexander Sheremetov, Rusolut;
- Harnessing Tech, Tradecraft and Crowdsourcing to Derail Modern Threats – Johna Dellingera, Microsoft;
- Wymagania SWIFT i DORA a bezpieczeństwo transakcji płatniczych – Adam Mizerski, Getin Noble Bank S.A.; ISACA Katowice Chapter;
- SIM SWAP - wybrane prawne i organizacyjne wyzwania prowadzenia postępowań przygotowawczych – Agnieszka Gryszczyńska, UKSW; Prokuratura Krajowa;
- Bezpieczeństwo płatności mobilnych w dobie oszustw w sieci, czyli rzecz o prewencji społecznej i współpracy z organami ścigania w perspektywie BLIKA – Anna Koral, PSP (BLIK);
- Metody zapobiegania phishingowi oraz ich skuteczność w serwisie OLX – Marcin Siemek, OLX;
- Przestępczość e-commerce z perspektywy agenta rozliczeniowego – Adam Węgrowski, PayU S.A.;

- Ciągłość działania banków w obliczu kryzysu wywołanego wojną w Ukrainie w świetle rekomendacji Związku Banków Polskich – Jarosław Biegański, FinCERT.pl-Bankowe Centrum Cyberbezpieczeństwa ZBP.

Odbyły się także warsztaty:

- Warsztaty: Cybertwierdza – prowadzący: Fundacja Bezpieczna Cyberprzestrzeń.

W drugim dniu (wtorek, 14.06.2022 r.) także w dwóch równoległych ścieżkach tematycznych wygłoszono następujące referaty:

- Blaski i cienie "Dyrektywy e-evidence" (CLOUD Act.) – Wojciech Wiewiórowski, Europejski Inspektor Ochrony Danych;
- Predictive policing, czyli czy można przewidzieć przestępczość – Krystian Wojciechowski;
- O interpretowaniu zagrożeń i ich skutków – Krzysztof Liderman, WAT;
- Komu potrzebny kolejny agent? – Michał Jarski, Forcepoint;
- Wykorzystanie narzędzi informatyki śledczej, analizy danych i OSINT-u w walce z kryzysem migracyjnym – Betina Tynka, Mediarecovery;
- Detekcja nadużyć online z wykorzystaniem technologii cyfrowej tożsamości – Jakub Antczak, LexisNexis® Risk Solutions;
- Ekstrakcja dowodów z urządzeń IoT z użyciem metody Chip-off – Michał Gmurek, Rusolut;
- Zagrożenia wektora webowego – Bartosz Kwitkowski, PreBytes
- Kryminalistyczne badanie dronów – Łukasz Grzyb, AMW;
- Nowoczesna dokumentacja 3D chemicznie ujawnionych śladów krwawych – Kacper Choromański, Uniwersytet Warszawski;
- Dyskrecja i rozwaga ochronią Cię przed utratą tożsamości. Czyli o spoofingu w telefonii mobilnej – Krzysztof Czarnacki, Polkomtel, Paweł Baraniecki;
- Spoofing – case study – Michał Gołda, Wojciech Smoleń, Prokuratura Regionalna Warszawa;
- QR-code – jaką pojemność ma idea? – Grzegorz Piaskowski, KWP Katowice;
- Zonda – Artur Kubiak, Zonda;
- Zonda - studium przypadku – Marcin Borówka, Zonda;
- Najnowsze trendy przestępczości kryptowalutowej – Jacek Charatynowicz, CBŚP;

- Możliwości ustalenia w blockchain na przykładach prowadzonych spraw – Paweł Gonkiewicz, KWP Kraków;
- Ustalenie składników majątkowych i zabezpieczenie mienia w postaci kryptowalut – Robert Kawęcki, CBŚP Lublin;
- Stan regulacji prawnych związanych z kryptowalutami – Wojciech Ryżowski, GIIF;
- Jak UKNF widzi kwestię kryptoaktywów i technologii blockchain – Jakub Karmowski, UKNF;
- Wykorzystanie analityki grafowej doidentyfikacji działań dywersyjnych na wschodniej flance NATO – Łukasz Wołonciej, Kamil Góral, DataWalk;
- „Narzędzia hackerskie" – aspekty prawne i techniczne – Filip Radoniewicz, ASzWoj.

Odbyły się także warsztaty:

- Warsztaty: SPARTA – prowadzący: BI KGP, PPBW, MCC (wyłącznie dla funkcjonariuszy);
- Warsztaty: Case Study: Zabezpieczenie dowodów i śladów w środowiskach zwirtualizowanych i data center - apsekty prawne – Michał Paluszek, 3S Data Center, Krzysztof Szukała, 3S Data Center;
- Warsztaty: Case Study: Zabezpieczenie dowodów i śladów w środowiskach zwirtualizowanych i data center – Andrzej Szymczak, Vmware Łukasz Wimowski, Altpi (Partner Veeam) Anna Krakowska, Sekurak (wyłącznie dla funkcjonariuszy);
- Warsztaty: Hands-On Virus Total Andrea Lois, Google Cloud Security (Virus Total) – Anna Krakowska, Sekurak (wyłącznie dla funkcjonariuszy);
- Warsztaty: Studium przypadku przestępczej działalności w sieci na przykładzie prowadzonej sprawy operacyjnej – prowadzący: Żandarmeria Wojskowa, VSData (wyłącznie dla funkcjonariuszy);
- Warsztaty: Zabezpieczanie cyfrowego materiału dowodowego, za pomocą narzędzi linuksowych – prowadzący: Kacper Kulczycki, 1HSDR&C.

W trzecim dniu (środa, 15.06.2022 r.) wygłoszono następujące referaty:

- Propaganda i dezinformacja w cyberprzestrzeni – Piotr Dela, Robert Janczewski, Jakub Syta, MMC;

- Nieskuteczne zabezpieczanie danych internetowych na wniosek-prywatny, czyli rzecz o tym, jak e-przedsiębiorcy nieświadomie (?) pomagają przestępcom – Maciej Kołodziej, e-Detektywi sp. z o.o.;
- Oszustwo na Midasa czyli inwestor rynku forex, modus operrandi i trudności dowodowe – Dariusz Podufalski, Prokurator Bydgoszcz;
- Operacja Winnti: branża gier wideo w realnym zagrożeniu? – Marek Piotr Stolarski, Techland S.A.;
- Credential stuffing na bazie ataku na Profil Zaufany - studium przypadku – Kamil Kołodziejczyk, Rafał Zatara, WCB KSP;
- Konsumpcja treści w dobie pandemii i metody przeciwdziałania ich kradzieży – Teresa Wierzbowska, Stowarzyszenie Sygnał;
- Akcja „follow the money" – o odcinaniu piratów od źródeł finansowania – Karolina Makowska, Stowarzyszenie Sygnał;
- Naprawa szkody w praktyce – analiza przypadków – Łukasz Sternowski, Stowarzyszenie Sygnał;
- OSINT w identyfikacji naruszeń praw własności intelektualnej – narzędzia i efekty – Michał Otrębski, NAGRA;
- Problemy dowodowe w postępowaniach dotyczących sharing – Tomasz Szymula, Stowarzyszenie Sygnał;
- All the Jazz – Zbigniew Jakubowski, Compendium;
- Stochastyczne efekty w nowych typach pamięci półprzewodnikowych na potrzeby bezpieczeństwa układów elektronicznych – Piotr Wiśniewski, Romuald B. Beck, CEZAMAT, Politechnika Warszawska;
- Projekty europejskie z obszaru cyberbezpieczeństwa – Marek Wierzbicki, Klaudia Kaczmarek, Polska Platforma Bezpieczeństwa Wewnętrznego.

Oddana w państwa ręce monografia składa się 15 zróżnicowanych tematycznie rozdziałów oraz jednego załącznika. Zakres tematyczny niniejszej publikacji jest szeroki. W monografii dominuje wieloaspektowe spojrzenie na tematykę cyberprzestępczości obejmujące zagadnienia prawne, techniczne i organizacyjne, przedstawione w wymiarze praktycznym i teoretycznym.

Życząc czytelnikom przyjemnej lektury zachęcamy do kontaktu z redaktorami, w sprawie kolejnych edycji konferencji i monografii.

Jerzy Kosiński (j.kosinski@amw.gdynia.pl)
Robert Janczewski (r.janczewski@amw.gdynia.pl)

Rozdział 1

Zagrożenia informacyjne w cyberprzestrzeni - dezinformacja i propaganda

Piotr DELA[1]

STRESZCZENIE: W artykule przedstawiono najważniejsze elementy zagrożeń informacyjnych w cyberprzestrzeni główną uwagę skupiona na dwóch głównych aspektach tych zagrożeń, a mianowicie dezinformacji i propagandzie.

SŁOWA KLUCZOWE: cyberprzestrzeń, walka informacyjna, dezinformacja, propaganda.

Wstęp

Informacja zawsze stanowiła zasób strategiczny. Decydowała o zwycięstwach i porażkach, kreowała poglądy i postawy, wyznaczała kierunki działania, oblała władców, wzniecała rewolucje, powodowała biedę lub decydowała o bogactwie. Z tego też względu stanowiła najcenniejszy zasób, który należało za wszelką ceną chronić i jednocześnie nieustannie pozyskiwać, zdobywać. Współcześnie, w świecie, w którym króluje sieci Internet, dostęp do informacji stał się niebywale prosty i szybki. Środowisko te, określane także mianem cyberprzestrzeni spowodowało równocześnie, nieznane wcześniej, wyzwania związane z ochroną posiadanych zasobów informacyjnych. Informacja stała się zasobem, o który toczone są walki w świecie rzeczywistym, ale coraz częściej w cyberprzestrzeni. Dlatego też rozwijane są w coraz większym stopniu systemy ochronno-obronne, które mają przeciwstawić się coraz bardziej wyrafinowanym metodom ataku ukierunkowanym na przejęcie, modyfikację lub zniszczenie informacji. To swoisty wyścig zbrojeń, w którym przewagę zawsze będzie posiadał agresor jako ten, który posiada inicjatywę i przewagę informacyjną.

[1] Prof. dr hab. inż., e-mail: p.dela@amw.gdynia.pl; p.dela@akademiakaliska.edu.pl; ORCID: https://orcid.org/0000-0003-3643-3759

O wiele większym wyzwaniem, przed którym stoją współczesne państwa i społeczeństwa jest wykorzystanie informacji jako narzędzia ataku, broni służącej do ataku na konkretną grupę osób, społeczeństwo, naród, państwo. Informacja jako broń wykorzystywana była zawsze, niemniej jednak nigdy nie było to stosowane na taką skalę, jak współcześnie. Związane to jest oczywiście z rozwojem cyberprzestrzeni, która jest doskonałym środowiskiem rozprzestrzeniania informacji do ogromnej liczby osób w bardzo krótkim czasie.

Sama *informacja*, postrzegana w tym przypadku jako narzędzie ataku, definiowana jest różnorodnie, czasami wręcz sprzecznie lub zamiennie z takim określeniami jak dane, wiedza czy mądrość. Z punktu widzenia nauki, w ujęciu zarówno teoretyków, jak i praktyków, *informacja* jest pojęciem pierwotnym, niedającym się zdefiniować, zidentyfikować, zaszufladkować. Uwarunkowane to jest między innymi tym, że informacja funkcjonuje w środowisku politycznym, fizycznym, matematycznym, ekonomicznym, religijnym, prawnym i wielu innych. Znamienna grupa autorów rezygnuje z definiowania informacji, poprzestając na jej intuicyjnym i potocznym rozumieniu. Należy jednak zaznaczyć, że sam termin *informacja* wywodzi się z łacińskiego słowa *informatio*, określanego jako *wyobrażenie, wyjaśnienie, zawiadomienie*, co pozwala na wyciągnięcie wniosków, że dotyczy ona sfery postrzegania przez odbiorcę tejże informacji. Patrząc przez pryzmat dorobku wielu pokoleń naukowców zajmujących się teorią informacją można dostrzec, że największy dorobek w tym obszarze mieli Claude E. Shannon, Norbert Wiener, Russell L. Ackoff, Andrew Webster. Identyfikowali oni informację jako [8]:

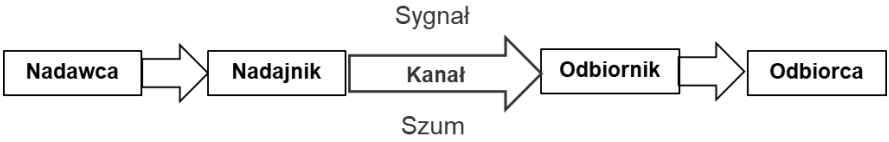
- *Informacja to komunikacja, łączność, w wyniku której likwiduje się nieokreśloność (Claude E. Shannon).*
- *Informacja jest nazwą treści zaczerpniętej ze świata zewnętrznego, nie jest więc ani materią, ani energią (Norbert Wiener).*
- *Jest to przekazywanie wiedzy do odbiorcy informacji, ze względu na jej wartość, umożliwiające zmniejszenie niepewności działania odbiorcy informacji (Russell L. Ackoff).*
- *Informacja jest to wiedza przekazywana przez innych ludzi bądź uzyskiwana przez studia, obserwacje, badania (Andrew Webster).*

W polskiej przestrzeni znamienne są podglądy Leopolda Ciborowskiego, który podjął się analizy terminu *informacja*, powołując się na definicje

stworzone przez naukowców z obszaru cybernetyki i fizyki. Zauważył, że informacja jest bodźcem oddziałującym na układ recepcyjny człowieka, który skutkuje stworzeniem, w jego wyobraźni, przedmiotu myślowego, odzwierciedlającego obraz rzeczy kojarzącym się z tym bodźcem. Ciborowski zauważa, że związek między człowiekiem i informacją jest nierozerwalny: *tak jak foton nie może istnieć bez pędu, tak informacja nie może istnieć bez umysłu ludzkiego. Tylko ten organ natury ludzkiej dostosowany jest do nieskończonego przetwarzania transformowanych doznań recepcyjnych w wyobrażenia informacyjne.* […] *każda informacja jest szczególną formą sygnału, która oprócz wspólnych cech wyróżnialności, właściwych dla sygnału i informacji, posiada jeszcze tę właściwość, że inspiruje umysł ludzki do tworzenia pewnej wyobraźni [4].* Tym samym można uznać, że informacja jest zależna od człowieka, gdyż powstaje w jego umyśle. Z kolei Piotr Sienkiewicz postrzega informację jako *zbiór faktów, zdarzeń, cech, obiektów ujęty w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne [21]*. Pogląd ten jest zbieżny z poglądami Ciborowskiego, z tym, że w powyższej definicji nie zdefiniowano kim jest odbiorca informacji. Należy domniemywać, że jest nim człowiek.

Informacja jest podstawą do budowania każdego systemu wiedzy i wartości. Warunkuje sukces w każdej dziedzinie, w szczególności w takich sferach, jak: gospodarka, ekonomia, polityka, bezpieczeństwo, nauka. Powyższe jest prawdziwe wtedy i tylko wtedy, gdy system wiedzy będzie budowany w oparciu o wiarygodne i aktualne informacje, a procesy przekazywania informacji nie będą zakłócane lub manipulowane.

W przytaczanych definicjach pojawia się aspekt przekazywania informacji, określany jako komunikacja, komunikowanie. Zgodnie z zapisami encyklopedycznymi komunikowanie to: *podać coś do wiadomości; przekazać jakąś informację, zawiadomić o czymś[22]*. *Komunikować się* zdefiniowano jako: *utrzymywać z kimś kontakt, porozumiewać się*. Przekazywanie informacji w akcie komunikowania, postrzegane jako proces komunikacji międzyludzkiej, zostało zobrazowane w modelu Claude Shannon, na rysunku 1 [9].



Źródło: M. Rehfisch, Omnichannel Banking: A Prerequisite for a Seamless Customer Journey, https://www.knowis.com/blog/omnichannel-banking-a-prerequisite-for-a-seamless-customer-journey, stan z dn. 29 czerwca 2021.

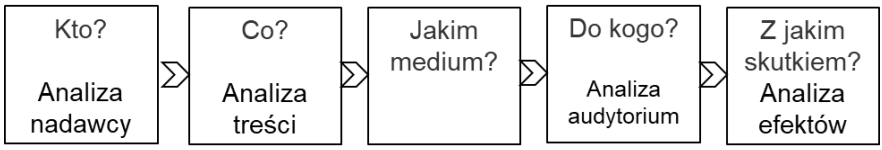
Rysunek 1. Model komunikacyjny Shannona

W powyższym modelu proces przekazywania informacji rozpoczyna się od nadawcy, określanego zamiennie mianem źródła informacji. Przekaz ten (informacja w postaci danych) jest przetwarzany przez nadajnik w sygnał (zrozumiały dla systemów technicznych), który za pośrednictwem kanału jest przekazywany do odbiornika, gdzie następuje jego zamiana na postać zrozumiałą dla odbiorcy (dane, które odbiorca potrafi przekształcić w informację). Sam sygnał jest podatny na różnorodne szumy (najczęściej są to zakłócenia wynikające ze złożoności systemu technicznego), mające wpływ na jego poprawną interpretację przez odbiornik. Komunikacja w tym modelu może być podzielona na osiem zasadniczych elementów [9]:

1. Źródło jest twórcą aktu komunikacji;
2. Przekaz jest treścią komunikacji, informacją, która jest przekazywana;
3. Koder przetwarza informację w formę, która może być zakomunikowana, także w postaci, która nie jest bezpośrednio rozumiana przez ludzkie zmysły;
4. Kanał jest medium lub systemem transmisyjnym używanym dla przekazu komunikatu z jednego miejsca do innego;
5. Dekoder odwraca proces kodowania;
6. Odbiorca jest adresatem komunikacji;
7. Sprzężenie zwrotne między źródłem a odbiorcą może służyć do regulacji przepływu komunikacji;
8. 8. Szum jest niepożądanym zniekształceniem, które może zakłócać wymianę informacji.

Model Shannona jest wykorzystywany w systemach technicznych, a jego najprostszymi reprezentantami są modele odniesienia ISO/OSI i TCP/IP. Szum powstający w kanale komunikacyjnym jest pochodną stosowanych rozwiązań technicznych i związaną z nimi niezawodnością i wydajnością. Szum może być również powodowany celowym oddziaływaniem na funkcjonalność kanałów komunikacyjnych. W tym przypadku mamy do czynienia z działaniami ukierunkowanymi na funkcjonalność systemów technicznych, najczęściej określanych jako cyberzagrożenia.

Odmiennie proces przekazywania informacji jest postrzegany w modelu Horolda Lasswell, który odnosi się do form międzyludzkiego komunikowania, w których nadawca za główny cel przekazu stawia sobie zmianę postaw, poglądów lub zachowania odbiorców. Model ten jest wykorzystywany do tworzenia kampanii informacyjnych, prowadzonych za pośrednictwem środków masowego przekazu, ukierunkowanych na manipulowanie świadomością odbiorców. Współcześnie środowiskiem przekazu sprzyjającym manipulowaniu jest cyberprzestrzeń z wiodącą rolą portali społecznościowych. Omawiany model składa się z pięciu zasadniczych części, przedstawionych na rysunku 2 [9].



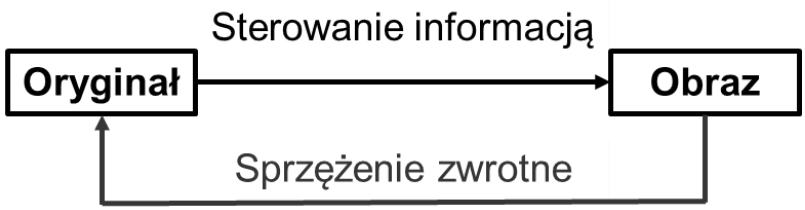
Źródło: M. Rehfisch, Omnichannel Banking: A Prerequisite for a Seamless Customer Journey, https://www.knowis.com/blog/omnichannel-banking-a-prerequisite-for-a-seamless-customer-journey, stan z dn. 29 czerwca 2021.

Rysunek 2. Model analizy aktu komunikowania Harolda Lasswella

Przeprowadzone analizy wykazały, że współcześnie informacja jest czymś dużo więcej niż tylko wiadomością, znakiem lub inną formą komunikowania. W swojej istocie jest ona zarówno opisem rzeczywistości, jak i odzwierciedleniem tej rzeczywistości, niekoniecznie z nią zgodnym.

Analizy wykazały, że podstawą współczesnych zagrożeń informacyjnych jest sterowanie informacją, której podwaliny wywodzą się z cybernetyki, a konkretnie z pracy Norberta Wienera zatytułowanej Cybernetics *or Control*

and Communication in the Animal and the Machine [26]. Z kolei Marian Mazur w opracowaniu Jakościowa *teoria informacji [18]* przedstawił i wyodrębnił te elementy cybernetyki, które są wykorzystywane głównie jako narzędzie walki informacyjnej. Przedmiotami stworzonej teorii sterowania informacją, głównie w ujęciu jakościowym są systemy i relacje zachodzące między nimi, co przedstawiono na rysunku 3 [18].



Źródło: M. Rehfisch, Omnichannel Banking: A Prerequisite for a Seamless Customer Journey, https://www.knowis.com/blog/omnichannel-banking-a-prerequisite-for-a-seamless-customer-journey, stan z dn. 29 czerwca 2021.

Rysunek 3. Proces sterowania i tworzenia informacji

W powyższym ujęciu *sterowanie informacją*, pomiędzy oryginałem a obrazem, polega na transformacji informacji zarówno wiernej, jak i zniekształconej. Przykładem systemu korzystającego ze sprzężenia zwrotnego jest człowiek, postrzegany jako jednostka sterowalna, podatna na manipulacje, perswazję, czy też działania pod przymusem, a zarazem sterująca, motywująca inne osoby do działania. Sterowanie informacją może mieć formę aktywną, w której generowane są informacje ukierunkowane bezpośrednio na sterowanie obiektem oddziaływania, jak również formę pasywną, w której informacja jest biernie wykorzystywane do sterowania wieloma obiektami.

Dezinformacja

W najprostszym ujęciu *dezinformacja* jest przeciwieństwem informacji i oznacza informacją fałszywą, niezgodną z prawdą. Jest ukierunkowana na wprowadzanie w błąd odbiorcy informacji, co zostało odzwierciedlone w encyklopedycznej i słownikowej definicji, mówiącej, że jest to wprowadzenie *kogoś w błąd przez podanie mylących lub fałszywych informacji [11].* Inne

definicje identyfikują dezinformację także jako *proces polegający na celowym, błędnym informowaniu [16]*, lub też jako *sytuację, w której brakuje rzetelnych informacji [6]*.

Termin dezinformacja po raz pierwszy pojawił się w 1926 roku w londyńskim miesięczniku *The Whitehall Gazette & St James's Review [24]*. Określenia tego użyto do opisu działania sowieckich służb specjalnych. Rok później, w piśmie *Siegodnia,* wspomniano, że dezinformacja należy do głównych działań GPU (Państwowy Zarząd Polityczny przy Ludowym Komisariacie Spraw Wewnętrznych Rosyjskiej Federacyjnej Socjalistycznej Republiki Radzieckiej) [7]. Paradoksem definicyjnym dezinformacji jest to, że historia powstania samego terminu związana jest z bezpośrednio z sowiecką dezinformacją. Jest to związane z definicją zawartą w *Wielkiej Encyklopedii Radzieckiej* z 1952 roku, w której to odniesiono się do jej *rzekomego* francuskiego pochodzenia i jej powszechnym stosowaniu przez kapitalistyczne media do, jak to określono, ogłupiania ludzi. Do dziś treści te są powszechnie używane do identyfikowania pochodzenia dezinformacji [19].

Inny pogląd na dezinformację został zidentyfikowany przez Vladimira Volkoffa, który postrzega ją zarówno w ujęciu *wąskim,* jak i *szerokim. W wąskim tego słowa znaczeniu mieści się ona w połowie drogi między wprowadzeniem w błąd a wpływaniem. Podczas gdy wprowadzanie w błąd* […] *jest czynnością jednorazową, związaną z konkretnym zadaniem, dopuszcza pewną amatorszczyznę, wykorzystuje najprzeróżniejsze środki i zmierza do wmówienia pewnych określonych rzeczy określonym osobom, dezinformacja jest prowadzona w sposób systematyczny, fachowy zawsze za pośrednictwem mass mediów i jest adresowana do opinii publicznej, a nie sztabów krajów – obiektów działań. I analogicznie: podczas gdy wpływanie przejawia się w działaniach pozornie niezorganizowanych, oportunistycznych, głównie ilościowych, dezinformacja stawia sobie za cel realizację konsekwentnego programu zmierzającego do zastąpienia w świadomości, a przede wszystkim podświadomości mas będących przedmiotem tych działań, poglądów uznanych za niekorzystne dla dezinformatora takimi, które uważa on za korzystne dla siebie [25]*. Vladimir Volkoff zidentyfikował także metody dezinformacji, takie jak [25]: odwrócenie faktów, negacja faktów, mieszanie prawdy i kłamstwa, rozmycie, kamuflaż, interpretacja, generalizacja, ilustracja, nierówna reprezentacja, równa reprezentacja. Techniki te, stosowane są we wszelkiego rodzaju manipulacjach informacyjnych oraz kampaniach dezinformacyjnych i nie wyczerpują całego arsenału metod i narzędzi dezinformacji.

Początków dezinformacji można dopatrywać się już w starożytności, w najstarszych rozwiniętych cywilizacji czy też początkach zorganizowanych konfliktów zbrojnych. Przykładem mogą być rozważania Sun Tzu, który uważał, że *wojna jest to wprowadzanie w błąd. Jeśli zatem jesteś zdolny, udawaj mało zdolnego. Gdy porywasz swoje wojska do działania, udawaj bierność. Jeżeli twój cel jest bliski, zachowuj się tak, jakby był odległy. A gdy jest odległy, udawaj, że jest bliski [23].* W każdym konflikcie niezbędnym, kluczowym elementem jest umiejętność i zdolność wprowadzania przeciwnika w błąd, poprzez podawanie fałszywych informacji i tworzenia na ich podstawie fałszywego obrazu otoczenia. Dezinformacja jest zjawiskiem ponadczasowym, mocno zapisanym w przeszłości, teraźniejszości i przyszłości. Jest naturalnym elementem stosunków społecznych.

Dezinformacja posiada wymiar taktyczny i strategiczny. Taktyczna trwa krótko, kilka miesięcy, a jej główny cel jest ukierunkowany na wprowadzanie w błąd w jednej lub kilku powiązanych ze sobą kwestiach. Przykładami tego rodzaju dezinformacji mogą być np. podsunięcie fałszywych danych nowego rodzaju uzbrojenia, zmodyfikowanie danych statystycznych w celu wywołania opinii, iż stan gospodarki danego państwa jest lepszy lub gorszy od rzeczywistego, opublikowanie sfałszowanych materiałów kompromitujących polityka, partię lub też rząd. Z tego typu dezinformacją mamy do czynienia w trwającym konflikcie w Ukrainie

Z kolei dezinformacja strategiczna związana jest z systematycznym i długotrwałym przekazywaniu fałszywych informacji oraz zmodyfikowanych sygnałów politycznych, których głównym celem jest wytworzenie błędnego (zmodyfikowanego przez dezinformatora) obrazu rzeczywistości, ukierunkowanego na błędną ocenę sytuacji przez odbiorcę przekazów informacyjnych. To działanie ukierunkowane na wprowadzenie w błąd rywala, oponenta, adwersarza, co do podstawowych kwestii polityki państwa [14]. W przeciwieństwie do dezinformacji taktycznej, dezinformacja strategiczna jest prowadzona nawet kilkadziesiąt lat i należy do sfery działalności służb specjalnych. Przykłady dezinformacji strategicznej można znaleźć w książce Roya Godsona i Jamesa J. Wirtza *Stategic denial and deception [10]*.

Znamiennym przykładem kompleksowego dezinformowania jest teoria opracowana przez rosyjskiego psychologa i matematyka Władimira Lefewra, określana mianem *zarządzanie refleksyjne [27] (ang. reflexive control)*. Dezinformacja tego typu polega na tworzeniu specyficznego modelu obiektu podlegającemu sterowaniu. Obiekt ten, a jest nim osoba, grupa osób, społeczeństwo lub nawet cały naród, tworzy w swojej świadomości, nie tylko własny obraz świata, ale również posiada zdolności do analizowania własnych

myśli i wyobrażeń [2]. Według Lefewra zarządzanie refleksyjne to *podstępne, iluzoryczne działania oparte na prowokacji, intrygach i kamuflażu, wykorzystywanych do sterowania obrazami świata w świadomości podmiotu poznającego [13]*. Zastosowanie zarządzania refleksyjnego może doprowadzić do masowych zmiany w nastawieniu społeczeństwa. Do najważniejszych metod zalicza się [2]:

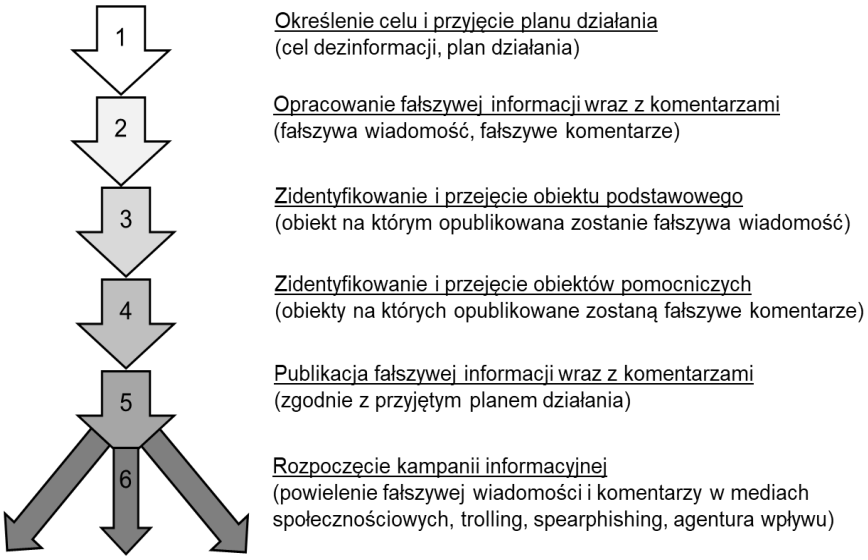
- metodę nacisków siłowych poprzez demonstrowanie siły militarnej, tworzenie sojuszy wojskowych, wsparcie dla wewnętrznych sił antyrządowych;
- metodę wywierania wpływu na podejmowanie decyzji przez przeciwnika, publikację fałszywych doktryn, strategii, planów, zamiarów;
- metodę kreowania i przekazywania fałszywych informacji o aktualnej sytuacji;
- metodę wpływania na czas decyzji przeciwnika poprzez eskalację nieprzewidywanych działań zbrojnych.

Wszystkie powyższe metody są wykorzystywane w konflikcie na Ukrainie.

Krajem, w którym dezinformacja stanowiła istotne narzędzie polityki państwa był od początków jego powstania Związek Radziecki. Było to podyktowane, przyjętą przez bolszewików, polityką konfrontacji z zachodem i szerzeniem koncepcji oblężonej twierdzy. Dezinformacja w wydaniu sowieckim skupiała się na planowych, kompleksowych i skoordynowanych kampaniach, będących częścią przedsięwzięć realizowanych w ramach tak zwanych *aktywnych środków* (*ang. active measures)*. Przypuszcza się, że na realizację działań związanych z dezinformacją Związek Radziecki wydał od 3 do 4 mld USD, a w realizację przedsięwzięć z tym związanych było zaangażowanych nawet 15000 osób [1]. W opinii Richarda Shultza i Raya Godsona w realizację kampanii *active measures* zaangażowane były dwa departamenty Komitetu Centralnego Komunistycznej Partii Związku Radzieckiego: Departament Informacji Międzynarodowej i Departament Międzynarodowy, oraz Zarząd A, stanowiący element I Dyrektoriatu KGB [2].

Dezinformacja może być realizowana za pomocą różnorodnych formy, według odmiennych planów, w różnym czasie, zgodnie z przyjętym celem działania. Zasadniczym celem tych działań jest oszustów, wprowadzenie w błąd odbiorcy informacji co do faktycznych zamiarów i planów dezinformatora. Naturalnym środowiskiem dezinformacji jest współcześnie

cyberprzestrzeń. W procesie dezinformacji realizowanej w cyberprzestrzeni można wyróżnić: określenie celu dezinformacji i planu jej przeprowadzenia, przygotowanie fałszywej informacji wraz z komentarzami, zidentyfikowanie i przejęcie obiektu użytego do dezinformacji, zidentyfikowanie i przejęcie obiektów pośrednich dla zwiększenia zasięgu oddziaływania, publikacja fałszywej informacji wraz z komentarzami, rozpoczęcie kampanii informacyjnej w portalach społecznościowych związaną z powielaniem treści umieszczonych w obiektach pośrednich, wzmocnienie przekazu poprzez rozsyłanie maili z przejętych kont pocztowych osób, które mają uwiarygodnić przekaz. Powyższe etapy zaprezentowano na rysunku 4.



Źródło: Opracowanie własne.
Rysunek 4. Etapy dezinformacji realizowanej w cyberprzestrzeni

Reasumując, dezinformacja jest zaplanowanym przekazem informacyjnym realizującym przyjęte cele taktyczne (krótka perspektywa czasowa) lub strategiczne (długa perspektywa czasowa). Dezinformacja taktyczna związana jest najczęściej z bieżącą sytuację i dotyczy spraw aktualny. Może być ona wspierana fałszywymi informacjami, fakenewsami łatwymi do zidentyfikowania w krótkiej perspektywie czasowej. Niemniej jednak pozwala ona na sterowanie zachowaniami odbiorców informacji, szczególnie w środowi-

sku podatnym na insynuacje. Dezinformacja strategiczna, z uwagi na realizację celów długoplanowych, wieloletnich, jest niezmiernie trudna do zidentyfikowania. Jej identyfikacja wymaga stosownego odniesienia czasowego, pozwalającego na zidentyfikowanie w przeszłości sterowanych przekazów informacyjnych, specyficznych dla danego środowiska.

Propaganda

Zagrożeniem informacyjnym bezpośrednio związanym z potrzebą wpływania na jednostki, społeczeństwa i narody jest *propaganda*. Z pierwszymi przypadkami tego typu działań mieliśmy do czynienia już w kulturze mezoamerykańskiej i egipskiej, gdzie zapisy, najczęściej w postaci hieroglifów, przedstawiały historię w sposób korzystny dla ich twórcy, najczęściej dla władców lub kapłanów. W tych czasach tylko elity posiadały umiejętność tworzenia hieroglifów, przez co przekaz był jednokierunkowy, skierowany od władzy do ludu. Pierwsze znane określenie terminu *propaganda* pochodzi z roku 1622, kiedy to Papież Grzegorz XV powołał Kongregację Propagandy Wiary (*łac. Congregatio de Propaganda Fide*). Do powszechnego obiegu termin propagandy wszedł w okresie pierwszej wojny światowej jako nowatorska technika perswazji i oddziaływania na społeczeństwo [3]. Propagandę postrzegano wtedy jako rozprzestrzenianie stronniczych idei i poglądów, często używając przy tym podstępu, kłamstwa czy manipulacji. Największy swój rozwój propagandy związany był z narodzinami systemów totalitarnych takich jak faszyzm i komunizm. Od tego momentu termin *propaganda* obejmuje swoim zakresem sugestię i wywieranie wpływu, z wykorzystaniem zdobyczy techniki (kino, radio, telewizja, Internet) i mechanizmami psychologicznymi. W przekazach propagandowych powszechnie wykorzystywane są obrazy, slogany, stereotypy, uprzedzenia i emocje. Są to swoiste komunikaty stworzone na potrzeby, z góry określonego, celu, mające skłonić odbiorcę tegoż komunikatu do dobrowolnego przyjęcia punktu widzenia zawartego w komunikacie i uznania go za swój [5].

Współcześnie propaganda definiowana jest jako *proces składający się z planowanego użycia każdej formy publicznych lub masowo wytwarzanych komunikatów zaprojektowanych tak, aby wpływały na umysły i emocje wybranej grupy odbiorców, w z góry określonym celu (społecznym, militarnym, ekonomicznym, politycznym) [15]*. Kluczowymi elementami propagandy są plany działania i realizowane cele. Bez planu i przyjętego celu działania nie można mówić o propagandzie, lecz jedynie o kłamstwie lub manipulacji. Nie każde

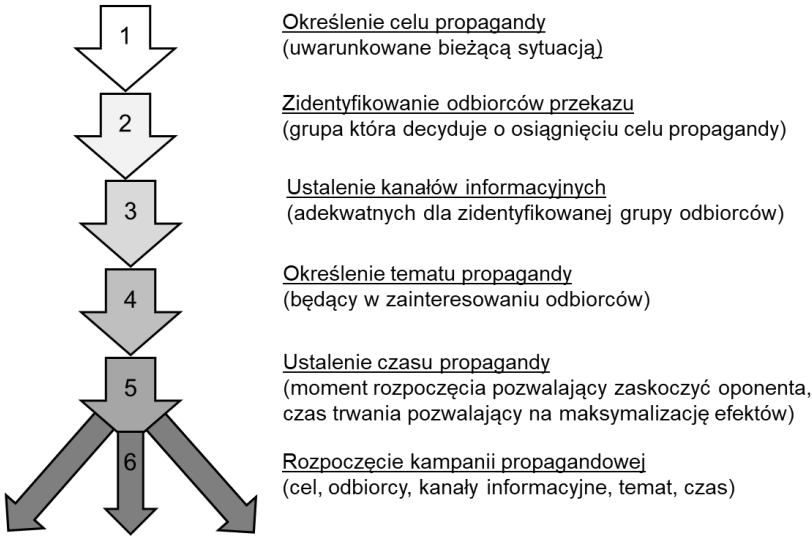
kłamstwo i manipulacja pojawiające się w przestrzeni informacyjnej są propagandą, ale każda kampania propagandowa jest oparta w znacznej części na kłamstwach i manipulacji.

Propaganda realizowana jest według schematu składającego się pięciu podstawowych etapów określanych, od pierwszych liter ich angielskich nazw jako STASM. Zostały one zidentyfikowane przez Paula M.A. Linebargera w książce *Psychological warfare,* w postaci [15]:

- S - *Source* (źródła – kanały informacyjne propagandy);
- T - *Time* (czas rozpoczęcia i prowadzenia kampanii propagandowej);
- A - *Audience* (publiczność – odbiorcy propagandy);
- S - *Subject* (temat – sprawa, której dotyka kampania propagandowa, gwarantująca realizację celu działania);
- M - *Mission* (misja – cel kampanii propagandowej powiązany najczęściej z celem politycznym).

Kanały informacyjne, za pomocą których prowadzona będzie kampania propagandowa odgrywają istotną rolę, gdyż muszą być one zgodne z preferencjami odbiorców propagandy. Współcześnie są to: prasa, telewizja, ulotki, Internet, wiece, bezpośrednie spotkania, fałszywe autorytety, agenci wpływu, celebryci, influencerzy itp. Prowadzenie kampanii propagandowej z wykorzystaniem kanałów informacyjnych, których nie wykorzystują odbiorcy przekazów jest bezcelowe, nie gwarantujące sukcesu przekazu. *Czas* jest związany z ustaleniem, kiedy i jak długo będzie prowadzona kampania propagandowa. Jego precyzyjne określenie jest niezwykle istotne, albowiem łatwiej jest wpływać na społeczeństwo będące w kryzysie, stojące przed wyzwaniami lub wyborami, jednocześnie nie dając przeciwnikowi czasu na stosowną reakcję. Element ten jest kluczowym czynnikiem w kampaniach informacyjnych związanych z wyborami, a dobór czasu jest także podyktowany percepcją grupy docelowej i budowaniem w tej grupie odpowiednich przekonań, poglądów, nastroju sprzyjającego propagandyście. *Publiczność,* będąca grupą docelową kampanii propagandowej, charakteryzuje się odpowiednimi systemami wartości, przekonaniami, nawykami, kulturą, tradycjami i środowiskiem informacyjnym z którego pozyskuje wiedzę na temat otaczającej rzeczywistości. Wobec powyższego inny przekaz będzie kierowany do ludzi wykształconych, świadomie korzystających ze sprawdzonych źródeł informacji, inny z kolei do osób budujących swoje poglądy na podstawie mediów społecznościowych, czy też ulubionych lub jedynie dostępnych kanałów

informacyjnych. *Temat propagandy* jest związany z oczekiwaniami wybranej grupy docelowej (*publiczności*), niejako rozwiązujący stojące przed nią problemy lub trafiający w ich oczekiwania, upodobania, wartości lub gusty. Ostatnim elementem, najważniejszym, jest *cel,* dla którego realizowana jest kampania propagandowa. To podstawowy element jaki powinien zostać określony już na początku planowania kampanii propagandowej. Jest to zgodne z zasadami sztuki wojennej i regułami prakseologii. Na rysunku 5. przedstawiono proces organizowania kampanii propagandowej.



Źródło: Opracowanie własne.
Rysunek 5. Proces tworzenia kampanii propagandowej

Patrząc na uwarunkowania, w których funkcjonują współczesne społeczeństwa i rozwój środowiska informacyjnego, w którym coraz większą rolę odgrywa cyberprzestrzeń, można stwierdzić, że proces propagandy jest uwarunkowany wieloma różnorodnymi czynnikami. Do najważniejszych z nich możemy zaliczć: aktywność propagandystów, media społecznego przekazu, dostęp do sieci Internet w tym do mediów społecznościowych, organizacje rządowe i pozarządowe, grupy społeczne, systemy wartości, kultura, tradycje, systemy ekonomiczne, prawne i polityczne. Komunikaty generowane w przekazach propagandowych funkcjonują w szeroko postrzeganej obręczy kulturowej (ang. *cultural rim*), która jest determinowana kontekstem społeczno-

historycznym (ang. *social-historical context*). Wobec powyższego, nie można rozpatrywać propagandy w oderwaniu od uwarunkowań danego społeczeństwa. Funkcjonuje ono bowiem opierając się na swoich systemach wartości, kulturze, doświadczeniach, przekonaniach i historii. Propaganda, uwzględniająca powyższe aspekty, ma wpływ na kształt kultury, ale kultura oddziałuje na kształt propagandy. Propaganda najczęściej ukierunkowana jest w konkretną grupę społeczną, co wymusza uwzględnienia wielu innych czynników związanych z cechami tej grupy, takimi jak: zamożność, status społeczny, wykształcenie, zainteresowania, nastawienie, przynależność.

Kolejnymi istotnymi aspektami propagandy są jej źródło oraz stopień prawdziwości czy też zakłamania. Wyróżniane są trzy podstawowe rodzaje propagandy [12]: biała (ang. *overt or white propaganda*), szara (ang. *gray propaganda*) i czarna (ang. *covert or black propaganda*). Propaganda biała, to działania, w których zarówno źródło, jak i pochodzenie informacji są dobrze znane odbiorcom. To najczęściej przekazanie oficjalnego stanowiska rządu, agencji rządowej czy też każdej innej organizacji w sposób jawny, przy założeniu, że przekazywane w nich informacje są podawane w sposób wybiórczy (celowy), z uwzględnieniem wyłącznie informacji sprzyjających stronie przekazującej i jednoczesnym pomijaniem faktów niewygodnych. W przypadku propagandy szarej źródło informacji nie jest znane (jawne), można jedynie przypuszczać jego pochodzenia, natomiast sama informacja jest korzystna bądź też niekorzystna dla określonej grupy odbiorców, uwarunkowana celem kampanii propagandowej. Informacje są podawane w taki sposób, aby cechowały się znamionami wycieku informacji, np. w postaci nieoficjalnego stanowiska rządu, partii czy też organizacji. Propaganda czarna jest w swej istocie budowana na manipulacji, kłamstwie i fałszu. W tym przypadku zarówno źródło informacji, jak i sama informacja są fałszywe. Celem tego typu propagandy jest uzyskanie w docelowej grupie odbiorców odpowiedniego efektu psychologicznego, ukierunkowanego na całkowitą zmianę postrzegania bieżącej sytuacji politycznej, społecznej, ekonomicznej, militarnej itp. Współcześnie, propaganda tego typu jest powszechnie wykorzystywana, chociażby przy okazji wyborów, referendów i innych ważnych dla danego społeczeństwa sytuacji, a środowiskiem jej rozprzestrzeniania jest cyberprzestrzeń.

Podobnie jak w przypadku dezinformacji, także w odniesieniu do propagandy można wyróżnić dwie zasadnicze kategorie propagandy - taktyczną i strategiczną [15]. Są one związane z okresem ich prowadzenia i przyjętymi celami działania. Propaganda taktyczna jest ukierunkowana bezpośrednio do wybranej grupy odbiorców, na przykład żołnierzy biorących udział w walce,

w celu wywarcia na nich odpowiedniego wrażenia, przekonania do własnych poglądów, zdemoralizowania i zniechęcenia do jakiegokolwiek działania czy też poświęcenia. Jej oddziaływanie w czasie jest bezpośrednio związane z czasem prowadzenia operacji militarnych. Propaganda taktyczna może być także związana z wywołaniem w społeczeństwie paniki ukierunkowanej na podejmowanie nieprzemyślanych działań np. wypłat gotówki z kont bankowych, wykupowane żywności, materiałów sanitarnych czy też paliw. Z kolei propaganda strategiczna jest związana z realizacją celów strategicznych, rozłożonych w długim przedziale czasu, sięgającym nawet kilkadziesiąt lat. Jej głównym celem jest stworzenie nowej świadomości (np. nowego systemu wartości lub nowego poglądu na otoczenie) wśród grupy docelowej, zgodnej z przyjętym celem strategicznym.

W literaturze można znaleźć również inne rodzaje i formy propagandy. W zależności od aktywności stron prowadzących kampanie propagandowe wyróżnia się [15] propagandę defensywną (ang. *defensive propaganda*) i ofensywną (ang. *offensive propaganda*). Pierwsza z nich jest wykorzystywana do wzmocnienia pozytywnego nastawienia społeczeństwa w stosunku do planów i przedsięwzięć realizowanych prze państwo. Drugi rodzaj propagandy jest stosowany w celu zmiany, niezgodnego z założonymi celami propagandystów, nastawienia społeczeństwa. Z punktu widzenia celu kampanii propagandowej wyróżniana jest [15]: propaganda konwersyjna *(*ang. *conversionary propaganda*), propaganda dzieląca (ang. *divisive propaganda*), propaganda scalająca (ang. *consolidation propaganda*) i przeciwpropaganda (ang. *counterpropaganda*). Główny cel propagandy konwersyjnej ukierunkowany jest na konwersję, czyli zmianę świadomości, poglądów i lojalności jednostki w stosunku do danej grupy społecznej i ich przekierowanie na inną, pożądana grupę społeczną. Propaganda dzieląca polega na rozbiciu jedności wybranej grupy społecznej (społeczeństwa). Chodzi w niej o stworzenie lub wzmocnienie podziałów, a tym samym zmniejszenie siły oddziaływania społeczeństwa (grupy). Odmienne cele realizowane są w propagandzie scalającej, gdzie głównym zadaniem jest likwidacja istniejących podziałów i zjednoczenie społeczeństwa wokół wspólnej sprawy, wspólnych wartości. Przeciwpropaganda jest ukierunkowana na osłabienie lub też całkowite uniemożliwienie osiągnięcia celów propagandy stosowanej przez propagandystę. Elementami propagandy są także *techniki,* za pomocą których jest ona prowadzona. Do najważniejszych można zaliczyć [17]: zapewnienie (ang. *assertion*), owczy pęd (ang. *bandwagon*), naciąganie faktów (ang. *card stacking*), błyskotki

(ang. *glittering generalities*), mniejsze zło (ang. *lesser of two evils*), doczepianie ogólników (ang. *name calling*), wskazywanie wroga (ang. *pinpointing the enemy*), ludowość (ang. *plain folks*), uproszczenie (*ang. simplification*), referencję (ang. *testimonials*), przenoszenie (ang. *transfer*).

Podsumowując, identyfikacja propagandy wymaga ustawicznego wyciągania wniosków z przeszłości. Analiza historycznych kampanii propagandowych pozwala dostrzec, które z metod i narzędzi były wykorzystywane, które z nich były skuteczne, w jakim środowisku propaganda była prowadzona, w jakim czasie realizowano przekazy i jakie kanały komunikacyjne były do tego wykorzystywane.

Zakończenie

Dezinformacja i propaganda we współczesnym społeczeństwie jest coraz częściej wykorzystywana do realizacji celów politycznych czy interesów narodowych. Ich rozwój związany jest bezpośrednio z rozwojem ludzkości, a w szczególności z wykorzystywanymi kanałami komunikacyjnymi. W przeszłości ich zasięg był mocno ograniczony, tak jak ograniczone były środki przekazu. Wraz z rozwojem społecznym dezinformacja i propaganda zyskiwały na znaczeniu i stały się skutecznym narzędziem wpływu, a w dobie cyberprzestrzeni można się pokusić o stwierdzenie, że święcą one triumfy.

Autor zdaje sobie sprawę z tego, że problematyka dezinformacji i propagandy we współczesnym społeczeństwie jest bardzo skomplikowana i niejednorodna. Często trudno odróżnić co jest dezinformacją lub propagandą, a co nią nie jest. Tym bardziej, że Internet, a w szczególności portale społecznościowe są doskonałym środowiskiem dla dezinformacji i propagandy ukierunkowanych na indywidualne preferencje jej użytkowników. Wszyscy użytkownicy sieci są zalewani informacjami z wielu źródeł i to czy przekazy te zostaną uznane za prawdziwe zależy tylko od samych użytkowników, ich kompetencji, świadomość i wiedzy.

Należy podkreślić, że propaganda i dezinformacja są procesami stosowanie zaplanowanymi w czasie, krótkookresowymi (taktycznymi) lub długookresowymi (strategicznymi) ukierunkowanymi na realizację przyjętych celów politycznych, ekonomicznych, społecznych i innych. Cele te są uwarunkowane zdolnościami podmiotu, który realizuje tego rodzaju kampanie informacyjne. Zdolności wyrażają się w głównej mierze posiadanym potencjałem ludzkim i finansowym niezbędnym do realizacji kampanii propagandowych i dezinformacyjnych.

Bibliografia

1. Ajir M., Vailliant B., *Russian Information Warfare: Implications for Deterrence Theory*, [w:] Strategic Studies Quarterly, Fall 2018; https://www.jstor.org/stable/26481910?seq=1#metadata_info_tab_contents, [15.12.2020].
2. Aleksandrowicz T., *Podstawy walki informacyjnej*, Editions Spotkania, Warszawa 2016.
3. Aronson E., Pratkanis A., *Wiek propagandy*, Państwowe Wydawnictwo Naukowe, Warszawa 2004.
4. Ciborowski L., *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń 1999.
5. Chorobiński A., *Walka informacyjna jako fundamentalny składnik działalności terrorystycznej w przyszłości;* http://konkursy.byd.pl/userfiles/files/chorobinski.pdf, [11.09.2019].
6. Dubisz S., *Uniwersalny słownik języka polskiego*, t. I, Wydawnictwo PWN, Warszawa 2003.
7. Dziak J.J., *Chekisty: A History of the KGB*, Lexingon Books, Lexington 1987.
8. Flakiewicz W., *Podejmowanie decyzji kierowniczych*, Państwowe Wydawnictwo Ekonomiczne, Warszawa 1973.
9. Goban-Klas T., Sienkiewicz P.*, Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania,* Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.
10. Godston R., Wirtz J.J., *Strategic denial and decption: the twenty-first century challenge*, National Strategy-Information Center, Washington, D.C. 2012.
11. https://sjp.pwn.pl/sjp/dezinformacja;2554971.html, [11.09.2019].
12. Jowert G.S., O'Donnell V., *Propaganda and persuasion*, Sage Publications, Washington D.C. 2006.

13. Kuzior A., Kwiliński A., *Zarządzanie refleksyjne – prolegomena*, https://www.researchgate.net/publication/353352807_Zarzadzanie_refleksyjne_-_prolegomena_A_Kuzior_A_Kwilinski, [7.02.2022].
14. Lewczenko S., *Private Channel* [w:] *Influence: A KGB Disinformation Tool, Counterpoint: A monthly report on Soviet Active Measures*, t. 3, kwiecień 1988 nr 11.
15. Linebarger P.M.A., *Psychological warfare*, Combat Forces Press, Washington D.C. 1954, Second Edition Reprinted by Combat Forces Press, Washington, D.C. 1972.
16. Markowski A., *Wielki słownik poprawnej polszczyzny*, Wydawnictwo PWN, Warszawa 2004.
17. Materiały z przedmiotu *Foreign Propaganda, Perceptions, and Policy*, w The Institute of World Politics, Washington D.C., autumn 2017.
18. Mazur M., *Jakościowa teoria informacji*, Wydawnictwo Naukowo Techniczne, Warszawa 1970.
19. Pacepa I. M., Rychlak R. J., *Dezinformacja. Były szef wywiadu ujawnia metody dławienia wolności, zwalczania religii i wspierania terroryzmu*, Helion, Gliwice 2013.
20. Shultz R.H., Godson R., *Dezinformatsia. Active Measures in Soviet Strategy*, Pergamon Press, Nowy Jork 1984.
21. Sienkiewicz P., *Systemy kierowania*, Wiedza Powszechna, Warszawa 1989.
22. *Słownik języka polskiego*, t. I, Wydawnictwo Naukowe PWN, Warszawa 1993.
23. Sun Tzu, *Sztuka wojny*, Wydawnictwo Przedświt, Warszawa 1994.
24. The Embassies and Foreign Affairs, „The Whitehall Gazette & St James's Review", Londyn 1926.
25. Volkoff V., *Psychosocjotechnika*, d*ezinformacja - oręż wojny*, Antyk, Warszawa 1999.

26. Wiener N., *Cybernetics: Or Control and Communication in the Animal and the Machine*, (Hermann & Cie) & Camb. Mass. (MIT Press), Paris 1948.
27. Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI wieku*, Przegląd Bezpieczeństwa Wewnętrznego nr 12/15.

Abstract

INFORMATION THREATS IN CYBERSPACE -
DISINFORMATION AND PROPAGANDA

Summary: The article presents the most important elements of information threats in cyberspace, focusing on the two main aspects of these threats, namely disinformation and propaganda.

Keywords: cyberspace, information warfare, disinformation, propaganda.

Rozdział 2

Odpieranie ataku ransomware przez wykrywanie akcji payloadu

Adam E. PATKOWSKI[1]

STRESZCZENIE: W tekście przedstawiono metodę detekcji działania części roboczej (payload) oprogramowania ransomware. Zakładano, że oprogramowanie ransomware jest nieznane lub zmodyfikowane i nierozpoznawalne metodami sygnaturowymi. Istotą postępowania jest obserwacja zachowania się procesów w systemie i rozpoznawanie pojawiających się symptomów ze stopniowym utwierdzaniem się w przekonaniu, że trwa atak. Opóźnienie alarmu jest dobierane tak, aby minimalizować zarówno ryzyko błędów fałszywych alarmów, jak i ryzyko wynikające opóźnionego wykrywania ataku.

SŁOWA KLUCZOWE: ransomware, exploit/payload, cyberatak, symptomy, entropia, anomalie.

Wstęp

W 1994 r. Adam Young i Moti Yung zaprezentowali koncepcję, którą podsumowali potem w 2004 r. w [5]. Sprowadzała się ona do spojrzenia na kryptografię z punktu widzenia napastnika i wskazała możliwości wykonywania w komputerze zaatakowanym przez wirus szyfrowania zasobów kluczem publicznym, do którego klucz prywatny zanany jest wyłącznie twórcy wirusa. Idea szyfrowania asymetrycznego jako metody uczynienia niedostępnymi pewnych zasobów informacyjnych stała się podstawą oprogramowania ransomware, pozwalającego napastnikowi żądać okupu za przywrócenie dostępności tych zasobów. Obecnie ten typ malware daje największe zyski przy minimalnym ryzyku, więc jest również przedmiotem szczególnie starannych analiz w oczekiwaniu najnowszych rozwiązań. Wysokie zyski motywują (i czynią opłacalnymi) przygotowywanie malware specjalnie na potrzeby pojedynczych ataków (tzw. *targeted attacks*). To ogranicza rozpoznawanie ich metodami sygnaturowymi. W niniejszym tekście zaprezentowano propozycję

[1] Dr inż., e-mail: adam.patkowski@wat.edu.pl; ORCID: 0000-0002-3717-3381

rozpoznawania ataków ransomware, a dokładniej ataków, w których zasadniczym elementem jest przekształcanie zasobów informacyjnych atakowanego systemu do postaci czyniącej je nieużytecznymi dla właściciela.

Ransomware

Ogólnie rzecz biorąc ransomware to oprogramowanie przeprowadzające lokalny atak DoS (*Denial of Service* – odmowy dostępu) na zasoby informacyjne użytkownika systemu i przedstawiające żądanie zapłaty okupu za odzyskanie dostępu do informacji. Żądanie okupu może nadejść innym kanałem. W ogólnym przypadku żądanie okupu nie musi oznaczać wyłącznie okupu za przywrócenie dostępu – może stanowić także opłatę za nieujawnianiu ataku, jeśli mogłoby to zaszkodzić wizerunkowi instytucji-ofiary. Z historii ataków ransomware wynika, że żądanie okupu niekoniecznie musi oznaczać, że rzeczywiście informacje stały się niedostępne. Co gorsza jednak żądanie okupu wcale nie oznacza, że informacje będzie można odzyskać po uiszczeniu żądanej kwoty.

Klasyczny atak ransomware to atak na dostępność i integralność zasobów informacyjnych jednocześnie. Uzyskanie efektu niedostępności następuje dzięki szyfrowaniu plików w zaatakowanym systemie. Wykorzystywane są szyfry asymetryczne, przy czym klucz odszyfrowywania pozostaje niedostępny w rękach napastnika.

Do niedawna (do 2019 roku) grasowały głównie tzw. „wirusy ransomware": oportunistyczne oprogramowanie rozprowadzane różnymi znanymi sposobami, zwykle przez wabienie na agresywną stronę WWW, z której przeprowadzane były tzw. „ataki u wodopoju". To stosunkowo proste oprogramowanie święciło triumfy głównie na komputerach domowych i w słabo zabezpieczonych instytucjach publicznych (szpitale, administracja…) powodując znaczne szkody. Ale zaczęło się dużo dawniej…

1989 – zbudowano AIDS (lub PC Cyborg): to „koń trojański" rozprowadzany na dyskietkach, po 90 restartach komputera szyfrował (prostym algorytmem symetrycznym zawartym w kodzie) pliki ofiary i drukował żądanie wniesienia „opłaty licencyjnej" (199$).

Do ok. 2010 panowały głownie tzw. blokery, zwykle tylko pozorujące niedostępność systemu.

2011 – po raz pierwszy CpCode wykorzystywał algorytm asymetryczny (RSA).

2013 – Cryptolocker – pierwszy wykorzystujący silne współczesne algorytmy asymetryczne; od tej daty rozpoczęła się fala ataków „oportunistycznych".

2016 – masowo występowały programy szyfrujące; w tym Petya, który szyfruje cały dysk komputera.

2017 – oprogramowanie WannaCry zdolne do ataków w sieciach Ms Windows (wykorzystywało eksploit *EthernalBlue*) szyfrujący; pojawił się NotPetya tylko niszczący, bez możliwości przywrócenia informacji; po raz pierwszy przektoczono 1 mln $ okupu.

Koniec 2018 – program szyfrujący Ryuk dystrybuowany za pomocą zaadaptownych „wirusów" Emotet lub Trickbot, wykorzystywanych jako tzw. droppery.

2020 – pojawienie się „poziomu biznesowego" wraz z grupą DarkSide i ataki ransomware, których skutki były dostrzegalne w skali krajów i światowych korporacji.

Szczególnie interesująca jest działalność grupy DarkSide; to hakerzy współpracujący z tą grupą przeprowadzili atak na operatora rurociągu Colonial Pipeline, który wywołał poważne perturbacje na rynku paliw we wschodnich i południowych stanach USA. To tylko jeden ze stymulowanych przez DarkSide ataków – od połowy 2020 roku poszkodowanych w wyniku działań tej grupy zostało kilkadziesiąt osób i podmiotów, w tym operatorzy pól naftowych, kancelarie prawne i banki. Działalność grupy nie ogranicza się do USA. Nowością działania grupy DarkSide było to, że nie jest to grupa dokonująca ataków, ale przede wszystkim dostawca narzędzi i usług dla zgłaszających się właściwych wykonawców ataków. Model działania przypomina model afiliacyjny: narzędzia i usługi do realizacji ataków ransomware udostępniane są w podobny sposób, w jaki McDonald's lub Biedronka obsługują swoich franczyzobiorców: zapewniany był marketing, ludzie, a przede wszystkim oprogramowanie ransomware, a nawet hosting stron na potrzeby ujawniania przejętych danych. Atak na operatora mającego ponad 5000 mil rurociągu Colonial Pipeline, przesyłającego paliwo z teksańskiego Houston na wschodnie wybrzeże USA, wywarł znaczące wrażenie społeczne. Firma wypłaciła pięciomilionowe odszkodowanie (DarkSide pobierała od 10 do 25 proc. prowizji z każdej z takich płatności). Grupa DarkSide padła ofiarą własnego sukcesu – rząd USA podjął bliżej nieznane działania, w rezultacie których przestępcy ogłosili zaprzestanie działalności „z powodu presji ze strony USA", zaś FBI podało, że odzyskało 2,3 mln $ z okupu. Co prawda w darknecie w połowie 2021 r. pojawiły się ogłoszenia nowej grupy BlackMatter – przypuszcza się, że to rodzaj „rebrandingu" DarkSide.

Istotnym wnioskiem jest przejście także wytwarzania oprogramowania z garaży entuzjastów na poziom biznesowy – może mniej elastyczny, ale z pewnością zapewniający wyższą jakość, efektywność i dopracowanie szczegółów nowego malware. Symptomatyczne jest też poszukiwanie (ogłoszenia a darknecie) przez grupę BlackMatter tzw. „brokerów bezpośredniego dostępu" co jest eufemizmem oznaczającym werbowanie tzw. „insiderów" zatrudnionych w atrakcyjnych miejscach i gotowych za stosownym wynagrodzeniem uławić przeniknięcie malware do sieci swego pracodawcy. Najlepiej zainstalowanie…

Niezmienniki – specyficzne cechy ataku

Algorytm włamania (w ubiegłym wieku „eksploit") można podzielić na dwie części. Pierwsza z tych części pozwala na uzyskanie w atakowanym systemie swobody sterowania jego działaniem w stopniu wystarczającym, by można było wykonać część druga. Tę pierwszą część algorytmu nazwano „exploit". Druga część to właściwe działania na szkodę ofiary. Tę część nazwano „payload". Podział jest wygodny, ponieważ exploity można łączyć z różnymi payloadami i również payloady można poprzedzać różnymi exploitami.

W przypadku ransomware część stanowiąca exploit może być praktycznie dowolna z grupy skutkujących możliwością uruchomienia dowolnego kodu (*impact: arbitrary code execution*). Wbrew pozorom ta grupa – dość wąska w obszarze aktywnych wykorzystywalnych błędów oprogramowania – jest bardzo szeroka: oprócz wykorzystania tzw. dropperów (zwykle zaadaptowanego oprogramowania „wirusowego") obejmuje także sabotaż, ataki social engineering i ataki na łańcuch dostaw. Oznacza to, że trudno wskazać cechy exploitów specyficzne dla ataków ransomware.

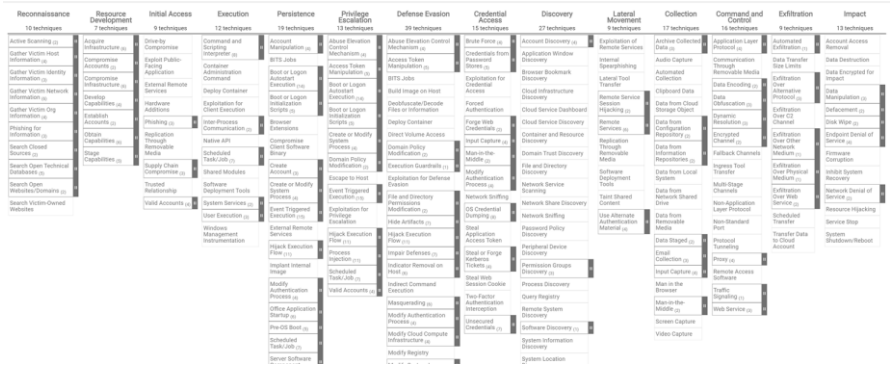
Natomiast po wprowadzeniu kodu payloadu do komputera ofiary i jego uruchomieniu działania to zwykle:

- Szyfrowanie plików i niszczenie oryginałów.
- Wyświetlenie informacji o sukcesie ataku i żądania okupu.

Jeśli ransomware jest „uczciwy" i rzeczywiście przewiduje, po zapłaceniu okupu, udostępnienie sposobu odszyfrowywania plików, to przed szyfrowaniem następuje komunikacja z *Command Center* (dla pozyskania klucza publicznego do szyfrowania i dla zaewidencjonowania ataku). Istotną częścią całego ataku, chociaż nie ujmowaną w schematach, jest zapewnienie bez-

piecznego pozyskania okupu przez napastników. Samo pozyskanie okupu wymaga wcześniejszych przygotowań, zaś odtworzenie dostępności danych ofiary wymaga zwykle bezpiecznego z punktu widzenia napastnika udostępnienia ofierze kluczy i/lub programu deszyfrującego.

W schematach frameworka MITRE ATT@CK ujęty jest tylko niewielki, chociaż kluczowy, fragment całości ataku ransomware:



Źródło: *https://attack.mitre.org/matrices/enterprise/*.

Rysunek 1. Specyficzne działania payload w MITRE ATT&CK Enterprise – oznaczono ramką (kolumna Impact) w obrazie

To dwie techniki (z trzynastu) w skrajnej prawej kolumnie na Rys. 1.: „*Data Encyption for Impact*" oraz „*Data Destruction*". Pierwsza z nich zapewnia odzyskanie danych po zapłacie okupu, druga jest właściwum działaniem pozbawiającym dostępu do danych. Może być wykorzystana dodatkowo technika „*Inhibit System Recovery*".

We wpisie [4] w firmowej witrynie Bridewell przedstawione wybrane najpoważniejsze zagrożenia[2] ransomware (z bazy danych Cyber Threat Intelligence firmy Bridwell) zmapowane na framework Mitre ATT&CK. Wybrano te, które: były wielokrotnie użyte; miały szczególnie szkodliwe skutki, zarówno pod względem technicznym, jak i komercyjnym; były udostępniane w modelu ransomware-as-a-service (RaaS) i należą do klasy „celowanych" (*targeted*) czyli indywidualizowanych na potrzeby konkretnych ataków. Co interesujące, we wszystkich faza szyfrowania poprzedzona była fazą skrytego

[2] Wg stanu na I kwartał 2021 r.

wyprowadzania informacji w zaatakowanych systemów. Dla każdego z wybranych narzędzi ataku wykonano mapowanie elementów ataku na MITRE ATT&CK. Porównanie **DarkSide Ransomware** (od sierpnia 2020), **Avaddon** (lipiec 2020), **Conti** (wersja **Ryuk**, od grudnia 2019) i **Sodinokibi** (inaczej **REvil**, od kwietnia 2019) wskazuje, że jedyną wspólną częścią są wymienione wcześniej techniki szyfrowania danych *Data Encrypted for Impact* (T1486) i *Inhibit System Recovery* (T1490). Co ciekawe, oczywiste usuwanie oryginałów zaszyfrowanych plików zostało najwyraźniej zakwalifikowane do tych technik, a nie do techniki *Data Destruction*.

W lipcu 2021 w darknecie pojawiły się ogłoszenia wspomnianej już grupy BlackMatter poszukującej „brokerów początkowego dostępu": osoby, które znają sieci korporacyjne i ułatwią do nich dostęp. Oferowano 100 000$ za dostęp dla osadzenia ransomware i wycieku danych. Wygląda na to, że rozbudowana część „exploit" w oprogramowaniu tej grupy będzie służyć tylko do odwrócenia uwagi od rzeczywistej drogi infiltracji – maskowania sabotażysty.

Cechy detekcyjne ataku ransomware

Biorąc pod uwagę, że exploit ataków ransomware jest silnie zmienny, nie można uznać jego cech za jednoznacznie użyteczne w wykrywaniu takich ataków. Po zebraniu elementów stałych, spodziewanych w większości współczesnych ataków ransomware można wskazać następującą listę cech detekcyjnych:

1. Liczne odczyty kolejnych plików.
2. Liczne operacje szyfrowania – objawem będzie znaczne obciążenie procesora.
3. Liczne zapisy zmodyfikowanych zawartości plików pod zmienionymi względem oryginałów (czasem nieznacznie) nazwami i/lub rozszerzeniami nazw
4. Liczne kasowania kolejnych plików

Kluczowe jest tu słowo „liczne". Należy się spodziewać, że takie działania będą wykonywane w ramach pojedynczego procesu (w wielu wątkach, rzadziej jako wiele instancji z tego samego macierzystego pliku kodu). Oprócz tych cech można spodziewać się jednorazowych, a więc mniej zwracających

uwagę operacji: odwołania do serwera „Command Center" napastnika dla pobrania publicznego klucza szyfrowania i zaewidencjonowania ataku oraz umieszczenia sygnalizacji żądania okupu w zaatakowanym systemie.

Działania w fazie przekazania okupu i przekazania danych niezbędnych do odzyskania informacji nie mają wartości detekcyjnej.

Na poziomie operacji na plikach spodziewane jest wykonywanie kolejnych działań związanych z „obsługą" każdego pojedynczego pliku **A** danych oryginalnych przetwarzanych do zaszyfrowanej postaci **R**:

- Otwarcie pliku A do odczytu
- Utworzenie (Create) pliku **R** do zapisu
- Wielokrotnie:
- Odczyt bloku z **A**
- Szyfrowanie
- Zapis bloku do **R**
- Zamkniecie pliku **R**
- Zamknięcie pliku **A**
- Usunięcie pliku **A**

To może nie być tak proste: ten porządek może nie być stały ani unikalny. Szyfrowanie plików może być realizowane albo szybko, ale zauważalnie – przez wiele wątków; albo „pełzająco" z odstępami w czasie. Alternatywą dla działania „po jednym pliku" może być najpierw wielokrotne szyfrowanie plików, a dopiero potem kasowanie oryginałów – przy znaczącym wzroście zajętości dysku. Radykanie rózne jest podejście zastosowane w malware Petya, który podmieniał MBR (*Master Boot Record*) dysku startowego, zaś po restarcie wykonywał szyfrowanie całego dysku… Nieunikalność działań według wskazanego schematu wynika z jego podobieństwa do innych, typowych operacji na plikach. Np. pojedyncze szyfrowanie pliku nie różni się specjalnie od Bogu ducha winnej edycji pliku lub operacji operacji zrzucania pliku tymczasowego… Tylko plik zaszyfrowany znacznie bardziej różni się od źródłowego.

Z pewnością w fazie szyfrowania plików charakterystyczne jest masywne tworzenie nowych plików i kasowanie innych – być może realizowane naprzemiennie i zapewne z tego samego procesu. Tworzone pliki są zaszyfrowane i zwykle mają charakterystyczne nazwy lub rozszerzenia nazw oraz mają wysoką entropię (losowość) wynikającą ze specyfiki szyfrowania. Ponadto najczęściej zachowują lokalizację w drzewie katalogów.

W przypadku plików we współczesnym systemie zwykle spełniają one pewne warunki wewnętrznej integralności, które przestają być spełnione po zaszyfrowaniu. Większość plików ma określony nagłówek, który zawiera zestaw bajtów identyfikacyjnych (zwanych „bajtami magicznymi"), które identyfikują zawartość plików. Ponadto wewnętrzna struktura plików jest zgodna z ich typem, identyfikowanym na podstawie rozszerzenia nazwy pliku. „Typowe" pliki (dokumenty, pliki baz danych itd.) – a te są zwykle najcenniejsze ze względu na atrybut dostępności – są dość łatwe do sprawdzenia na zgodność z typem i integralność struktury.

Atak powoduje również tzw. anomalie: zdarzenia/działania w systemie różne od „normalnych" zachowań w tym systemie. Problemem jest definicja i zapis cech „normalności" oraz określenie owej „normalności" lokalnie dla każdego systemu.

Entropia

Jeśli pliki są zaszyfrowane, to mają pewną interesującą cechę: wysoką losowość zawartości. Oznacza to brak jakichkolwiek regularności w zawartości takich plików. Istnieją pewne problemy z formalnym określeniem miar dla takich cech. Zwykle rozważa się cechę nazywaną entropią plików. Entropia to miara chaosu – w drastycznym uproszczeniu (użytecznym ze względu na złożoność obliczeniową metody wyznaczania) im bardziej podciągi binarne (ustalonej długości) badanego ciągu mają rozproszone wartości, tym wartość tej miary dla ciągu jest większa. Maksymalna wartość będzie wówczas, gdy wszystkie różne podciągi ciągu wystąpią równolicznie.

Badania i wykorzystanie w praktyce miar entropii/regularności/losowości do detekcji niepożądanych zdarzeń w obszarze bezpieczeństwa inforacyjnego jest modne od początku obecnego wieku. Przykładami są badanie losowości generatorów w grach liczbowych; wykrywanie steganografii, wykrywanie kluczy kryptograficznych w zrzutach pamięci itp. w informatyce śledczej; również badania entropii ruchu sieciowego dla wykrycia ataków.

Pliki zaszyfrowane cechują się wysoką entropią. Niestety tę właściwość pliki zaszyfrowane dzielą z plikami skompresowanymi (zip i podobne), a praktycznie wszystkie pliki współczesnego pakietu Office (docx, xlsx czy pptx) to skompresowane („zzipowane") struktury informacji. Poniżej podano wartości miary entropii dla plików różnych typów (o różnych rozszerzeniach)

wyznaczone za pomocą pogramu sigcheck[3] Microsoftu (ze zbioru narzędzi Sysinternals Suite) dla jednobajtowych ciągów (wartość maksymalna: 8):

- **.txt** 4.828 - 4.885
- **.ppt** 7.564
- **.pdf** 7.937
- **.pptx** 7.96 [skompresowany]
- **.mp4** 7.971 [skompresowany]
- **.zip** 7.998 [skompresowany]
- .pptx.**pgp** 8 [plik .pptx zaszyfrowany algorytmem AES, nie PGP]
- .ppt.**pgp** 8 [plik .ppt zaszyfrowany AES]

Nie dyskwalifikuje to entropii jako cechy detekcyjnej, ale znacznie osłabia pewność detekcji wyłącznie na podstawie tej cechy. Jednak w polaczeniu z innymi cechami można uznać entropię za użyteczną: typ pliku, nagłówek i rozkład entropii pliku muszą do siebie pasować! Jeśli entropia jest wysoka, a tego dopasowania nie ma, to zapewne plik jest „ransomwared". Dla każdego typu pliku można też wskazać pewną regularność struktury, w której obszary o różnej entropii występują zgodnie z ogólnym wzorcem. W plikach zaszyfrowanych praktycznie nie występują obszary o obniżonej entropii.

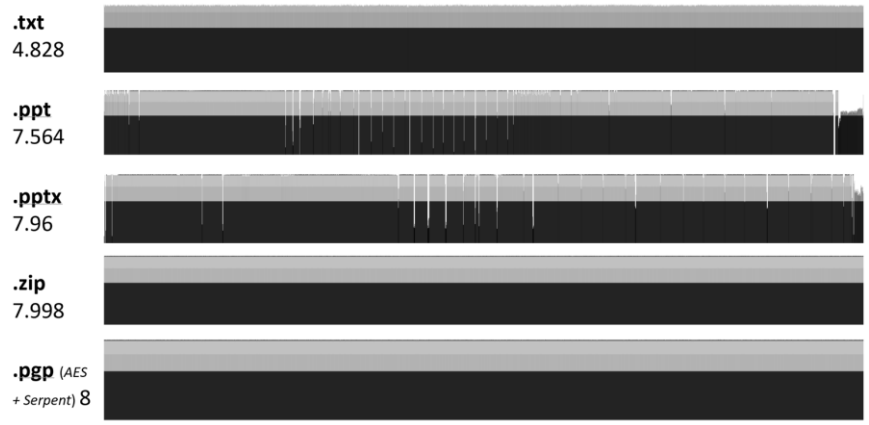
W praktyce użyteczne może być uwzględnianie – zamiast pojedynczej wartości entropii dla całego pliku – pewnego wektora: rozkładu entropii. Rozkładem entropii pliku nazwano wykres lub tabelę wartości entropii dla kolejnych bloków (o zadanej długości) zawartości pliku. Na Rys. 2 przedstawiono przykłady rozkładów entropii dla plików różnych typów – rysunek ten może służyć wyłącznie do ilustracji: pliki były bardzo różnej długości, zaś użyty program skaluje obrazy do tej samej szerokości, sam wybór plików był arbitralny i dość przypadkowy. Do wygenerowania obrazów rozkładów użyto programu Gynvaela Coldwinda o nazwie **Ent**[4] z 2009 roku,

Pewien problem techniczny stanowić może wyliczanie wartości entropii dla strumienia zapisywanych do pliku danych. Nie trzeba liczyć współczynnika entropii dla całego pliku, wystarczy wyznaczać go dla bloków o wybranej, stałej długości. Można także zaniechać badania pliku po pierwszym napotkanym bloku o niskiej losowości – oznacza to, że plik nie jest standardowo szyfrowany. Niestety ta metoda zawiedzie w przypadku, gdy

[3] Zob.: https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck
[4] Zob.: https://gynvael.coldwind.pl/?id=157

oprogramowanie szyfruje tylko fragmenty plików co pozwala mu niszczyć pliki „z mniejszym wysiłkiem", a także wprowadzać w błąd właśnie mechanizmy detekcji wykorzystujące badanie wartości entropii. Niestety, nowsze oprogramowanie ransomware wykorzystuje właśnie mechanizm częściowego szyfrowania plików.

Wykorzystanie badania entropii dla wykrycia ataku ransomware w systemach backupowych zaproponowano w „Machine learning based file entropy analysis for ransomware detection in backup systems" ([1]). Sformułowanie uniwersalnych reguł identyfikacji zaszufrowanych plików za pomocą entropii nie wydajesię możliwe, przyjęto więc założenie, że pliki kopii archiwalnych powinny mieć podobne cechy regularności jak poprzednie wersje tych kopii, a symptomem ataku ransomware będzie odstępstwo od tej zasady. Metod sztucznej inteligencji (uczenia się) użyto dla wyznaczenia właśnie opisów regularności i dopuszczalnych odchyleń między kolejnymi wersjami kopii. Należy zwrócić uwagę, że to (przedstawione uproszczeniu) podejście odwołuje się do pewnego lokalnego wzorca „normalności", a zatem jest rodzajem wykrywania anomalii.



Źródło: opracowanie własne.

Rysunek 2. Ilustracja rozkładów entropii dla wybranych plików (w lewej kolumnie poniżej typu podano wartość entropii dla całego pliku)

Anomalie i ich wykrywanie

Można zastosować wspomniane podejście szerzej: rejestrować „wzorzec poprawności" dla wszystkich plików w konkretnym systemie i badać anomalie – wykraczanie poza dopuszczalne wartości np.: znanych typów plików, gęstości odwołań do plików czy rozkładów entropii dla plików. Rejestrowanie wzorca poprawności czy „normalności" wymaga fazy rejestrowania zachowań systemu w warunkach niezakłócanych, a zatem fazy uczenia się systemu. W istocie – to tworzy prosty system samouczący. Na marginesie warto wspomnieć, że do kategorii anomalii można zaliczyć też odwołania do tzw. „honeyfiles" pełniących rolę sygnalizatorów, chociaż listy honeyfiles są zawsze określane arbitralnie, a nie metodą uczenia się.

Anomalie definiowane są jako wartości parametrów systemu wykraczające poza dopuszczalne (zdefiniowane enumeracyjnie lub przez określenie wartości granicznych) zakresy określone w tzw „profilu". Profil to wektor parametrów i zbiór dopuszczalnych wartości dla każdego parametru. Dla parametrów skalarnych wystarczy podanie wartoci granicznych dopuszczalnego przedziału, w innych przypadkach zapis może być bardziej złożony (np. enumeracyjny). Samouczenie polega na obserwacji (przez tzw. okres uczenia) wartości parametrów w „żywym" systemie, uznanie wszystkich napotkanych wartości za dopuszczalne i określenie na tej podstawie profilu. To tzw. metoda „białych list". Pewne wartości profilu mogą wstępnie być nadawane arbitralnie.

Anomalie rejestrowane są w trakcie fazy detekcji następującej po fazie uczenia się. W tej fazie po wykryciu anomalii wznoszony jest alarm. Jedną z reakcji na alarm może być interwencja arbitra (zwykle człowieka) podejmującego decyzję o włączeniu zarejestrowanych, powodujących alarm wartości parametrów do profilu. Taka korekta podejmowana jest po stwierdzeniu fałszywego alarmu, czyli błędu drugiego rodzaju.

Anomalie (wykrycia anomalii) to lokalne symptomy wykrywanych, niepożądanych zdarzeń.

Symptomy działania payloadu ransomware i detekcja

Wśród symptomów trwania ataku ransomware, a dokładniej fazy szyfrowania plików danych ofiary i niszczenia ich oryginałów, można podzielić na uniwersalne, związane z entropią oraz lokalne. Symptomy uniwersalne to takie, które będą takie same w różnych systemach komputerowych, zaś lokalne to anomalie specyficzne dla systemu. Symptomy związane z entropią

wyróżniono ze względu na techniczne właściwości ich rejestracji, które nie są przedmiotem niniejszego opracowania.

Podstawowym symptomem jest (być może rozłożone w dłuższym okresie) zdarzenie polegające na otwarciu pewnego pliku A, następnie sekwencyjny odczyt zawartości całego pliku (A), zamknięcie pliku (A) i kasowanie piku tego pliku (A).

Pełnym symptomem jest wystąpienie w trakcie trwania symptomu podstawowego (od otwarcia pliku A do skasowania tego pliku) zdarzenie polegające na utworzeniu nowego pliku B, zapis zawartości tego pliku (B) i zamknięcie tego pliku (B).

Symptomy drugorzędne to zdarzenia, które występują w trakcie trwania symptomu pełnego potwierdzające atak. Poniżej przedstawiono możliwe symptomy trzeciorzędowe:

1. Nazwa/rozszerzenie pliku B zawierające fragmenty nazwy/rozszerzenia pliku A.
2. Niezgodność nagłówka pliku B z typem (rozszerzeniem nazwy) tego pliku.
3. Niezgodność struktury pliku B z nagłówkiem.
4. Brak integralności wewnętrznej struktury pliku B.
5. Duża entropia pliku B.
6. Znacząco większa entropia pliku B względem pliku A.
7. Anomalia: niezgodność rozkładu entropii pliku B z rozszerzeniem pliku B.
8. Anomalia: nieznany typ pliku B.
9. Anomalia: nieznana nazwa pliku B dla lokalizacji (katalogu).

Symptomy 1-4 to symptomy uniwersalne, 4-7 to symptomy związane z entropią, zaś 7-9 oznaczają wykrycie anomalii.

Wystąpienie symptomu pierwotnego nie jest silną przesłanką do podjęcia alarmu ransomware, znacznie mocniejszą przesłanką będzie wystąpienie symptomu pełnego. Symptomy drugorzędne wzmacniają hipotezę o działaniu payloadu ransomware. Jednak dopiero wielokrotne wystąpienia pełnych symptomów sygnalizują „masowe operacje…" charakterystyczne dla ataku. Możan zaproponować mechanizm obserwujący operacje plikowe w systemie komputerowym, rejestrujący zdarzenia i wykrywający symptomy. Można

również przyjąć pewien system punktowy, w którym wystąpienie pełnego objawu dodaje do wielkości alarmowej pewną liczbę w_0 zwiększaną i dodatkowe wartości punktowe w_2 za każdy wykryty symptom trzeciorzędowy związany z tym symptomem pełnym. To podejście zapewnia ocenę „siły" wzmocnienia hipotezy o ataku z pojedynczego zdarzenia potencjalnie interpretowanego jako szyfrowanie pliku.

W systemie można zdefiniować pewną zmienną decyzyjną zliczającą punkty kolejnych symptomów w zadanym oknie zdarzeniowym. Przez okno zdarzeniowe rozumie się (przez analogię do „okna czasowego") ciąg, o zadanej liczności, kolejnych zdarzeń w systemie komputerowym, w rozpatrywanym przypadku operacji otwarcia pliku i operacji usunięcia pliku. Osiągnięcie przez zmienną decyzyjną zadanej wartości progowej powinno uruchomić alarm. Manipulowanie wartością punktową oceny pojedynczego wystąpienia zdarzenia pełnego (z uwzględnieniem dodatkowych symptomów) oraz wartością wyzwalającą alarm może pozwolić na osiągnięcie wysokiej pewności detekcji przy niskim ryzyku fałszywych alarmów.

Podejmowanie decyzji o alarmie

Pomijając subtelności doboru punktowania symptomów o różnym stopniu potwierdzenia, można na potrzeby niniejszego opisu uprościć zaproponowany model podejmowania decyzji o alarmie. Uproszczenie polega na rozważaniu wyłącznie wystąpień pełnych symptomów i założenie, że pojedynczy pełny symptom może sygnalizować szyfrowanie pojedynczego, referencyjnego pliku, zaś strata związana z taką utratą dostępności pliku jest stała i równa S_1. W takim przypadku zmienna decyzyjna d może reprezentować liczbę zarejestrowanych pełnych symptomów. Zaś osiągnięcie przyjętego progu D symptomów przez zmienną decyzyjną d oznacza stratę o wartości $D*S_1$, o ile rzeczywiście trwa atak ransomware. Jeśli alarm jest fałszywy, koszt wzniesienia takiego alarmu to oszacowana wartość S_2. Jak łatwo zauważyć im bardziej odkładana jest decyzja o alarmie (większa przyjęta wartość progowa D), tym bardziej rosną straty wywołane przez atak.

W tym modelu konieczne jest wprowadzenie oceny prawdopodobieństwa p(d), że ciąg d wystąpień kolejnych symptomów rzeczywiście oznacza atak. Intuicyjnie występowanie kolejnych symptomów w serii wzmacnia hipotezę, że trwa atak ransomware – szanse, że tak jest rosną z każdym kolejnym plikiem i spadają szanse fałszywego alarmu. Równocześnie, jak wskazano w poprzednim akapicie, z każdym zaszyfrowanym plikiem rosną

straty wynikające z utraty danych. Odległość między początkiem ataku, a decyzją o alarmie można mierzyć liczbą zaszyfrowanych referencyjnych plików. To „opóźnienie detekcji", to właśnie wartość zmiennej decyzyjnej d.

Należy wybrać taką wartość opóźnienia D, która minimalizuje ryzyko R(d) (wartość oczekiwaną strat) po podjęciu decyzji z opóźnieniem d symptomów:

$$R(d)=p(d)*d*S_1 + (1-p(d))*S_2$$

Gdzie: R(d) – ryzyko przy opóźnieniu d;

d – opóźnienie;

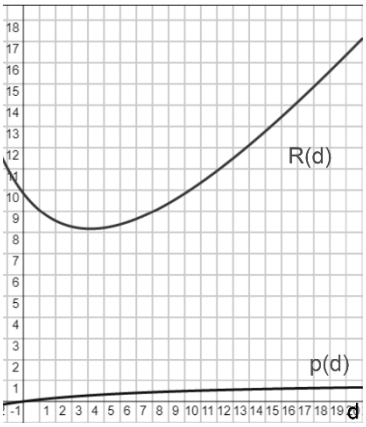
p(d) – prawdopodobieństwo poprawnej identyfikacji ataku przy opóźnieniu d;

1-p(d) – prawdopodobieństwo fałszywego alarmu przy opóźnieniu d;

S_1 – strata w wyniku zaszyfrowania jednego pliku referencyjnego;

S_2 – strata w wyniku fałszywego alarmu.

Ta wartość D to dopuszczalne opóźnienie, które wyznacza maksymalną liczbę plików, które „mają" procedury detekcyjne na podjęcie decyzji o alarmie/interwencji.



Obecnie głównym problemem pozostaje określenie zależności prawdopodobieństwa p(d) poprawnego rozpoznania ataku od liczby (lub wagi, w przypadku uwzględniania symptomów drugorzędnych) d rozpoznanych wcześniej symptomów (opóźnienia). Z oczekiwania monotonicznego, chociaż nieliniowego, przebiegu tej funkcji wynika, że funkcja ryzyka R(d) jest krzywą drugiego stopnia.

Można sformułować zadanie optymalizacji wyznaczania dopuszczalnego opóźnienia. Funkcja kryterium powinna być opisana na zbiorze procedur detekcyjnych, parametryzowanych przydziałem wartości wag (punktów) symptomom (także drugorzędnym). Można również rozważyć uwzględnienie różnej wartości poszczególnych chronionych zasobów informacyjnych.

Należy także zwrócić uwagę, że oprócz funkcji p(d) prawdopodobieństwa poprawnej decyzji o wykryciu ataku po rozpoznaniu d symptomów, także wartości strat w wyniku opóźnienia mogą nie być łatwe do określenia. Wynika to zarówno z nierównej wartości strat wynikających z utraty poszczególnych plików, jak i z trudności oszacowania przyszłego zapotrzebowania na

utracone pliki. Niebagatelną rolę odegra także zastosowanie środków zabezpieczeń takich jak kopie zapasowe, w wyniku których straty określone są nie użytecznością utraconych plików, ale pracochłonnością i czasem przywracania tych plików z kopii.

Uwagi końcowe

W przedstawionej metodzie wykrywania akcji części roboczej (payloadu) oprogramowania ransomware przyjęto, że oprogramowanie ransomware jest nieznane lub zmodyfikowane i nierozpoznawalne metodami sygnaturowymi. Istotą postępowania jest obserwacja odwołań do plików wykonywanych przez procesy w systemie i rozpoznawanie pewnych symptomów przy czym dopuszcza się podjęcie decyzji o alarmie dopiero po wystąpieniu ustalonej liczby symptomów. Przedstawione problemy decyzyjne w praktyce będą jednak łatwiejsze do rozwiązania ze względu na to, że zapewne podobne systemy będą projektowane do współpracy z innymi mechanizmami łagodzącymi skutki atakóe ransomware. To oznacza większą tolerancję ryzyka wynikającego z dopuszczenia pewnego czasu działania ransomware w systemie.

Co prawda twórcy ransomware znają techniki analizy danych, używają więc prostych sztuczek do maskowania masowego szyfrowania plików, takich jak:

- tylko częściowe szyfrowanie plików (np. tylko sekcje nagłówka) lub
- generowanie w trakcie operacji zapisu obszarów o niskiej entropii, aby uzyskać mniejszy ślad szyfrowania
- losowanie nazw nowych plików
- zmniejszanie gęstości charakterystycznych operacji: „pełzający" atak, w którym tworzenie zaszyfrowanych kopii jest znacznie rozciągnięte i odsunięte w czasie od kasowania oryginałów.

Naszkicowana w rozdz. 5 metoda wykrywania, nawet ograniczona symptomów uniwersalnych, pozostanie jednak skuteczna.

Na koniec warto wspomnieć o interesującej możliwości wsparcia zaproponowanego sposobu detekcji przez zastosowanie mechanizmu opóźnionego zapisu (co dotyczy również operacji kasowania) plików.

Przyjęcie pewnego dopuszczalnego opóźnienia interwencji względem początku ataku oznacza, że nawet przy minimalizacji oczekiwanych strat takie straty mogą nastąpić. Rozwiązaniem jest wykorzystanie buforowania i opóźnionego zapisu na nośniki: pliki mogą oczekiwać przez pewien czas na ostateczne zapisanie w miejsce docelowe. W czasie oczekiwania modyfikowana zawartość danych pozostaje nienaruszona na dyskach i możliwe jest ocalenie danych w przypadku wykrycia akcji ransomware. To da bezkarny czas na podjęcie decyzji o alarmie, a dokładniej pozwoli zwiększyć wartość parametru nazwanego opóźnieniem D i zmniejszyć do zera początkowe straty wynikające z szyfrowania plików. Techniczne metoda opóźnionego zapisu są znane: w wykorzystywanych do izolowania procesów piaskownicach (sandboxes) wykorzystywane są katalogi różnicowe a w Linuxowych systemach live używana jest partycja różnicowa („persistence"). Dość odległym od omawianego jest też zastosowanie strategii „write-back" (vs. „write-through") w pamięciach buforowych (caches).

Bibliografia

1. Lee K., Lee SY., Yim K.: *Machine learning based file entropy analysis for ransomware detection in backup systems*, IEEE Access, 2019.
2. Magida A.M et al.: *Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms*, Journal of Reliable Intelligent Environments, Springer Nature Switzerland AG, July 2019
3. Nieuwenhuizen D.: *A behavioural based approach to ransomware detection*, MWR Labs Whitepaper, MWR Labs, 2017.
4. Riley M.: *2021 Ransomware and the Mitre Att&ck Framework*. Bridewell Consulting. 2021. https://www.bridewellconsulting.com/2021-ransomware-and-the-mitre-attck-framework
5. Young A. L., Yung M.: *Malicious Cryptography: Exposing Cryptovirology*, Wiley Publishing, Inc., 2004.

Abstract

FENDING OFF A RANSOMWARE ATTACK
BY DETECTING PAYLOAD ACTIVITY

Summary: The text presents a method of detecting the activity of the ransomware payload. The ransomware was assumed to be unknown or modified and

unrecognizable by signature methods. The essence of the procedure is to observe the behavior of processes in the system and to recognize the emerging symptoms with gradual reassurance that an attack is underway. The alarm delay is selected to minimize both the risk of false alarms and the risk of delayed attack detection.

Keywords: ransomware, exploit/payload, cyberattack, symptoms, entropy, anomalies

Rozdział 3

Automatyzacja zapytań deanonimizacyjnych w sieci Bitcoin

Przemysław RODWALD[1]
Nicola KOŁAKOWSKA[2]

STRESZCZENIE: Pseudoanonimowa natura Bitcoina umożliwia przyporządkowywanie adresów do klastrów, a w pewnych przypadkach identyfikację podmiotów, do których adresy przynależące do danego klastra należą. Manualne poszukiwanie tych powiązań należy do czynności żmudnych oraz czasochłonnych. Wzrastająca liczba komercyjnych narzędzi wspomagających deanonimizację, ze względu na wysokie koszty korzystania z nich, nie zawsze oznacza ich większą dostępność wśród organów procesowych. Istnieje więc realna potrzeba stworzenia otwarto źródłowego darmowego rozwiązania wspomagającego ten proces. W niniejszym artykule przedstawiono założenia dla projektowanego rozwiązania, pokazano jego implementację i zasadę działania oraz finalnie udostępniono skrypt realizujący automatyzację zapytań do wybranych serwisów internetowych umożliwiających deanonimizację adresów BTC. Skrypt został udostępniony pod adresem https://rodwald.pl/blog/182/BTC.py.

SŁOWA KLUCZOWE: Bitcoin, deanonimozacja, automatyzacja

Wstęp

Bitcoin, pomysł na cyfrową walutę, która nie jest emitowana przez żaden urząd centralny, został przedstawiony w 2008 roku przez Satoshi Nakamoto [7], a w styczniu 2009 rozpoczął tworzenie swojego łańcucha bloków (ang. *blockchain*). Od tego czasu, z wizjonerskiej koncepcji przemienił się w najpopularniejszą kryptowalutę o kapitalizacji rynkowej sięgającej 900 mld USD[3]. Ta dominacja w świecie kryptowalut ma także swoje odzwierciedlenie

[1] Dr inż., Katedra Informatyki, Akademia Marynarki Wojennej Śmidowicza 69, 81-127 Gdynia, https://orcid.org/0000-0003-4261-8688.
[2] Studentka, Akademia Marynarki Wojennej Śmidowicza 69, 81-127 Gdynia.
[3] Według https://coinmarketcap.com/currencies/bitcoin/ na dzień 30.03.2022 kapitalizacja wynosiła 901.61B$

w działalności przestępczej, choć próby oszacowania skali jej popularności nie są spójne. Według raportu Chainalysis bezprawne wykorzystywanie kryptowalut stanowi niewielką część ich ogólnego wykorzystania, odpowiadając jedynie za 0,15% wolumenu wszystkich transakcji kryptowalutowych w roku 2021 [2]. Z kolei badania przeprowadzone w środowisku akademickim podają, że około 23% transakcji jest powiązanych z działalnością przestępczą [4]. Istotna różnica w oszacowaniu może mieć swoje źródło w przyjętych odmiennych metodologiach przeprowadzonych analizy transakcji. Ale oba środowiska zgadzają się co do tego, że odsetek osób wykorzystujących kryptowaluty do różnych form nielegalnych działań w porównaniu z legalnym ich użyciem zmniejsza się, chociaż sumaryczna kwota wyrażona w wartościach bezwzględnych ciągle rośnie [3].

Adresy i realizowane pomiędzy nimi transakcje można monitorować za pomocą eksploratorów bloków (ang. *blockchain explorer*). Jednak w narzędziach tego typu trudno doszukiwać się informacji o „właścicielu" danego adresu. Istnieją jednak narzędzia (darmowe oraz komercyjne) starające się zarówno dostarczyć informacje o prawdopodobnej przynależności danego adresu do pewnego podmiotu (np. giełdy kryptowalutowej, miksera), jak i narzędzia wizualizujące przeprowadzone transakcje. Ręczne śledzenie transakcji za pośrednictwem różnych eksploratorów lub narzędzi do wizualizacji to kluczowa umiejętność analityka śledczego [5]. Ta czasochłonna i często monotonna praca może jednak zostać częściowo zautomatyzowana, usprawniając proces analizy. Taki też jest główny cel badań prezentowanych w tej pracy – stworzenie narzędzia automatycznie odpytującego wybrane serwisy w poszukiwaniu danych deanonimizacyjnych.

Klastrowanie adresów BTC

Grupowanie adresów w klastry (ang. *clustering*) jest kluczowym elementem procesu deanonimizacji [5]. Mając wiedzę o przynależności danego adresu do konkretnego podmiotu zainteresowane organy (na przykład organy ścigania) mogą zwrócić się do zidentyfikowanego podmiotu z żądaniem ujawnienia danych osobowych właściciela badanego adresu. Wszystkie metody grupujące adresy w klastry pozwalają identyfikować dany podmiot, gdy choć jeden adres należący do danego klastra zostanie poprawnie przyporządkowany do realnego podmiotu (giełdy, sklepu, itp.). W samym łańcuchu bloków informacja ta nie jest przechowywana, czasami poza transakcjami wydobywczym w których to spółdzielnie wydobywcze ujawniają swoją tożsamość, głownie ze względów marketingowych. Z pomocą przychodzą nam zasoby

Internetu, gdzie w wielu miejscach (specjalizowane serwisy deanonimizacyjne, fora dyskusyjne związane z kryptowalutami, strony podmiotów ujawniające adresy ich portfeli w celu dokonywania darowizn, itp.) można odnaleźć informacje jednoznacznie wiążącą dany adres z konkretnym podmiotem.

Tematyka agregacji adresów poruszana była w literaturze szczególnie intensywnie w 2013 roku. Wówczas to Ron i Shamir [11] przeanalizowali łańcuch transakcji pokazując wyniki statystyczne dla typowych zachowań użytkowników sieci Bitcoin bazując na budowanych grafach transakcyjnych. W tym samym roku w kilku pracach [1, 6, 8, 9] pokazano heurystyki pozwalające grupować adresy w taki sposób, iż prawdopodobnie będą należały one do tego samego podmiotu.

Pierwsza heurystyka, prezentowana w wyżej cytowanych pracach i nazywana tam *idioms-of-use* lub *multi-input transactions*, polega na grupowaniu adresów wejściowych wchodzących w skład pojedynczej transakcji. Jeśli dwa lub większa liczba adresów wejściowych wchodzi w skład pojedynczej transakcji to zakłada się, że są one kontrolowane przez ten sam podmiot. Heurystykę należy zawęzić tylko do adresów wejściowych wymagających jednego klucza prywatnego i definiuje się ją następująco:

> *Heurystyka 1. Jeśli dwa lub większa liczba adresów wejściowych wymagających użycia pojedynczego klucza prywatnego wchodzi w skład pojedynczej transakcji to są one kontrolowane przez ten sam podmiot.*

Praktyczne wykorzystanie tej heurystyki jest stosunkowo łatwe. Jeżeli wśród adresów wejściowych pewnej transakcji będzie adres zidentyfikowany wcześniej przez analityka i przyporządkowany konkretnemu podmiotowi, to nowe adresy wejściowe także mogą zostać przypisane do danego podmiotu.

Druga heurystyka polega na grupowaniu jednego z adresów wyjściowych (tak zwanego adresu reszty) z adresami wejściowymi wchodzącymi w skład pojedynczej transakcji. Jeśli transakcja zawiera dwa adresy wyjściowe to zakłada się, że jeden z nich kontrolowany jest przez ten sam podmiot co adresy wejściowe. Heurystyka ta nazywana jest w literaturze *shadow adresses* lub *change closure*.

> *Heurystyka 2. Jeśli transakcja składa się z dwóch adresów wyjściowych to jeden z nich kontrolowany jest przez ten sam podmiot co adresy wejściowe.*

Heurystyka ta opiera się dodatkowo na założeniu, że użytkownicy rzadko przekazują środki do dwóch różnych odbiorców podczas jednej pojedynczej transakcji. Główną trudność stanowi tutaj poprawne zidentyfikowanie adresu reszty spośród dwóch adresów wyjściowych. Kilka scenariuszy pomagających identyfikować adres reszty zaprezentowano w pracy [10].

Te teoretyczne podstawy stojące za zagadnieniem grupowania adresów w klastry są wykorzystywane w dostępnych narzędziach wspomagających proces deanonimizacji, zarówno tych komercyjnych (np.: Chainalysis, CipherTrace, Qlue, MerkleScience, Scorechain, Coinfirm, Cheksy, Ikna.io) jak i darmowych (np.: walletexplorer.com, sydeus.rodwald.pl, graphsense.info). Narzędzia te dzięki wykorzystaniu heurystyk tworzą własne, często unikalne powiązania adresów z konkretnymi podmiotami.

Założenia projektowe

Projektując rozwiązanie autorzy kierowali się następującymi założeniami:

- implementacja w darmowym środowisku programistycznym,
- otwarto-źródłowy charakter projektu oparty na licencji open-source,
- „lekkość" rozwiązania polegająca na nie przechowywaniu danych transakcyjnych (aktualnie[4] pełny węzeł bitcoina zawierający wszystkie dane transakcyjne zajmuje ponad 450 GB[5]) lecz wykorzystaniu danych udostępnianych przez serwisy będące eksploratorami bloków,
- odporność na ograniczenia narzucone przez źródła danych – skrypt powinien zatrzymywać swoje działanie na wymuszony przez limity zapytań okres, a następnie automatycznie wznawiać swoje działanie,
- różnorodność źródeł danych – skrypt powinien pozyskiwać dane z wielu[6] darmowych źródeł danych, zarówno dotyczących danych deanonimizacyjnych jak i danych sankcyjnych,

[4] Ilekroć w artykule użyte jest słowo „aktualnie", przywoływany jest stan na styczeń 2023 roku.
[5] https://www.blockchain.com/explorer/charts/blocks-size
[6] W zasadzie wszystkich darmowym źródeł danych znanych autorom.

– elastyczność rozwiązania – polegająca na takiej jego konstrukcji, aby w przyszłości łatwo można będzie go rozbudowywać o inne potencjalne źródła danych.

Źródła danych transakcyjnych

Pierwszym zagadnieniem analizowanym przy projektowaniu rozwiązania był wybór źródła danych transakcyjnych, a więc danych znajdujących się w blockchain-ie bitcoina. Zdecydowano się na duplikację danych transakcyjnych, a jako dwa niezależne źródła danych wybrano serwisy blockchain.info oraz blockcypher.com.

Blockchain.info jest jednym z najpopularniejszych eksploratorów bloków. Udostępnia on bezpłatne API[7] nie wymagając przy tym klucza dostępowego. W celu pobrania danych transakcyjnych dla poszczególnych adresów należy zwrócić uwagę na limit pobieranych transakcji który nie może przekroczyć 50 transakcji na jedno zapytanie. W celu pobrania i przeanalizowania wszystkich transakcji dla analizowanego adresu należy więc w kolejnych zapytaniach pobierać kolejne porcje do maksymalnie 50 transakcji.

Przykładowe wywołanie zapytania:

```
https://blockchain.info/ra-
waddr/1AXZ1SwA2uW2cYoKmH23XgDyWGdEf3RwRB?limit=50&offset=0
```

Przykładowa odpowiedź systemu:

```
{
 "hash160":"6880546084e8d9ed7cbe123d687c349312f5c250",
 "address":"1AXZ1SwA2uW2cYoKmH23XgDyWGdEf3RwRB","n_tx":24,"n_unredeemed":0,
 "total received":401160000,"total sent":401160000,"final balance":0,"txs":[{"
…
}
```

Blockcypher.com jest drugim eksploratorem bloków z którego zdecydowano się skorzystać w niniejszym rozwiązaniu. Udostępnia API wraz ze szczegółową dokumentacją do niego[8]. W zależności od zakupionego pakietu oferuje inne limity zapytań, przy czym pakiet darmowy cechuje się następującymi ograniczeniami: 2000 zapytań dziennie, 200 zapytań na godzinę oraz 3 zapytań na sekundę. Także tutaj należy zwrócić uwagę na limit transakcji dla poszczególnego adresu (20 transakcji).

[7] https://www.blockchain.com/explorer/api/blockchain_api
[8] https://www.blockcypher.com/dev/bitcoin/

Przykładowe wywołanie zapytania:

```
https://api.blockcypher.com/v1/btc/main/addrs/
1AXZ1SwA2uW2cYoKmH23XgDyWGdEf3RwRB/full?limit=20&token=[PRIVATE_TOKEN]
```

Przykładowa odpowiedź systemu:

```
{
 "address": "1AXZ1SwA2uW2cYoKmH23XgDyWGdEf3RwRB",
 "total received": 401160000, "total sent": 401160000,
 "balance": 0, "unconfirmed balance": 0, "final balance": 0,
 "n_tx": 24, "unconfirmed_n_tx": 0, "final_n_tx": 24, "hasMore": true,
 "txs": [
…
}
```

Źródła danych deanonimizacyjnych

Jednym z ważniejszych elementów implikujących skuteczność proponowanego rozwiązania był wybór źródeł danych dostarczających dane o podmiotach, do których adresy przynależą. Zdecydowano się na możliwie szerokie podejście do tego zagadnienia i pobieranie danych z czterech źródeł danych: walletexplorer.com, sydeus.rodwald.pl, graphsense.info oraz ikna.io.

Walletexplorer.com to jeden z bardziej wartościowych darmowych projektów dla informatyka śledczego. Dostarcza informacji o zidentyfikowanych podmiotach, aktualnie dla blisko 37 milionów adresów[9]. Autorem serwisu jest Aleš Janda, który aktualnie pracuje dla komercyjnego rozwiązania chainanalysis.com. System udostępnia API, gdzie jako klucz API należy podać adres e-mail. Zgodnie z korespondencją z autorem systemu, ograniczenia w działaniu udostępnionego API to dwa zapytania na sekundę, a wymaganym parametrem jest „*caller*", który to stanowi w zasadzie dowolny ciąg znaków[10]. Podejście takie powoduje łatwość zastosowania mechanizmu omijającego zastosowane przez autora ograniczenia – w zapytaniach można podawać różne wartości parametru „*caller*".

Przykładowe wywołanie zapytania:

```
http://www.walletexplorer.com/api/1/address-lookup?                    ad-
dress=16SbwNa22nBwhLtg6HzWVYFQiUxtNzAUpt&caller=[PRIVATE_CALLER]
```

Przykładowa odpowiedź systemu:

```
{"found":true,"label":"BTC-e.com",
"wallet_id":"000003a2f31608c0","updated_to_block":766467}
```

[9] Obliczeń dokonano za pomocą skryptu parsującego dane z serwisu walletexplorer.com. Otrzymany wynik zweryfikowano u autora serwisu.

[10] "The parameter "caller" is whatever string you want and it's used for personal statistics only."

Sydeus.rodwald.pl to autorski system wykorzystywany przez autora do realizacji ekspertyz na potrzeby organów procesowych. Aktualnie w bazie systemu znajduje się ponad 142 miliony identyfikowalnych adresów i dla każdego nowego bloku dodawanego do blockchaina bitcoina system uruchamia skrypty implementujące omawiane heurystyki. Ze względów wydajnościowych dostęp do serwisu został ograniczony tylko do zalogowanych użytkowników, które stanowią organy procesowe które uzyskały dane dostępowe w ramach wykonywanych ekspertyz. Autor na potrzeby niniejszego rozwiązania utworzył API umożliwiające zautomatyzowane odpytywanie systemu, w którym należy podać indywidualny klucz API (parametr „*apikey*").

Przykładowe wywołanie zapytania:

```
https://sydeus.rodwald.pl/api.php?address=115DL5MannhGS3rsmYYxCCZcHHekw8WDSP
&apikey=[PRIVATE_API_KEY]&crc=7ca422ee84a0ab2b8a686b1c8b773e90
```

Przykładowa odpowiedź systemu:

```
{"sydeus":{"result":"success","entity":"10xBitco.in","category":"gambling"}}
```

Graphsense.info to platforma do analizy kryptoaktywów opracowana pod kierownictwem AIT (Austriackiego Instytutu Technologii), przy finansowaniu z programu KRYPTOMONITOR Austriackiej Agencji Promocji Badań Naukowych. Jest ona dostarczana jako oprogramowanie typu OpenSource, na warunkach licencji MIT. Można ją pobrać bezpłatnie do samodzielnego hostowania jak również korzystać bezpłatnie z wersji udostępnionej pod adresem demo.graphsense.info[11]. System udostępnia dobrze udokumentowaną dokumentację API[12]. Aktualna liczba zidentyfikowanych adresów przekracza 140 milionów, zaś limity zapytań wynoszą 1000 zapytań na godzinę.

[11] https://graphsense.info/about/
[12] https://api.graphsense.info/

Przykładowe dwuetapowe wywołanie zapytania (po wcześniejszej autoryzacji). W pierwszym kroku zapytanie o wartość parametru "entity" dla wskazanego adresu:

```
https://api.graphsense.info/btc/addresses/1DhHNputMZ1FCBjE6ED23bFtrDBv4GcYnK
```

Przykładowa odpowiedź systemu:

```
{
"address": "1DhHNputMZ1FCBjE6ED23bFtrDBv4GcYnK",
"balance": {
 "fiat_values": [
   { "code": "eur", "value": 108.94 },{ "code": "usd", "value": 106.09 }
  ], "value": 547350 },
    "entity": 45964491,
…
}
```

A następnie dla uzyskanej wartości „entity" zapytanie o "tagi":

```
https://api.graphsense.info/btc/entities/45964491/tags?level=entity
```

Przykładowa odpowiedź systemu:

```
{
"entity_tags": [

  {
   "active": true,
   "category": "exchange",
   "currency": "BTC",
   "is_cluster_definer": true,
   "is_public": true,
   "label": "huobi.com",
   "lastmod": 1636416000,
   "source": "https://chain.info/richlist",
   "tagpack_uri": "chaininfo.yaml",
   "address": "35hK24tcLEWcgNA4JxpvbkNkoAcDGqQPsP",
   "entity": 471871368
  }
 ]
}
```

Ikna.io – to serwis udostępniany przez założoną w 2021 roku firmę Iknaio świadczący usługi zbudowane na bazie platformy analitycznej GraphSense. System, analogicznie jak jego pierwowzór, także udostępnia dostęp poprzez API[13], zaś samo API i realizacja zapytań jest bliźniaczo podobna do graphsense. Aktualnie w bazie systemu znajduje się blisko 260 milionów otagowanych adresów, zaś limity zapytań uzależnione są od wybranego pakietu[14]: zaczynając od 1000 zapytań miesięcznie dla darmowego pakietu „Free", poprzez 10000 zapytań dla płatnego pakietu oznaczonego jako „Advanced",

[13] https://api.ikna.io/
[14] https://www.ikna.io/#packages

a kończąc na 100000 zapytań dla płatnego pakietu oznaczonego jako „Professional". Płatne pakiety, poza tak zwanymi etykietami publicznymi (ang. *public tags*) dodatkowo udostępniają etykiety zastrzeżone (ang. *proprietary tags*).
Dodatkowo rozważano pozyskiwanie danych z serwisu **bitcoinwhoswho.com**. Serwis ten udostępnia dane o: wystąpieniach adresów na stronach internetowych, adresach zidentyfikowanych jako scamy oraz tagach przypisanych do poszczególnych adresów. Poza dostępem poprzez interfejs webowy dane są udostępniane poprzez API[15], do którego pozyskano klucz dostępowy. Jednak ze względu na restrykcyjny limit zapytań, wynoszący jedno zapytanie na dobę, oraz ogólne problemy z dostępem do systemu (częste zawieszanie się strony, brak odpowiedzi na zapytania API, długi czas oczekiwania na odpowiedź API) nie zdecydowano się na pobieranie danych z tego serwisu.

Źródła danych sankcyjnych

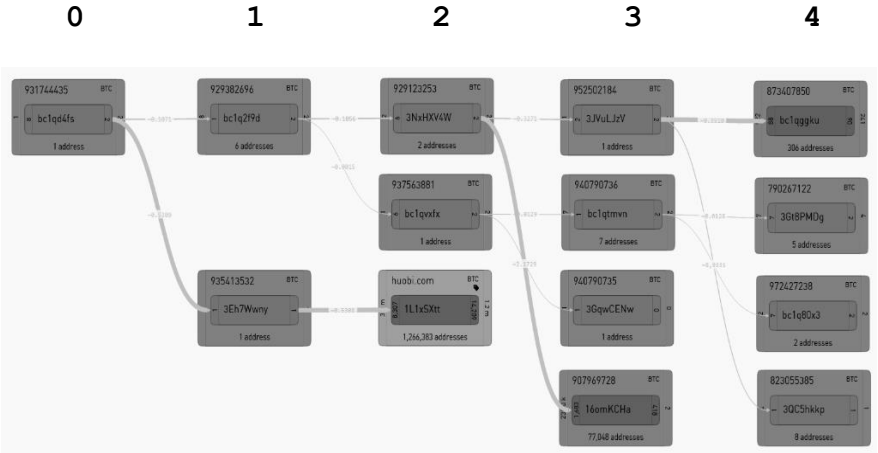
Ostatnią kategorią pozyskiwanych danych są dane o adresach objętych sankcjami. Dane te zdecydowano się pozyskiwać z dwóch źródeł: Chainalysis.com oraz BitcoinAbuse.com. Pojęcie adresów objęty sankcjami (w skrócie adresy sankcyjne) dotyczy podmiotów wymienionych na listach embarga gospodarczego, na przykład przez Stany Zjednoczone, Unię Europejską lub ONZ, z którymi podmioty podlegające tym jurysdykcjom mają zakaz prowadzenia interesów. Chainalysis oferuje bezpłatne narzędzie do sprawdzania występowania adresów na listach z sankcjami o nazwie „Free Crypto Sanctions Screening Tools", które poza interfejsem webowym daje także możliwość wywoływania zapytań API. BitcoinAbuse.com to publiczna baza danych adresów BTC wykorzystywanych przez oszustów, hakerów i przestępców. Także tutaj występuje ograniczenie wynoszące średnio 30 żądań na minutę lub jedno żądanie co dwie sekundy.

Implementacja

Zdecydowano się na realizację rozwiązania za pomocą skryptu napisanego w języku Python. Podczas realizacji projektu napotkano i rozwiązano szereg problemów, w tym te związane z limitami zapytań do poszczególnych

[15] https://www.bitcoinwhoswho.com/api/index

źródeł danych. Wprowadzono także dwa dodatkowe parametry występujące wewnątrz skryptu: *epoch* – określający maksymalną liczbę kolejnych epok dla których skrypt będzie się wykonywał, *max* – określający maksymalną liczbę adresów wejściowych/wyjściowych dla których będzie następowało kolejne zagnieżdżenie. Wizualizacja obu parametrów została pokazana na rysunku 1, dla parametrów *epoch* = 4 oraz *max* = 50: analizowany adres *bc1qd4fs...* najpierw sprawdzany jest w źródłach danych deanonimizacyjnych i sankcyjnych (jeśli zostały zaznaczone). Adres ten transferuje środki na dwa adresy *bc1q2f9d...* oraz *3Eh7Wwny...* które w kolejnej epoce są analizowane w źródłach danych. Z adresu *bc1q2f9d...* środki transferowane są tylko na jeden adres *1L1xSXtt...,* który ze względu na liczbę adresów wyjściowych (14209) przekraczającą ustawiony parametr *max* nie będzie w kolejnej epoce dalej analizowany (zaznaczony został na rysunku kolorem czerwonym, podobnie jak dwa inne adresy *16omKCHa...* oraz *bc1qggku...* dla których także liczba adresów wyjściowych przekracza parametr *max*). Działanie algorytmu zostaje zakończone na czwartej epoce ze względu na ustawiony parametr *epoch* = 4. W przedstawionym scenariuszu przeanalizowanych więc zostanie 14 adresów.



Źródło:

https://demo.graphsense.info/graph/btc/address/bc1qd4fsst4k0fjnr9jls3gtjt8y7yk4rzk70k3n38, dostęp: 31.01.2023.

Rysunek 1. Wizualizacja parametrów epoch=4 oraz max=50

Zrzut ekranu prezentujący fragment skryptu BTC.py został zaprezentowany na rysunku 2. Cały skrypt, gotowy do pobrania, znajduję się pod adresem https://rodwald.pl/blog/182/BTC.py.

```
for j in range(list_of_address_len):
    ...

    #sydeus
    sydeus_add = requests.get("https://sydeus.rodwald.pl/api.php?address=" + list_of_address[j] + "&apikey=" + sydeus_apikey + "&cc=" + hash_result)
    sydeus_add = json.loads(sydeus_add.text)
    sydeus_add = sydeus_add.get('sydeus')
    if 'success' in sydeus_add.values():
        data_sydeus.append([list_of_address[j], sydeus_add.get('entity')])

    #walletexplorer
    walletexplorer_add = requests.get("http://www.walletexplorer.com/api/1/address-lookup?address=" + list_of_address[j] + "&caller=" + caller_name)
    walletexplorer_add = json.loads(walletexplorer_add.text)
    if 'label' in walletexplorer_add.keys():
        data_walletexplorer.append([list_of_address[j], walletexplorer_add.get('label')])

    #graphsense
    graphsense_add = requests.get("https://api.graphsense.info/btc/addresses/" + list_of_address[j] + "?include_tags=true", headers=headers_graphsense)
    graphsense_add = json.loads(graphsense_add.text)
    graphsense_add = graphsense_add.get('entity')
    graphsense_add = str(graphsense_add)
    graphsense_add = requests.get("https://api.graphsense.info/btc/entities/" + graphsense_add + "/tags?level=entity&pagesize=10", headers=headers_graphsense)
    graphsense_add = json.loads(graphsense_add.text)
    graphsense_add = graphsense_add.get('entity_tags')
    if not graphsense_add:
        pass
    else:
        graphsense_add = graphsense_add[0]
        if 'label' in graphsense_add.keys():
            data_graphsense.append([list_of_address[j], graphsense_add.get('label')])
    ...
```

Źródło: https://rodwald.pl/blog/182/BTC.py, dostęp: 31.01.2023.

Rysunek 2. Fragment skryptu BTC.py

Działanie skryptu

W celu uruchomienia skryptu należy najpierw zainstalować środowisko Python, najlepiej w najnowszej stabilnej wersji. Skrypt uruchamia się w środowisku Python podając jako dane wejściowe trzy parametry adres BTC który chcemy analizować, serwisy (a dokładniej pierwsze litery nazw serwisów) z których zasobów chcemy pozyskać dane oraz kierunek przeszukania (IN lub OUT, domyślnie ustawiony OUT). Aktualnie serwis obsługuje zapytania do czterech wyżej omówionych serwisów deanonimizacyjnych (ich wywołania prezentują się następująco: walletexplorer.com [W], sydeus.rodwald.pl [S], graphsense.info [G], ikna.io [I]) oraz dwóch serwisów sankcyjnych (chainalysis.com [C], bitcoinabuse.com [B]).

Zdecydowanie zalecaną czynnością przez uruchomieniem skryptu jest zwrócenie się do właścicieli systemów blochchair.com, graphsense.info, ikna.io, chinalysis.com z prośbą o uzyskanie własnego klucza dostępowego

(API). Większość z wymienionych systemów dysponuje formularzami służącymi temu celowi: [I][16], [C][17], [B][18]. W przypadku serwisu graphsense [G] w celu uzyskania klucza należy wysłać taką prośbę na adres e-mail[19]. Należy przy tym zauważyć, że część z wymienionych serwisów generuje i udostępnia klucze tylko dla zgłoszeń realizowanych z adresów rządowych[20]. Niepozyskanie powyższych kluczy (wszystkich lub wybranych) skutkować będzie działaniem skryptu dla podstawowej i domyślnej jego konfiguracji: dane transakcyjne są wówczas pobierane z systemu blockchain.info, natomiast dane deanonimizacyjne z systemu walletexplorer.com. Dane sankcyjne nie są domyślnie pobierane, gdyż każdy z serwisów je udostępniających wymaga podania klucza autoryzacyjnego.

Po pozyskaniu powyższych kluczy API, należy je wpisać w odpowiednie miejsca skryptu. Znajdują się one, jednoznacznie opisane, w jego początkowej części, co pokazano na rysunku 3.

```
apikey_blockcypher = "de183fd2..."
apikey_sydeus   = "6071f9bb..."
apikey_chainalysis = {'X-API-Key':'b88847f0...', 'Accept':'application/json'}
apikey_graphsense = {'Authorization':'b/EVrO1e...'}
...
```

Źródło: BTC.py, dostęp: 31.01.2023.

Rysunek 3. Przykładowe zanonimizowane uzupełnienie pozyskanych kluczy API wewnątrz skryptu BTC.py

Skrypt, jak większość projektów informatycznych we wstępnej fazie swojego istnienia, na mocy zgłaszanych uwag i sugestii podlegał modyfikacjom. Jedną z nich była próba agregacji pozyskanych danych deanonimizacyjnych. Agregacja okazała się niezbędna, gdyż ze względu na zastosowanie różnych źródeł danych, wyniki pozyskiwane z nich nie muszą wskazywać na to samo źródło pochodzenia. Dodatkowo dane pozyskiwane nie zawsze mają identyczną postać mimo wskazywania na ten sam podmiot (na przykład Yo-

[16] https://www.ikna.io/order/free
[17] https://www.chainalysis.com/free-cryptocurrency-sanctions-screening-tools/
[18] https://www.bitcoinabuse.com/register
[19] contact@graphsense.info, źródło: https://graphsense.info/news/
[20] Pod pojęciem adresu służbowego rozumie się tutaj adres e-mail na przykład w domenach @prokuratura.gov.pl, @*.policja.gov.pl, a nie adres będący na przykład w domenach @gmail.com, @wp.pl.

Bit.net oraz yobit). Do realizacji tego zagadnienia zdecydowano się na wykorzystanie klasy *SequenceMatcher* dostępnej w module *difflib* środowiska Python.

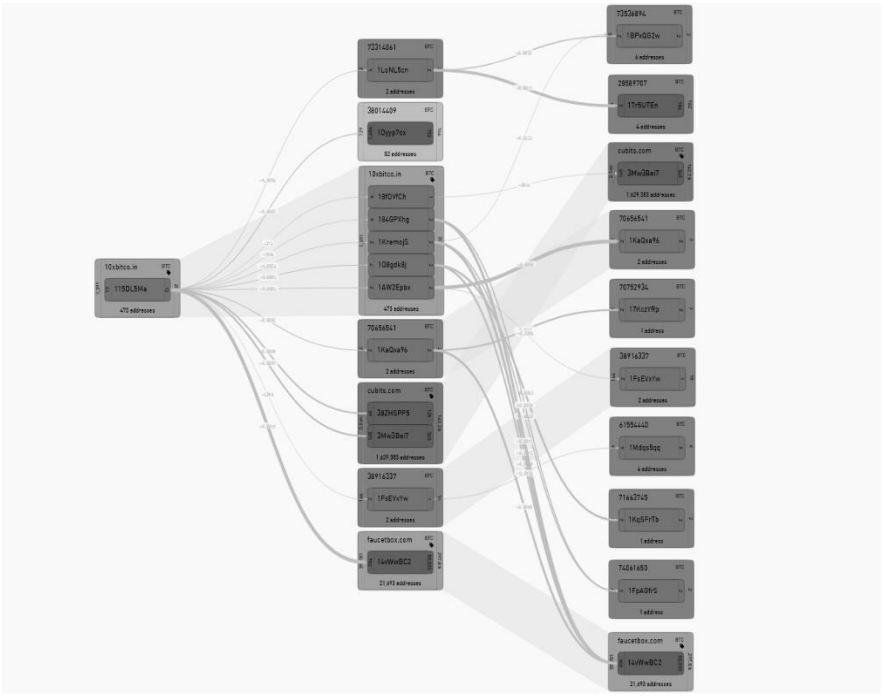
W aktualnym rozwiązaniu zdecydowano się więc na umieszczaniu w pliku wynikowym znaku (+ lub –) informującego o poprawnej agregacji danych, co zostało zaprezentowane na rysunku 4. Symbol + należy interpretować na jeden z następujących wariantów: a) pozyskano dane deanonimizacyjne tylko z jednego źródła, lub b) pozyskano dane deanonimizacyjne z co najmniej dwóch źródeł i reprezentują one ten sam podmiot. Symbol – należy natomiast rozumieć jako sytuację gdy co najmniej dwa źródła danych deanonimacyjnych udostępniły informacje o danym podmiocie lecz dane te pomiędzy sobą się różnią (wskazują na inny podmiot).

```
Address|Sydeus|Graphsense|Similarity|PreviousAddress|Epoch

115DL5MannhGS3rsmYYxCCZcHHekw8WDSP|10xBitco.in|10xBitco.in| + |None|0

14vWwBC2VFGF7nFLDWxSQWoaPiDuPeHfBk|FaucetBOX.com|faucetbox| + |115DL5...|1
18fDVfCh7jQPKPe7sXrijcRwTKSyB2JBiT|10xBitco.in|10xbitco.in| + |115DL5...|1
184GPXhgWr1e3VxPM57NZ1mnoogtpwEQPk|10xBitco.in|10xbitco.in| + |115DL5...|1
1KremojSu99KDq4QwCjBcnJb6GwdXUivS8|10xBitco.in|10xbitco.in| + |115DL5...|1
1Q8gdk8j2gTxVcRpJeDV4SmcJVXSH9K9UL|10xBitco.in|10xbitco.in| + |115DL5...|1
1AW2EpbxFVLbugMNYJzpyWeBXcXsUk7k3M|10xBitco.in|10xbitco.in| + |115DL5...|1
38ZHSPP5J2mojAmQaafeZctC8BMrPNZ5L1|Cubits.com|cubits.com| + |115DL5...|1
3Mw3Bei7T18s6MDB19FCXs3nPgXmACLfXg|Cubits.com|cubits.com| + |115DL5...|1
1Dyyp7oxDnyPJV7hiUkpqh61YLyydZYwrQ|Coinbase.com|| + |115DL5...|1
```

Źródło: BTC.py 115DL5MannhGS3rsmYYxCCZcHHekw8WDSP SG OUT, dostęp: 31.01.2023

Rysunek 4. Przykładowa zawartość pliku wynikowego skryptu BTC.py

Wizualną interpretację dla pokazanego na rysunku 4 pliku wynikowego zaprezentowano na rysunku 5 pochodzącym z systemu GraphSense. Kolorem czerwonym zaznaczono na nim adresy które nie były w skrypcie w kolejnych epokach analizowane ze względu na parametr *max*. Dodatkowo kolorem zielonym zaznaczono adres *1Dyyp7ox...* który został zidentyfikowany tylko w systemie sydeus.



Źródło:

demo.graphsense.info/graph/btc/address/115DL5MannhGS3rsmYYxCCZcHHekw8WDSP, dostęp: 31.01.2023

Rysunek 5: Analiza adresu 115DL5MannhGS3rsmYYxCCZcHHekw8WDSP w systemie GraphSense

Kolejną modyfikacją było wyraźne wskazanie adresów sankcyjnych. Przy dużych plikach wynikowych niejako ginęły wyniki identyfikacji adresów sankcyjnych stąd celowym było pewne ich wyróżnienie w pliku wynikowym. W aktualnym rozwiązaniu zdecydowano się na dodaniu informacji o zidentyfikowaniu adresu jako objętego sankcjami poprzez symbol literę **S** następującą po wyniku działania agregacji. W przypadku identyfikacji negatywnej lub braku identyfikacji używany jest symbol **_**.

Podsumowanie

Rosnąca popularność kryptowalut, także do popełniania przestępstw polegających na ich wyłudzaniu lub ich wykorzystywaniu w procederze „prania"21 pieniędzy [10] powodują zauważalny wzrost liczby postępowań dotyczących kryptowalut.

Zaproponowany skrypt ma celu wspomóc organy procesowe w próbie identyfikacji podmiotów, do których adresy BTC mogą przynależeć. Należy zauważyć, że czynność ta jest niejako pierwszym krokiem w trzyetapowej próbie identyfikacji rzeczywistego właściciela adresu. W drugim kroku organ procesowy powinien zwrócić się do zidentyfikowanych dzięki niniejszemu skryptowi podmiotów z żądaniem udzielenia informacji o danych powiązanych z danym adresem zgromadzonych w systemie. Większość podmiotów podlegających procedurom KYC/AML dysponuje co najmniej następujących zbiorem danych: adres e-mail (wymagany do założenia konta w systemie), numer telefonu (weryfikowany poprzez wysłanie kodu na SMS), dane osobowe (podawane podczas identyfikacji i weryfikacji), skan dokumentu tożsamości (zapisywany podczas procesu weryfikacji), skan potwierdzający adres (wyciąg z rachunku bankowego, płatności za energię, …), historia wpłat/wypłat (zarówno FIAT jak i krypto), historia transakcji (zarówno FIAT ‹-› krypto jak i krypto ‹-› krypto), historia logowań (adresy IP, metadane, …), a ostatnio dodatkowo jeszcze oświadczenia o źródle pochodzenia środków i dowody potwierdzające składane oświadczenia (z wykonywania zawodu / pensji: potwierdzenia przelewów lub pasków wynagrodzenia za okresy bezpośrednio poprzedzające wpłaty oraz pokrywające depozyty; z darowizny: umowę darowizny lub potwierdzenie zgłoszenia do Urzędu Skarbowego oraz potwierdzenie otrzymania przelewu na konto; ze spadku: akt dziedziczenia i potwierdzenie otrzymania przelewu na konto; z inwestycji: potwierdzenie zakończenia lokaty lub przelew z innej inwestycji; z kopania kryptowalut: potwierdzenie otrzymania nagrody za wykopany urobek, adres na który wpływa nagroda lub zrzut ekranu z poola; z innego źródła, np. innej krypto-giełdy: inny dokument potwierdzający to źródło, np. historia portfela na innej stronie

[21] Potoczne określenie „prania" pieniędzy (ang. *money laundering*) polega na wprowadzeniu do legalnego obrotu pieniędzy lub innych wartości majątkowych pochodzących z nielegalnych źródeł oraz zatarcie śladów pierwotnego pochodzenia środków.

internetowej)[22]. W trzecim kroku instytucja obowiązana powinna udostępnić posiadane przez nią dane organom procesowym.

Zaprojektowany system ze względu na swoją modułową budowę jest przygotowany do rozszerzania o ewentualne inne źródła danych. Jego wykorzystanie wymaga dla pewnych źródeł danych pozyskania indywidualnego klucza API przez przedstawicieli organów procesowych.

Autor w ramach swoich badań oraz czynności procesowych wykonywanych jako biegły sądowy z tematyki kryptowalut planuje dalszy rozwój zaproponowanego rozwiązania, w szczególności implementację skryptów dla innych kryptowalut.

Źródła:

- Androulaki E., Karame G.O., Roeschlin M., Scherer T., Capkun S., *Evaluating User Privacy in Bitcoin*, Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859, Springer, Berlin, Heidelberg, 2013.
- Chainalysis, *The 2022 crypto crime report*, https://go.chainalysis.com/2022-Crypto-Crime-Report.html, 2022.
- Europol, *Cryptocurrencies - tracing the evolution of criminal finances*, Publications Office of the European Union, ISBN 978-92-95220-37-9, 2021.
- Foley S., Karlsen J.R., Putnins T.J., *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?* The Review of Financial Studies, 32(5), 1798–1853, 2019.
- Furneaux, N., *Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence.* John Wiley & Sons, 2018.
- Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D., Voelker G.M., Savage S., *A fistful of bitcoins: characterizing payments among men with no names*, Proceedings of the 2013 conference on Internet measurement conference. ACM, 2013.

[22] Przykładowa zawartość oświadczenia wymagana przez giełdę ZondaGlobal, https://kyc.zonda.exchange/

- Nakamoto S., *Bitcoin: a peer-to-peer electronic cash system*, https://bitcoin.org/bitcoin.pdf, 2008.
- Ortega M.S., *The bitcoin transaction graph anonymity*. Master's thesis, Universitat Oberta de Catalunya, 2013.
- Reid F., Harrigan M., *An analysis of anonymity in the bitcoin system*, Security and privacy in social networks, Springer, New York, 2013.
- Rodwald, P., *Kryptowaluty z perspektywy informatyki śledczej,* Akademia Marynarki Wojennej, Gdynia, ISBN 978-83-959756-7-7, 2021.
- Ron D., Shamir A., *Quantitative analysis of the full bitcoin transaction graph*, International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013.

Rozdział 4

Ochrona zasobów informacyjnych przed atakami wrogich podmiotów zorganizowana na podstawie uznanych wzorców, baz wiedzy i standardów – zarys metodyki

Krzysztof LIDERMAN[1]

STRESZCZENIE: w opracowaniu przedstawiono koncepcję wykorzystania, dostępnych bezpłatnie, uznanych idei i frameworków w organizacji ochrony zasobów informacyjnych przed atakami (sieciowymi) wrogich podmiotów. Podstawą koncepcji jest przedstawiona w rozdz. 2 metodyka reakcji na incydenty z zakresu bezpieczeństwa informacyjnego firmy IBM. Wykorzystano w niej model diamentu i Cyber Kill Chain. Proponuje się rozwinięcie działań w ramach tej metodyki o zalecenia wynikające z MITRE ATT&CK. W niniejszym opracowaniu scharakteryzowano także krótko wszystkie trzy ww. elementy.

SŁOWA KLUCZOWE: ochrona zasobów informacyjnych przed atakami, Cyber Kill Chain, Diamond Model, MITRE ATT&CK

Wstęp

Wraz z rozwojem elektronicznego przetwarzania zasobów informacyjnych wzrosło zainteresowanie bezpieczeństwem tego procesu, w szczególności możliwością jego wykorzystania przez wrogie podmioty indywidualne lub grupowe do realizacji własnych celów, niezgodnych z oczekiwaniami legalnego dysponenta zasobu. Zagrożenia dla zasobów informacyjnych można sklasyfikować następująco:

[1] Dr inż., Military University of Technology E-mail: krzysztof.liderman@wat.edu.pl; ORCID: 0000-0001-2345-6789

1. „Siły wyższe” – zdarzenie zewnętrzne, niemożliwe (lub prawie niemożliwe) do przewidzenia, którego skutkom nie można zapobiec, w tym zjawiska przyrodnicze (jak np. emisja ujawniająca) oraz zjawiska społeczno-polityczne (jak np. terroryzm).
2. Działania ludzi:
   2.1. Celowe (nieuprawnione i przestępcze):
      - działania personelu, w tym podsłuchy różnego typu i kradzieże oraz zagubienia nosicieli informacji (sprzętu i dokumentów);
      - działania osób postronnych (klienci, „hakerzy”), w tym różnego typu podsłuchy i kradzieże nosicieli informacji (dokumentów i sprzętu).
   2.2. Błędne[2]

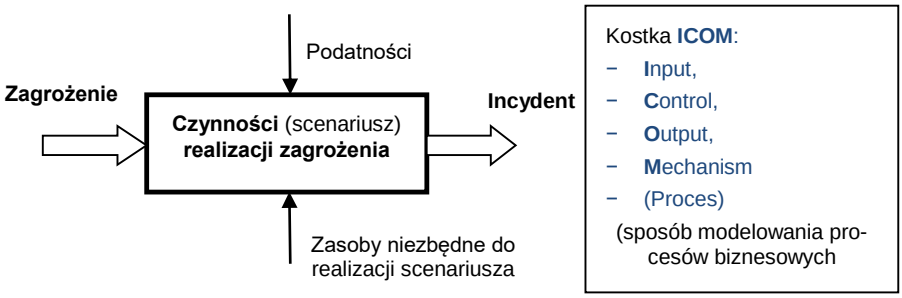
Wspomniane działania „wrogich podmiotów” mieszczą się w punkcie 2.1 powyższej klasyfikacji. Wynik skutecznej realizacji takich działań to incydent (z zakresu bezpieczeństwa informacyjnego, patrz rys. 1). Wśród incydentów związanych z podklasą 2.1 można wyróżnić pewien sposób ich realizacji – ataki na systemy komputerowe i informację, w szczególności ataki zdalne, prowadzone z wykorzystaniem sieci i systemów teleinformatycznych. Na potrzeby tego opracowania przyjęto, że atak na system informacyjny i informację w nim przetwarzaną to nieuprawnione, celowe działanie człowieka powodujące niepożądaną zmianę wymaganych wartości istotnych kryteriów jakości informacji[3]. Na rysunku 1 pokazano proces realizacji zagrożenia przestawiony za pomocą kostki ICOM.

Ze względu na masowość i zakres terytorialny ataków (praktycznie cały świat), pojawił się problem usystematyzowania przeciwdziałań w skali globalnej.

W warstwie strategicznej do działań takich należy powołanie ponadnarodowych organów takich jak Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA[4]) oraz opracowanie odpowiednich jednolitych rozwiązań organizacyjno-prawnych, jak RODO czy NIS i NIS2 w Europie. Do tej warstwy można przypisać także wyspecjalizowane ponadnarodowe komórki organów ścigania, jak Europejskie Centrum ds. walki z Cyberprzestępczością (EC3, European CyberCrime Center).

---

[2] Przykład z 04.10.2021 – awaria Facebooka ☺.
[3] Takich jak np. tajność, integralność czy dostępność zasobu informacyjnego.
[4] Aktualna nazwa to *Agencja Unii Europejskiej ds. Cyberbezpieczeństwa*.



Źródło: opracowanie własne.
Rysunek. 1. Proces realizacji zagrożenia

W warstwie operacyjnej z kolei, do przeciwdziałań atakom należy m.in. dostarczenie różnego rodzaju wyspecjalizowanym komórkom technicznym organizacji (agencji, urzędów, firm, zakładów przemysłowych itp.)[5], narzędzi systematyzujących, ujednolicających i ułatwiających ich pracę. Przyjęcie przez te komórki pewnej wspólnej, ogólnej koncepcji działań (np. modelu opisanego w rozdz. 2) i rozwiązań precyzujących fragmenty ogólnej koncepcji, takich jak *kill chain* oraz usystematyzowanych matryc pojęciowych takich jak *ATT&CK* firmy MITRE, dostarcza nie tylko wspólnej, ponadnarodowej płaszczyzny koncepcyjnej i komunikacyjnej, ale przede wszystkim w dużym stopniu „automatyzuje" pracę takich komórek.

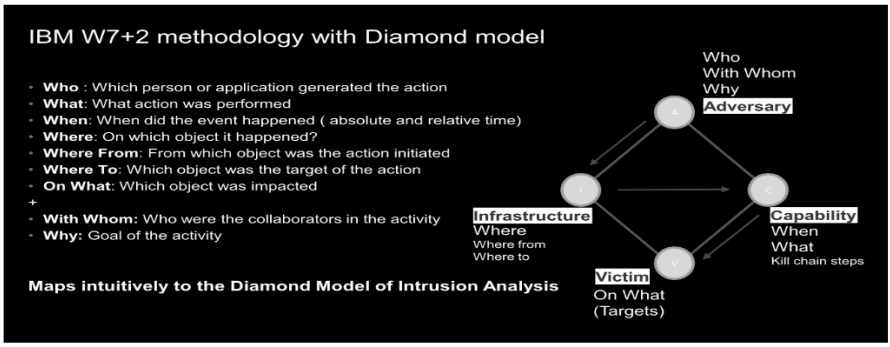
W niniejszym opracowaniu przedstawiono znane i, co ważne, uznane i stosowane koncepcje i frameworki: *Cyber Kill Chain* (rozdz. 4), *Diamond Model* (rozdz. 3), *MITRE ATT&CK* (rozdz. 5). Że opisywane w tym opracowaniu koncepcje i frameworki powinny być znane współczesnym specjalistom od „bezpieczeństwa", może świadczyć np. zestaw wymagań rekrutacyjnych firmy IBM na stanowisko analityka bezpieczeństwa[6], gdzie wymaga się m.in. „… *familiarity with common cyber intrusion frameworks such as Cyber Kill Chain, Diamond Model, MITRE ATT&CK".*

[5] Znanych zwykle pod nazwami takimi jak *Security Operation Center* (SOC), *Computer Emergency Response Team* (CERT) czy *Computer Security Incident Response Team* (CSIRT).

[6] The Security Operations Center Analyst I position is a Tier 1 position within our Managed Security Services SOC. Za: https://careers.ibm.com/job/16480337/security-operations-center-analyst-i-remote/?codes=IBM_ CareerWebSite (dostęp 26.09.2022).

Metodyka firmy IBM

Podstawowe pytania podczas analizy działań wrogiego podmiotu to: KTO, CO, KIEDY, GDZIE, DLACZEGO, JAK[7]. Są to pytania na które powinno znaleźć się odpowiedź podczas obsługi incydentu z zakresu bezpieczeństwa informacyjnego. Uzyskane odpowiedzi pozwalają sprawnie przygotować reakcję na działania atakującego podmiotu. Istotna jest przy tym kolejność, w jakiej uzyskuje się odpowiedzi na takie pytania i możliwości wykorzystania uzyskanych odpowiedzi do dalszych działań, w szczególności uzyskania kolejnych odpowiedzi na pytania ze zbioru pokazanego na rys. 2.



Źródło: materiały szkoleniowe firmy IBM.

Rysunek. 2. Wykorzystanie modelu diamentu i kill chain w metodyce firmy IBM obsługi incydentu typu „atak"

Firma IBM zaproponowała bowiem pewne systematyzujące podejście, bazujące na modelu diamentu (patrz rozdz. 3 i rys. 2) do rozwiązania problemu obejmującego identyfikację:

1. **Kto/co** spowodował(-o) określone działanie/akcję (*who*).
2. **Jakie** działanie/akcja została wykonana (co się wydarzyło – *what*).
3. **Kiedy** działanie/akcja została wykonana (zarówno w jednostkach absolutnych czasu jak i w odniesieniu do innych działań, tj. w umieszczeniu określonej akcji na osi czasu – *when*).

[7] Anglojęzyczny akronim to 5W1H. Ten zbiór pytań pomocny w rozwiązywaniu problemów różnych typów jest nazywany czasami metodą Kiplinga (od poematu opublikowanego przez Rudyarda Kiplinga w 1902 roku "Just So Stories".

4. **Na którym obiekcie** ujawniły się skutki działań wykonywanych przez wrogi podmiot[8] (na którym obiekcie w atakowanej sieci/systemie została wykryta wroga akcja – *where*).
5. **Z którego obiektu** została zainicjowana wroga akcja (*where from*).
6. **Który obiekt był celem** wrogiej akcji[9] (*where to*).
7. **Na którym obiekcie**(-ach) zostały wykonane wrogie działania (*on what*).
8. **Kto/co współdziałał**(-o) z wrogim podmiotem (*with whom*).
9. **Jaki był cel wrogich działań** (dlaczego je wykonano – *why*).

Jak pokazano na rys. 2, w węźle *Capability* modelu diamentu proponuje się wykorzystanie procesu *kill chain* (patrz rozdz. 4) do znalezienia odpowiedzi na pytanie *what*. Uzyskana odpowiedź powinna umożliwić przypisanie zidentyfikowanej akcji do odpowiedniej pozycji łańcucha działań *kill chain*. W praktyce będzie to oznaczało przypisanie działań do odpowiedniego wiersza tabeli 1 (patrz rozdz. 4). W zasadzie na tym kończy się propozycja firmy IBM – działania wrogiego podmiotu zostały zidentyfikowane, a wrogi podmiot powinien być już namierzony.

W tym opracowaniu proponuje się rozszerzenie przedstawionej propozycji o kolejne działania wykonywane przez broniący się podmiot – wykonanie przeciwdziałań dopasowanych do odpowiednich elementów *kill chain* (wierszy w tabeli 1) które to działania można pogrupować tak, jak pokazują to nagłówki kolumn tabeli 1. W celu przypisania wybranej przeciwakcji (tj. wpisania jej do odpowiedniego pola tabeli 1) proponuje się wykorzystanie bazy wiedzy (frameworku) MITRE ATT&CK (patrz rozdz. 5).

W zasadzie przedstawiona propozycja wpisuje się w proces obsługi incydentu (w tym przypadku – z zakresu bezpieczeństwa informacyjnego).

[8] Nie musi to być obiekt docelowy!

[9] Obiekt, na którym została wykryta wroga akcja (punkt 5) nie musi być obiektem docelowym wrogich działań – może to być obiekt pośredni, wykorzystany przez wrogi podmiot do dalszych działań np. w ramach ataku APT.

Pomija ona jednak dwa istotne elementy tego procesu – wykrycie incydentu/ataku[10] i przekazanie do obsługi. W tym opracowaniu zakłada się, że te dwie wymienione czynności warunkujące uruchomienie procesu obsługi, zostały skutecznie zrealizowane.

Model diamentu

Model diamentu dotyczy aktywności podmiotu wykonującego atak, czyli ciągu zdarzeń opisanego przez cztery podstawowe (ang. *core*) elementy, nazywane dalej cechami:

1. Intruza (ang. *adversary*).
2. Infrastrukturę.
3. Możliwości (ang. *capability*) wrogiego podmiotu.
4. Poszkodowanego (ang. *victim*).

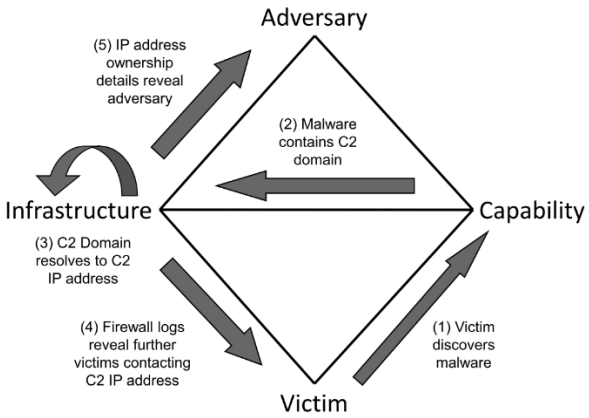
Występujące pomiędzy tymi cechami relacje są przedstawione przy pomocy grafu zaaranżowanego do postaci kryształu diamentu (stąd nazwa modelu: *diamond model*; po polsku „model diamentu" lub „model diamentowy" – brak jest powszechnie uznanego polskiego określenia), gdzie wierzchołkami są ww. cechy, co pokazano na rys. 3. Podmiotem (atakującym, w opracowaniach anglojęzycznych *adversary*) jest aktor/organizacja wykorzystująca możliwości (capability) przeciwko poszkodowanemu (victim) do osiągnięcia założonych celów. Wyróżnia się podmiot-operatora który wykonuje działania skierowane przeciwko poszkodowanemu i podmiot-klienta (w szczególnym przypadku może to być ta sama osoba lub grupa) który czerpie korzyści z wykonywanych działań.

Przykładowy ciąg zdarzeń przedstawiony na rys. 3 jest następujący:

1. Poszkodowany wykrywa malware w swojej sieci.

[10] W efekcie w tym opracowaniu pominięto np. problematykę wykrywania działań wrogiego podmiotu. Wskaźnik infiltracji (IoC – *Indicator of Compromise*) jest elementem danych (zapisem w dziennikach zdarzeń systemu/urządzenia, fragmentem zarejestrowanego ruchu sieciowego, itp.) który może być użyty do zidentyfikowania działalności wrogiego podmiotu. Często rozróżnia się wskaźnik infiltracji (IoC) od wskaźnika ataku (IoA). IoC jest statyczny – można go wykorzystać gdy atak jest zakończony (bazuje na obserwowalnych skutkach ataku). IoA jest dynamiczny – pozwala namierzać wrogi podmiot podczas jego działań (bazuje na obserwowalnych, dynamicznych śladach działania wrogiego podmiotu).

2. Wyniki analizy malware wskazują na domenę command-and-control (C2).
3. Domena C2 wskazuje na związany z nią adres IP, pod którym jest hostowany kontroler sterujący malwarem.
4. Zapisy w dziennikach zdarzeń zapory sieciowej wskazują na inne zainfekowane hosty w sieci poszkodowanego − to hosty, które próbują się łączyć z wykrytym adresem IP kontrolera malwaru.
5. Dane rejestracyjne adresu IP atakującego podmiotu ujawniają kolejne o nim informacje.



Źródło: 1.Caltagirone S., Pendergast A., Betz Ch.: The Diamond Model of Intrusion Analysis, DoD Report, Juli 2013.
Rysunek. 3. Model diamentu

W modelu zdefiniowano także cechy wyższego rzędu (ang. meta-feature):

- stempel czasowy dla początku i końca zdarzenia (ang. *timestamp*),
- fazę,
- rezultat,
- kierunek,
- metodykę,
- zasoby.

Te cechy wspierają tworzenie złożonych konstrukcji modelujących działania atakującego podmiotu, takie jak wątki aktywności i grupy aktywności (szczegóły – patrz [1] i [2]).

Każda z cech zdarzenia, zarówno podstawowa jak i meta, ma przypisaną pewną wartość pewności, która w tym ogólnym modelu jest niezdefiniowana, ponieważ w każdej implementacji modelu ta wartość może być inaczej interpretowana. Ogólnie, w modelu diamentu ciąg zdarzeń składający się na atak (scenariusz takiego ataku) jest przedstawiany jako pojedyncze zdarzenie **E** opisywane przez pewien zbiór cech tj. etykietowaną n-tkę, której każdy element zawiera informacje o danej cesze z dołączoną wartością pewności (ang. *confidence*) [1].

$$\begin{aligned}\boldsymbol{E} = \langle &\langle Adversary, Confidence_{adversary}\rangle,\\ &\langle Capability, Confidence_{capability}\rangle,\\ &\langle Infrastructure, Confidence_{infrastructure}\rangle,\\ &\langle Victim, Confidence_{victim}\rangle,\\ &\langle Timestamp_{start}, Confidence_{timestamp_{start}}\rangle,\\ &\langle Timestamp_{end}, Confidence_{timestamp_{end}}\rangle,\\ &\langle Phase, Confidence_{phase}\rangle,\\ &\langle Result, Confidence_{result}\rangle,\\ &\langle Direction, Confidence_{direction}\rangle,\\ &\langle Methodology, Confidence_{methodology}\rangle,\\ &\langle Resources, Confidence_{resources}\rangle\rangle\end{aligned}$$

Każdy z elementów entki może być uszczegółowiony przez dołączenie do niego n-tki dokładniej opisującej daną cechę.

$$\begin{aligned}\langle Victim, Confidence_{victim}\rangle = &\\ &\langle\langle Organization, Confidence_{organization}\rangle,\\ &\langle HostIPAddress, Confidence_{IP}\rangle,\\ &\langle Hostname, Confidence_{Hostname}\rangle,\\ &\langle Application, Confidence_{Application}\rangle,\\ &\langle TCPPort, Confidence_{TCPPort}\rangle\rangle\end{aligned}$$

Podstawową możliwością (według autorów [1]) udostępnianą przez model diamentu jest wykorzystanie techniki nazywanej *pivoting* (brak sensownego odpowiednika w języku polskim) polegającej na wybraniu jednego

elementu i wykorzystaniu go w połączeniu z danymi źródłowymi do wykrycia innych powiązanych elementów (na rys. 3 takich „pivotów" jest pięć).

Gwoli ścisłości należy dodać, że nazwa „model diamentu" jest też używana jako nazwa innych modeli, z innych obszarów zastosowań (por. np. *https://www.marketing91. com/porters-diamond-model/*).

„Kill chain" i „Intrusion kill chain"

Fraza „kill chain" oznacza systematyczny proces rozpoznawania i angażowania w określone (kontrolowane przez broniącego się), działania atakującego podmiotu tak, aby uzyskać pożądane rezultaty. Wojskowa doktryna namierzania USA (*U.S. military targeting doctrine*. U.S. DoD, 2007) definiuje czynności tego procesu (znanego pod akronimem F2T2EA) jako:

1. Znajdź (*find*) u przeciwnika punkty nadające się do związania go walką.
2. Ustal (*fix*) jego lokalizację.
3. Śledź go (*track*) i obserwuj.
4. Oddziałuj na jego słabe punkty (*target*) aby uzyskać pożądane efekty.
5. Zwiąż walką (*engage*) przeciwnika.
6. Oceń (*assess*) efekty.

Jest to zintegrowany, całościowy proces nazywany „łańcuchem" w tym sensie, że brak któregoś z ww. elementów czyni ten proces nieskutecznym. Ten znany z klasycznego współczesnego pola walki proces został zaadaptowany do działań w cyberprzestrzeni.

„Intrusion kill chain" oznacza łańcuch działań tworzony przez podmiot atakujący („kill chain" z poprzedniego akapitu jest na niego odpowiedzią), składających się na atak. Przyjmuje się, że działanie podmiotu przeprowadzającego dowolny atak typu „włamanie", da się zdekomponować do łańcucha następujących czynności:

1. Rozpoznanie (*reconnaissance*).
2. Wytworzenie narzędzia ataku (uzbrojenie; *weaponization*).
3. Dostarczenie (do systemu poszkodowanego; *delivery*).
4. Wykorzystanie (przez dostarczone narzędzie podatności w systemie poszkodowanego; *exploitation*).
5. Instalacja (wrogiego kodu lub programów w systemie poszkodowanego; *installation*).

6. Sterowanie (przez atakujący podmiot zainstalowanym w systemie poszkodowanego wrogim kodem lub programem; *command and control* − C2).
7. Akcja na osiągniętym zasobie docelowym (*actions on objectives*).

Zaprezentowane w ostatnim akapicie podejście zostało opracowane przez firmę Lockheed Martin jako **Cyber Kill Chain® framework** który jest częścią modelu **Intelligence Driven Defense®**[11] − identyfikacji i zapobiegania działaniom podmiotu atakującego [10]. Zainteresowani mogą znaleźć szczegóły w opracowaniu firmowym „*GAINING THE ADVANTAGE Applying Cyber Kill Chain® Methodology to Network Defense*"[12] [11].

Przykład 1 – atak (za [2]):

W przypadku ataku na sieć komputerową (ang. *computer network attack*; CNA) lub szpiegostwa komputerowego (ang. *computer network espionage*; CNE), poszczególne elementy „intrusion kill chain" można opisać następująco:

1. **Rozpoznanie** – badanie, identyfikacja i selekcja potencjalnych celów często reprezentowanych przez wyniki przeszukiwania Internetu, takie jak publikacje z konferencji, adresy e-mail, relacje pomiędzy użytkownikami Internetu czy informacje o wybranych technologiach.
2. **Uzbrojenie** – wytworzenie „broni", np. połączenie trojana zdalnego dostępu z exploitem w dostarczalny payload w przypadku wytwarzania zautomatyzowanych narzędzi ataku (weaponizer). Często pliki z aplikacjami np. typu Adobe Portable Document Format (PDF) czy Microsoft Office documents (DOC/DOCX) służą jako „uzbrojeni" dostarczyciele.
3. **Dostarczenie** – umieszczenie „broni" w docelowym środowisku. Wykorzystywane są: załączniki do e-maili, strony internetowe i wymienne dyski USB.
4. **Wykorzystanie** – po tym jak exploit został dostarczony do komputera poszkodowanego, jest uruchamiany kod przygotowany przez podmiot atakujący. Zwykle wykorzystuje się podatności systemu

[11] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[12] Dostępnym pod https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/ Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

operacyjnego lub jakiejś aplikacji lub użytkownika zainfekowanego komputera (socjotechnika) albo eskalowanie uprawnień w systemie do uzyskania możliwości samodzielnego wykonania dowolnego kodu.

5. **Instalacja** – instalacja trojana zdalnego dostępu lub tylnego wejścia do systemu (*backdoor*) w systemie komputerowym poszkodowanego, co pozwala podmiotowi atakującemu na trwałą obecność w tym systemie/środowisku i wykonywanie rozłożonych w czasie działań określanych jako APT (Advanced Persistent Threat).
6. **Sterowanie** – z zainfekowanego komputera musi zostać ustanowione połączenie (kanał *Command and Control*; C2) ze znajdującym się (gdzieś) w Internecie serwerem sterującym, ponieważ malware APT bardziej wymaga ręcznego sterowania niż zautomatyzowanych połączeń i działań. Po utworzeniu kanału C2, podmiot atakujący ma pełen dostęp do docelowego środowiska.
7. **Realizacja celów podmiotu atakującego** (akcja na osiągniętym zasobie docelowym) – dopiero po przejściu wszystkich ww. sześciu etapów podmiot atakujący może podjąć działania realizujące jego cele. Zwykle tymi celami są:
   - skryte wyprowadzenie informacji (*exfiltration*) na które składa się zbieranie, odszyfrowywanie i wydobywanie informacji ze środowiska poszkodowanego;
   - naruszenie integralności lub gwarantowanej dostępności zasobów informacyjnych.
   - wykorzystanie przejętego zasobu jako punktu bazowego do dalszych działań w sieci poszkodowanego.

Przykład 2 – **obrona** (za [2]):

Na przykład dla etapu wykorzystania (exploitation):

- hostowy system wykrywania działań intruzów (HIDS) wykrywa pasywnie exploita,
- aktualizacja (patching) przerywa całkowicie działanie exploita;

- system przeciwdziałania nieuprawnionemu wykonywaniu kodu (DEP)[13] przerywa działanie exploita natychmiast po jego uruchomieniu.

***** Koniec przykładów *****

Inne możliwości obrony przed intruzem wskazane w tabeli 1 to tradycyjne systemy wykrywania działań intruzów (*Network Intrusion Detection Systems*; NIDS), kontrola dostępu poprzez listy dostępu zapór sieciowych (*Access Control Lists*; ACL), dobre praktyki utwardzania systemów (w tym zapisy w dziennikach zdarzeń) oraz czujny użytkownik systemu który może wykryć podejrzaną aktywność w systemie.

Generalnie, wielu producentów narzędzi programowych oraz niezależnych organizacji (takich jak ISACA, por. rys. 4) próbuje tworzyć zbiory różnych narzędzi przydatnych do pacyfikowania działań podmiotu atakującego lub wskazać usługi systemowe które w tym celu można wykorzystać[14].

Tab. 1. Etapy działań intruza i możliwości przeciwdziałania (za [2])**.**

OBRONA / ATAK	**Wykrycie** *detect*	**Odmowa** *deny*	**Przerwanie** *disrupt*	**Osłabianie** *degrade*	**Zwodzenie** *deceive*	**Niszczenie** *destroy*
Rozpoznanie *reconnaissance*	Web analytics					
Uzbrojenie *weaponization*	NIDS	NIPS				
Dostarczenie *delivery*	Czujny użytkownik	Proxy filter	In-line AV	Kolejkowanie		
Wykorzystanie *exploitation*	HIDS	Aktualizacje	DEP			
Instalowanie *installation*	HIDS	„chroot" jail[15]	AV			

[13] DEP (*Data Execution Prevention*) jest zabezpieczeniem spotykanym we współczesnych systemach operacyjnych które ma uniemożliwić wykonywanie kodu z segmentu danych. Jest to ochrona przed exploitami wykorzystującymi przepełnienie bufora.

[14] W praktyce będzie to wypełnianie poszczególnych komórek tabeli 1 nazwami odpowiednich produktów (takich jak IDS-y czy zapory sieciowe) lub procesów systemowych.

[15] „Chroot jail" jest sposobem na izolowanie procesów i ich procesów potomnych od reszty systemu. Sposób ten powinien być stosowany tylko do procesów które nie mają uprawnień roota.

Sterowanie *Command&Control*	NIDS	Firewall ACL	NIPS	Tarpit[16]	Przekierowanie DNS	
Realizacja celów intruza *actions on objectives*	Analiza zapisów w dziennikach zdarzeń			Quality of Service	Honeypot	

Cyber Kill Chain Stage Mapping for Passive and Active Tools

Cyber Kill Chain Stage	Goal of Stage	Passive (Detect) Tools	Active Tools	Comment
1. Reconnaissance	To gather information about an attack target	Enable Microsoft Defender Firewall audit *(pfirewall.log)*	Use Microsoft Defender Firewall	Disables (blocks) all unused ports and inbound connections to reduce the attack surface and network recon surface for the attacker. By default, the Microsoft Defender Firewall log is disabled.
			Restrict site permissions in Microsoft Edge	Enables "ask before accessing" or "block" to reduce disclosure of data for the attacker within recon via web.
			Restrict clients allowed to make remote calls to Security Account Manager (SAM)	Reduces enumeration of users and groups in the local Security Account Manager (SAM) database and active directory within internal recon. By default, for "Network access: Restrict clients allowed to make remote calls to SAM," there is not access to check for older operating systems; there is only access to members of BUILTIN\Administrators for newer operating systems.
			Restrict authenticated users allowed to use NetSessionEnum function	Reduces session enumeration where users and service accounts are logged (internal recon). By default, "authenticated users" allows the use of the NetSessionEnum method.
2. Weaponization	To prepare malware or exploit	In practice, cybersecurity specialists often cannot stop actions that occur outside the enterprise IT infrastructure. It is helpful to be aware of malware and exploit trends.		

Źródło: Liderman K.: *Zarządzanie ochroną informacji sterującej w sieciach i systemach przemysłowych*. W: Kosiński J. (red.): *Przestępczość teleinformatyczna 2020*. Rocznik Bezpieczeństwa Morskiego. Str. 41-78. AMW. Gdynia. 2021.

Rysunek. 4. Przykład możliwości zastosowania narzędzi Windows w łańcuchu Kill Chain.

Framework MITRE ATT&CK®

Framework ATT&CK jest powszechnie akceptowaną i ogólnie dostępną bazą wiedzy[17] o taktykach i technikach wykorzystywanych do nieuprawnionych i/lub przestępczych działań przez podmioty grupowe

[16] „Tarpit" jest usługą systemu komputerowego, która celowo opóźnia obsługę przychodzących połączeń.

[17] W literaturze anglojęzycznej jest nazywana jednak *Framework.*

i indywidualne, zbudowaną na podstawie obserwacji rzeczywistego świata. ATT&CK dostarcza szczegółów działania ponad stu podmiotów grupowych (stan na połowę roku 2022), w tym stosowanych przez nie technik i programów[18].

ATT&CK opisuje działania tych podmiotów poprzez stosowane taktyki, techniki i procedury (TTP), które układają się w czteropoziomowy schemat czynności i ich opisów o wzrastającej szczegółowości:

1. **Taktyki** reprezentują „co" (*what*) i „dlaczego" (*why*) poprzez wskazanie podzbiorów technik i subtechnik w ATT&CK. Przekładają się one na techniczne cele podmiotów, przesłanki do wykonania określonych akcji i możliwe akcje.
2. **Techniki** reprezentują „jak" (*how*) − poprzez wykonanie jakich akcji podmioty osiągają założone cele taktyczne.
3. **Subtechniki** dostarczają bardziej szczegółowego opisu technik. Są często związane z określonym systemem operacyjnym lub platformą, przy czym nie wszystkie techniki są rozwijalne do subtechnik.
4. **Procedury** są konkretyzacjami (instancjami) sposobów użycia danych technik lub subtechnik.

ATT&CK jest zorganizowany wokół tzw. „domen technologicznych" tworzących środowisko operacyjne dla (wrogich) podmiotów. Obecnie (rok 2022) dostępne są następujące domeny:

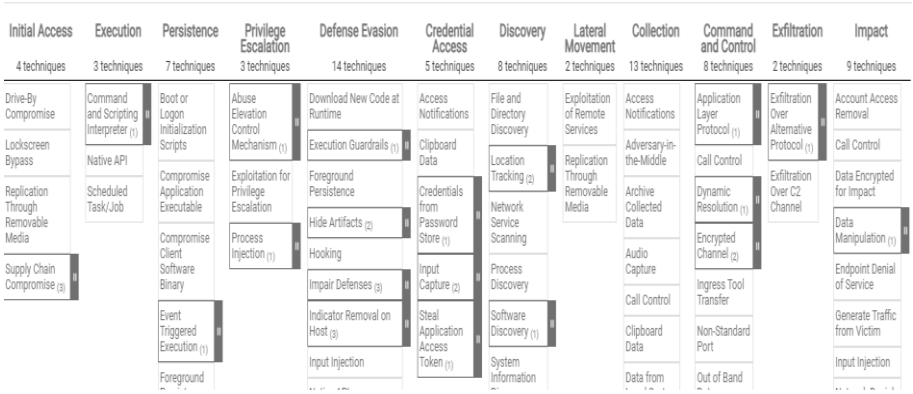
1. MITRE ATT&CK − **Enterprise**:
   - Platform-based: Windows, Linux i MacOS;
   - Cloud Matrix: AWS (Amazon Web Service), GCP (Google Cloud Platform), Azure;
   - Office 365, Azure AD, Software-as-a-Service (SaaS);
   - Network Matrix: Network infrastructure devices.

2. MITRE ATT&CK − **Mobile**: dostarcza opisu taktyk i technik dostępu do platform Androidowych i iOS.

[18] Należy korzystać tylko z oryginalnej strony https://attack.mitre.org – klikanie w linki podane w spisach różnych (np. w [5] w appendix A) często przenosi do stron starych lub nieaktualnych!

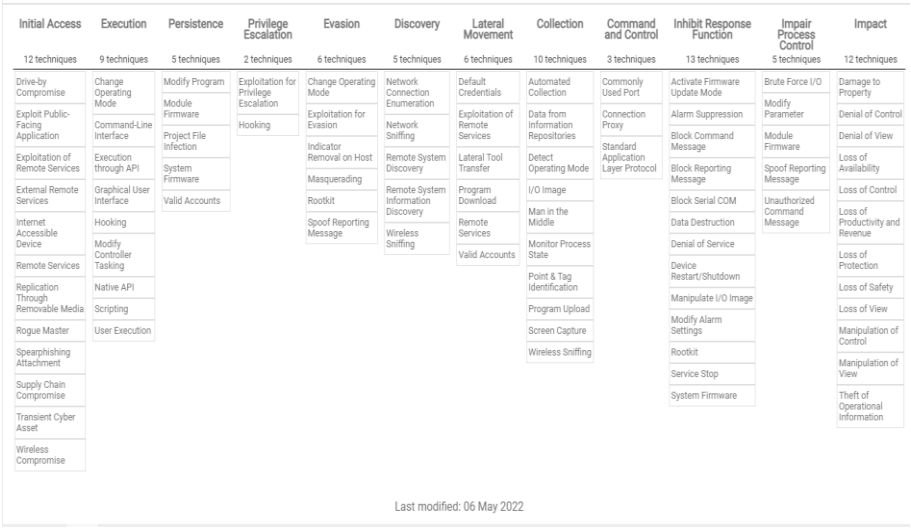
3. MITRE ATT&CK − **Industrial Control Systems** (ICS): dostarcza opisu taktyk i technik których pierwszoplanowym celem jest zakłócenie sterowania procesami przemysłowymi, w tym systemów SCADA (Supervisory Control and Data Acquisition) i konfiguracji innych systemów przemysłowych.

Jak można zauważyć (patrz rys. 5-7), poszczególne domeny różnią się ilością taktyk (Enterprise – 14, Mobile i ICS – 12), ich rodzajami oraz ilościami technik (w ramach taktyki) w zależności od domeny. Tabele 2-4 pokazują rozwinięcie taktyka-technika-procedura dla domeny Enterprise i taktyki TA0008.



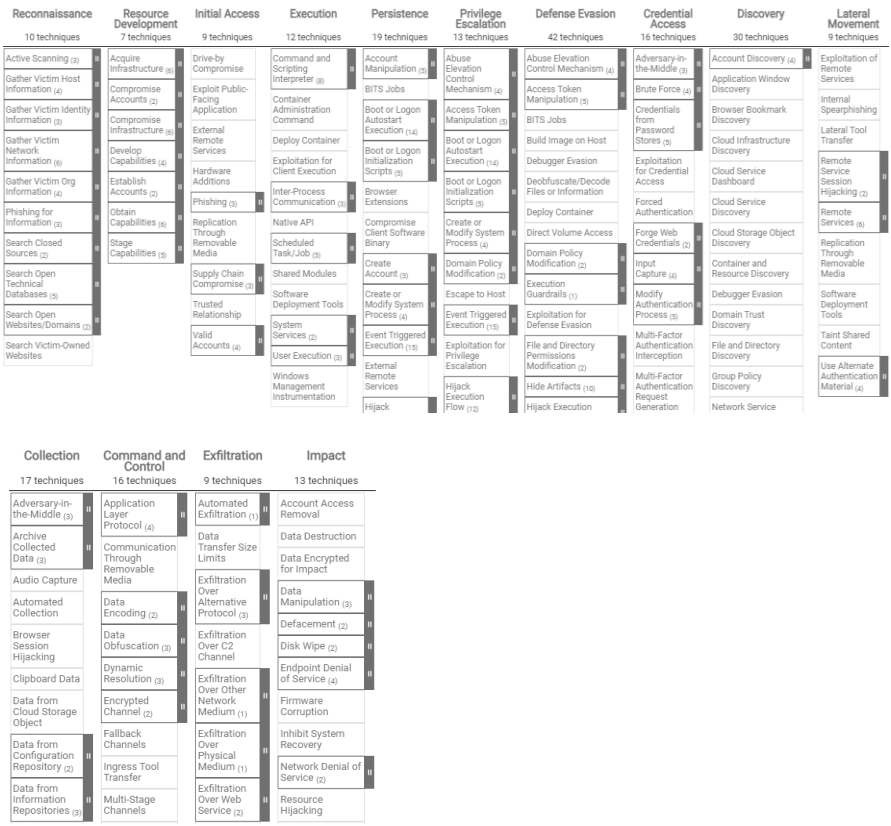
Źródło: ICS matrix; fragment.

Rysunek. 5. Macierz taktyk i technik dla systemów przemysłowych



Źródło: Mobile matrix; fragment.

Rysunek. 6. Macierz taktyk i technik dla systemów mobilnych



Źródło: Enterprise matrix; fragment.

Rysunek. 7. Macierz taktyk i technik dla systemów przedsiębiorstw

Tab. 2. Taktyki dla Enterprise (za https://attack.mitre.org/tactics/enterprise/) – **symbol, nazwa i opis** (tlumaczenie własne).

ID	NAME	DESCRIPTION
TA0043	*Reconnaissance*	Podmiot atakujący zbiera informacje przydatne do planowania przyszłych działań.
TA0042	*Resource Development*	Podmiot atakujący identyfikuje i zbiera zasoby przydatne do wsparcia jego przyszłych działań.
TA0001	*Initial Access*	Podmiot atakujący uzyskuje dostęp do sieci atakowanego podmiotu.
TA0002	*Execution*	Podmiot atakujący uruchamia złośliwy kod u podmiotu atakowanego.
TA0003	*Persistence*	Podmiot atakujący umacnia zdobyty przyczółek w sieci atakowanego podmiotu.
TA0004	*Privilege Escalation*	Podmiot atakujący próbuje uzyskać wyższe uprawnienia do działania w sieci atakowanego podmiotu.
TA0005	*Defense Evasion*	Podmiot atakujący wykonuje działania maskujące, utrudniające wykrycie jego działań ofensywnych w sieci atakowanego podmiotu.
TA0006	*Credential Access*	Podmiot atakujący próbuje wykraść dane uwierzytelniające z sieci atakowanego podmiotu.
TA0007	*Discovery*	Podmiot atakujący próbuje rozpoznać środowisko podmiotu atakowanego.
TA0008	*Lateral Movement*	Podmiot atakujący wykorzystuje w środowisku podmiotu atakowanego techniki z grupy TA0008 umożliwiające mu działania na różnych zasobach sieci atakowanego podmiotu.
TA0009	*Collection*	Podmiot atakujący próbuje zebrać informacje dotyczące założonego celu ataku.
TA0011	*Command and Control*	Podmiot atakujący ustanawia skryty kanał (lub kanały) komunikacyjny z serwerem CC .
TA0010	*Exfiltration*	Podmiot atakujący próbuje wyprowadzić dane z atakowanego systemu.
TA0040	*Impact*	Podmiot atakujący próbuje wykonać manipulacje na danych atakowanego systemu, uszkodzić go lub zniszczyć zasoby informacyjne.

W tabeli 3 pokazano fragment zbioru technik wykorzystywanych w ramach taktyki *Lateral Movement*.

Tab. 3. Techniki dla Enterprise, taktyka: Lateral Movement – symbol, nazwa i opis (fragment tabeli z https://attack.mitre.org/tactics/TA0008/).

ID	Name	Description
T1210	Exploitation of Remote Services	Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.
T1534	Internal Spearphishing	Adversaries may use internal spearphishing to gain access to additional information or exploit other users within the same organization after they already have access to accounts or systems within the environment. Internal spearphishing is multi-staged campaign where an email account is owned either by controlling the user's device with previously installed malware or by compromising the account credentials of the user. Adversaries attempt to take advantage of a trusted internal account to increase the likelihood of tricking the target into falling for the phish attempt.
T1570	Lateral Tool Transfer	Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e. Ingress Tool Transfer) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation. Adversaries may copy files between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over SMB/Windows Admin Shares to connected network shares or with authenticated connections via Remote Desktop Protocol.

W tabeli 4 z kolei, pokazano znane exploity (procedury) wykorzystywane w ramach techniki T1210 (*Exploitation of Remote Services*).

Tab. 4. Przykłady procedur dla: podmiot(*Enterprise*), taktyka(*Lateral Movement*), technika(*T1210*) – symbol, nazwa i opis (fragment tabeli z https://attack.mitre.org/techniques/T1210/).

ID	Name	Description
G0007	APT28	APT28 exploited a Windows SMB Remote Code Execution Vulnerability to conduct lateral movement.[5][6][7]
S0606	Bad Rabbit	Bad Rabbit used the EternalRomance SMB exploit to spread through victim networks.[8]
S0608	Conficker	Conficker exploited the MS08-067 Windows vulnerability for remote code execution through a crafted RPC request.[9]
G0035	Dragonfly	Dragonfly has exploited a Windows Netlogon vulnerability (CVE-2020-1472) to obtain access to Windows Active Directory servers.[10]

Podsumowanie

W [3] oraz [4] przedstawione są poglądy autora niniejszego opracowania na zakres wiedzy który powinien być przekazywany studentom na specjalnościach informatycznych związanych z bezpieczeństwem informacyjnym (cyberbezpieczeństwem) w zakresie systemów przemysłowych. Jednak jedną z podstaw ogólnego wyszkolenia „bezpiecznika" powinna

być znajomość sposobów realizacji celowych zagrożeń[19] dla zasobów informacyjnych oraz znajomość metod i narzędzi umożliwiających skuteczne przeciwdziałanie takim realizacjom.

Jako podstawę proponuje się zapoznanie studentów z rozbudowanym narzędziem informacyjnym (*framework*) MITRE ATT&CK. Narzędzie to jest obecnie podstawą działań w zakresie bezpieczeństwa informacyjnego prowadzonych przez wiele uznanych firm z branży „bezpieczeństwa". Wykorzystanie tego narzędzia powinno się wpisywać w pewien usystematyzowany model ukierunkowany na analizę działań wrogiego podmiotu i możliwości przeciwdziałania. Za taki model proponuje się przyjąć zmodyfikowaną koncepcję firmy IBM opisaną w rozdz. 2. Zalecenia normatywne, które powinny być dla inżyniera podstawowymi elementami ukierunkowującymi jego działania przy projektowaniu, konstrukcji, wdrażaniu i ocenie rozwiązań i produktów oraz tzw. „dobre praktyki" opracowane przez uznane organizacje oraz stosowane i doskonalone w praktyce na całym świecie przez firmy zajmujące się zabezpieczeniem zasobów informacyjnych[20], są kolejnymi, wartymi uwagi „gotowcami" usprawniającymi pracę osób odpowiedzialnych za bezpieczeństwo informacyjne.

Bibliografia

1. Caltagirone S., Pendergast A., Betz Ch.: *The Diamond Model of Intrusion Analysis,* DoD Report, Juli 2013.
2. Hutchins Eric M., Cloppert Michael J., Amin Rohan M.: *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. In L. Armistad, editor, International Conference on Information Warfare and Security, volume 6, pages 113–125. Academic Conferences International, Academic Publishing International Unlimited, 2011.
3. Liderman K.: *Ochrona informacji sterującej w sieciach i systemach przemysłowych – propozycja podstaw edukacyjnych*. Przegląd Teleinformatyczny. Str. 3-30. Nr 8(26) 1-4. WAT. Warszawa. 2020.

[19] Potocznie nazywanych atakami.

[20] Na przykład w zakresie tzw. *Operational Technology* proponuje się zapoznanie studentów z „dobrymi praktykami" dotyczącymi zabezpieczania sieci i systemów przemysłowych, opublikowanymi [8] przez *Bundesamt für Sichercheit in der Informationstechnik*.

4. Liderman K., *Zarządzanie ochroną informacji sterującej w sieciach i systemach przemysłowych*. W: Kosiński J. (red.): Przestępczość teleinformatyczna 2020. Rocznik Bezpieczeństwa Morskiego. Str. 41-78. AMW. Gdynia. 2021.
5. *Best Practices for MITRE ATT&CK® Mapping*, Cybersecurity and Infrastructure Security Agency (CISA), June 2021.
6. *Matching Microsoft Security Tools With the Cyber Kill Chain*, ISACA Journal, vol. 4, 2022.
7. https://www.cisecurity.org/controls/: *Implementation Guide for Industrial Control Systems*, Version 7, CIS Controls™ (dostęp 22.05.2020).
8. *ICS Security Compendium*. V. 1.23. Federal Office for Information Security (BSI). Germany. 2013.
9. https://attack.mitre.org (dostęp 22.09.2022).
10. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (dostęp 26.09.22).
11. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/ cyber/ Gaining_the_Advantage_Cyber_Kill_Chain.pdf (dostęp 26.09.2022).

Krzysztof LIDERMAN

Abstract

INFORMATION RESOURCES PROTECTION AGAINST ATTACKS BY HOSTILE ENTITIES, ORGANIZED ON A BASIS ACKNOWLEDGED FRAMEWORKS, KNOWLEDGE BASE AND STANDARDS − METHODOLOGY OUTLINE

Summary: The contents of this chapter present free of charge acknowledged frameworks, knowledge base and standards used for information resources protection against attacks by hostile entities. The basis of the concept, how utilize this in practice, is IBM's methodology presented in chapter 1. The methodology uses the Diamond Model and the Cyber Kill Chain process. In this paper the MITRE ATT&CK knowledge base of adversary tactics and techniques has been proposed to develop activities under IBM's methodology. All three mentioned elements were also briefly described.

Keywords: information resources protection against attacks, Cyber Kill Chain, Diamond Model, MITRE ATT&CK.

Rozdział 5

Ekstrakcja dowodów z urządzeń IoT z wykorzystaniem metody Chip-off

Michał GMUREK, Sasha SHEREMETOV, Igor LOSKUTOV [1]

STRESZCZENIE: Artykuł opisuje teorię oraz zastosowanie metody odzyskiwana danych Chip-off na podstawie kilku badanych urządzeń IoT, wyposażonych w pamięć NAND Flash. W oparciu o badane urządzenia oraz ich specyfikację, wymienione są korzyści wykorzystania tej metody w praktyce. Omawiane są dane uzyskane z badanych urządzeń oraz możliwości ich potencjalnego wykorzystania w kryminalistyce komputerowej.

SŁOWA KLUCZOWE: Internet of things, IoT, NAND Flash, chip-off, odzyskiwanie danych, kryminalistyka cyfrowa.

Wstęp

Obecnie na rynku konsumenckim dostępnych jest wiele różnego rodzaju urządzeń elektronicznych. Zaliczyć do nich możemy m.in. wyposażenie Smart Home, kamery bezpieczeństwa, wielorakie sensory, inteligentne głośniki, inteligentne zegarki i oczywiście smartfony. Każde z wymienionych urządzeń posiada możliwość przetwarzania, zbierania oraz wymiany danych między innymi urządzaniami za pośrednictwem interfejsów sieciowych oraz protokołów komunikacyjnych. Urządzania tego typu określane są mianem IoT (ang. Internet of things)[1] i bez wątpienia jest to najpopularniejszy rodzaj wykorzystywanych w dzisiejszych czasach urządzeń. Obecnie szacuje się, że na świecie jest ok. 14 miliardów takich urządzeń, a do 2030 roku, ich ilość może oscylować w granicy 30 miliardów[2]. Statystycznie możemy stwierdzić, że obecnie każda osoba na świecie posiada przynajmniej dwa takie urządzenia.

[1] Rusolut sp. z o.o., Warsaw, Poland

Metody odzyskiwania danych Chip-off, zastosowanie oraz zalety

Każde urządzenie elektroniczne ze względu na swoje przeznaczenie może gromadzić różnego rodzaju dane. Dane te są zbierane i zapisywane za pośrednictwem kontrolera/procesora na nośniku pamięci, którym w większości przypadków jest chip pamięci NAND Flash[3]. Dostęp do danych, które zostały zgromadzone w pamięci, poprzez standardowy interfejs, z różnych względów nie zawsze jest możliwy lub nie daje pożądanych rezultatów. Przyczyn może być wiele, począwszy od fizycznego uszkodzenia kontrolera pamięci, płytki PCB, bądź innego komponentu, poprzez logiczne wykasowanie danych oraz metadanych systemu plików, którego następstwem jest brak widocznych danych poprzez standardowy interfejs. W takiej sytuacji jednym z rozwiązań, aby dane wyodrębnić, jest zastosowanie konkretnej metody odzyskiwania danych z nośników Flash – Chip-off.

Metoda Chip-off opiera się na wylutowaniu kości pamięci oraz wyczytaniu jej zawartości, czyli tzw. obrazu fizycznego. Uzyskany w ten sposób obraz należy następnie poddać fizycznej rekonstrukcji, czyli odwrócić operację oraz algorytm, według którego kontroler zapisywał dane do pamięci. Następnym krokiem jest odtworzenie logicznego porządku bloków z zapisanymi danymi oraz odbudowa obrazu logicznego wraz z systemem plików.

Rys. 1. Procedura odzyskiwania danych metodą Chip-off

Zastosowanie metody Chip-off niesie za sobą wiele korzyści, nie tylko w odniesieniu do urządzeń IoT, ale także względem standardowych nośników danych, takich jak: karty microSD, SD, CF, pendrive oraz niektórych

modeli dysków SSD, które nie wykorzystują szyfrowania sprzętowego. Do głównych zalet możemy zaliczyć:

- Brak ryzyka nadpisania już zapisanych danych na nośniku pamięci.
- W przypadku niektórych urządzeń, dostęp do wszystkich danych zapisanych na urządzeniu.
- Dostęp do danych chronionych hasłem przez Kontroler.
- Możliwość odzyskania danych z uszkodzonych urządzeń.
- Dostęp do logicznie usuniętych danych poprzez standardowy interfejs np.: USB, eMMC[4].

Wbudowane systemy pików urządzeń IoT wykorzystujących pamięć NAND Flash

Ze względu na charakterystykę oraz właściwości pamięci NAND, aby dane mogły być bezpiecznie przechowywane bez ryzyka ich utraty lub uszkodzenia, niezbędne jest odpowiednie nimi zarządzanie. Dlatego też, każde urządzenie, które pracuje z pamięcią NAND musi wypełniać podstawowe funkcje[5][6], takie jak:

- Wear-Leveling, czyli optymalizacja zużycia bloków pamięci NAND.
- Operacje odświeżania bloków z zapisanymi danymi.
- Translacja fizycznej formy zapisanych danych do postaci obrazu logicznego.

W przypadku standardowych nośników danych, takich jak np: dyski SSD, wszystkie wymienione funkcje są wykonywane przez kontroler według jego wewnętrznego oprogramowania(firmware), natomiast zarządzanie plikami oraz ich metadanymi odbywa się za pośrednictwem osobnego systemu plików np.: NTFS, exFAT, FAT32, EXT4.

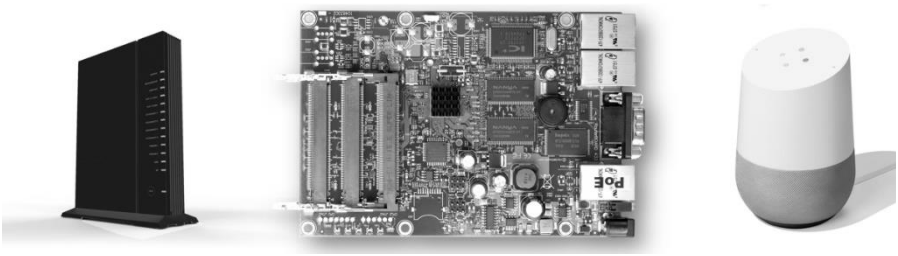
Urządzenia IoT pod tym względem różnią się od standardowych nośników danych, gdyż większość z nich charakteryzuje się raczej niską pojemnością, ze względu na typ przechowywanych danych. W rezultacie, w tych urządzeniach często wykorzystywane są niestandardowe tzw.: fizyczne/wbudowane systemy plików(Embedded File System) które odpowiadają za zarządzenie pamięcią NAND oraz samymi danymi, tak jak to ma miejsce w przypadku osobnego systemu plików. Przykładami takich systemów są m.in.: YAFFS[7], UBI FS, NAND FS oraz RAW File system.

Ze względu na specyfikę niektórych fizycznych systemów pliku, takich jak chociażby YAFFS2, dane które zostały usunięte bądź zmienione przez oprogramowanie lub użytkownika, nie będą wymazywane fizycznie z nośnika pamięci. Jedynym przypadkiem fizycznego „usunięcia" przestarzałych danych, jest nadpisanie ich nowymi danymi przez kontroler. W praktyce przekłada się to w znacznym stopniu na możliwości analizy kryminalistycznej, gdyż poprzez fizyczny dostęp do pamięci NAND jesteśmy w stanie prześledzić wszystkie dane, które zostały tam zapisane. Oznacza to, że jeżeli dane nie zostały nadpisane przez kontroler, będziemy mieć do nich dostęp i możliwość przeanalizowania ich zawartości.

Badane urządzenia

Podstawą do rozważań oraz potencjalnych możliwości wykorzystania danych pochodzących z urządzeń IoT w kryminalistyce, będą stanowić trzy badane urządzenia. Tymi urządzeniami są odpowiednio:

- Router Calix 844E-1
- Router Mikrotik RB433GL
- Głośnik Google Home Speaker



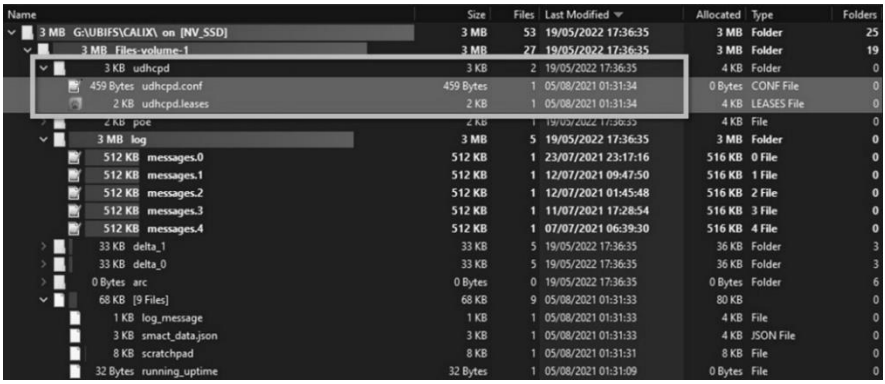
Zdj. 1. Badane urządzenia

Calix 844E-1

Jak w każdym przypadku, aby możliwa była wymiana pakietów sieciowych pomiędzy kilkoma urządzaniami niezbędne jest urządzenie, które umożliwia taka wymianę. W odniesieniu do sieci domowych w większości przypadków będą to routery.

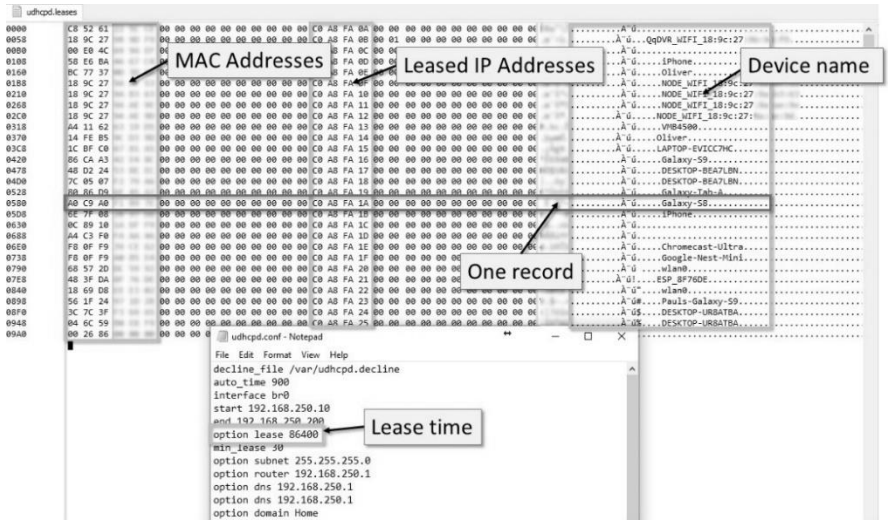
Pierwszym omawianym urządzeniem będzie router wykorzystywany właśnie w takiej sieci, Calix 844E-1. Celem analizy urządzania było wydobycie listy urządzeń, które były podłączone do sieci routera w ostatnim czasie. Taką listę można zazwyczaj pobrać bezpośrednio z oprogramowania sieciowego routera, natomiast w tym przypadku hasło dostępowe było nieznane. Stanowiło to jedną z przyczyn, która zadecydowała o wyborze metody Chip-off, do odzyskania szukanych danych.

Urządzenie zostało rozmontowane, a następnie chip pamięci NAND zlokalizowany i wylutowany z PCB. Urządzanie korzystało z popularnego typu pamięci TSOP48[3] o pojemności 256MB. Zawartość chipu została wyczytania i po wstępnej analizie okazało się, że urządzenie korzystało z fizycznego systemu plików UBI FS. W kolejnym kroku, bazując na strukturach systemu plików, udało się odbudować pełny obraz logiczny z routera.



Zdj. 2. Obraz systemu plików UBI FS, routera CALIX 844E-1

Znajdowało się tutaj wiele plików odpowiadających za parametry oraz oprogramowanie samego routera. Oprócz logów i ustawień, dostępny był także folder programu uDHCP który przydziela lokalne adresy IP urządzeniom podłączonym do sieci routera. Folder zawierał dwa pliki **conf** oraz **leases.** Po krótkiej analizie w celu zrozumienia struktury binarnej pliku, uzyskano wszystkie niezbędne informacje.



Zdj. 3. Zawartość wyodrębnionych plików conf oraz leases

Plik **leases** zawierał szczegółowe dane o urządzeniach, które łączyły się z siecią routera, takie jak: Adres fizyczny MAC, Wynajęty adres IP oraz nazwę samego urządzenia. Dodatkowo w pliku **conf** określony był okres, wynoszący 24 godziny, przez który konkretnemu urządzeniu przydzielany był adres IP. Dodatkowo z systemu plików UBI FS posiadaliśmy informację o dacie modyfikacji ww. plików. Łącząc te wszystkie dane w całość możemy dojść do konkluzji, że urządzenia wymienione w pliku **leases** łączyły się z siecią routera w ciągu 24 Godzin, licząc wstecz od daty modyfikacji tego pliku.

Mikrotik RB433GL

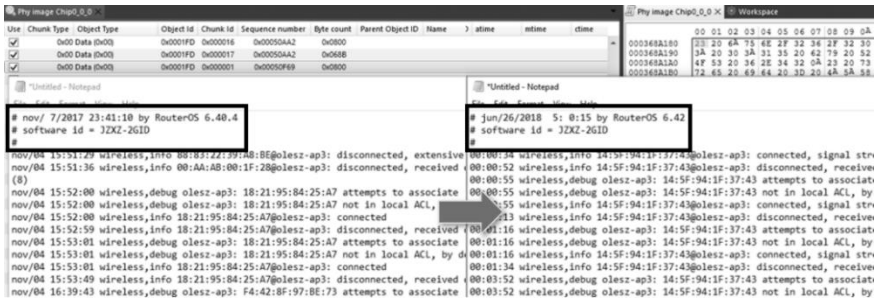
Statystycznie średnia długość użytkowania telefonu komórkowego wynosi 2 lata, po tym okresie zazwyczaj kupujemy nowe urządzenie, a stare jest odsprzedawane, utylizowane bądź nie nadaje się do ponownego użycia. Podobna sytuacja dotyczy także innej elektroniki codziennego użytku, jak i również kolejnego urządzenia, które zostanie omówione.

Router Mikrotik RB433GL został zakupiony na aukcji internetowej jako uszkodzony. Rzeczywiście, w pierwszej chwili nie udało się go uruchomić, natomiast po kilku drobnych naprawach udało się uzyskać dostęp do

oprogramowania sieciowego urządzenia. Router został przywrócony do ustawień fabrycznych i nie było na nim żądanych danych, które można by powiązać z poprzednim właścicielem.

Po wyczytaniu zawartości chipu pamięci, na którym router zapisywał dane oraz wstępnej rekonstrukcji, okazało się, że urządzenie pracuje na fizycznym systemie plików YAFFS2. Pod kątem analizy fizycznej zawartości pamięci NAND, ten system plików daje bardzo szerokie możliwości. Każda fizyczna strona w pamięci NAND jest dokładnie opisana za pomocą kilku struktur systemu plików, które są alokowane w obszarze serwisowym kontrolera. Na ich podstawie istnieje możliwość prześledzenia dokładnej historii modyfikacji konkretnych plików, które były zapisywane na urządzeniu.

Z urządzenia udało się wyodrębnić wiele danych, jednak jednym z istotniejszych oraz potencjalnie możliwym do praktycznego wykorzystania podczas dochodzenia był plik **Oleszna_ap3_ap4.log.txt.** Plik zawierał logi systemowe routera, informacje o zdarzeniach z wyszczególnionym dokładnym czasem wystąpienia oraz adres fizyczny MAC urządzenia, którego zdarzenie dotyczyło. Ten plik posiadał wiele wersji z różnych przedziałów czasowych. W sumie udało się wyodrębnić całą jego historię z okresu od **07.11.2017** do **26.08.18**.



Zdj. 4. Zawartość pliku Oleszna_ap3_ap4.log.txt z okresu 07.11.17 i 26.08.18.

Dzięki specyfice systemu plików YAFFS2, który nie wymazuje bloków zawierających przestarzałe dane (może je tylko nadpisać) oraz typowi danych zapisywanych przez router, które nie mają dużego rozmiaru, co w praktyce nie spowodowało nadpisania starych danych. Uzyskane dane zlokalizowane na chipie NAND prawdopodobnie pochodziły z całego okresu pracy routera.

Google Home Speaker

Inteligentne głośniki to całkiem powszechnie wykorzystywane urządzenia domowe ze względu na prostotę oraz wygodę użytkowania. W dużej mierze wykorzystywane są do sterowania innym wyposażeniem Smart Home w obrębie sieci domowej. W tym rozdziale przyjrzymy się jakie dane potencjalnie możliwe do wykorzystania taki głośnik może zawierać.

Omawiany Google Speaker, podobnie jak poprzednie urządzenie również pochodzi z aukcji internetowej. W tym przypadku urządzenie korzystało z niestandardowego chipu pamięci NAND, BGA68. Po wyczytaniu zawartości pamięci okazało się, że wykorzystywany system do zarządzania plikami i pamięcią NAND, to również YAFFS w wersji 2.

Uzyskane dane z pamięci NAND w dużej mierze miały charakter systemowy. Były to pliki takie jak parametry, konfiguracje, logi oraz certyfikaty.

Zdj. 5. Przykłady wyodrębnionych plików Google Speakera, z systemu pików YAFFS2

Odzyskanych zostało również kilka plików o charakterze personalnym lub mogącym pomóc zidentyfikować konkretne urządzenie. Do takich plików zaliczymy m.in.:

- Settings
- Metrics_client_ID
- Mac_address
- Client.crt
- Client.crt.gen2

W pliku Settings, można było znaleźć dane o lokalizacji geograficznej, najprawdopodobniej samego głośnika. Metrics_client_ID zawierał identyfikator użytkownika Google, który potencjalnie może zostać wykorzystany do identyfikacji powiązanego konta Google lub danych pochodzących od konkretnego użytkownika. Kolejnym plikiem jest mac_address z adresem fizyczny karty sieciowej głośnika, który może się okazać pomocny w przypadku posiadania danych z routera, do którego sieci był podłączony głośnik. Dodatkowo w plikach Client.crt dostępne były certyfikaty SSL, które służą do szyfrowania komunikacji pomiędzy konkretnym urządzeniem i głośnikiem. W przypadku gdy próbka takowej komunikacja została wcześniej podsłuchana, istnieje możliwość jej odszyfrowania i odczytania.

Wykorzystanie danych pochodzących z takiego głośnika, w zależności od przypadku, może okazać się bardzo korzystne z perspektywy kryminalistyki, gdyż musimy pamiętać, że system plików wykorzystywany przez urządzenie to YAFFS2. Dzięki specyfice tego systemu, będziemy mogli prześledzić historię modyfikacji konkretnego pliku np.: settings, zawierającego dane o pozycji geograficznej. W związku z czym możliwe będzie ustalenie lokalizacji głośnika na przestrzeni jakiegoś czasu, bądź nawet od początku jego funkcjonowania.

Podsumowanie

Szeroko wykorzystywane obecnie urządzenia IoT stawiają przed nami całkiem nowe możliwości. Rosnąca z roku na rok moc obliczeniowa oraz pojemność sprawią, że w przyszłości tego typu urządzenia będą gromadzić jeszcze więcej danych, które będzie można potencjalnie wykorzystać podczas dochodzeń kryminalistycznych. Omówione w niniejszym artykule urządzenia oraz wykorzystanie metody chip-off do ich analizy, udowodniło jak wiele danych tego typu urządzenia mogą przechowywać. Ze względu na wykorzystywane systemy plików, możliwe było prześledzenie historii modyfikacji konkretnych plików oraz ustalenie dokładnego czasu, kiedy modyfikacje następowały. Biorąc pod uwagę także specyfikę zarządzania blokami danych przez niektóre z tych systemów, przestarzałe dane nie są wymazywane fizycznie przez kontroler, a jedynie mogą zostać nadpisane nowymi. Z tego powodu uzyskane dane bezpośrednio z chipów pamięci mogły pochodzić z nawet całego okresu funkcjonowania urządzeń, gdyż typ zapisywanych danych nie zajmował dużej przestrzeni w pamięci NAND. W praktyce oznacza to, że aby kontroler wypełnił pamięć i zaczął nadpisywać stare dane, potrzeba nawet kilku miesięcy działania.

Bibliografia

1. Samuel Greengard, The Internet of Things
2. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030 https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide
3. Open NAND Flash Interface (ONFI) Specifiation https://www.onfi.org/specifications
4. A. Fukami, S. Sheremetov, F. Regazzoni, Z. Geradts and C. De Laat, "Experimental Evaluation of e.MMC Data Recovery," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2074-2083, 2022, doi: 10.1109/TIFS.2022.3176187.
5. Yixin Luo, Yu Cai, Saugata Ghose, Jongmoo Choi, Onur Mutlu, Improving NAND Flash Memory Lifetime with Write-hotness Aware Retention Management https://ieeexplore.ieee.org/document/7208284
6. A. Fukami, S. Ghose, Y.Luo, Y. Cai, O.Mutlu “Improving the reliability of chip-off forensic analysis of NAND flash memory devices”, in Przestepczosc Teleinformatyczna 2018, ISSN 1898-3189
7. Aleph One Ltd, Charles Manning, Yaffs 2 Specification https://yaffs.net/yaffs-2-specification
8. D. Pawlaszczyk, J. Friese, C. Hummert, “"Alexa, tell me …" - A forensic examination of the Amazon Echo Dot 3 rd Generation,” International Journal of Computer Sciences and Engineering, Vol.7, Issue.11, pp.20-29, 2019.

Abstract

CHIP OFF EVIDENCE EXTRACTION FROM IOT DEVICES

Summary: This article describes theory and usage of chip-off data recovery method based on a few examined IoT devices, equipped with NAND flash memories. Based on examined devices and their specification, listed are benefits of usage of this method in practise. Data extracted from these devices is discussed and possibility of their potential usage in computer forensics is determined.

Keywords: Internet of things, IoT, NAND Flash, chip-off, data recovery, digital forensics.

Rozdział 6

Trendy występujące na rynku kryptoaktywów

Jacek CHARATYNOWICZ[1]

STRESZCZENIE: W rozdziale przedstawiono zidentyfikowane trendy występujące na rynku kryptoaktywów, które mogą mieć znaczenie dla budowania strategii bezpieczeństwa finansowego oraz formułowania odpowiednich zadań dla instytucji i służb państwowych w zakresie przeciwdziałania zagrożeniom

SŁOWA Kluczowe: kryptoaktywa, trendy na rynku kryptoaktywów, bezpieczeństwo finansowe

Wstęp

Rynek kryptoaktywów podlega zmianom i przeobrażeniom zarówno o charakterze wewnętrznym, jak i zewnętrznym. Wewnętrzne procesy związane są z rozwojem technologicznym i infrastrukturalnym tego systemu, powstawaniu nowych projektów o charakterze użytkowym, płatniczym czy inwestycyjnym. Kryptoaktywa, to już nie tylko kryptowaluty, ale też tokeny (wymienialne i niewymienialne), rozwój tzw. Initial Coin Offering (ICO), Initial Token Offering (ITO), jak również giełd/kantorów kryptowalutowych, czy firm pożyczkowych i powierniczych. Natomiast w ujęciu zewnętrznym sektor ten ulega przemianom prawnym, ekonomicznym i technologicznym, które uwarunkowane są koniunkturą występującą w otoczeniu obszaru kryptoaktywów, czyli polityczną sytuacją międzynarodową, tendencjami na rynku finansowym i w gospodarce, presją regulacyjną czy też stroną psychologiczno-behawioralną uczestników tego obszaru aktywności człowieka.

W związku z tym, w branży kryptoaktywów można wyróżnić już pewne trendy charakterystyczne dla tej technologii. Trend, zgodnie z internetowym słownikiem języka polskiego[2], to istniejący w danym momencie kierunek rozwoju w jakiejś dziedzinie. Pewne powtarzające się procesy,

---

[1] Dr, j.charatynowicz@gmail.com, ORCID: 0000-0003-0484-4078.

[2] https://sjp.pwn.pl/sjp/trend;2578635.html (dostęp: 14.09.2022).

zmieniające się wartości kryptoaktywów w określonym czasie, rozwój biznesu, związane z czynnikami zewnętrznymi jak i wewnętrznymi, które mogą mieć istotne znaczenie z punktu widzenia tego rynku.

W rozumieniu nauk ekonomicznych trend stanowi przejaw długookresowej zmiany, w górę lub w dół, jakieś zmiennej ekonomicznej[3]. Natomiast w naukach o bezpieczeństwie trendy to tendencje, kierunki zmian mające wpływ na środowisko bezpieczeństwa, ich identyfikowanie, analizowanie ma istotne znaczenie z punktu widzenia budowania strategii bezpieczeństwa finansowego państwa.

Przedmiotem niniejszego artykułu jest przedstawienie trendów występujących na rynku kryptoaktywów uwzględniając uwarunkowania prawne i otoczenie regulacyjne, przenikanie do systemów transakcyjnych, czy też rozwój przestępczości w obszarze kryptoaktywów. Ponadto, przedmiotem opracowania będą niedające się przewidzieć zdarzenia, tendencje, procesy, które mogą mieć znaczenie dla perspektyw rozwoju rynku kryptoaktywów (czarne łabędzie).

W przedmiotowym artykule wykorzystano metodę analizy i syntezy dostępnego piśmiennictwa, metodę przypadków, wykorzystywaną w obserwacji rynku kryptoaktywów, ich otoczenia prawnego, ekonomicznego i perspektyw regulacyjnych kryptoaktywów.

Wzrost zainteresowania kryptoaktywami

Od początku funkcjonowania rynku kryptoaktywów, z uwagi na innowacyjny charakter rozwiązań transakcyjnych, wykorzystanie w wielu modelach biznesowych oraz związany z tym potencjał inwestycyjny, budził on zainteresowanie polskich uczestników rynku. Aktualnie na terenie RP funkcjonuje co najmniej 224 bitomatów[4] (na dzień 22 września 2022 r. – 204, 3 marca 2022 r. - 105, w 2020 r. - 67). Dynamika wzrostu tych urządzeń wskazuje, że przybywa osób, które są zainteresowane szybką wymianą kryptowalut, np. na gotówkę (pomimo wysokich prowizji od takich transakcji).

---

[3] D.R. Kamerschen, R.B. McKenzie, C. Nardinelli, *Ekonomia*, Wyd. Fundacja Gospodarcza NSZZ Solidarność, 1991, s. 152.

[4] https://coinatmradar.com/bitcoin-atm-near-me/ (dostęp: 28.01.2023).

W jednym bitomacie można także dokonywać kupna / sprzedaży poszczególnych rodzajów kryptowalut[5].

Warto również dodać, iż wraz z rozwojem bitomatów rośnie również kapitalizacja i dochody branży zajmującej się rozwojem tego segmentu działalności gospodarczej, tj. produkcji urządzeń związanych z rynkiem kryptowalut, budowanie bezpiecznych aplikacji wiążących rynek FIAT z kryptowalutami, urządzeń i aplikacji służących do przechowywania kryptowalut, w tym np. podmiotów z sektora FinTech, które do działalności w zakresie usług płatniczych, money transfer łączą również segment kryptowalut.

Należy tu postawić pewne zastrzeżenie - sytuacja geopolityczna oraz zakłócenia w dostawach towarów, w tym surowców energetycznych związane z agresją zbrojną Federacji Rosyjskiej na Ukrainę i powiązany z tym kryzys energetyczny, surowcowy i finansowy, implikuje również zmiany na rynku kryptoaktywów. Nie tylko związane z posiadanymi zasobami, aktywami, które lokowane są w obszarach mało ryzykownych (np. rynek nieruchomości), ale również kwestią psychologiczną, związaną z zaufaniem do rynku.

Z uwagi na zdecentralizowany charakter obrotu kryptowalutami nie jest możliwe szczegółowe opisanie wartości transakcji realizowanych w kryptowalutach, w tym zakresie można zaprezentować dane szacunkowe. Z przeprowadzonych przez Narodowy Bank Polski w 2020 r. badań, pt. *Zwyczaje płatnicze w Polsce w 2020 r.* wynika, że ta metoda płatności wykorzystywana była przez respondentów w trakcie ostatnich 12 miesięcy sporadycznie - tylko przez 0,2 % badanych. Najwięcej transakcji zostało zrealizowanych gotówkowo (97,9 %) – przy czym nie można wykluczyć, iż w tym przypadku również miały one związek z kryptowalutami.

Branża kryptoaktywów nieustanie się rozwija - zwiększa się ilość kryptoaktywów, indywidualnych i instytucjonalnych uczestników obrotu, rodzaj świadczonych usług oraz kapitalizacja rynku. Szacuje się, że obecnie około 1 mld ludności na świecie korzysta z giełd kryptowalut, ponad 300 mln posiada kryptowaluty, w tym Bitcoin i Ethereum oraz istnieje ponad 18 000 firm, które akceptują kryptowaluty jako zapłatę za swój produkt lub usługę[6].

Z danych firmy Chainalysis wynika, że Polacy w 2020 r. zarobili na handlu bitcoinami ponad 200 mln USD. Plasowało to krajowych uczestników

---

[5] Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2021 roku, s. 34-35.

[6] https://earthweb.com/cryptocurrency-statistics/ (dostęp: 01.02.2023 r.).

rynku na 21 miejscu na świecie, tuż za Australią oraz Indiami. W kontekście osiąganych na tym rynku zysków to lepszy wynik osiągnęli mieszkańcy Czech, którzy uzyskali w tym okresie 281 mln USD oraz mieszkańcy Ukrainy z wynikiem wynoszącym około 400 mln USD. Największy dochód osiągnęli w 2020 r. Amerykanie – aż 4,1 mld USD, na drugim miejscu znaleźli się Chińczycy z zyskiem wynoszącym 1,1 mld USD, na trzecim Japończycy z ok. 900 mln USD[7].

Z raportu Chainalysys „The 2022 Geography of Cryptocurrency Report" wynika, że w okresie między lipcem 2021 a czerwcem 2022 r., do czterech największych rynków kryptoaktywów należały:

1. Europa – wartość transakcji 1,3 bln USD;
2. Ameryka Północna – wartość transakcji 1,15 bln USD;
3. Centralna i Południowa Azja – wartość transakcji 932 mld USD;
4. Południowa Azja – wartość transakcji 777,5 mld USD.

Polska w tym badaniu osiągnęła wartość transakcji ok. 75 mld USD. Europa jest największą na świecie gospodarką kryptograficzną[8]. Użytkownicy i instytucje w całym regionie w okresie od lipca 2021 r. do czerwca 2022 r. otrzymały kryptowalutę o wartości 1,3 biliona USD, a ponadto w Europie Zachodniej, uwzględniając takie czynniki jak: wartość transakcji usług zcentralizowanych, transakcje typu P2P czy transakcje DeFi, występuje sześciu z czterdziestu największych użytkowników kryptowalut: Wielka Brytania, Niemcy, Francja, Hiszpania, Portugalia i Holandia.

Impulsem do takiego rozwoju rynku, były kwestie związane z atrakcyjnym i wciąż innowacyjnym charakterem projektu kryptoaktywów, decentralizacją i anonimowością, zapewnieniem cyberbezpieczeństwa giełd/kantorów kryptowalutowych, doświadczenia uczestników rynku oraz regulacje prawne, które w następstwie podnosiły bezpieczeństwo obrotu i zaufanie do tego projektu.

Rynek kryptowalut staje się obszarem w coraz większym stopniu regulowanym, w różnych aspektach jego funkcjonowania. W rejestrze działalności prowadzonym w zakresie walut wirtualnych przez Izbę Administracji Skarbowej w Katowicach, na 23 maja 2022 r. figurowało 313 podmiotów, na-

[7] https://bomega.pl/polacy-zarobili-ponad-200-mln-usd-na-bitcoinach/ (dostęp 29.01.2023).

[8] W inny sposób przedstawione dane stawiałyby rynek azjatycki jako największy rynek kryptoaktywów z wartością transakcji ok. 1,7 bln USD.

tomiast na 25 stycznia 2023 r. już 610, w różnych formach prowadzenia działalności gospodarczej: zarejestrowanej w CEIDG, spółki z ograniczoną odpowiedzialnością czy prostej spółki akcyjnej.

Dostępne dane wskazują, iż pomimo wątpliwości co do statusu prawnego kryptowalut, skomplikowanej infrastruktury tego systemu, czy ostrzeżeniach publicznych instytucji państwowych w kontekście identyfikowanych ryzyk związanych z obrotem, cieszą się one rosnącą popularnością, przede wszystkim jako instrument o charakterze płatniczym i inwestycyjnym. Świadczy o tym wzrost wartości najpopularniejszej z kryptowalut - Bitcoina, która po spadkach ceny spowodowanej m. in. agresją FR na Ukrainę, upadłości firm związanych z cyfrowymi aktywami, powrócił do tendencji wzrostu jego wartości.

Trend regulacyjny

Już od początku funkcjonowania rynku kryptowalut powstało pytanie, czy w kontekście jego regulacji należy adoptować funkcjonujące przepisy prawne do tego innowacyjnego projektu, czy też, celem precyzyjnego opisania prawnych aspektów problematyki tych aktywów, tworzyć nowe, ustanowić ramy prawne działalności, regulatora i nadzór nad tym rynkiem. W przypadku polskiego systemu prawnego obserwujemy system mieszany, tj. w niektórych obszarach interpretuje się przepisy prawne i odnosi do rynku kryptowalut, np. w kontekście uznania kryptowalut za prawo o charakterze majątkowym, z puntu widzenia prawa cywilnego, czy też jako znak legitymacyjny w kontekście możliwości emisji tokenów.
Natomiast w innych obszarach, jak np. przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu, usługi płatnicze, tworzy się rozwiązania nowe, niejednokrotnie implementując rozwiązania europejskie.

Niezależnie od powyższych rozważań trend regulacyjny można obserwować od początku funkcjonowania tych walut, w różnych aspektach jego oddziaływania, prawa cywilnego, podatkowego, w kontekście przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, czy też usług płatniczych.

Fundamentalną kwestią jest, iż kryptowaluty, na gruncie ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu zostały ujęte w katalogu wartości majątkowych, przez które rozumie się prawa majątkowe lub inne mienie ruchome lub nieruchomości, środki płatnicze, instrumenty finansowe w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, inne papiery wartościowe, wartości

dewizowe oraz waluty wirtualne[9]. Ponadto zdefiniowano, że „rachunek wirtualnej waluty to prowadzony w formie elektronicznej zbiór danych identyfikacyjnych zapewniających osobom uprawnionym możliwość korzystania z jednostek walut wirtualnych, w tym przeprowadzania transakcji ich wymiany[10]". Natomiast poprzez transakcję rozumie się „czynność prawną lub faktyczną, na podstawie, której dokonuje się przeniesienia własności lub posiadania wartości majątkowych, lub czynność prawną lub faktyczną dokonywaną w celu przeniesienia własności lub posiadania wartości majątkowych.[11]" W wyniku nowelizacji ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[12], weszły w życie kolejne rozwiązania w obszarze rynku kryptowalut, tj. w przypadku świadczenia usług w zakresie obrotu lub wymiany między kryptowalutami a walutą fiducjarną, jest ono traktowane jako działalność regulowana. W związku z tym wprowadzono obowiązek dokonania wpisu do rejestru walut wirtualnych prowadzonego przez ministra właściwego do spraw finansów publicznych. Natomiast brak spełnienia tego wymogu grozi karą administracyjną o wysokości do 100 000 zł. Zgodnie z nowymi przepisami powyższa działalność może być wykonywana jedynie przez osoby fizyczne, które nie zostały prawomocnie skazane za umyślne przestępstwo: przeciwko działalności instytucji państwowych oraz samorządu terytorialnego, przeciwko wymiarowi sprawiedliwości, wiarygodności dokumentów, mieniu, obrotowi gospodarczemu czy interesom majątkowym i obrotowi pieniędzmi, a także osoby prawne bądź jednostki organizacyjne, w których wspólnicy nie zostali prawomocnie skazani na zasadach określonych powyżej w stosunku do osób fizycznych lub za przestępstwo skarbowe.

Ostatnim kierunkiem regulacyjnym jest stworzenie ram organizacyjnych dla możliwości zamrażania aktywów osób objętych sankcjami, w związku z agresją zbrojną Federacji Rosyjskiej na Ukrainę. Uwzględniając zyskujące na znaczeniu alternatywne instrumenty transferu środków pieniężnych i wartości majątkowych, ustalono, że rynek kryptowalut, z uwagi na nieuregulowany charakter, może być dogodnym miejscem do ukrywania

[9] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 poz. 593, ze zm.) art. 2 ust. 2 pkt 27.
[10] Tamże, art. art. 2 ust. 2 pkt 17e.
[11] Tamże, art. 2 ust. 2 pkt 21.
[12] Ustawa o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw Dz.U. z 2021 r. poz. 815.

i przenoszenia aktywów przez obywateli FR objętych sankcjami[13]. W celu przeciwdziałania potencjalnego omijania sankcji, 14 kwietnia 2022 r. Komisja Nadzoru Finansowego podjęła uchwałę nr 111/22 w sprawie okoliczności istotnych dla oceny rękojmi w sprawach z zakresu rynku finansowego w związku z agresją Federacji Rosyjskiej wobec Ukrainy. W przedmiotowej uchwale „rękojmia" oznacza gwarancję, zapewnienie o czymś, a więc obiektywny brak niedających się usunąć wątpliwości co do zaistnienia w przyszłości określonego stanu. Oznacza to, iż odnośnie podmiotu licencjonowanego, a także jego znaczących udziałowców oraz osób nim zarządzających – jako wywierających kluczowy wpływ na działalność tego podmiotu – nie mogą zachodzić jakiekolwiek niedające się usunąć wątpliwości, że działalność ta będzie prowadzona w sposób prawidłowy – praworządny, uczciwy, transparentny, ostrożny i stabilny.

Ponadto, 10 czerwca 2022 r. Komisja Nadzoru Finansowego opublikowała Komunikat dotyczący sankcji i stosowania przepisów ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, w przypadku współpracy z podmiotami branży walut wirtualnych. KNF „oczekuje od podmiotów nadzorowanych zachowania najwyższej staranności oraz ostrożności przy podejmowaniu i kontynuowaniu współpracy z podmiotami branży walut wirtualnych lub dostawcami usług płatniczych czy innych usług finansowych dla takich podmiotów, zwłaszcza w związku z wypełnianiem obowiązków wynikających z przepisów ustawy. Przede wszystkim w zakresie właściwego stosowania przez instytucje obowiązane wzmożonych środków bezpieczeństwa finansowego, w tym gruntowne monitorowanie stosunków gospodarczych z klientami oraz wzmożoną czujność w zakresie bieżącej analizy transakcji przez nich realizowanych, również na rzecz innych dostawców usług finansowych (w tym także nadzorowanych) i ich klientów[14]".

---

[13] Zgodnie z artykułem K. Rębisza, *Bitcoin nowym Rublem*, opublikowanym w gazecie Parkiet - FBI i prokuratura złożyły do sadu oskarżenie przeciwko obywatelowi USA o używanie kryptowalut do obchodzenia sankcji. Niewymieniony z nazwiska oskarżony miał przekazać 10 mln dol. w Bitcoinach na Kubę, do Iranu, Korei Północnej, Syrii lub do Rosji. Rosjanie są jednymi z największych posiadaczy kryptowalut na świecie. Według Bloomberga, powołującego się na źródła pochodzące z ministerstwa finansów Rosji, aż 12 proc. wszystkich światowych zasobów kryptowalut znajduje się w ich rękach. Daje to więc zawrotną liczbę blisko 240 mld USD.

[14] https://www.knf.gov.pl/komunikacja/komunikaty?articleId=78557&p_id=18 (dostęp 29.01.2023).

31 lipca 2014 r. Rada UE wydała Rozporządzenie nr 833/2014 dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie, w ramach którego zastosowano ograniczenia dotyczące dostępu do rynku kapitałowego wobec niektórych instytucji finansowych. W wyniku uchwalenia Rozporządzenia Rady (UE) 2022/394 z dnia 9 marca 2022 r. zmieniono środki ograniczające w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie, rozszerzając katalog zbywalnych papierów wartościowych o kryptoaktywa, które podlegają zbyciu na rynku kapitałowym, z wyjątkiem instrumentów płatniczych.

Warto również przedstawić założenia projektu Rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptograficznych oraz zmieniająca dyrektywę UE 2019/1937 dnia 24 września 2020 r. COM (2020) 593, w którym zawarto propozycję regulacji kryptoaktywów. Przedmiotowa koncepcja regulacyjna ma przełomowy charakter dla uczestników, jak również perspektyw rozwoju tego rynku.

Celem projektu jest m. in. wprowadzenie:

- ujednoliconych pojęć: definicji kryptoaktywów, technologii DLT, emitenta, tokenów, emisji publicznej, doradztwa w zakresie kryptoaktywów, zarządzanie portfelem,
- wymogów organizacyjnych i prawnych względem uczestników obrotu - emitentów kryptoaktywów, dostawców usług oraz oferty kryptoaktywów;
- przepisów w zakresie identyfikacji nadużyć podobnych jak na rynku kapitałowym (przeciwdziałanie ujawnianiu i wykorzystywaniu informacji poufnej, manipulacji wartością),
- wymogów opracowania dokumentów informacyjnych analogicznych jak dla rynku kapitałowego. *White paper* powinien zawierać informacje o mechanizmie stabilizacji, polityce inwestycyjnej dotyczącej aktywów rezerwowych, rozwiązań w zakresie przechowywania aktywów rezerwowych oraz praw przysługującym posiadaczom,
- obowiązku publikowania informacji bieżących na temat liczby tokenów w obiegu, jak również o zdarzeniach, które mogą mieć lub mają istotny wpływ na wartość tokenów,
- obowiązku spełniania przez członków organu zarządzającego wymogów kompetencji i reputacji,

- mechanizmów kontroli i zarządzania ryzykiem,
- wymogów w zakresie posiadania funduszy własnych – w celu ograniczenia zagrożenia dla stabilności finansowej,
- rejestru dokumentów informacyjnych prowadzonych przez Europejski Urząd Nadzoru Giełd i Papierów Wartościowych,

czy też stosowanie przepisów w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Przenikanie kryptoaktywów do rynków finansowych

Kolejną kwestią są ryzyka związane z przenikaniem mechanizmów transakcyjnych (kryptowalut) do tradycyjnych rozwiązań finansowych. W coraz większym stopniu kryptoaktywa powiązane są z takimi usługami jak: pożyczkowe, powiernicze, inwestycyjne czy płatnicze. Przykładem tego są zarówno firma Revolut, świadcząca usługi finansowe, która oferuje swoim klientom możliwość nabywania za pośrednictwem serwisu kryptowalut oraz firma Coinbase, która daje możliwość pożyczania kryptowalut[15]. Powstają fundusze inwestycyjne oraz ETF (ang. exchange traded fund – fundusz notowany na giełdzie, odwzorowujący zachowanie wybranego aktywa lub indeksu, cechujący się niskimi kosztami) czy CFD (ang. contract for difference – kontrakty na różnicę cenową), których portfel przewiduje możliwość inwestycji w kryptoaktywa.

W związku z powyższym regulacje prawne, akceptacja kryptoaktywów przez inne segmenty rynku finansowego, stały wzrost zainteresowania oraz spekulacyjny charakter rynku kryptoaktywów implikuje kolejne zagrożenia związane z możliwością gwałtownych zmian cen instrumentów powiązanych z kryptoaktywami lub wręcz prowadzi do upadku niektórych projektów.

Przykładem takiego działania jest koncepcja stablecoinów opartych o projekty algorytmiczne – przykładem takiego projektu jest TerraUSD, który w celu utrzymania wartości waluty opiera swoje zabezpieczenie na kodzie

[15] SEC grozi pozwaniem Coinbase w związku z pożyczkami kryptowalutowymi, https://www.pb.pl/sec-grozi-pozwaniem-coinbase-w-zwiazku-z-pozyczkami-kryptowalutowymi-1126819 [dostęp: 10.09.2021].

transakcyjnym, kreując w ten sposób popyt i podaż, w celu zachowania stabilności i równowagi kursu. Jest to koncepcja odmienna od stablecoinów opartych o walutę tradycyjną FIAT, towar lub inną kryptowalutę. Podmioty wydające stablecoin, w tym przypadku, dokonują transakcji (operacji) rynkowych mających na celu zachowanie stabilności wartości danej kryptowaluty. Jednakże, *czarne łabędzie* występujące na rynku spowodowane nagłymi spadkami wartości kryptowalut spowodowały również niepewność rynku stablecoina.

Nowym obserwowanym trendem występującym na rynku kryptowalut, uwarunkowanym agresją Federacji Rosyjskiej na Ukrainę i stosowaniem sankcji Unii Europejskiej i USA wobec osób odpowiedzialnych za tę agresję oraz pełniących istotne wojskowe i polityczne funkcje, jest zainteresowanie tym instrumentem obywateli FR, przede wszystkim jako forma zachowania wartości przed inflacją oraz uchylenia się od sankcji finansowych[16]. Warto przypomnieć, iż sankcje wobec obywateli FR dotyczyły m. in. blokady dostępu do międzynarodowego systemu transakcyjnego SWIFT. „Rosjanie są jednymi z największych posiadaczy kryptowalut na świecie. Według Bloomberga, powołującego się na źródła pochodzące z ministerstwa finansów Rosji, aż 12 proc. wszystkich światowych zasobów kryptowalut znajduje się w ich rękach. Daje to więc zawrotną liczbę blisko 240 mld USD.[17]”

Podsumowując, rynek kryptoaktywów staje się jednym z obszarów transakcyjnych coraz bardziej powiązany z globalnymi finansami. Oczywiście nie są to zależności, które na obecnym etapie rozwoju kryptowalut mogą zagrozić stabilności sektora bankowego, usług inwestycyjnych, powierniczych czy płatniczych. Ale w dłuższej perspektywie, uwzględniając możliwość załamania wartości kryptoaktywów, mogą doprowadzić do ich poważnego zakłócenia – działając tym samym na szkodę inwestorów indywidulanych i instytucjonalnych.

---

[16] K. Wysota, *Kryptoluka w sankcjach*, Puls Biznes nr 40 z 1 marca 2022 r., s. 4.

[17] K. Rębisz, Bitcoin nowym Rublem, https://www.parkiet.com/kryptowaluty/art36100541-bitcoin-nowym-rublem [dostęp: 12.05.2022].

Rozwój przestępczości

Polska Policja nie prowadzi dokładnych statystyk związanych z nieprawidłowościami w obrocie kryptowalutami[18], w związku z powyższym nie można szczegółowo wskazać na zagrożenia związane z obrotem kryptoaktywami, natomiast według raportu firmy CipherTrace, w 2020 r. o 57 proc. zmniejszyła się wartość skradzionych lub wyłudzonych kryptowalut do poziomu 1,9 mld USD. Rok wcześniej (2019) kwota ta sięgała 4,5 mld USD[19].

Zgodnie z raportem[20] Chainalysis wartość przychodów cyberprzestępców, które uzyskali w kryptowalutach wzrosła o 79 % z 7,8 mld USD w 2020 r. do 14 mld USD mld w 2021 r. Natomiast udział nielegalnej działalności w całkowitym wolumenie transakcji kryptowlautowych pozostaje niski i wynosi 0,15 % w 2021 r.

Kradzież kryptowalut wzrosła, w 2021 r. skradziono kryptowaluty o wartości około 3,2 mld USD - wzrost o 516% w porównaniu z 2020 r. Około 2,3 mld USD z tych środków — 72% sumy z 2021 r. - zostało skradzione z protokołów DeFi.

Przychody z oszustw wzrosły o 82% w 2021 r. do 7,8 mld USD skradzionych ofiarom przestępstw w obrocie kryptowalutą, biorąc pod uwagę ilość kryptowalut wysyłanych z nielegalnych adresów na adresy hostowane przez usługi cyberprzestępcy wyprali w 2021 r. kryptowalutę o wartości 8,6 miliarda dolarów.

Zgodnie z informacją firmy Chainalysys[21], 2022 r. był rekordowy w kontekście ataków hackerskich na infrastrukturę podmiotów zajmujących się kryptowalutami, gdzie ujawnione straty to kwota 3,8 mld USD, natomiast 82% wszystkich skradzionych kryptowalut zostało wykradzionych z usług DeFi. Ponadto, z analiz Chainalysys wynika koncentracja uzyskanych aktywów w nielegalnych punktach wypłat, gdzie np. 4 adresy depozytowe otrzymały łącznie 1,1 mld USD nielegalnych środków w 2022 r., a tylko

---

[18] Z uzyskanej odpowiedzi z Biura Kadr, Szkolenia i Obsługi Prawnej KGP (Kwo-883/22/PM) wynika, że ze względu na sposób i zakres gromadzonych danych statystycznych nie ma możliwości przygotowania danych w ujęciu wskazującym na udział/wykorzystanie kryptowalut do popełnienia czynów karalnych.

[19] https://www.pb.pl/w-2020-r-bylo-mniej-przestepstw-zwiazanych-z-kryptowalutami-1106786.

[20] Chainalysys, The 2022 Crypto Crime Report Original data and research into cryptocurrency-based crime, wyd. 02.2022.

[21] Weekly brief Chainalysys, 01.02.2023.

21 adresów depozytowych odpowiada za 50% wszystkich środków wysyłanych przez oprogramowanie ransomware do platform fiducjarnych. Zidentyfikowano również wzrost liczby podziemnych usług prania pieniędzy, z niestandardową infrastrukturą, o różnym stopniu zaawansowania.

Kryptoaktywa z uwagi na cechy tego instrumentu – anonimowy i zdecentralizowany charakter obrotu, kryptograficzne zabezpieczenie transakcji, niskie koszty transakcyjne, innowacyjność i popularność, są szczególnie predestynowane do wykorzystywana do różnego rodzaju przestępstw.

Przestępstwa związane z kryptowalutami możemy podzielić również na następujące kategorie:

- przestępstwa popełniane przy użyciu kryptowalut (ukrywanie majątku, pranie pieniędzy, integralne transakcje związane z czynem zabronionym – np. nabyciem towaru, którego posiadanie jest zabronione lub wykorzystanie do szantażu, w tym ransomware);
- przestępstwa popełniane w celu uzyskania kryptowalut (oszustwa finansowe na rynku forex i kryptowalut, emisja ICO, ITO).

Do najczęściej występujących zagrożeń przestępczością związanych z obrotem kryptowalutą należy zaliczyć:

- pranie pieniędzy pochodzących z różnych form przestępczości pospolitej, poważnej, jak również z przestępczości zorganizowanej;
- oszustwa związane z pozorną emisją kryptowalut (ICO);
- ukrywanie mienia pochodzącego z różnych form przestępczości, w tym przestępczości zorganizowanej;
- wykorzystywanie kryptowalut do nabywania mienia, którym legalny obrót jest zabroniony (środki odurzające i substancje psychotropowe, broń, treści zawierające utwory chronione prawe autorskim, pornografia dziecięca);
- wykorzystywanie do transakcji towarzyszących zjawiskom wymuszeń rozbójniczych, porwań, szantażów komputerowych (np. ransomware);
- manipulacja wartością i wykorzystanie informacji poufnych, przy czym metody wykorzystywane przez sprawców są analogiczne do stosowanych działań przestępczych na rynku kapitałowym. Na obecnym etapie rozwoju rynku kryptowalut brak jest stosownych regulacji

prawnych zabezpieczających rynek i jego uczestników przed takim działaniem sprawców;

– ataki hackerskie na giełdy/kantory kryptoaktywów, jak również na podmioty gospodarcze oferujące emisję/wymianę kryptoaktywów w ramach usług o charakterze inwestycyjnym.

Czarne łabędzie rynku kryptoaktywów

W zmiennym i trudnym do prognozowania środowisku bezpieczeństwa mogą wystąpić zdarzenia, czynniki, procesy istotne z punktu widzenia bezpieczeństwa, które na podstawie dostępnej wiedzy nie mogą być właściwie prognozowane. W literaturze przedmiotu, czasopiśmiennictwie określa się je mianem „czarnych łabędzi"[22], czyli obszarem niewiedzy. Są to zdarzenia, sytuacje, które nie wpisują się w opracowywane modele i pozostają poza marginesem obserwowanej i analizowanej rzeczywistości, co w konsekwencji narusza prognozowane tendencje[23].

W kontekście kryptoaktywów czarnym łabędziem jest sytuacja geopolityczna - agresja zbrojna Federacji Rosyjskiej na Ukrainę, która wpłynęła na rynki finansowo-gospodarcze poprzez zakłócenia w międzynarodowych łańcuchach dostaw różnego rodzaju towarów, w tym surowców energetycznych. Ponadto, z uwagi na niepewność na rynkach kapitałowych, wzrost cen i towarzysząca tym procesom inflacja wpłynęła bezpośrednio na zakłócenia rynku kryptoaktywów[24]. Choć na początku 2023 r. na rynku kryptoaktywów widać już tendencje progresywne, wzrost wartości najbardziej popularnej kryptowaluty.

Kolejnym, niedającym się przewidzieć skutkiem rozwoju technologicznego może być wykorzystanie systemu kwantowego w różnych obszarach cyberprzestrzeni, w tym na rynku kryptoaktywów[25]. Z jednej strony może być wykorzystany do wydobywania kryptowalut, co może znacznie przyspieszyć

---

[22] N. Taleb, *Czarny łabędź. O skutkach nieprzewidywanych zdarzeń*, Wyd. Kurhaus Publishing, Warszawa 2014,

[23] T.R. Aleksandrowicz, *Kluczowe megatrendy w bezpieczeństwie państwa XXI w.,* Wyd. Difin, Warszawa, 2020, s. 8.

[24] Zgodnie z tezą artykułu M. Smiłowskiego, *O hossę na bitcoinie nie będzie łatwo*, zamieszczonym w Pulsie Biznesu w dniu 10 stycznia 2023 r., w 2022 r. cena Btc spadła o 58%.

[25] E. Lihodei, *Czy komputery kwantowe stanowią zagrożenie dla branży krypto*?, https://pl.beincrypto.com/komputery-kwantowe-nie-zagrazaja-krypto/ (dostęp 29.01.2023).

proces emisji kryptoaktywów. Natomiast innym zagrożeniem jest wzrost mocy obliczeniowych systemu kwantowego i w konsekwencji możliwość złamania klucza kryptograficznego (SHA-256), który implikowałby przenoszeniem wartości do dowolnego portfela publicznego. Na obecnym etapie rozwoju systemu kwantowego moc obliczeniowa nie jest wystarczająca do złamania blockchain kryptowalut, jednak nie można wykluczyć tego w przyszłości[26].

Innym z zagadnień jest kwestia postępujących regulacji kryptowalut. Czy instrument, który powstał jako odpowiedź na wzrastającą falę kryzysu finansowego spowodowaną upadkiem czwartego co do wielkości amerykańskiego banku inwestycyjnego Lehman Brothers, w związku z kryzysem na rynku kredytów hipotecznych i jednoczesnym spadkiem zaufania wśród społeczeństwa, będzie dalej traktowany jak innowacyjny i alternatywny do tradycyjnych rynków? Tym bardziej, iż pełną regulację kryptowalut zapowiadają kraje niestabilnej demokracji lub wręcz kraje totalitarne z Federacją Rosyjską na czele. Przedmiotowy zabieg ma na celu uniknięcie z jednej strony sankcji ekonomicznych w związku z agresją zbrojną na Ukrainę, inflacją, czy też ukrywanie majątków pochodzących z różnych form przestępczości. Taki zabieg nie będzie budził zaufania do tych rozwiązań transakcyjnych, może mieć również długofalowo wpływ na ryzyko reputacyjne tych instrumentów.

Analizując to zagrożenie warto wskazać na niestabilność tego rynku, uwarunkowaną decentralizacją, brakiem regulatora i nadzoru nad tym rynkiem, możliwością manipulacji wartością kryptowalut, czy też rekomendacji w zakresie cyberbezpieczeństwa podmiotów świadczących usługi na tym rynku.

W tym względzie istotne jest wykorzystanie, analogicznie jak w przypadku rynku kapitałowego, sztucznej inteligencji do podejmowania decyzji inwestycyjnych, tym bardziej w przypadku znacznej zmienności wartości jednostek kryptowalut. Automatyzacja transakcji na rynku jest jednym z kluczowych wyzwań dla strategii inwestycyjnych. Taka sytuacja implikuje zagrożenia dla inwestorów indywidulanych i instytucjonalnych w kontekście możliwości przejęcia kontroli nad tymi systemami przez grupy przestępcze, wynajętych przez państwo, instytucję czy grupę wpływu, specjalistów, celem przejęcia kontroli nad tymi aktywami.

---

[26] Więcej na ten temat: G. Kubera, *Czy można złamać zabezpieczenia Bitcoina? Zagrożeniem komputery kwantowe*, https://www.computerworld.pl/news/Czy-mozna-zlamac-zabezpieczenia-Bitcoina-Zagrozeniem-komputery-kwantowe,436047.html (dostęp 29.01.2023).

Kolejną kwestią jest rozwój rynku kryptoaktywów w różnych aspektach funkcjonowania – emisji kryptowalut, wydawania tokenów o charakterze użytkowym, płatniczym czy inwestycyjnym, usług pożyczkowych, powierniczych, czy w zakresie stabilizacji ich wartości. W ten sposób, obok regulowanego rynku finansowego, powstał alternatywny, nie nadzorowany przez instytucje państwowe, rynek kryptoaktywów. Wobec zwiększającej się kapitalizacji instrumentów tego rynku, ilości funkcjonujących podmiotów, powiązania transakcyjne i usługowe, taka sytuacja sprzyja destabilizacji pozostałych rynków finansowych. W sposób inspirowany zarówno transakcyjne, informacyjnie czy behawioralnie można wpływać na tradycyjne instrumenty rynku finansowego. A w przypadku załamania wartości chociażby wybranych elementów rynku kryptoaktywów można w ten sposób wpływać na zachowania społeczne.

Czarnymi łabędziami rynku były również zakłócenia występujące na tym rynku powodowane kryzysem finansowym i inflacją co spowodowało spadek zaufania nie tylko do tradycyjnych rozwiązań inwestycyjnych, ale również tych opartych o blockchain. W przypadku scentralizowanych giełd kryptowalutowych takich jak Coinbase, Kraken czy Binance to obroty na tych platformach spadły o ok. 46 %[27], jak również w wyniku tendencji rynkowych lub działań zarządów platform zajmujących się emisją kryptowalut doszło do spektakularnych upadłości firm pożyczkowych[28], czy inwestycyjnych.

Podsumowując, państwo/państwa odstępując od regulacji rynku kryptoaktywów tracą kontrolę i nadzór nad istotnym segmentem alternatywnych rozwiązań finansowych i mogą przyczyniać się do osłabiania i destabilizacji tradycyjnych rynków. Pewnym rozwiązaniem jest projektowane rozporządzenia MiCA, które w sposób kompleksowy będzie regulowało kwestie związane z emisją, nadzorem i funkcjonowaniem instytucji kryptoaktywów. Jednak z uwagi na ograniczony, europejski obszar regulacji nie będzie on dotyczył największych i rozwijających się, północnoamerykańskich i azjatyckich rynków, przez co straci na sile oddziaływania.

---

[27] W. Zieliński, *Kryptowaluty na bruku. Spektakularny spadek aktywności*, Pakiet, https://www.parkiet.com/kryptowaluty/art37739061-kryptowaluty-na-bruku-spektakularny-spadek-aktywnosci (dostęp 01.02.2023).

[28] W. Zieliński, *Genesis zbankrutowała, 100 tys. kredytodawców na lodzie, Parkiet, https://www.parkiet.com/gospodarka-swiatowa/art37812331-genesis-zbankrutowala-100-tys-kredytodawcow-na-lodzie (dostęp. 01.02.2023).*

Podsumowanie

Analiza strategiczna trendów występujących na rynku kryptoaktywów jest istotnym elementem z punktu widzenia opracowywania strategii bezpieczeństwa finansowego. Przedmiotowa strategia powinna zawierać szczegółową analizę tendencji występujących na rynku kryptoaktywów, posiadane zasoby osobowe, analityczne i operacyjne oraz formułować zadania dla organów państwa, celem mitygacji zagrożeń związanych z tym rynkiem.

Warto podkreślić, iż przedmiotowe trendy są ze sobą ściśle powiązane, a identyfikowane tendencje oddziałują na siebie, jak np. wzrost przestępczości, zagrożenia wykorzystywania instytucji rynku kryptoaktywów (giełdy, kantory kryptowalutowe, giełdy OTC), do legalizowania korzyści, czy też przenikanie tradycyjnych rozwiązań finansowych – karty płatnicze, usługi pożyczkowe czy powiernicze z regulacją rynku.

W związku z powyższym przez instytucje i służby właściwe w zakresie przeciwdziałania praniu pieniędzy, finansowania terroryzmu, ukrywania mienia oraz oszustw w cyberprzestrzeni, powinna być wykonywana analiza strategiczna tego zjawiska, celem podnoszenia poziomu ochrony bezpieczeństwa finansowego państwa. Z uwagi na charakter zjawiska należy w tym przypadku stosować podejście multidyscyplinarne, integrujące działalność prawną, techniczną i ekonomiczną. W tym celu należałoby podjąć współpracę międzyinstytucjonalną z zaangażowaniem przedstawicieli świata nauki i prywatnej przedsiębiorczości.

Pomimo degresji na rynku (spadek wartości, upadłości podmiotów z rynku kryptoaktywów – giełd, instytucji powierniczych) kryptoaktywa w dalszym ciągu cieszą się zainteresowaniem uczestników rynku, zarówno detalicznych jak i instytucjonalnych. W związku z powyższym kilkumiesięczny okres załamania na rynku nie przekreślił aspiracji tego rynku, jak również możliwości dalszego jego rozwoju.

Bibliografia

1. Aleksandrowicz, T.R., *Kluczowe megatrendy w bezpieczeństwie państwa XXI w.*, Wyd. Difin Warszawa, 2020.
2. Taleb N., *Czarny łabędź. O skutkach nieprzewidywanych zdarzeń*, Wyd. Warszawa 2014.
3. Kamerschen D.R., McKenzie R.B., Nardinelli C., Ekonomia, Wyd. Fundacja Gospodarcza NSZZ Solidarność, 1991.

4. Kubera G., *Czy można złamać zabezpieczenia Bitcoina? Zagrożeniem komputery kwantowe*, https://www.computerworld.pl/news/Czy-mozna-zlamac-zabezpieczenia-Bitcoina-Zagrozeniem-komputery-kwantowe,436047.html (dostęp: 31.01.2023).
5. Lihodei E., *Czy komputery kwantowe stanowią zagrożenie dla branży krypto?*, https://pl.beincrypto.com/komputery-kwantowe-nie-zagrazaja-krypto/ (dostęp 29.01.2023).
6. Rębisz K., *Bitcoin nowym Rublem*, https://www.parkiet.com/kryptowaluty/art36100541-bitcoin-nowym-rublem (dostęp: 12.05.2022).
7. Smiłowski M., *O hossę na bitcoinie nie będzie łatwo*, Puls Biznesu z 10.01.2023 r, nr 6.
8. Wysota K., *Kryptoluka w sankcjach*, Puls Biznesu nr 40 z 1.03.2022 r.
9. Zieliński W., *Kryptowaluty na bruku. Spektakularny spadek aktywności*, Pakiet, https://www.parkiet.com/kryptowaluty/art37739061-kryptowaluty-na-bruku-spektakularny-spadek-aktywnosci (dostęp: 01.02.2023).
10. Zieliński W., *Genesis zbankrutowała, 100 tys. kredytodawców na lodzie*, Parkiet, https://www.parkiet.com/gospodarka-swiatowa/art37812331-genesis-zbankrutowala-100-tys-kredytodawcow-na-lodzie (dostęp. 01.02.2023).
11. *Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2021 roku*.
12. https://coinatmradar.com/bitcoin-atm-near-me/ (dostęp: 28.01.2023).
13. https://earthweb.com/cryptocurrency-statistics/;(dostęp: 01.02.2023).
14. https://bomega.pl/polacy-zarobili-ponad-200-mln-usd-na-bitcoinach/ (dostęp 29.01.2023)
15. https://www.pb.pl/w-2020-r-bylo-mniej-przestepstw-zwiazanych-z-kryptowalutami-1106786.
16. Chainalysys, The 2022 Crypto Crime Report Original data and research into cryptocurrency-based crime, wyd. 02.2022.
17. Chainalysys, Weekly brief Chainalysys, 01.02.2023.
18. Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. nr 5

19. Rozporządzenie Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie.
20. Rozporządzenie Rady (UE) 2022/394 z dnia 9 marca 2022 r. zmieniające rozporządzenie (UE) nr 833/2014 dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie,
21. Uchwałę nr 111/22 Komisji Nadzoru Finansowego z dnia 14 kwietnia 2022 r. w sprawie okoliczności istotnych dla oceny rękojmi w sprawach z zakresu rynku finansowego w związku z agresją Federacji Rosyjskiej wobec Ukrainy. https://www.knf.gov.pl /knf/pl/komponenty/img/Uchwa%C5%82a_111_2022_77789.pdf.
22. Komunikat Komisji Nadzoru Finansowego dotyczący sankcji i stosowania przepisów ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, w przypadku współpracy z podmiotami branży walut wirtualnych. https://www.knf.gov.pl/komunikacja/komunikaty?articleId=78557&p_id=18.

Abstract

TRENDS IN THE CRYPTOCURRENCY MARKET

Summary: The chapter presents the identified trends in the crypto-assets market that may be important for building a financial security strategy and formulating appropriate tasks for state institutions and services in the field of counteracting threats

Keywords: crypto-assets, trends on the crypto-assets market, financial security

Rozdział 7

Osint i wojna czyli mocno subiektywny przegląd źródeł informacji

Krystian WOJCIECHOWSKI[1]

STRESZCZENIE: W rozdziale opisano, wybrane rozwiązania cyfrowe wykorzystywane przez władze Ukrainy przed i po rozpoczęciu obecnej fazy działań wojennych. Wskazano na rolę i wykorzystanie komunikatora Telegram, zarówno jako źródła informacji, jak i medium społecznościowego. Ponadto na przykładach opisano wagę geolokacji materiałów i wskazano portale, kanały publikujące mapy ilustrujące tematy odnoszące się do wojny. W dalszej części artykułu opisano przykładowe, zarówno rosyjskie, jak i ukraińskie oraz pro ukraińskie źródła informacji publikujące w internecie oraz mediach społecznościowych

Słowa kluczowe: geolokacja, media społecznościowe, wojna, Rosja, Ukraina, Twitter, Telegram, analiza informacji, weryfikacja informacji, źródła otwarte, wywiad otwarto źródłowy

Wstęp

Trwająca od 24 lutego 2022 roku, aktywna faza wojny rosyjsko-ukraińskiej odbywa się bezpośrednio na naszych oczach. Obie strony aktywnie wykorzystują nowoczesne środki komunikacji cyfrowej a w szczególności internet i media społecznościowe zarówno do informowania jak i propagandy czy prób zastraszania przeciwnika. Niniejszy rozdział powstawał w zasadzie od pierwszego dnia obecnego konfliktu. W moim obszarze zainteresowań były przede wszystkim narzędzia wykorzystywane przez obie strony do zarządzania informacjami cyfrowymi i źródła otwarte dokumentujące przebieg wydarzeń oraz umożliwiające weryfikację informacji. W rozdziale opisuję wybrane przy-

[1] mł. insp. policji w stanie spoczynku, w przeszłości funkcjonariusz dochodzeniowy i analityk kryminalny od 2000 roku, kierownik SAK, naczelnik Wydziału Wywiadu Kryminalnego KWP w Gdańsku, analityk wywiadu w międzynarodowej korporacji. Dzisiaj wykładowca akademicki, przedsiębiorca, analityk, biegły sądowy, konsultant w zespole Hexagon Public Safety.

kłady wykorzystania komunikatora Telegram, który stał się w tej wojnie jednym z podstawowych i najszybszych przekaźników informacji. Ponadto wskazuję przykłady stron internetowych, kanałów w mediach społecznościowych lub serwisów, które mogą stanowić źródło informacji. Ogromna dostępność materiałów źródłowych z obecnego konfliktu powoduje zalew komentarzy, analiz i ocen. Trudno wskazać wiarygodne źródła, dlatego w rozdziale staram się odnieść także do tematu oceny informacji. Naturalnie w tak dynamicznym konflikcie, gdy źródła należy dopasowywać do konkretnych wydarzeń, istnieje potrzeba stałego zwiększania liczby i zasięgu źródeł przy jednoczesnym utrzymywaniu ścisłych zasad oceny i weryfikacji informacji.

Kiedy w połowie 2018 roku poproszono mnie o przygotowanie krótkiego kursu osintowego dla przedstawicieli policji ukraińskiej nie zdawałem sobie sprawy jak bardzo różna jest tamtejsza sfera internetu. Wojna na wschodzie Ukrainy trwała już cztery lata, rosyjski internet powoli, ale nieubłaganie zamykał się a Ukraina była wciąż w połowie drogi między zachodem a wschodem, pomiędzy Google a Yandexem, Facebookiem a Vkontakte. Wiele narzędzi doskonale pracujących w zachodniej sferze internetowej zwyczajnie nie sprawdzało się. Za to korzystanie z formalnie zablokowanych i dostępnych za pośrednictwem VPN narzędzi i stron rosyjskich przynosiło wielokrotnie doskonałe rezultaty. Wtedy po raz kolejny sprawdziło się stwierdzenie, że w pracy ze źródłami otwartymi nie tylko elastyczność, ale także nadmiarowość źródeł pomaga w odniesieniu sukcesu.

Jednym z kompletnie dla mnie nowych narzędzi był komunikator Telegram. W tym czasie w Polsce był to po prostu kolejny po Messengerze, czy Whatsappie sposób na komunikację poza siecią telefonii komórkowej.

Już pierwszego dnia poproszono mnie o pomoc i przyjrzenie się specyficznym graffiti znajdującym się na większości budynków, mostów czy czasem nawet rynnach. Wszystkie zaczynały się od znaku „@", po którym była nazwa. Czasem pojawiał się dodatkowy komunikat ze słowem „Telega" i skróty oznaczające nazwy substancji. W ten sposób na reklamowano sklepy internetowe sprzedające narkotyki poprzez Telegram.

Źródło: Zasoby własne.

Rysunek 2. Reklama sklepów internetowych sprzedających narkotyki poprzez Telegram

Policjanci z wydziałów do walki z narkotykami mieli ogromny problem z ujawnianiem sprawców tych przestępstw. Telegram uchodził za całkowicie anonimowy komunikator, co w połączeniu z systemem płatności internetowych mocno utrudniało proces wykrywczy. Jako jedno z proponowanych narzędzi powstał prototyp mapy ewidencjonującej wszystkie graffiti na danym terenie. Taka mapa pozwalała, nie tylko zobrazować miejsca położenia napisów, ale także, np. wskazać miejsca aktywności konkretnych grup.

Na rysunku 2 widoczny jest fragment mapy z uwzględnieniem części kijowskiej dzielnicy Podole. W tym czasie działał już w Telegramie, prawdopodobnie pierwszy oficjalny, bot „OpenDataUA" dostarczający dane dotyczące danych rejestrowych firm, osób, pojazdów i nieruchomości. Dzisiaj ma on także formę osobnej aplikacji na urządzenia mobilne. Narzędzie działało sprawnie i dostarczało wystarczającej ilości informacji biznesowej i sądowej. W 2019 roku, już w trakcie kampanii wyborczej na ulicach Kijowa zaczęły się pojawiać banery informujące o inicjatywie „Kyiv Smart Forum 2019".

Źródło: Zasoby własne.

Rysunek 2. Mapa reklam sklepów internetowych sprzedających narkotyki w części kijowskiej dzielnicy Podole

Zaczęto budować także państwowy system nowoczesnych usług cyfrowych. Cyfryzacja Ukrainy mocno przyspieszyła i w efekcie już w lutym 2020 roku powstała aplikacja „Dija" pozwalająca użytkować miedzy innymi cyfrowe dokumenty osobiste. W Kijowie z kolei powstała aplikacja „Kijów cyfrowy". Początkowo miała wspomóc, np. zarządzanie systemem płatnych miejsc parkingowych i umożliwić zakupy biletów na metro.

Źródło: Zasoby własne.

Rysunek 3. Banery informujące o inicjatywie „Kyiv Smart Forum 2019"

Jesienią 2021 roku „Patrulna Policja" anonsowała oficjalnie wprowadzenie pierwszego narzędzia wspomagającego walkę z handlem narkotykami za pośrednictwem Telegramu. Bot pod nazwą @Drughunters_Ukraine_bot miał pomóc w identyfikacji i dotarciu do osób zaangażowanych w proces ukrywania narkotyków na terenie miast.[2]

Źródło: Zasoby własne.

Rysunek 4. Bot @Drughunters_Ukraine_bot pomagający w identyfikacji i dotarciu do osób zaangażowanych w proces ukrywania narkotyków

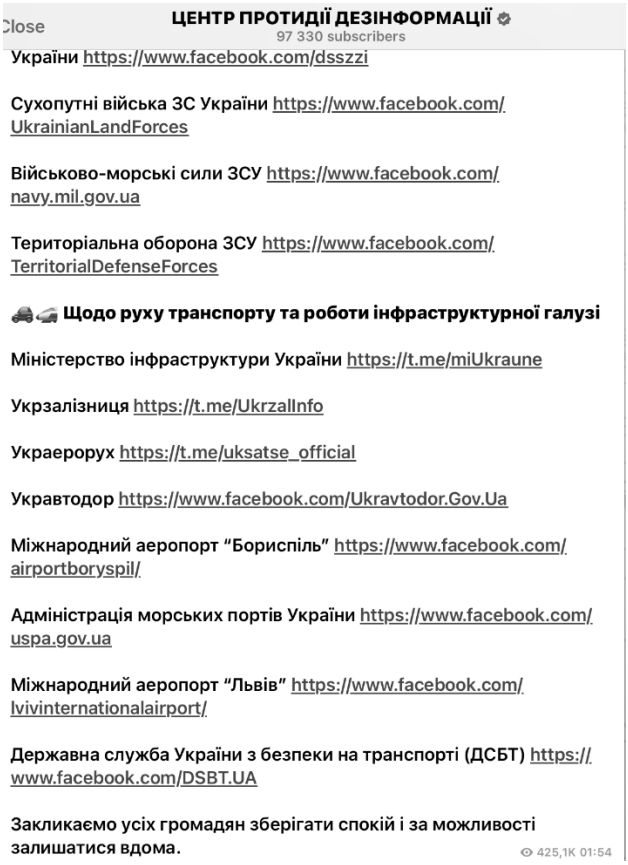
Kilka tygodni później podobne narzędzie uruchomiła kolejna służba policyjna, mianowicie „Kiber Policja". czyli jednostka w pełni zorientowana na zwalczanie przestępczości w sieci.

Od chwili rozpoczęcia działań wojennych w lutym 2022 roku najważniejszym wyzwaniem okazało się zapewnienie przepływu informacji do obywateli i jednoczesna koordynacja zbierania informacji użytecznych władzom.

W pierwszych kilku dniach część ukraińskich instytucji wskazywała na swoje profile na portalu Facebook jako na źródło informacji. Jednakże bardzo szybko pojawiła się tendencja do przenoszenia niemal całości informacji do kanałów Telegramu.

Na rysunku 5 pokazano przykład zbiorczej listy linków informacyjnych opublikowanych na kanale Centrum Działania Dezinformacji.

[2] https://mvs.gov.ua/uk/press-center/news/patrulna-policiya-zapustila-cat-bot-dlya-borotbi-z-narkozlicinami-oleksii-bilosickii



Źródło: Zasoby własne.

Rysunek 5. Linki informacyjne opublikowane na kanale Centrum Działania Dezinformacji

Od początku działań wojennych władze ukraińskie przekazują społeczeństwu jasny komunikat na temat konieczności dbania o swój telefon komórkowy. Zawsze powinien on być pod ręką, gdy tylko istnieje możliwość powinien zostać naładowany, podobnie jak powerbank.

Powstały listy aplikacji, które powinno się instalować na swoim urządzeniu mobilnym. W pierwszej kolejności była to właśnie „Dija", która już nie tylko pozwalała potwierdzić tożsamość, ale także, np. wnioskować o zapomogę, słuchać radia nadającego komunikaty wojenne, czy też dla relaksu pokierować wirtualnym … Bayraktarem. W Polsce „Dija" została włączona

w aplikacje „mObywatel".[3] W przeciwieństwie do 2014 roku obie strony zabraniały użytkowania aplikacji „Zello". Jest to aplikacja przekształcająca telefon komórkowy w radiotelefon co pozwala w ten sposób kontaktować się w większej grupie osób. W 2014 roku aplikacja odegrała ważną rolę w koordynacji działań zarówno ukraińskich, jaki i separatystycznych. Dzisiaj uznano ją za zbyt niebezpieczną.

Bardzo szybko okazało się jednak, że dochodzi do masowych ataków hakerskich, przede wszystkim nakierowanych na konta na Telegramie. Pojawiła się duża kampania na temat bezpiecznego korzystania z telefonów komórkowych. Pod hasłem „Cyfrowa higiena smartfona" krok po kroku wyjaśniano jak powinno się zabezpieczyć telefon komórkowy i konta na poszczególnych portalach. Wojna nie wyeliminowała istniejących zagrożeń, np. phishingu, ale bardzo szybko pojawiły się nowe zagrożenia, np. kampanie dezinformacyjne mające na celu spowodowanie dodatkowego chaosu w państwie.

Jednym z aktywnych podmiotów informujących na temat zasad użytkowania telefonów w wojennej rzeczywistości było (i jest nadal) wspomniane już Centrum Przeciwdziałania Dezinformacji.

[3] https://www.gov.pl/web/mobywatel-w-aplikacji/ua

Źródło: Zasoby własne.

Rysunek 6. Strona Centrum Przeciwdziałania Dezinformacji

W pierwszych tygodniach gorącego konfliktu istniało bardzo duże zapotrzebowanie na informacje na temat działań wroga. Wtedy powrócono do botów na portalu Telegram.

Świeżo uruchomiony przez „Kiber Policję" bot @stopdrugsbot (rys. 7) miał służyć do przekazywania informacji na temat działań dywersyjnych.

Źródło: Zasoby własne.

Rysunek 7. Bot @stopdrugsbot służący także do przekazywania informacji na temat działań dywersyjnych

Kolejny policyjny bot „@Ukraine_avanger_bot" służy do zbierania informacji na temat niewybuchów, wrogiej techniki wojskowej, obecności okupantów a także urządzeń i znaków ułatwiających wojskom okupacyjnym poruszanie się w terenie. Dodatkowo za pośrednictwem tego bota można informować policję o podejrzanych o sprzyjanie agresji rosyjskiej oraz przestępcach dokonujących kradzieży opuszczonego mienia.

Źródło: Zasoby własne.

Rysunek 8. Bot „@Ukraine_avanger_bot" do zbierania informacji na temat niewybuchów, wrogiej techniki wojskowej, obecności okupantów, a także urządzeń i znaków ułatwiających wojskom okupacyjnym poruszanie się w terenie

Swojego bota uruchomiła także Służba Bezpieki Ukrainy: @Stop_russian_war_bot" , podobnie jak zakładka w aplikacji „Dija" o nazwie „eWorog" miał ułatwiać lokalizację wrogich jednostek.

Źródło: Zasoby własne.

Rysunek 9. Bot @Stop_russian_war_bot" ułatwiający lokalizację wrogich jednostek

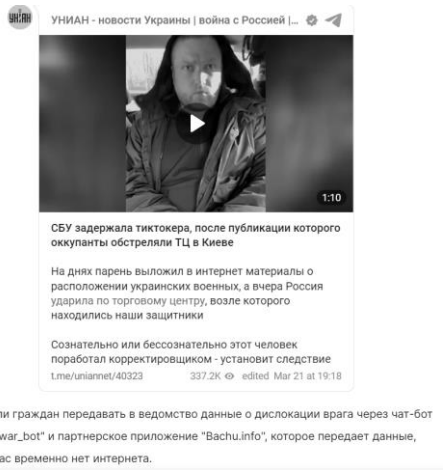
Wymienione boty to tylko kilka przykładów z początku wojny. Z każdym miesiącem powstawały nowe, włącznie ze specjalizowanymi, ułatwiającymi żołnierzom rosyjskim oddanie się do niewoli lub raportowanie o zniszczeniach, czy zbrodniach wojennych.

Od początku wojny dużym problemem były niekontrolowane publikacje w internecie, szczególnie w mediach społecznościowych. Każdego dnia powstawały nowe kanały na Telegramie publikujące coraz bardziej szokujące materiały. Większość z tych kanałów miała na uwadze informowanie i podniesienie morale mieszkańców, ale wielokrotnie publikowane w ten sposób materiały pomagały wrogowi.

Dość szybko zorientowano się, że geolokalizacja fotografii wrzuconych nawet na prywatny kanał Telegramu, czy konto na Tik Toku może spowodować wymierne szkody.

Jednym z pierwszych takich przykładów jest ostrzelanie przez Rosjan centrum handlowego Retroville w Kijowie, które miało miejsce w dniu 20 marca 2022 roku. W wyniku ostrzału rakietowego z kierunku północnego zniszczeniu uległo całe centrum handlowe znajdujące się na terenie osiedla mieszkaniowego. Zginęło minimum osiem osób. Bardzo szybko ustalono, że powodem ostrzału było opublikowanie na Tik Toku filmiku, na którym widoczne były pojazdy Sił Zbrojnych Ukrainy kryjące się w pobliżu rampy służącej do wyładunku towaru.

Sprawca został zatrzymany już następnego dnia. Służba Bezpieczeństwa Ukrainy opublikowała filmik, na którym opowiadał on o swoim zachowaniu. W informacji prasowej agencja „Unian" informowała (rys. 10), że w trakcie śledztwa SBU korzystało z danych uzyskanych za pośrednictwem bota „@Stop_russian_war_bot" oraz aplikacji „Bachu.info".



Źródło: Zasoby własne.

Rysunek 10. Informacja agencji „Unian" informująca o korzystaniu w trakcie śledztwa SBU z bota „@Stop_russian_war_bot" oraz aplikacji „Bachu.info"

Kilka dni później reporter należącej do rosyjskiej armijnej telewizji „Zwiezda", Murad Gazdiev, na żywo relacjonował wyładunek wozów opancerzonych i czołgów w okupowanym Bierdiansku nad morzem Czarnym.[4]

[4] https://www.bbc.com/news/world-europe-60859337

Operacja wyładunku była nietypowa, bo użyte barki transportowe zaprojektowano do desantu na bałtyckich plażach, a nie wyładunku w porcie. Cała czynność trwała na tyle długo, że strona ukraińska zdążyła przygotować atak rakietowy. Kilka minut po reportażu media społecznościowe zostały zalane zdjęciami dymiących okrętów.

Źródło: Zasoby własne.

Rysunek 11. Fragment reportażu Murada Gazdieva relacjonującgo wyładunek wozów opancerzonych i czołgów w okupowanym Bierdiansku

Wspomniane przypadki wykorzystania geolokacji do ataku na wroga to tylko jedne z pierwszych. Od początku wojny obie strony miały świadomość wagi geodanych.

Po ataku na C.H. Retroville oficjalnie wprowadzono zakaz publikowania zdjęć i filmów mogących identyfikować miejsca dyslokacji wojska lub np. efekty bombardowania. Zabroniono także używania rejestratorów samochodowych.

Źródło: Zasoby własne.

Rysunek 12. Zasady publikowania zdjęć i materiałów filmowych

Zasady publikowania zdjęć i materiałów filmowych były i są w dużej mierze przestrzegane. Stąd też bywają nawet dłuższe okresy, gdy w sieci brak informacji, np. z frontu.

Rosjanie podobnie jak Ukraińcy mają świadomość wagi jaką daje geolokacja danych. Przykład ostrzelania CH Retroville pokazuje, że wywiad jednostki okupującej okolicę Irpienia, Buczy i lotniska w Hostomelu prowadził rozpoznanie także z wykorzystaniem Tik Toka.

Tuż po ogłoszeniu tzw. częściowej mobilizacji, w dniu 05.10.2022 roku Rosyjskie Stowarzyszenie Weteranów Afganistanu opublikowało broszurę pod tytułem „Żyję, walczę, wygrywam! Zasady życia na wojnie”[5] Książeczka napisana prostym, potocznym językiem składa się z krótkich rozdziałów opisujących przygotowanie i prowadzenie działań wojennych z poziomu świeżo zmobilizowanego, frontowego dowódcy i żołnierza. Znajdziemy tutaj kilka odniesień do geolokalizacji oraz korzystania z nowoczesnych urządzeń elektronicznych. Już same tytuły rozdziałów wiele mówią o stosunku autorów do możliwości korzystania z telefonów komórkowych w trakcie działań wojennych: „Idiota z telefonem komórkowym jest swoim własnym wrogiem” i „Zdjęcia na portalach społecznościowych - szpiegowski skarb”. W jednym z

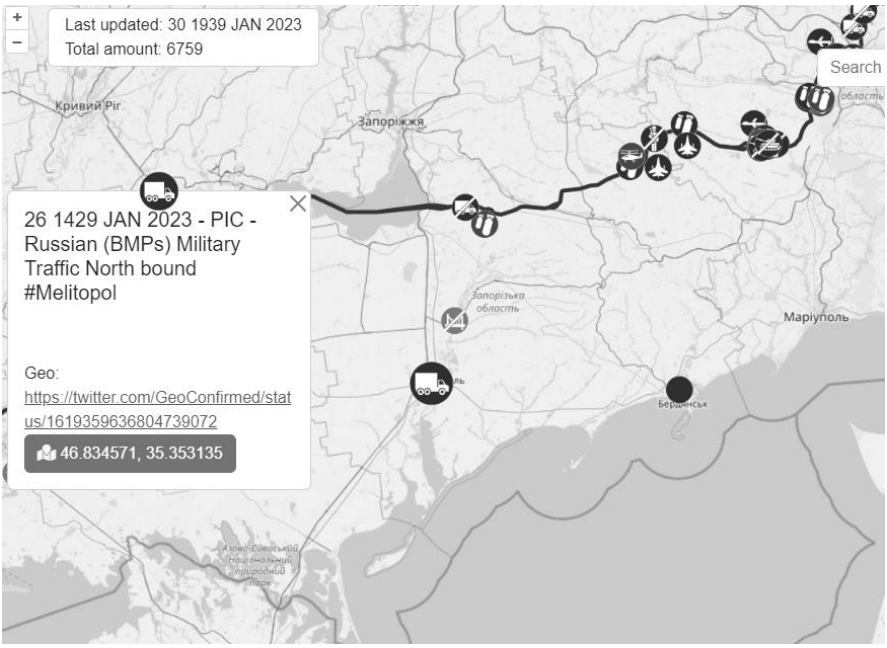
[5] Живу, сраЖаюсь, побеЖдаю! Правила жизни на войне https://lostarmour.info/books/warbook.pdf rozdziały 17 i 18.

kolejnych rozdziałów autorzy proponują, aby patrole lub posterunki blokadowe przeglądały zawartość telefonów komórkowych podejrzanych osób i „całkiem przypadkowo" niszczyły te telefony, np. zrzucając na ulicę.
Nie sposób powiedzieć jak wielu mobilizowanych żołnierzy przeczytało tę broszurkę, ale do oddziału pochodzącego z okolic Samary, który został zakwaterowany w budynku internatu w miejscowości Makiejewka zapewne porady nie dotarły.
Oddział składający się z około 400 świeżo mobilizowanych żołnierzy przygotowywał się do świętowania Nowego Roku, jednakże minutę po północy na budynek tymczasowych koszar spadły rakiety systemu Himars. Do dzisiaj nie ustalono liczby poległych w wyniku tego ostrzału. Władze rosyjskie pośrednią winą obciążyły samych mobilizowanych żołnierzy, którzy mieli aktywnie korzystać z mediów społecznościowych i telefonów komórkowych[6].

Serwisy mapowe

Każdy zainteresowany działaniami wojennymi na Ukrainie znajdzie w sieci wiele serwisów publikujących mapy działań wojennych. Większość opiera się na publikacjach otwarto źródłowych uzupełnianych i aktualizowanych w miarę pojawiania się nowych danych. Jednym z wyróżniających się serwisów jest Geoconfirmed[7]. Jego internetowa część to prosta mapa z naniesionymi ikonami zidentyfikowanych i podzielonych według kategorii miejsc. Do obsługi serwisu wykorzystywane jest konto w portalu Twitter. Dzięki takiemu rozwiązaniu setki osób z całego świata uczestniczy w lokalizowaniu pojawiających się fotografii i filmów. Serwis ma możliwość filtrowania wyszukiwań po dacie wydarzenia, co znacznie ułatwia znalezienie interesującego materiału.
Poniżej na rys. 13 przedstawiono przykładowe zdarzenie zarejestrowane w Melitopolu.

[6] https://cyberdefence24.pl/armia-i-sluzby/ukrainski-atak-w-makiejewce-telefony-zdradzily-pozycje-rosjan
[7] https://geoconfirmed.azurewebsites.net



Źródło: Zasoby własne.

Rysunek 13. Geolokalizacja zdarzenia w Melitopolu

Z Ukraińskich źródeł, jedną z najlepszych map dostarcza kanał Telegramu DeepStateUA[8] . Ich mapa jest często aktualizowana i bardzo czytelna. Ponadto DeepStateUA stara się umieszczać na mapie nie tylko dane z frontu, a także szerszy kontekst, publikując informacje o rozmieszczeniu jednostek wojskowych na terenie Białorusi, Rosji czy Naddniestrza.

[8] https://deepstatemap.live/en#8/47.065/33.821

Źródło: Zasoby własne.

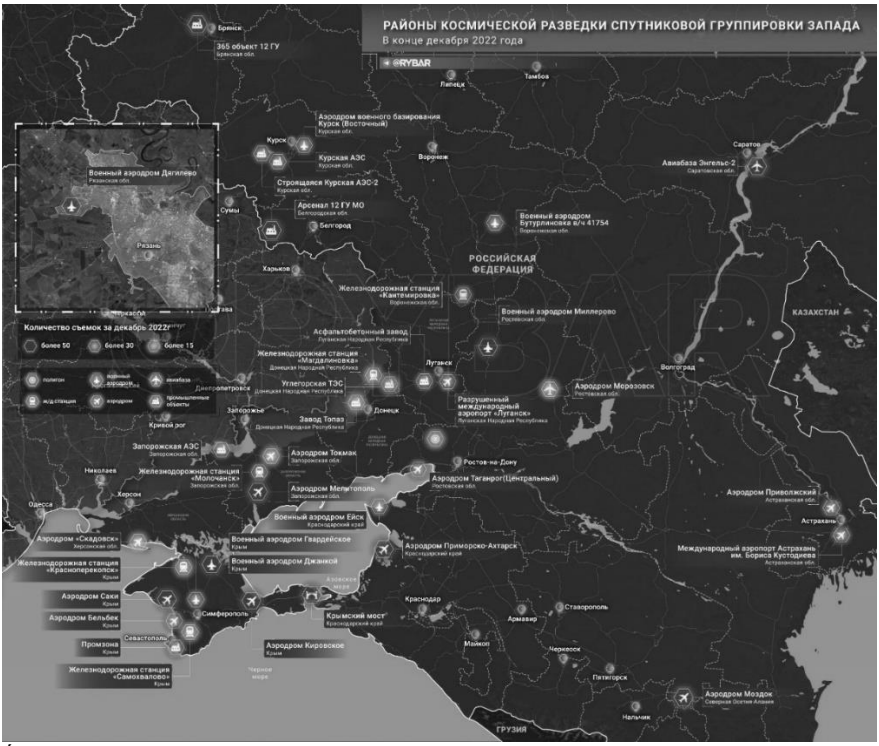
Rysunek 14. Kanał Telegramu DeepStateUA

Ze źródeł rosyjskich najdokładniejsze wydają się być mapy i opracowania przygotowywane przez zespół Michaiła Zwinczuka publikującego pod nazwą „Rybar”[9]. Od początku wojny jest to kanał wyraźnie stojący po stronie rosyjskiej, jednakże jego publikacje, jakkolwiek propagandowe, z racji najczęściej dość wysokiego poziomu mogą służyć jako materiał do kolejnej weryfikacji. Szczególnie ciekawe są tematyczne mapy publikowane na tym kanale, zwykle także w wysokiej rozdzielczości i często dodatkowo w języku angielskim.

Poniżej, na rysunku 15, znajduje się przykład mapy będącej załącznikiem do analizy wskazującej potencjalne przyszłe cele SZU na terenie Rosji. Analiza powstała tuż po atakach na lotnisko w mieście Engels w pobliżu Sa-

[9] https://oko.press/rybar-niezalezny-kanal-rosyjski-wywiad

ratowa, na którym stacjonowała jednostka rosyjskiego lotnictwa strategicznego. W opracowaniu Rybara sugeruje się, że zakupiono w firmie Maxar zdjęcia satelitarne Rosji wykonane przez tę firmę w grudniu 2022 roku. W ten sposób porównując fotografowane miejsca ze znanymi lokalizacjami jednostek wojskowych powstała mapa potencjalnych celów.



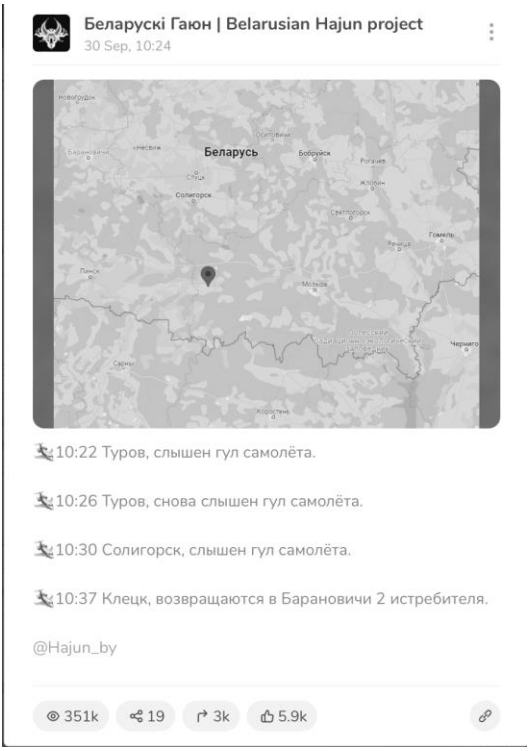
Źródło: Zasoby własne.

Rysunek 15. Kanał Michaiła Zwinczuka „Rybar"

Swój własny serwis mapowy prowadzi także białoruski niezależny kanał „Belaruski Hajun".[10] Na kanale publikowane są, niemalże całodobowo, informacje o kierunkach przemieszczania się jednostek wojskowych białoruskich

[10] Telegram @hajun_by

i rosyjskich. Kanał uchodzi za bardzo wiarygodny i dokładny. Każda informacja na temat startu rosyjskich myśliwców z rakietami „Kindżał" wywołuje na Ukrainie natychmiastową reakcję w postaci ogłoszenia alarmu powietrznego.



Źródło: Zasoby własne.
Rysunek 16. Kanał „Belaruski Hajun"

Z zachodnich materiałów publikujących sytuację taktyczną i analizy taktyczno-strategiczne wyróżniają się szczególnie te przygotowywane przez „Institute of the study of war".[11] Materiały publikowane na stronach instytutu są przedmiotem szerokich komentarzy i uważa się je za jedne z najlepszych źródeł wiedzy o sytuacji na froncie. Są one użyteczne wtedy, gdy mamy do czynienia z tzw. „reżymem ciszy" stosowanym przez SZU jako element wojny informacyjnej.

[11] https://www.understandingwar.org/

Drugim bardzo popularnym źródłem są komunikaty analityczne brytyjskiego wywiadu wojskowego. W krótkiej dobrze napisanej informacji analitycznej użytkownik twittera otrzymuje codzienne podsumowanie sytuacji wojennej. Materiały te są szeroko powielane i publikowane przez, np. anglojęzyczny dziennik KyivPost [12].

Wojna na Ukrainie pokazuje siłę nowoczesnego wywiadu elektronicznego, ale też pozwala spojrzeć na siły i środki niezbędne do pozyskania informacji ze źródeł elektronicznych. Tysiące osób śledzi na portalu „Flight Radar 24" aktywność lotnictwa państw NATO i Rosji oraz coraz częściej także Iranu.

Jednakże taka analiza ma swoje oczywiste ograniczenia, ponieważ trudno zobaczyć pewien kontekst ogólny działań.

Analitycy projektu „Orion Intel"[13], co dwa tygodnie na swoim koncie twitterowym, publikują tematyczne mapy zebrane z otwartych źródeł. Jedne z ciekawszych stanowią właśnie mapy aktywności lotnictwa NATO. Źródłem danych są oczywiście serwisy otwarte, widzimy tylko te loty które odbywały się z włączonymi transponderami, ale siłą tej mapy jest agregacja danych.

Źródło: Zasoby własne.

Rysunek 17. Projekt „Orion Intel"

[12] https://www.kyivpost.com/post/5442

[13] https://www.orionintel.net

„Orion Intel" co pewien czas publikuje także mapy tematyczne, np. ilustrujące uszkodzenia infrastruktury krytycznej czy mostów na terenie Ukrainy.
Ukraiński projekt „Mapa Odbudowy" stara się na bieżąco uzupełniać zarówno zniszczenia, jak i postępy prac odbudowy.[14] Portal nie koncentruje się tylko na infrastrukturze krytycznej czy budynkach zabytkowych lub należących do administracji, ale także na budynkach mieszkalnych. Każde doniesienie o uszkodzeniach jest geolokalizowane, opisane i zawiera w miarę możliwości zdjęcia oraz linki do materiałów źródłowych.
Kolejnym przykładem źródeł informacji są opracowania mapowe opisujące zbrodnie wojenne popełnione przez wojska okupacyjne.
Jedną z pierwszych takich map była opublikowana na stronach serwisu Google praca pod tytułem „Skąd pochodzą Orki". Mapa opierała się na danych żołnierzy rosyjskich stacjonujących na terenie Buczy i Irpienia w pierwszych miesiącach wojny. Dane te opublikował na swojej stronie internetowej Główny Zarząd Wywiadu Ministerstwa Obrony Ukrainy [15].
Mapa została już usunięta z serwisu Google jako naruszająca zasady, ale dane na stronie internetowej wywiadu wojskowego stale są aktualizowane.

Źródło: Zasoby własne.
Rysunek 18. Projekt „Skąd pochodzą Orki"

[14] https://reukraine.shtab.net/
[15] https://gur.gov.ua/content/war-criminals-rf.html

Pod każdą pinezką mapy znajdowały się dane personalne żołnierza, jego numer telefonu i adresy kont społecznościowych. Dzisiaj rolę takiego serwisu agregującego dane na temat zbrodni wojennych ma realizować portal podlegający pod Biuro Prokuratora Generalnego Ukrainy[16]. Portal ten w prosty sposób pozwala nadsyłać precyzyjne informacje o zdarzeniach, posiada także dedykowane aplikacje mobilne ułatwiające raportowanie.

Źródło: Zasoby własne.

Rysunek 19. Portal Biura Prokuratora Generalnego Ukrainy

Portal „Warcrimes.gov.ua" zdecydowanie nastawiony jest na zbieranie informacji, która jest następnie procesowo weryfikowana. Poza pokazaną powyżej na rys. 18, nieaktualną mapą nie publikuje on danych o zdarzeniach. Jednakże na Telegramie stosunkowo łatwo znajdziemy wiele kanałów specjalizujących się w publikacji pełnych danych żołnierzy i cywilów zaangażowanych bezpośrednio w zbrodnie lub wspierających rosyjską agresję.

[16] https://warcrimes.gov.ua

Ukraińska strona od początku wojny stara się publikować jak najwięcej informacji o stratach rosyjskich jednocześnie milcząc o stratach własnych. Co pewien czas słyszymy, jednakże z ust, np. prezydenta Ukrainy, że straty po ich stronie także są wysokie. Wiele źródeł internetowych próbuje szacować realne straty i jest to trudne. Mamy do czynienia z dużymi rozrzutami danych podawanych przez obie strony.

Total casualties

Breakdown	Casualties	Time period	Source
Civilians	**7,000–29,125+** killed (est.)[72][note 5]	24 February – 11 October 2022	Ukrainian government
	6,221 killed, **9,371** wounded (conf. minimum, thought higher)	24 February – 9 October 2022	United Nations[73]
Ukrainian forces (ZSU, NGU, SBGS)	**10,000** killed, **30,000** wounded, **7,200** missing (**5,600** captured)	24 February – 3 June 2022	Ukrainian government[74][75][76][77]
	61,207 killed, **49,368** wounded	24 February – 21 September 2022	Russian government[78][79][80]
Ukrainian forces (ZSU)	**≈9,000** killed	24 February – 21 August 2022	Ukrainian government[81]
Russian and allied forces (VSRF, Rosgvardiya, FSB, PMC Wagner, DPR & LPR)	**70,000–80,000** killed and wounded (**20,000** killed)	24 February – 8 August 2022	US estimate[82][83]
	62,870 losses[a]	24 February – 10 October 2022	Ukrainian government[84]
Russian forces (VSRF, Rosgvardiya, FSB)	**7,184** killed (conf. minimum by names)	24 February – 7 October 2022	BBC News Russian & Mediazona[89]
Russian forces (VSRF)	**5,937** killed	24 February – 21 September 2022	Russian government[90]
Donetsk PR forces	**3,272** killed, **13,924** wounded	26 February – 6 October 2022	Donetsk PR[91]
Luhansk PR forces	**500–600** killed	24 February – 5 April 2022	Russian government[92]

Źródło: https://en.wikipedia.org/wiki/Casualties_of_the_Russo-Ukrainian_War.
Rysunek 20. Dane o zagregowanych stratach wojennych wg Wikipedii

Pomimo pewnych nieścisłości i wynikających z wojennej taktyki informacje strony ukraińskiej pozwalają na pewien ogląd sytuacji. W przeciwieństwie do nich rosyjskie dane najczęściej sprawiają wrażenie całkowicie sfabrykowanych.

Dotyczy to nie tylko strat osobowych, ale także, a może przede wszystkim utraconego i zniszczonego sprzętu. Codzienne komunikaty rosyjskiego Ministerstwa Obrony bardzo często informują o zniszczeniu większej liczby zachodniego sprzętu niż oficjalnie przekazano Ukrainie. Przykładem jest komunikat przedstawiony przez rzecznika ministerstwa generała Konaszenkowa, w którym informował on o zniszczeniu 44 baterii Himars.

W styczniu tuż, po informacji o możliwych dostawach czołgów Abrams rosyjski internet z dumą prezentował zdjęcie pierwszego zniszczonego pod Bachmutem amerykańskiego czołgu. Podano nawet, że tego czynu dokonali żołnierze oddziału należącego do tzw. „Grupy Wagnera". Zdjęcie opubliko-

wane w sieci i powielane przez wiele rosyjskich kanałów, rzeczywiście przedstawiało zniszczony czołg Abrams. Jednakże warunki otoczenia zewnętrznego, czyli jasny piasek i znajdujące się w oddali palmy wskazywały raczej na Irak. Ostatecznie zdjęcie zostało zidentyfikowane jako wykonane właśnie w trakcie działań wojennych w Iraku.

Obecnie najpewniejszym źródłem informacji o stratach w sprzęcie wojennym jest bloger kryjący się pod kryptonimem „Oryx".[17] Oprócz strony internetowej ma on także bardzo aktywny profil na Tweeterze. Blog od początku wojny zbiera i weryfikuje oraz geolokalizuje straty sprzętu obu stron.

Źródło: Zasoby własne.

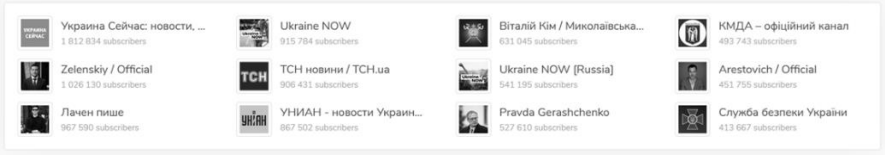
Rysunek 21. Blog informujący o stratach w sprzęcie wojennym „Oryx"

W sprawie strat osobowych jednym z aktywnych źródeł weryfikacji informacji są dziennikarze rosyjskiej sekcji BBC. Dobrym przykładem takiej weryfikacji jest, np. artykuł na temat ofiar ostrzału tymczasowych koszar w Makiejewce.[18] Artykuł ujawnia warsztat pracy dziennikarzy, którzy szukając danych personalnych ofiar sprawdzają media społecznościowe, lokalną prasę, kanały Telegramu i np. strony internetowe należące do Cerkwi. W ten sposób zidentyfikowano 89 ofiar. Jest to liczba daleko niższa od wstępnych szacunków strony ukraińskiej i niektórych rosyjskich korespondentów wojennych, którzy wstępnie szacowali liczbę zabitych na około 400 osób.

[17] https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html
[18] https://www.bbc.com/russian/features-64389529

Tak jak na każdej wojnie część informacji zawdzięczamy dziennikarzom pracującym bezpośrednio w strefie działań wojennych. Jednym z pierwszych dziennikarzy ukraińskich, którzy realizowali projekty medialne związane z wojną był Wołodymyr Zołkin. Jego wywiady z jeńcami rosyjskimi przyniosły w pierwszych tygodniach wojny ogromną ilość informacji na temat zachowań, kondycji czy motywacji żołnierzy rosyjskich. Po stronie ukraińskiej na bieżąco relacjonuje działania SZU także Jurij Butusow, który na bieżąco publikuje swoje krótkie reportaże z frontu, zarówno na kanale w Telegramie, jak i na Youtube.

Ukraińskie kanały informujące o przebiegu działań wojennych częściej informują, niż analizują sytuację. Zwykle robią to w zgodzie z obowiązującymi zasadami informowania społeczeństwa. Nie oznacza to przemilczania lub nieinformowania, ale raczej mają świadomość, iż np. otwarta krytyka może negatywnie wpływać na działania wojenne. Zgoła inaczej sytuacja wygląda z rosyjskimi kanałami tzw. korespondentów wojennych. Patrząc na rankingi popularności kanałów rosyjskich to właśnie korespondenci są najpopularniejszymi dostawcami informacji. Oczywiście inną kwestią jest czy to informacja wiarygodna. Ale wiele ukraińskich i zachodnich źródeł daje sygnały, że doniesienia kanału „Rybar", czy Aleksandra Koca są wnikliwie analizowane i sprawdzane. Przypadek Aleksandra Koca, który jest korespondentem wojennym gazety „Komsomolska Prawda" jest o tyle ciekawy, że w jego jawnie i oczywiście prorosyjskich, antyukraińskich i antyzachodnich publikacjach na Telegramie jest znacznie więcej swoistego umiaru, niż w artykułach publikowanych w prasie. Patrząc w ogólnie na popularność politycznych kanałów Telegramu na Ukrainie i w Rosji zauważymy, że w pierwszym z krajów bardzo popularne są kanały oficjalne, w tym kanał prezydenta Wołodymyra Zeleńskiego oraz agregatory informacji takie jak, np. „Truha". Istnieje też wiele lokalnych kanałów publikujących lub repostujących informacje z większych źródeł.



Źródło: Zasoby własne.

Rysunek 22. Przykłady kanałów publikujących lub repostujących informacje

W rosyjskiej sferze internetowej kanały związane z korespondentami wojennymi znajdują sie bardzo wysoko w skali popularności. Takie kanału jak „Readovka", „Kotsnews", „Shot" , „Archangel Specnaza" czy „Wojennyj obozrewatel" mają setki tysięcy obserwujących i komentujących. Sam „Rybar" dociera ze swoim przekazem do ponad miliona abonentów. Na tych kanałach czytelnik znajdzie wszystko, od głębokiej krytyki taktyki wojennej, narzekania na wyposażenie etc., do analiz na temat konieczności użycia broni masowego rażenia. Krytyka, która się tam pojawia nigdy nie jest krytyką „Specjalnej Wojennej Operacji" i prezydenta Rosji. Praktyka stosowania prawa w Rosji pokazała, że w ostatnich miesiącach znacznie drobniejsze wystąpienia przeciwko wojnie powodowały odpowiedzialność karną[19]. Nie oznacza to, że korespondenci wojenni są wyłączeni całkowicie spod odpowiedzialności. Po każdej kolejnej przegranej bitwie rozpoczyna się szukanie winnych i często to właśnie korespondenci są wskazywani jako jedna z przyczyn, jako ci którzy mówili za wiele.

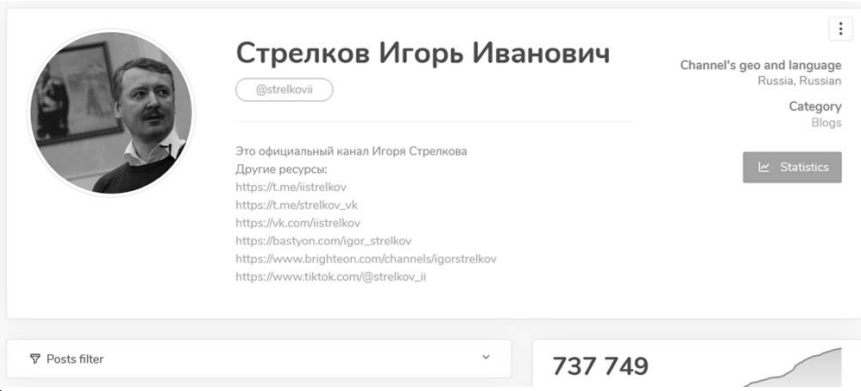
Na tym tle wyróżnia się jeszcze co najmniej jedna postać, a mianowicie Igor Girkin vel. Igor Strełkow. Były oficer FSB, jeden z inicjatorów antyukraińskiej rewolty na Donbasie w 2014 roku. Człowiek poszukiwany przez Trybunał Sprawiedliwości w Hadze za udział w zestrzeleniu malezyjskiego samolotu w 2014 roku [20]. Dzisiaj jest jednym z popularniejszych komentatorów i krytyków sposobu prowadzenia wojny. Oczywiście krytyka nie oznacza postawy antywojennej, wręcz przeciwnie.

Omawiając rosyjską sferę informacyjną warto także odnotować pewien fenomen, mianowicie kanał „General SVR". Już sama nazwa kanału na Telegramie, jak i na Youtube sugeruje, że jest to źródło wiedzy insiderskiej pochodzącej od wysokiego oficera Służby Wniesznej Razwiedki czyli wywiadu rosyjskiego. Kanał działa od 2020 roku, ma wielu oddanych czytelników, słynie z tego, że np. co pewien czas publikuje sensacyjne wiadomości na temat stanu zdrowia Władymira Putina. Na doniesienia tego kanału powoływała się wielokrotnie prasa, tak zachodnia, jak i polska. Dotychczas nic nie wskazuje, aby publikacje „generała" wykraczały poza kompilację materiałów z otwartych źródeł.

---

[19] https://amnesty.org.pl/rosja-nowe-przepisy-karne-by-stlumic-krytyke-wojny-w-ukrainie/

[20] https://www.rynek-lotniczy.pl/wiadomosci/dozywocie-kara-za-tragiczne-zestrzelenie-rejsu-mh17-nad-donbasem-16055.html



Źródło: Zasoby własne.

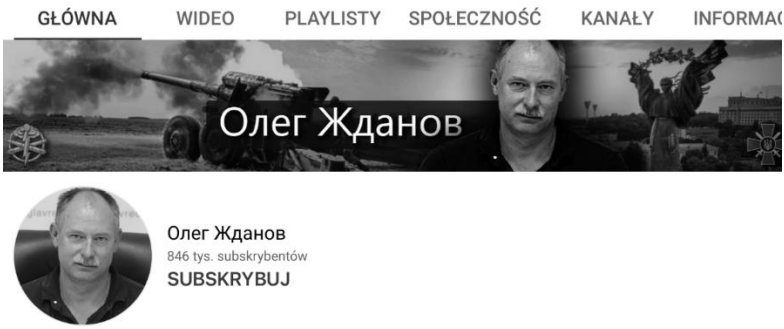
Rysunek 23. Kanał Igora Girkina vel. Igora Strelkowa

Do dzisiaj nie wiadomo, kto stoi za kanałem – zarówno oficjalne rosyjskie śledztwa, jak i dziennikarskie prowadzone przez wiele redakcji nie pozwoliły odpowiedzieć na to pytanie. Doniesienia kanału były wielokrotnie weryfikowane przez np. „Belingcat", zwykle z negatywnym wynikiem. Dlatego ich rekomendacja jest prosta – nie należy traktować go jako źródło informacji[21].

Zamiast podsumowania

Gdzie więc szukać źródeł wiarygodnej informacji o wojnie? Mając świadomość obiektywnych braków źródeł ukraińskich możemy weryfikując informację spokojnie na nich polegać. Jeśli szukamy dobrej i tworzonej na zimno analityki wojennej warto posłuchać codziennych audycji emerytowanego pułkownika SZU Olega Żdanowa. Codziennie bez emocji relacjonuje on sytuacje na froncie i możliwe scenariusze. Audycje dostępne są na Youtube.

[21] https://www.businessinsider.com/who-is-general-svr-telegram-account-seeding-wild-putin-stories-2022-12?IR=T



Źródło: Zasoby własne.

Rysunek 24. Kanał emerytowanego pułkownika SZU Olega Żdanowa

Dobra i ciekawa publicystyka pojawia się także na kanale Dimitrija Gordona. Jego audycja „W gostiach u Gordona" to wywiady z ważnymi i ciekawymi ludźmi. Oczywiście w obecnej sytuacji większość dotyczy sytuacji wojennej. Częstym gościem Gordona, podobnie jak i rosyjskiego opozycyjnego kanału „Popularna Polityka" jest Christo Grozev z Belingcatu.

Z innych niezależnych źródeł informacji z Rosji można polecić „Meduzę", „Bazę", „Nastojaszczie Wremja" i „The Insider". Większość tych rosyjskojęzycznych redakcji nadaje swój przekaz z krajów UE, głownie z Łotwy, a redakcje składają się z dziennikarzy, którzy wyjechali z Rosji.

Jak już wcześniej pisałem nie należy odrzucać także rosyjskich źródeł prowojennych. Zwykle łatwo je zidentyfikować po specyficznej retoryce, ale każdy ich komunikat należy próbować weryfikować w innych źródłach. Niestety nie każda fałszywa informacja jest tak łatwa do zweryfikowania jak wiadomość o zniszczonym czołgu Abrams.

Obecna faza wojny rozgrywa się na naszych oczach głownie dzięki materiałom publikowanym na kanałach Telegramu. Stał się on niekwestionowanym liderem w dostarczaniu informacji. Musimy mieć jednak świadomość, że kanał Telegramu to nie tylko przekaz w jedną stronę. Komentując czy wdając się w dowolną interakcje z innymi użytkownikami ryzykujemy, nie tyle hejtem, co możliwością utraty danych osobowych. Przez wiele ostatnich lat Telegram uchodził za całkowicie bezpieczny komunikator. Dzisiaj, co raz

częściej pojawiają się informacje na temat możliwości deanonimizacji użytkowników Telegramu.[22] Tego typu wiadomości pochodzą zarówno ze źródeł rosyjskich, jak i białoruskich. Mając to na uwadze należy tym bardziej zadbać o swoje bezpieczeństwo w trakcie pracy ze źródłami internetowymi.

Mam świadomość, że rozdział w żaden sposób nie wyczerpał kolejnych wątków. Dynamiczna sytuacja na froncie i wokół powoduje, że niemalże codziennie uzupełniać możemy nowe źródła informacji. W zasadzie, w zależności od zdarzenia pracę należy zaczynać od początku. W tym momencie wojny analityk powinien interesować się nie tylko Ukrainą, Rosją czy Białorusią, ale także Iranem czy szerzej Bliskim Wschodem. W swoim rozdziale chciałem jedynie zasygnalizować część możliwych źródeł i pokazać, że jesteśmy w stanie samodzielnie pozyskiwać wiarygodną informację.

[22] https://tadviser.com/index.php/Product:Telegram_Messenger#Russia__has_learned_to_deanonymize_channel_administrators_in_Telegram

Rozdział 8

O stanowczości opinii biegłego

Maciej SZMIT

STRESZCZENIE: W artykule przedstawiono rozważania odnośnie do zagadnienia stanowczości opinii biegłego w kontekście prawdopodobieństwa i wiarygodności wyników badań oraz pewności jaką w ich wyniku biegły uzyskuje.

Wstęp

Jednym z określeń stosowanych na określenie biegłych sądowych jest, brzmiące nieco przedmiotowo, wyrażenie „narzędzie sądu”[1]. Zasadniczo używa się go, aby zaznaczyć, że biegły pełni nie tylko rolę źródła dowodowego (jako autor opinii) ale bywa też konsultantem organu procesowego, uczestnicząc w czynnościach przez ten organ prowadzonych, na przykład w zabezpieczaniu materiału dowodowego, w przesłuchaniu świadków i stron, w oględzinach czy eksperymentach procesowych[2]. Z drugiej strony takie „przedmiotowe” określenie wskazuje, że biegły jest jedynie organem pomocniczym sądu[3], a więc jego swoboda decyzyjna jest bardzo ograniczona. Określenie przedmiotu i zakresu opinii należy do organu procesowego, natomiast w literaturze i orzecznictwie uznaje się, że w zakres tzw. autonomii biegłego wchodzi wybór metody i zakresu badań specjalistycznych[4].

---

[1] Zob. np. [1].
[2] Zob. np. [2] s. 45.
[3] Zob. np. Wyrok NSA z dnia 04.06.2001 (II SA 1434/00).
[4] por. Wyrok Sądu Najwyższego z 10 maja 1982 r. (II KR 82/82), Postanowienie Izby Karnej Sądu Najwyższego z 25 czerwca 2003 r. (IV KK 8/03), Wyrok Sądu Najwyższego z 7 lutego 1986 r. (IV KR 15/86).

O wyborze metody badania

Poszczególne metody badawcze różnią się między sobą pod względem dokładności i precyzji pomiarów, czułości i swoistości testów diagnostycznych czy powtarzalności i odtwarzalności wyników eksperymentów. W przypadku opiniowania informatycznego konieczność podjęcia decyzji odnośnie do wyboru konkretnego spośród różnych możliwych sposobów działania jest stosunkowo rzadsza niż w przypadku innych dziedzin, niemniej czasami ma miejsce i obejmuje kwestie takie, jak na przykład: tryb zabezpieczenia materiału dowodowego – wykonanie kopii bitowej (ang. aquisition) versus zatrzymanie oryginalnego nośnika (ang. collection), przeprowadzenie badania live versus badania post mortem czy decyzja o wykonaniu badania pełnego versus częściowego (z wykorzystaniem podejścia triage) czy o przeprowadzeniu badań niszczących (np. w przypadku informatyki śledczej decyzji o badaniu urządzenia, ingerencja w które prowadzi do zmiany zawartości pamięci, w tym metadanych) uniemożliwiających powtórzenie badań.

Wybór metody badawczej implikować może również stanowczość wniosków[5], jakie może przedstawić biegły. Na podstawie badania częściowego wartości cech statystycznych próbki nie można – na przykład – w sposób pewny określić punktowo wartości tych samych cech w populacji. Estymacja parametrów zbiorowości generalnej na podstawie wyników badań próby zawsze jest obarczona niepewnością, którą należy oszacować i którą – przy pisaniu opinii, trzeba poprawnie opisać. Jeśli – na przykład – po przebadaniu próbki wnioskowanie statystyczne pozwala na sformułowanie konkretnego wniosku (np. „z prawdopodobieństwem 0,98 nie można odrzucić hipotezy zerowej", albo „iloraz wiarygodności[6] wynosi 1000") to takie właśnie sformułowania powinny znaleźć się w opinii[7].

---

[5] Zob. [2] s. 91 i nast.

[6] ang. Likelihood Ratio, LR.

[7] Warto zauważyć tu różnicę w stosunku do np. konkluzji z audytu systemów zarządzania, gdzie na podstawie badań częściowych formułuje się wniosek w postaci quasi kategorycznej: „organizacja stosuje System Zarządzania (…) i spełnia wymagania normy (…)", choć o ile samo istnienie (mniej lub bardziej kompletnego i dojrzałego) systemu zarządzania można stwierdzić w sposób pewny, o tyle – częściowe przecież – badania audytowe formalnie pozwalałyby tylko na konstatację, że badane wyrywkowo elementy tego systemu działały zgodnie z wymaganiami normy, nie zaś, że cały system spełnia jej wymagania.

W praktyce często przyjmuje się, że odpowiedni sposób doboru próbki, w połączeniu z odpowiednio dużym jej rozmiarem, pozwala na uzyskanie odpowiedzi o tak wysokim prawdopodobieństwie, że osoba formułująca wniosek uzyskuje subiektywną (moralną) pewność odnośnie do jakiejś interpretacji otrzymanego wyniku (na przykład, że należy przyjąć hipotezę zerową albo że materiał kwestionowany jest identyczny z porównawczym). Niewątpliwie w takich wypadkach biegły nie może wprowadzać w błąd organu procesowego. Jak pisze Kazimierz Jaegermann ([5] s. 132–133) – „Język konkluzji opiniodawczej nie może stwarzać żadnych językowych wątpliwości co do tego, czy biegły *wie*, czy też, że biegły jest tylko *pewien*". Niewątpliwie również biegły może i powinien wyjaśnić organowi procesowemu, czym są iloraz wiarygodności czy współczynnik ufności in abstracto.

Pewność a stanowczość

Powstaje pytanie, czy jest rolą biegłego dzielenie się swoimi przekonaniami odnośnie do pewności subiektywnej z organem procesowym? Innymi słowy: czy i kiedy biegły może na podstawie swojej subiektywnej pewności wydać opinię stanowczą w sytuacji, gdy nie ma pewności fizycznej? W praktyce opiniodawczej niejednokrotnie można spotkać się z sytuacją, w której sąd – a częściej strona – naciska na biegłego, aby ten wydał opinię stanowczą. Biorąc pod uwagę, że w sprawach karnych biegły często bywa powoływany na etapie postępowania przygotowawczego, w oparciu o arbitralną i ostateczną decyzję organu je prowadzącego, nie można nie zauważyć groźby preferowania zlecania opinii biegłym mającym skłonność do wydawania opinii stanowczych. Istnieją też biegli gotowi takie opinie wydawać, nie zagłębiając się w subtelności rozważań o pewności moralnej i fizycznej (bezwzględnej)[8], w literaturze przedmiotu można też spotkać stanowiska usprawiedliwiające – przynajmniej po części – taki stan rzeczy i postulaty bardzo szeroko rozumianej współpracy biegłych ze śledczymi. Łatwo można sobie wyobrazić ryzyko związane z takimi tendencjami. Z drugiej strony oczywiście zdarzają się sytuacje, w których brak pewności fizycznej nie przeszkadza w żaden sposób

[8] O pojęciach pewności moralnej i fizycznej zob. np. [10].

w wydaniu opinii stanowczej[9], podobnie jak ma to miejsce w większości sytuacji życiowych.

Jak się wydaje, niemożliwe jest postawienie ścisłej granicy, od której można byłoby wydawać opinie stanowcze. W literaturze przedmiotu można znaleźć różne propozycje słownych opisów ilorazu prawdopodobieństwa. Na przykład w pracy [11] zamieszczone są następujące wartości ilorazu wiarygodności dla badań DNA[10]:

1–10 – dowód słaby;
10–100 – dowód średni;
100–1000 – dowód mocny;
powyżej 1000 – dowód bardzo mocny.

W pracy [12] przytoczona jest tabela, jak poniżej, zaczerpnięta z pracy [13], zawierająca następujące propozycje interpretacji:

Tabela 1. Tabela 2. Słowna interpretacja wartości ilorazu wiarygodności wg. J. Buckletona.

Wartość LR	ocena słowna	kierunek wnioskowania
1 000 000 + 100000 10000 1000 100 10	dowód ekstremalnie mocny dowód bardzo mocny dowód mocny dowód dobry dowód średni dowód słaby	wsparcie hipotezy oskarżenia (ślad pochodzi od podejrzanego/oskarżonego)
1	nierozstrzygający	brak wsparcia którejkolwiek z hipotez
0,1 0,01 0,001	dowód słaby dowód średni dowód dobry	wsparcie hipotezy obrony (ślad nie pochodzi od podejrzanego/oskarżonego)

[9] Choć może wydawać się to nieprawdopodobne, w pewnej sprawie dotyczącej fałszowania (licznych) dokumentów księgowych zapisanych jako pliki dyskowe na dysku twardym oskarżony postanowił przyjąć linię obrony opartą o spostrzeżenie, że zarówno podczas zapisywania, jak i podczas przechowywania plików na dyskach może dochodzić do uszkodzenia zapisów, w tym może się zdarzyć, że w miejsce zapisów prawidłowych w plikach pojawiają się zapisy interpretowane jako losowe znaki, w szczególności więc istnieje pewne niezerowe prawdopodobieństwo, że losowo pojawiły się zapisy sensowne ale nie odpowiadające rzeczywistym zdarzeniom ekonomicznym, ergo: istnieje możliwość, że dokumentów oskarżony nie sfałszował, ale że fałszywe zapisy pojawiły się przypadkiem. Choć prawdopodobieństwo takiego splotu okoliczności jest oczywiście skrajnie małe, jednak wątpliwości należy tłumaczyć na korzyść oskarżonego itd. Mimo woli nasuwa się tu analogia do znanego z popkultury twierdzenia o nieskończonej liczbie małp (por. np. https://pl.wikipedia.org/wiki/Twierdzenie_o_niesko%C5%84czonej_liczbie_ma%C5%82p).

[10] Zob. [11], s. 533.

0,0001	dowód mocny	
0,00001	dowód bardzo mocny	
0,000001	dowód ekstremalnie mocny	

Źródło: [13] s. 50 za [13] s. 169.

Już sam fakt funkcjonowania w literaturze przedmiotu różnych przyporządkowań wartości ilorazu wiarygodności do poszczególnych sformułowań musi budzić obawy, co do użycia poszczególnych werbalizacji (konieczne byłoby bowiem objaśnienie organowi procesowemu, którego odwzorowania zwolennikiem jest biegły).
Dodatkowym problemem, o którym należy pamiętać przy próbie interpretacji procesowego znaczenia wyników badań, są błędy poznawcze czy logiczne, które może popełnić osoba podejmująca się takiej interpretacji, nawet jeśli będzie niż biegły, który wykonał wszystkie czynności badawcze prawidłowo (np. błędy zaniedbywania miarodajności, ang. *base rate neglect* bądź *base rate fallacy* czy błąd odwracania prawdopodobieństw, ang. *invers fallacy* - znany jako „sofizmat prokuratora"), które będą prowadzić do nieuzasadnionego zwiększania lub zmniejszania kategoryczności wniosków (Zob. np. [6] s. 26 i nast.; [7] passim; [8], s. 101 i nast., [13]). W szczególności, w przypadku biegłego może to mieć miejsce w sytuacji, gdy – zgodnie ze zmianami 198 §1 KPK wprowadzonymi nowelizacją z 19 lipca 2019 r. – domyślnie biegły wydaje opinię bez dostępu do akt (por. np. [4]). Powstaje więc pytanie: po co biegły brać na siebie takie ryzyko, szczególnie że żaden przepis prawa nie zmusza go do wydawania opinii stanowczych ani do interpretowania wyników badania w kontekście toczącego się sporu sądowego? Oczywiście biegły musi wyjaśnić, w sposób zrozumiały dla osób nie dysponujących wiadomościami specjalnymi, znaczenie otrzymanych wyników, niemniej – jak się wydaje – powinien powstrzymać się od komentowania tego, czy prawdopodobieństwo „jeden na milion" to – w kontekście danej sprawy – dużo czy mało.

Zakończenie

W opiniowaniu sądowo-informatycznym stosunkowo często można w konkluzji umieszczać zdania pewne, np. „na dysku znajduje się plik zawierający zapisy, o których mowa w pytaniu", „komputer jest uszkodzony" itd., niepozostawiające wątpliwości co do bezwzględnego charakteru stwierdzonych faktów. Zaniżanie w takiej sytuacji kategoryczności wniosków w oparciu

o antycypację możliwości popełnienia błędu przez osobę formułującą wniosek byłoby podówczas oczywiście metodologicznie błędne, czy wręcz nieuczciwe (choć może ono mieć, niestety, uzasadnienie praktyczne, szczególnie wobec obaw związanych z wprowadzeniem przepisów o opinii nieumyślnie fałszywej[11]). Istnieje jednak szereg sytuacji, w których nie można osiągnąć wysokiego stopnia pewności. W szczególności na problemy takie biegli często napotykają w postępowaniach cywilnych, gdzie przedmiotem sporu bywa stopień zaawansowania realizacji projektu informatycznego czy ocena, jaka część wymogów została spełniona. W takich sytuacjach należałoby zalecić biegłym raczej asertywność i rezygnację z – nadmiernej skłonności do arbitralnego (a często źle metodologicznie uwarunkowanego) stanowczego formułowania zbyt daleko idących wniosków.

Bibliografia

[1]. Agnieszka Rybak: Czy biegli są biegli? „Rzeczpospolita" 17.09.2011 https://www.rp.pl/zawody-prawnicze/art14253211-czy-biegli-sa-biegli.

[2]. Szmit M.: Wybrane zagadnienia opiniowania sądowo-informatycznego, Wydanie II, rozszerzone i uzupełnione, Polskie Towarzystwo Informatyczne, Warszawa 2014.

[3]. Józef Gurgul: O wadliwości opinii biegłego w procesie karnym, „Prokuratura i Prawo", 4/2015.

[4]. Bartłomiej Rasała: Udostępnianie materiałów z akt postępowania przygotowawczego biegłym – geneza oraz praktyczne skutki zmian wprowadzonych ustawą z dnia 19 lipca 2019 r., „Studia Iuridica Toruniensia", tom XXIX.

[5]. K. Jaegermann: Opiniowanie sądowo-lekarskie. (Eseje o teorii), Wydawnictwo prawnicze, Warszawa 1991.

[6]. J. Wójcikiewicz: Temida nad mikroskopem, TNOiK, Toruń 2009.

[7]. J. Kunz: Błąd w opiniach sądowo-lekarskich w sprawach przestępstw przeciwko zdrowiu i życiu, Katedra Medycyny Sądowej Collegium Medicum UJ, Kraków 1999.

[11] Zob. np. [9].

[8]. Marek Z.: Błąd medyczny, Wydawnictwo Medyczne, Kraków 2007

[9]. Maciej Szmit, Jeszcze o statusie i odpowiedzialności biegłego, „Rocznik Bezpieczeństwa Morskiego", 2022, nr 2021.

[10]. Grocholewski Z.: Pewność moralna jako klucz do lektury norm procesowyc, „Ius Matrimoniale" 3 (9), 1988.

[11]. E. Gruza, M. Goc, J. Moszczyński: Kryminalistyka - czyli rzecz o metodach śledczych, WAiP, Warszawa 2008.

[12]. Kartasińska E.: Identyfikacja osobnicza na przykładzie opinii kompleksowej z zakresu badań daktyloskopijnych i genetycznych, Praca doktorska napisana pod kierunkiem prof. dr. hab. Tadeusza Tomaszewskiego, Uniwersytet Warszawski 2016.

[13]. Buckleton J., Triggs C. M., Walsh S. J.: Forensic DNA Evidence Interpretation, CRC Press, Boca Raton, 2005.

[14]. Wójtowicz A.: Jakie wnioski uznajemy za racjonalne? Wpływ prawdopodobieństwa apriorycznego na prawdopodobieństwo aposterioryczne, „Decyzje nr 29, 2018, DOI: 10.7206/DEC.1733.

Rozdział 9

Forensic analysis of flash memory using X-RAY and Logic Analyser

Sasha SHEREMETOV, Igor LOSKUTOV, Michal GMUREK [1]

SUMMARY: In this article we discover current state of digital forensics from memory chips, limitations and problems. We propose novel technologies for memory chip pinout analysis that help to address modern digital forensic challenges.

KEYWORDS: NAND memory, flash memory, chip-off data recovery, digital forensics, IoT, signal capture and analysis.

Introduction

The digital evidence in modern world has become one of the central parts of any investigation. People leave more and more traces in the virtual world online and offline. Devices and services tend to collect more statistical and user's data every hardware generation. The diversity of personal, portable, embedded, network and other digital devices that become an object of investigation, has drastically increased in the recent years, due to skyrocketing progress in the chip industry.

On the other hand, digital forensics is facing more challenges every year. As a result, it is far behind the market.

Listed below are the key issues:

- It's not just computer/mobile forensics any more, but digital forensics of everything
- The digital evolution is morphing uncontrollably
- Hardware vendors are rarely cooperating
- Modern hardware is multi-layered, so there is more than one technology involved

[1] Rusolut sp.z o.o., Warsaw, Poland

- Reverse engineering is by far one of the very few solutions

Because of the problems above, tons of evidence missed or ignored.[Fig.1]

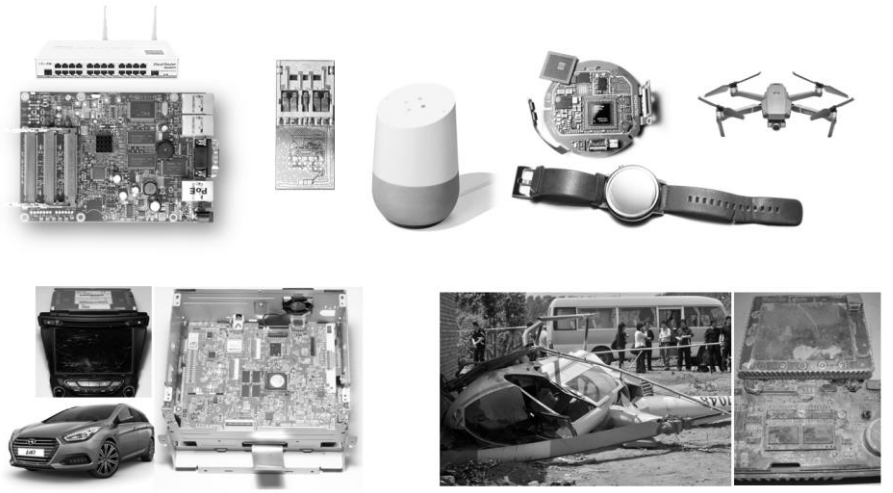


Figure 1. Possible sources of digital evidence that have flash memory onboard

Since most of the portable devices are based on solid state media, the flash memory is a main storage type. There are various interfaces and protocols, such as SPI, I2C, CFI, NAND. The NAND flash memory has become a standard on the market with capacities of more than 8-16MB per chip.

Current state

There are multiple levels when it comes to data extraction from flash memory based devices[1]:

- Logical acquisition of files
- Logical acquisition of file system/device image
- Physical acquisition of memory dump

By the physical connection and further data extraction all acquisition methods can be split into:

- connection via standard interface if exists
- connection via JTAG/UART/service port
- ISP connection directly to the memory chip with further physical image extraction.

- Chip-off with further physical image extraction out of memory chip.

3. Scope of problem

Many modern flash based devices do not have an interface that allows to extract the physical image of device, and in many cases even logical image extraction is problematic. Some of them do not have external interface at all (IoT, embedded devices, etc.).
The service protocols such as JTAG or UART allow to connect to device's controller. It is possible to read the content of the memory through controller, but it involves reverse engineering of controller's FW. It is practically ineffective, especially if device is not supported by any of the commercial digital forensic tools.
The data extraction through ISP method from the memory chip is possible, especially, in case of usage of eMMC chips[2]. The method requires to know the pinout/functional assignment of the chip's pins and the test pads/tracks on PCB where they are connected. It is not documented by manufacturer (even if it is, the schematics are not available for digital forensic specialist), however there are many pinouts available in the digital forensics community as well as in commercial data extraction tools. Hence, when it comes to the smartphones, it is relatively easy to find ISP pinout for the most popular devices. However, if device is not as common as a popular smartphone, any information about its schematics or pinout is hardly available.
When it comes to embedded devices such as microSD cards, damaged eMMC chips[3] and other so called "monolithic devices", the situation with image extraction is even worse, since only few commercial tools provide proprietary databases with pinouts, e.g. Visual NAND Reconstructor.

4. Proposed solution

The proposed solution is to find pinout and get access to the flash memory (ISP or chip-off) with the help of XRAY and logic analyser for further physical image extraction. The following questions have to be answered:

- where the power inputs of the chip are?
- where the control signals are?
- where the data signal lines are?

Typical interface of the flash NAND is represented on Fig.2

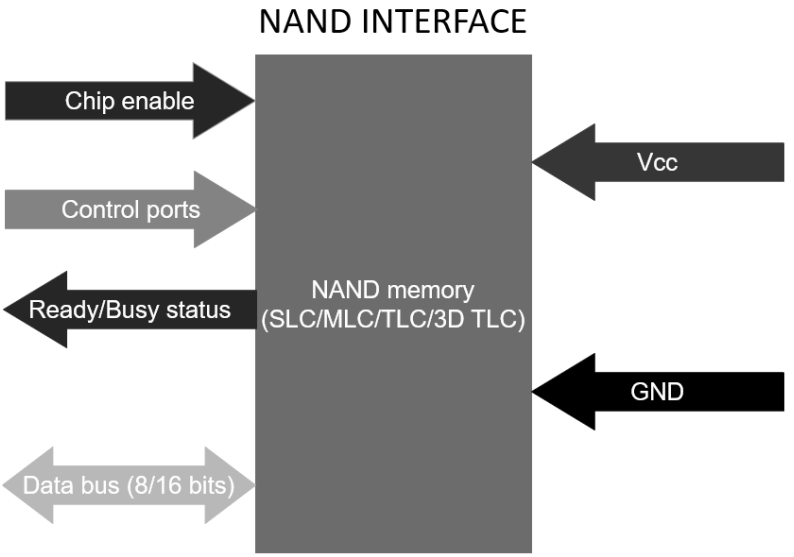


Figure 2. NAND flash interface and its signals

The Vcc and GND lines are power inputs. The Ready/Busy, Chip enable, Control ports are all comprise a group of control signals. The Data bus is 8-bit (rarely 16-bit) bidirectional bus where data flows in and out of the memory chip. These are signals that have to be precisely determined for connection to the reader.[Fig.3]

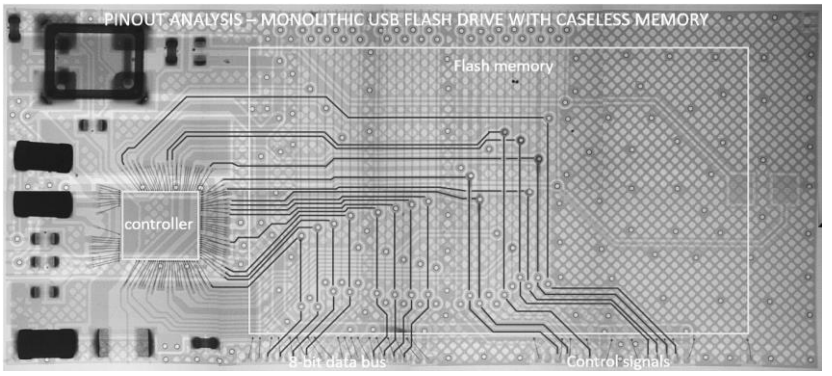


Figure 3. Embedded flash memory pinout analysis using XRAY

The process involves tracing wire bonding connections of the memory to flash controller's tracks on the PCB, with further detailed analysis of each group and signals within the group. Once pinout is found it can be also verified with logic analyser or tested directly in the reader.[Fig.4]. The method is somewhat universal and can be applied to all major NAND memory vendors, such as Micron/Intel, Sandisk/Toshiba, Hynix, Samsung.

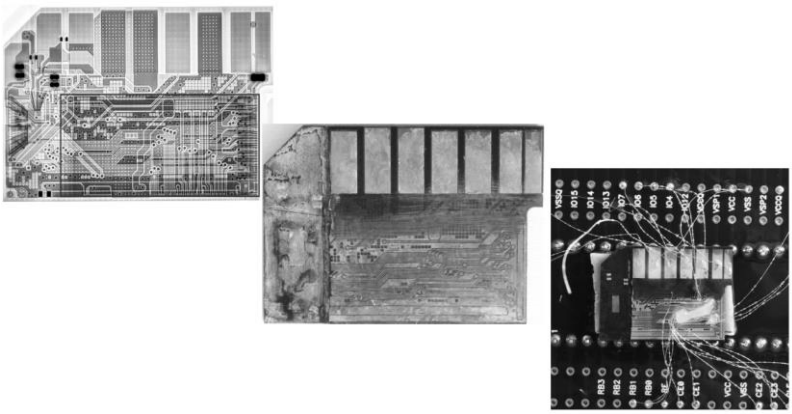


Figure 4. Device being analyzed and then wired up for reading

The technology of device analysis using XRAY is based on the statistical and empirical knowledges gained on practical analysis of a priori known devices and their pinouts. The process is accumulative - the more devices get analysed the easier it gets to analyse new device. It is also a limiting factor. If the newly released memory has new topology of wire bonding, it is hard to recognize it, until it was proven by alternative method, such as logic analyser.
Besides flash memory pinout identification, XRAY analysis can also be used for other digital forensic purposes[Fig.5]:

- Structural analysis of device
- Damage assessment
- PCB analysis

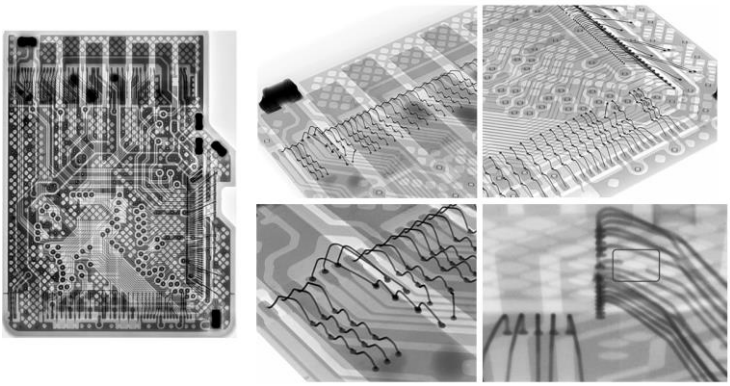


Figure 5. Device analysis using high resolution XRAY

The second approach to pinout analysis of the flash memory is, essentially, the "man-in-the-middle" attack on the data transfer channel with signal capturing using logic analyser. Unlike with XRAY analysis, device has to be at least partially functional, so controller can send commands. The Logic analyser should have at least 16-channel or better 32-channel.[Fig.6]

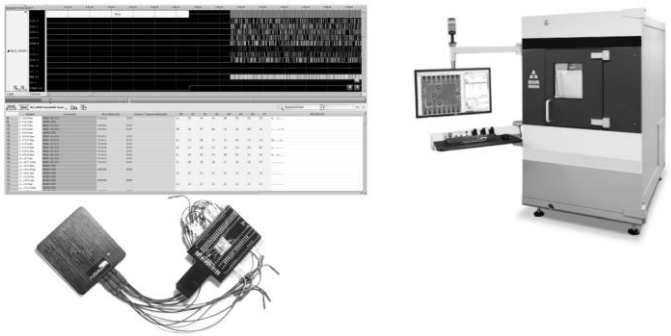


Figure 6. Logic analyser and XRAY machine

The test pads of flash device have to be soldered to the adapter and connected to logic analyser for signal capturing, while the interface of device (if exist) has to be connected to the system and powered up. Inside the logic analyser's software, the trigger must be set on one of the lines in order to start signal

capture by the rising/falling edge. Once the digital waveform is captured, signals have to be separated into two groups - databus and control, and then analysed separately.
The basic knowledge of NAND protocol and its commands is required in order to be able to recognize which signal is what. [Fig 7]

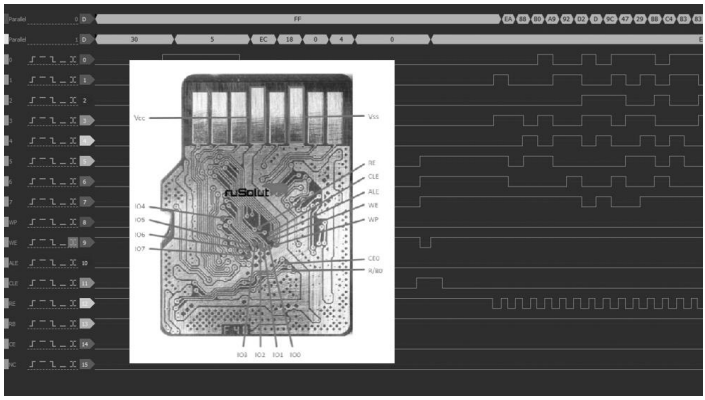


Figure 7. Wave forms of captured signals and final pinout of chip

When pinout is found, the only way to test it is to try to read something out of memory chip [4]. As a quick test, Read ID command "90h" of NAND protocol may be issued. When proper pinout is determined, memory chip should be properly soldered/connected to one of adapters[5] for further physical image extraction.

Conclusion.

These two techniques are paramount when it comes to analysis of non-standard devices with embedded memory or memory chip with unknown package. In many cases they both have to be used, especially if the wire bonding inside the memory chip is new. Sometimes using just one it is possible to find full pinout of the memory and successfully extract physical image for further processing and evidence analysis.

References

1. NISTIR 8354-DRAFT. Digital Investigation Techniques: A NIST Scientific Foundation Review https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354-draft.pdf
2. JESD84-A441 Standard https://www.jedec.org/document_search?search_api_views_fulltext=jesd84-a441
3. A. Fukami, S. Sheremetov, F. Regazzoni, Z. Geradts and C. De Laat, "Experimental Evaluation of e.MMC Data Recovery," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2074-2083, 2022, doi: 10.1109/TIFS.2022.3176187. https://ieeexplore.ieee.org/document/9777707
4. Reading dumps from chips. Article on www.rusolut.com https://support.rusolut.com/portal/en/kb/articles/read-chip
5. D. Pawlaszczyk, J. Friese, C. Hummert, “"Alexa, tell me …" - A forensic examination of the Amazon Echo Dot 3 rd Generation,” International Journal of Computer Sciences and Engineering, Vol.7, Issue.11, pp.20-29, 2019. https://www.ijcseonline.org/full_paper_view.php?paper_id=4939
5. A. Fukami, S. Ghose, Y.Luo, Y. Cai, O.Mutlu “Improving the reliability of chip-off forensic analysis of NAND flash memory devices”, in Przestepczosc Teleinformatyczna 2018, ISSN 1898-3189

Rozdział 10

Działania w cyberprzestrzeni podczas konfliktów hybrydowych – wnioski z wojny na Ukrainie

Jakub SYTA[1]

STRESZCZENIE: W niniejszym artykule przeglądowym przedstawiono wybrane sposoby wykorzystywania technologii informatycznych, które można było zaobserwować podczas wojny Rosji z Ukrainą w 2022 roku. Analiza zdarzeń pozwala na wysnucie wniosków dotyczących skuteczności różnych działań mających miejsce w cyberprzestrzeni, co może być istotne również w przyszłych konfliktach. Wnioski dotyczą zapewnienia niezakłóconej komunikacji, cyberataków niszczących fizyczne elementy infrastruktury, wykorzystywania telefonów komórkowych, skuteczności działań OSINT a także skuteczności działań dezinformacyjnych i propagandowych.

SŁOWA KLUCZOWE: cyberbezpieczeństwo, konflikt hybrydowy, Ukraina.

Wstęp

Wojna Rosji w Ukrainą rozpoczęta 24 lutego 2022 mimo wcześniejszych przewidywań nie obejmowała zmasowanych cyberataków na usługi kluczowe. Ich paraliż związany był przede wszystkim z bardzo brutalnym oddziaływaniem kinetycznym, zresztą wymierzonym bardzo często w ludność cywilną. Można jednak było zidentyfikować działania prowadzone w domenie informacyjnej i informatycznej – zarówno w zakresie systemów IT (information technology) jak i OT (operations technology).

Niniejsza praca ma na celu wskazanie wybranych zjawisk, które zdaniem Autora mogą być szczególnie istotne w przyszłości. Praca pisana jest w trakcie trwającej wojny, kiedy nie znane są jeszcze jej dalsze losy, ani rzeczywiste skutki opisywanych zdarzeń. Przypomina zdarzenia wykonywane

[1] Dr inż., e-mail: p.dela@amw.gdynia.pl; p.dela@akademiakaliska.edu.pl; ORCID: https://orcid.org/0000-0003-3643-3759

zarówno przez agresora jak i obrońców Ukrainy i ich sprzymierzeńców. Ze względu na opisywanie zjawisk, które zachodzą na bieżąco, praca nie jest jeszcze w stanie bazować na innych źródłach niż doniesienia prasowe.

Przegląd literatury

Wraz z upływającymi kolejnymi miesiącami wojny pojawiają się kolejne opracowania pokazujące konflikt z perspektywy działań realizowanych w cyberprzestrzeni. Wojna na Ukrainie bywa niekiedy nazywana „pierwszą cyberwojną" gdyż, jak pokazano w niniejszym artykule, ilość działań prowadzonych w cyberprzestrzeni jest znaczna. Autor szczególnie chciałby jednak podkreślić hybrydowy charakter wojny. Jest ona prowadzona nie tylko z wykorzystaniem regularnych sił zbrojnych, sił specjalnych i najemników ale są prowadzone działania psychologiczne wymierzone w mieszkańców Ukrainy, w ludność Rosji, ale również w mieszkańców państw niezgadzających się z polityką Kremla. Widoczne są działania prowadzone w obszarze dyplomacji, bardzo znaczną rolę odgrywa szantaż ekonomiczny[2]. Cyberataki oraz działalność w obszarze dezinformacji stanowią więc jedynie część znacznie szerszej całości. Tym samym raczej je należy postrzegać jako element uzupełniający[3].

Pierwsza interesująca publikacja dotycząca nadchodzących - nowych zjawisk w ramach konfliktu RU-UA pojawiła się jeszcze przed rozpoczęciem

---

[2] Štrucl D., Russian aggression on Ukraine: cyber operations and the influence of cyberspace on modern warfare. Contemporary Military Challenges 2022(2):103-123 2022. DOI: 10.33179/BSV.99.SVI.11.CMC.24.2.6 https://www.researchgate.net/publication/361569176_russian_aggression_on_ukraine_cyber_operations_and_the_influence_of_cyberspace_on_modern_warfare

[3] Maschmeyer L., Cavelty M. D., Goodbye Cyberwar: Ukraine as Reality Check, Policy Perspectives Vol. 10/3, May 2022 Policy Perspectives Vol. 10/3, May 2022 https://doi.org/10.3929/ethz-b-000549252 https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/549252/2/PP10-3_2022-EN.pdf

działań wojennych. Wykorzystywanie szkodliwego oprogramowania typu wiper w niespotykanej wcześniej ilości[4,5] wskazywało, że Rosja bardzo rozwinęła swoje zdolności techniczne. Późniejsza działalność Rosjan w cyberprzestrzeni nie dotyczyła jednak wyłącznie przełamywania zabezpieczeń. Dostępne opracowania wskazują na znaczną koncentrację działań w sferze informacyjnej[6,7] a także znaczne zaangażowanie aktywistów, którzy wykorzystują swoje umiejętności techniczne do atakowania wrogów[8].

Ponad rok po rozpoczęciu wojny widać, że konflikt ten, jest inny niż dotychczasowe[9]. Wymaga tym samym szczegółowych analiz by rozpoznać skuteczność poszczególnych działań, poznać ich ograniczenia a także przygotować zdolności defensywne jak również ofensywne w wybranych obszarach[10].

Obserwacje

Atak na Viasat oraz konieczność zapewnienia pewnej komunikacji

Viasat to nazwa zarejestrowanej w USA firmy świadczącej usługi internetu satelitarnego. Wśród jej klientów znajdowały się w lutym 2022 siły

---

[4] Destructive malware targeting Ukrainian organizations, Microsoft 2021 https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[5] Ukraina 2022 na cyfrowym froncie. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzenie, 2023 https://www.wojsko-polskie.pl/woc/u/4c/d1/4cd11eaf-3567-405d-994f-f88b6b45ad0b/ukraina_2022_na_cyfrowym_froncie.pdf

[6] Kowalska-Sendek M., Ukraina na cybernetycznym froncie, Polska Zbrojna 2022 https://polska-zbrojna.pl/home/articleshow/36629?t=Ukraina-na-cybernetycznym-froncie

[7] Krzykowski P. Konsekwencje wojny na Ukrainie w wymiarze żywnościowym, ekonomicznym i energetycznym, Roczniki Nauk Społecznych T.15(50) nr 4, Akademia Sztuki Wojennej 2022 https://ojs.tnkul.pl/index.php/rns/article/view/17785/16759

[8] Vicens A., A year of cyberwar' with Russia: An inside look from a top Ukrainian cybersecurity officialm Cyberscoop 2023 https://cyberscoop.com/victor-zhora-ukraine-russia-cyberwar-one-year/

[9] Fog of War. How the Ukraine Conflict Transformed the Cyber Threat Landscape. Mandiant 2023 https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

[10] Drążkiewicz A., Lekcja dla nas, poznajemy techniki przeciwnika. Gen. Molenda o działaniach Rosji w cyberprzestrzeni. Polskie Radio 24. 2022 https://polskieradio24.pl/130/4437/artykul/3088678,lekcja-dla-nas-poznajemy-techniki-przeciwnika-gen-molenda-o-dzialaniach-rosji-w-cyberprzestrzeni

zbrojne Ukrainy[11]. 24 lutego 2022 około godziny 5 rano, w momencie w którym prezydent Rosji Władimir Putin ogłosił atak na Ukrainę, przeprowadzono niszczycielski cyberatak na tysiące klientów firmy Viasat. Wymazał on oprogramowanie na klienckich modemach uniemożliwiając tym samym ich pracę. W rezultacie w znacznej mierze utrudniono skoordynowane prowadzenie obrony Ukrainy w pierwszych chwilach wojny[12]. Równocześnie tysiące przedsiębiorstw i osób prywatnych znajdujących się w krajach nieuczestniczących w konflikcie stało się ofiarami agresji cyberprzestępców pracujących dla rosyjskiego wojska[13]. Paraliż trwał kilka miesięcy, a koszty związane z dystrybucją tysięcy modemów oraz przerwanej pracy musiała pokryć prywatna firma.

Z tego cyberataku należy wysnuć bardzo istotne wnioski. Pokazał on, że poleganie przez istotne organizacje jedynie na jednym dostawcy Internetu jest niebezpieczne. Potrzebne jest zapewnienie stałej komunikacji wykorzystując zróżnicowane technologie dostarczane przez zróżnicowanych dostawców. Warto przy tym nadmienić, że po apelu obrońców Ukrainy o pomoc i dostarczenie internetu satelitarnego, osoby prywatne i organizacje dostarczyły tysiące zestawów Starlink a sama firma w trybie ekspresowym uruchomiła usługę w kraju[14]. W rezultacie kilka dni później rozpoczęły się zaawansowane ataki mające na celu zniszczenie i tego sposobu komunikacji satelitarnej. Ekspertom cyberbezpieczeństwa Starlink udało się jednak wyjść z tego obronną ręką[15].

---

[11] Corera G., Russia hacked Ukrainian satellite communications, officials believe, BBC 2022 https://www.bbc.com/news/technology-60796079

[12] Satter R., Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official, Reuters 2022 https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/

[13] Haertle A., Tysiące terminali internetu satelitarnego poważnie uszkodzonych w dniu ataku na Ukrainę Zaufana Trzecia Strona 2022 https://zaufanatrzeciastrona.pl/post/tysiace-terminali-internetu-satelitarnego-powaznie-uszkodzonych-w-dniu-ataku-na-ukraine/

[14] Olszewski D., Elon Musk udostępnia Starlink na Ukrainie, Computerworld 2022 https://www.computerworld.pl/news/Elon-Musk-udostepnia-Starlink-na-Ukrainie,436628.html

[15] Dunhill J., Pentagon Impressed By StarLink's "Eye-Wateringly" Swift Shut Down Of Russian Cyberattack IFLScience 2022 https://www.iflscience.com/pentagon-impressed-by-starinks-eyewateringly-swift-shut-down-of-russian-cyberattack-63401

Tym bardziej dużym zaskoczeniem były jesienne informacje w których Elon Musk groził wyłączeniem zestawów Starlink na Ukrainie[16]. Mimo, że ostatecznie się z tego wycofał, udowodnił swoim zachowaniem, że sposobów łączności dostarczanych przez prywatne organizacje nie należy traktować jako zaufanych. Tak istotne zagadnienie co najmniej wymaga redundancji. W przypadku potrzeby koordynacji działań, należy rozważyć wykorzystywanie internetu satelitarnego, światłowodowego, radiolinii a nawet łączności realizowanej z wykorzystaniem sieci miedzianych. A także zapewnienia by komunikacja nie bazowała wyłącznie na rozwiązaniach, które mogą z dnia na dzień przestać funkcjonować w wyniku decyzji biznesowej lub wręcz zachcianki.

Cyberataki niszczące fizyczną infrastrukturę

„Wiper" to określenie szkodliwego oprogramowania, które ma na celu trwale zniszczyć funkcjonowanie systemów informatycznych – najlepiej wręcz w sposób fizyczny lub przynajmniej uszkadzając sektory rozruchowe urządzeń, tak by uniemożliwić ich szybkie przeinstalowanie. Mimo, że takie ataki znane są już od wielu lat, to można było zaobserwować jedynie pojedyncze przypadki.

Na kilka tygodni przed inwazją, firma Microsoft wydała pilne ostrzeżenie. Ogłosiła, że udało się zidentyfikować szereg wiperów umieszczonych w różnych kluczowych systemach ukraińskich operatorów usług kluczowych[17]. Szybka reakcja spowodowała, że udało się zaktualizować oprogramowanie i usunąć niebezpieczny kod. Gdyby nie to, wojna mogłaby się potoczyć inaczej. Gdyby w wyniku ataku udało się masowo sparaliżować łączność internetową, zasilanie, dostawy wody. I inne usługi kluczowe Ukraińcom jeszcze trudniej byłoby przeciwstawiać się zmasowanym atakom wroga. Podkreśla to tym samym konieczność zapewnienia jeszcze szerszego monitoringu cyberbezpieczeństwa w zakresie usług kluczowych – w jeszcze większym stopniu wykorzystującym uczenie maszynowe do identyfikacji anomalii. Podkreślić tu należy, że podczas opisywanego w poprzednim rozdziale ataku na Viasat również wykorzystano wipera, co doprowadziło do zniszczenia tej formy łączności na okres wielu miesięcy.

---

[16] Khatsenkova S., Ukraine war: Backlash after Elon Musk says he can no longer fund Starlink satellites, Euronews 2022 https://www.euronews.com/2022/10/14/backlash-after-elon-musk-says-he-can-no-longer-fund-starlink-in-ukraine

[17] Destructive malware targeting Ukrainian organizations, Microsoft 2021 *op. cit.*

Bardzo interesującym i równocześnie istotnych cyberatakiem był atak przeprowadzony na białoruską kolej. Rząd Łukaszenki przystał na oczekiwanie Rosji i udostępnił agresorom swoje terytorium i infrastrukturę do przeprowadzania inwazji. Hakerom z grupy Białoruscy Cyberpartyzanci udało się jednak sparaliżować systemy zrządzające ruchem pociągów i znacząco opóźnić transporty rosyjskich czołgów[18]. Ochrona systemów transportowych i logistycznych przed cyberatakami staje się tym samym jeszcze bardziej potrzebna.

Ostatni z przykładów dotyczy mniej strategicznego obszaru, niemniej również pokazuje niszczycielski potencjał funkcjonalności wbudowanych w systemy IT – Bazując na publikowanych materiałach wydawać się może, że rosyjscy żołnierze, znaczną część energii poświęcali na szabrowanie. Relacje dostępne z Internecie pełne są przykładów sytuacji, gdy zwyczajnie kradli oni różnego rodzaju dobra. Między innymi ukradziono i przetransportowano do Czeczenii wart kilka milionów USD sprzęt rolniczy wyprodukowany przez firmę John Deere. Po tym gdy skradzione kombajny dotarły na miejsce przeznaczenia w Czeczeni, złodzieje zorientowali się, że w sposób zdalny zostały one trwale unieruchomione z wykorzystaniem funkcjonalności tzw. „kill switch"[19]. Smaczku historii dodaje fakt, że moment kradzieży traktorów z wykorzystaniem wojskowej ciężarówki oznaczonej „Z", został podobno nagrany przez kamerę CCTV[20].

Telefony komórkowe w rękach żołnierzy

Wojna spowodowała szereg sankcji, które między innymi skutkowały odcięciem Rosjan od wielu platform społecznościowych. Doprowadziło to do jeszcze większego rozkwitu rodzimego medium społecznościowego - Telegramu. Powszechne wykorzystywanie telefonów komórkowych przez żołnierzy, jak również połączony z tym pęd by zaistnieć w mediach

---

[18] Palczewski Sz. Białoruscy Cyberpartyzanci atakują systemy kolejowe. Utrudniają transport rosyjskich wojsk na Ukrainę, Cybersefence24 2022 https://cyberdefence24.pl/armia-i-sluzby/bialoruscy-cyberpartyzanci-pomagaja-ukrainie-utrudniaja-transport-sil-okupacyjnych-

[19] Roth E., Remote lockouts reportedly stop Russian troops from using stolen Ukrainian farm equipment. The Verge 2022 https://www.theverge.com/2022/5/2/23053944/russian-troops-steal-millions-farm-equipment-ukraine-disabled-remotely-john-deere

[20] Kuśmierek M., Rosjanie nakradli sprzętu rolniczego za 5 mln dolarów. Wywieźli go do Czeczenii i nie potrafią uruchomić Spider's Web 2922 https://spidersweb.pl/2022/05/rosjanie-nakradli-sprzetu-rolniczego-za-5-mln-dolarow-wywiezli-go-do-czeczenii-i-nie-potrafia-uruchomi.html

społecznościowych, doprowadził do wielu patologicznych sytuacji. Szeregi bandytów w rosyjskich mundurach rozpoczęło dokumentowanie dokonywanych przez siebie zbrodni wojennych[21]. Telegram został zalany relacjami z morderstw, gwałtów, tortur… To z kolei w oczywisty sposób wygenerowało potrzebę identyfikacji tych zbrodniarzy.

Oprogramowanie takie jak Clearview[22] uważane jest za bardzo kontrowersyjne. Może być wykorzystywane do identyfikowania demonstrantów i z tego powodu w demokratycznych państwach bywa rzadko wykorzystywane. Jednak konflikt na Ukrainie pokazał, że w pewnych sytuacjach bywa ono bardzo pomocne - oprogramowanie było bowiem wykorzystywane do identyfikacji zbrodniarzy wojennych. Niektórzy z nich nie próbowali nawet kryć swoich wizerunków podczas nagrań i relacji z przeprowadzanych zbrodni wojennych. Niekiedy udawało się jednak rozpoznawać nawet zamaskowanych bandytów po oczach czy tatuażach i w ten sposób docierać do ich rodzin z prawdziwym przekazem o tych „bohaterach", znęcających się nad cywilami.

W odpowiedzi na barbarzyński atak Ukraińcy rozpoczęli z kolei publikację zwłok agresorów w rożnym stopniu rozkładu, tak by napastnicy wiedzieli jaki los czeka ich jeśli nie zaniechają walk. Bardzo często umieszczany materiał ośmieszał poległych, publikując cytaty ze zdobytych wiadomości elektronicznych czy wpisów z mediów społecznościowych lub dokumentując popełnione przez nich grabierze. Identyfikacja znajdowanych zabitych rosyjskich żołnierzy prowadziła do tego, że można było kontaktować się z ich przyjaciółmi i rodzinami[23]. Informowanie o szczegółach śmierci, często bardzo dalekich od chlubnej i bohaterskiej narracji przekazywanej przez rządowe media, musiało mieć znaczny wpływ na ich bliskich.

---

[21] Macias A., UN report details horrifying Ukrainian accounts of rape, torture and executions by Russian troops CNBC 2022 https://www.cnbc.com/2022/10/28/russia-ukraine-war-un-report-details-accounts-of-rape-torture-and-executions.html

[22] Hart R., Clearview AI Fined $9.4 Million In U.K. For Illegal Facial Recognition Database. Forbes 2022 https://www.forbes.com/sites/roberthart/2022/05/23/clearview-ai-fined-94-million-in-uk-for-illegal-facial-recognition-database/

[23] Italiano L., Orecchio-Egresitz H., Ukraine and Russia have both weaponized facial recognition — in very different ways. Insider 2022 https://www.businessinsider.com/ukraine-russia-have-both-weaponized-facial-recognition-2022-3?IR=T

Warto jednocześnie zwrócić uwagę, że do identyfikacji oprawców wykorzystywano również inne źródła. Przypadki protestów przeciwko napaści na Ukrainę nie były w Rosji częste, ale za to każdorazowo były brutalnie tępione. Aresztowane osoby były następnie długo torturowane między innymi na komisariatach milicji[24]. Wykorzystujące dane, które wyciekły z popularnej aplikacji do dowozu żywności udało się zidentyfikować osoby torturujące niektórych z moskiewskich protestantów[25].

Rola OPSEC i PERSEC

Wiele z opisywanych wcześniej działań powiodło się w wyniku prowadzonych działań z zakresu OSINT[26]. Tym samym oznacza to, że ich „bohaterowie" nie zadbali właściwie o ochronę swojej tożsamości lub działań, innymi słowy nie zadbali o OPSEC[27]. Masowe wykorzystywanie mediów społecznościowych bezpośrednio w trakcie działań było jednym z najbardziej charakterystycznych elementów wojny. Prowadziło jednak do zdradzania lokalizacji w której materiał powstawał[28,29], podobnie zresztą jak materiały publikowane przez dziennikarzy[30]. A wykorzystując fałszywe profile na portalach randkowych identyfikowano bieżące miejsce postoju Rosjan[31].

---

[24] Vasilyeva N., Beatings and psychological torture: The fate that awaits Russian dissidents like Marina Ovsyannikova, The Telegraph 2022 https://www.telegraph.co.uk/world-news/2022/03/15/beatings-psychological-torture-fate-awaits-russian-dissidents/

[25] Ashley, How the food delivery app helped Russian women find torturers in the police station. News Rebeat 2022 https://newsrebeat.com/world-news/96916.html

[26] Ang. open source intelligence – sposób gromadzenia informacji bazujący na wykorzystywaniu powszechnie dostępnych danych

[27] Ang. operations security – zapobieganie ujawniania informacji pozwalających na identyfikację prowadzonych działań, w tym ich lokalizację

[28] Stokel-Walker C., Russia and Ukraine are both weaponising mobile phones to track troops, New Scientist 2022 https://www.newscientist.com/article/2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/

[29] Davis B., Speedo-wearing Russian tourist inadvertently reveals location of Putin's artillery in Crimea, Evening Standard 2022 https://www.standard.co.uk/news/uk/russian-tourist-ukraine-war-putin-target-geolocation-crimea-b1020094.html

[30] Ukraine hits Russian Wagner mercenary HQ in east, BBC 2022 https://www.bbc.com/news/world-europe-62547403

[31] Ankel S., Ukrainian hackers created fake profiles of attractive women to trick Russian soldiers into sharing their location, report says. Days later, the base was blown up. Business Insider 2022 https://www.businessinsider.in/tech/news/ukrainian-hackers-created-fake-profiles-of-attractive-women-to-trick-russian-soldiers-into-sharing-their-location-report-says-days-later-the-base-was-blown-up-/articleshow/94009908.cms

Siły Zbrojne Ukrainy bardzo szybko zrozumiały zagrożenia płynące z udostępniania informacji o lokalizacji swoich sił i bardzo głośno apelowały by nie rozpowszechniać informacji o ruchach ich wojsk. Jednocześnie przygotowano aplikacje **eBopor oraz** Diia, dzięki którym cywile mogli na bieżąco zgłaszać lokalizację wojsk agresora[32,33]. Umożliwiło to prowadzenie rozpoznania na zasadach „crowdsourcingu" i ułatwiało skuteczną eliminację przeciwników[34].

Zagadnienie podsłuchiwania rosyjskich telefonów komórkowych nie było szerzej dyskutowane w otwartych źródłach. Nie znane są szczegóły techniczne zastosowanych sposobów przejmowania treści rozmów i przesyłanych informacji. Wiadomo, że pierwotnie wojska rosyjskie zajmując teren Ukrainy niszczyły stacje bazowe. Jednak brak telefonii komórkowej spowodował znaczne zamieszanie w szeregach agresorów i tym samym zaprzestano tej praktyki. Z czasem Ukraińcy rozpoczęli publikowanie przechwyconych rozmów w których żołnierze skarżą się na głód i bałagan czy też otrzymują od rodzin instrukcje co jeszcze mają ukraść[35]. Czy Ukraińcy wykorzystali ataki typu downgrade czy w inny sposób przejmowano rozmowy – nie wiadomo w tym momencie. Nie wiadomo również jaka jest rzeczywista ilość przechwyconych rozmów oraz jaki jeszcze mają charakter. Nie zmienia to faktu, że posiadanie telefonów komórkowych podczas działań zbrojnych stanowi słaby punkt rosyjskiej agresji i jest bardzo dobrze wykorzystywane przez obrońców.

Jednocześnie warto zauważyć, że Ukraińcy często publikowali materiały: filmy, zdjęcia czy wiadomości z komunikatorów, które znajdowały się w telefonach komórkowych poległych rosyjskich żołnierzy. Czy były one pozyskiwane poprzez omijanie zabezpieczeń biometrycznych czy też z wykorzystaniem technik informatyki śledczej – nie wiadomo. Wiadomo jednak, że skala zjawiska jest duża i że prowadzi do identyfikacji coraz to kolejnych

---

[32] Radzewicz Sz., Ukraińcy mają aplikację, przez którą zgłaszają pozycje wojsk rosyjskich. eWróg został użyty już 200 tys. razy Spider's Web 2022 https://spiderweb.pl/2022/03/ewrog-aplikacja-wskazuje-wojska-rosyjskie.html

[33] Druziuk Y., A Citizen-like chatbot allows Ukrainians to report to the government when they spot Russian troops — here's how it works Insider 2022 https://www.businessinsider.com/ukraine-military-e-enemy-telegram-app-2022-4?IR=T

[34] Ukrainians use phone app to spot deadly Russian drone attacks The Guardian 2022 https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo

[35] Russian Soldiers Phone Calls https://www.nytimes.com/interactive/2022/09/28/world/europe/russian-soldiers-phone-calls-ukraine.html

zbrodni wojennych. A braki z zakresie PERSEC[36] wpływają na skuteczność działań wojsk rosyjskich i ich morale.

Dezinformacja i propaganda

Należy się spodziewać, że o sposób prowadzenia dezinformacji w wykonaniu rosyjskich władz i mediów będzie analizowany przez wiele kolejnych lat. Jawne kłamstwa i nielogiczne argumenty były powtarzane masowo szokując zagranicznych odbiorców choć, co dziwne, wydaje się były przez długi czas bezrefleksyjnie przyjmowane przez znaczną część rosyjskiego społeczeństwa. Opornych aresztowano i bito, bierny tłum chłonął informacje z mediów publicznych. Pomagały w tym hasła i symbole. „*Walka z faszyzmem*", „*Wyzwolenie Ukrainy*", słynne „Z" – dookoła tych symboli gromadzili się „rosyjscy patrioci". Wrogów narodu karano za szerzenie dezinformacji o rosyjskich siłach zbrojnych – w tym za nazywanie napaści na Ukrainę „wojną" z nie „operacją specjalną"[37]. Należy podkreślić, że tego typu działalność propagandowa nie była ograniczona tylko do terytorium Rosji. W krajach sąsiadujących bardzo wyraźnie można było obserwować działalność tzw. *pożytecznych idiotów*, którzy znacznie zwiększyli swoją aktywność wraz z wybuchem wojny[38].

W momencie napaści Ukraina również rozpoczęła masową akcję propagandową w mediach społecznościowych. Zbudowano legendę wokół obrony Wyspy Węży ze słynnym cytatem „*Русский военный корабль, иди нахуй*"[39]. W przestrzeni publicznej pojawił się legendarny pilot „Duch Kijowa"[40]. Odważni ukraińscy traktorzyści zyskali międzynarodową sławę, która doprowadziła do tego, że nawet Finlandia w odpowiedzi na rosyjskie

[36] Ang. personal security – bezpieczeństwo osobiste, zapobieganie ujawniania informacji pozwalających na identyfikację

[37] Russia fights back in information war with jail warning, Reuters 2022 https://www.reuters.com/world/europe/russia-introduce-jail-terms-spreading-fake-information-about-army-2022-03-04/

[38] Stodolak S., Zbiór pożytecznych idiotów jest coraz większy. Dlaczego uwierzyli Putinowi? Dziennik Gazeta Prawna 2022 https://www.gazetaprawna.pl/magazyn-na-weekend/artykuly/8413199,pozyteczni-idioci-putina-rosja-stone-kusturica-rourke.html

[39] Battle of Snake Island Русский военный корабль, иди на хуй https://www.youtube.com/watch?v=6_B1m5iNndg

[40] Michalik K., Duch Kijowa - bohater czy miejska legenda?, RMF 2022 https://www.rmf24.pl/raporty/raport-wojna-z-rosja/news-duch-kijowa-bohater-czy-miejska-legenda,nId,5884226#crp_state=1

groźby poinformowała o przemieszczeniu ciągników bliżej granicy[41]. Z drugiej strony bez oporów obśmiewano szabrowników w mundurach kradnących pralki, lodówki, a nawet garnki i klapki. Wielu z tych żołnierzy jednej z najpotężniejszych armii świata udało się potem namierzyć zdobywając z firm przewozowych informacje o nadawcach i paczkach, które przesyłali do swoich domów[42].

Propaganda była prowadzona również w znacznie bardziej aktywny sposób – z wykorzystaniem cyberataków, czyli poprzez tzw. „haktywizm". Pierwsze widoczne działania w tym zakresie miały miejsce tuż przed wojną, gdy zmodyfikowano szereg ukraińskich stron www zamieszczając informację o planowanym ataku na Ukrainę ze strony Polski. Od momentu rozpoczęcia wojny najbardziej widoczne były jednak działania różnych kolektywów haktywistów przeciwdziałających się polityce Federacji Rosyjskiej. Równocześnie z atakiem na Ukrainę rozpoczęły one masowe cyberataki skierowane w kierunku różnorakich rosyjskich podmiotów. Administracja, instytucje finansowe, media, operatorzy usług kluczowych, a nawet prywatne przedsiębiorstwa – wszyscy stali się celem. Hakerzy kilkukrotnie przejęli sygnał telewizyjny rosyjskich państwowych mediów publikują rzeczywiste informacje dotyczące wojny[43]. Przełamali zabezpieczenia kas powodując drukowanie na paragonach informacji o wojnie[44,45], przełamali zabezpieczenia firm prowadzących działalność na Krymie publikując obraz z nich z Internecie[46]

---

41 Finowie wyśmiewają ruchy wojsk rosyjskich przy granicy. Wysyłają swój "specjalny sprzęt", Onet 2022 https://wiadomosci.onet.pl/swiat/finowie-wysmiewaja-ruchy-wojsk-rosyjskich-przy-granicy-pokazuja-traktory/zysdn71

42 Coynash H., Belarusians name Russian soldiers caught on camera sending goods plundered in Ukraine to Russia, Kharkiv Human Rights Protection Group 2022 https://khpg.org/en/1608810358

43 Smith A., Anonymous news – live: Russian TV hacked with Ukraine footage in 'biggest op ever seen'. Yahoo News 2022 https://news.yahoo.com/anonymous-news-live-russian-tv-090008311.html

44 Kotowski A., GhostSec zhakował drukarki w Rosji. Zdalnie drukują informacje o wojnie na Ukrainie. Komputer Świat 2022 https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/ghostsec-zhakowal-drukarki-w-rosji-zdalnie-drukuja-informacje-o-wojnie-na-ukrainie/hrsft0c

45 Mazurkiewicz P., „Putin zabija" na rosyjskich paragonach. Anonymous włamali się do drukarek. Rzeczypospolita 2022 https://cyfrowa.rp.pl/bezpieczenstwo/art35915801-putin-zabija-na-rosyjskich-paragonach-anonymous-wlamali-sie-do-drukarek

46 Hackers play Ukrainian songs https://www.reddit.com/r/UkraineWarVideoReport/comments/wwl1u3/hackers_play_ukrainian_songs_and_watch_the/

a także publikując dokumenty wykradzione z wielu rosyjskich podmiotów. Akcje te zyskiwały bardzo duże poparcie na arenie międzynarodowej.

Agresja Rosji wyzwoliła iskrę, która spowodowała, że nie tylko hakerzy postanowili bronić Ukraińców, ale wręcz wiele innych osób postanowiło w jakiś sposób się zaangażować odpowiadając na apel ukraińskiego Ministra Cyfryzacji Mykhailo Fedorova[47]. Niektórzy wykorzystywali swoje komputery do przeprowadzania ataków DDoS na rosyjskie instytucje korzystając z dedykowanego oprogramowania[48]. Inni prowadzili działania z zakresu OSINT identyfikując zbrodniarzy wojennych. Jeszcze inni zaangażowali się w stworzenie i wykorzystywanie serwisu 1920.io za pośrednictwem którego wysłano miliony wiadomości sms na przypadkowe rosyjskie numery telefonów komórkowych pozyskany przy okazji różnych wycieków[49]. Wiadomości te miały na celu szerzenie prawdziwego obrazu wojny.

Mimo, że działalność kolektywów nie była w widoczny sposób koordynowana, prowadzone działania z pewnością angażowały czas rosyjskich ekspertów ds. cyberbezpieczeństwa oraz krzewiły w społeczeństwie prawdziwie informacje o wojnie. Jednak niektóre z działań, jak kradzież i publikacja danych osobowych rosyjskich żołnierzy i ich współpracowników, publikowanie informacji operatorów usług kluczowych, wewnętrznych informacji z banków czy identyfikowanie biznesowych powiązań rosyjskich oligarchów mogły mieć większy wpływ na losy wojny niż może się to wydawać w pierwszej chwili. Świadomość, że anonimowość żołnierzy przestaje istnieć oraz topniejące w oczach fortuny oligarchów i ich rodzin z pewnością zyskały należytą uwagę.

Kluczowe tutaj okazało się uzyskanie przez Ukraińców międzynarodowej sympatii. Zwykła apatia tłumów, jakże często widoczna w przypadku

---

[47] Szpor G., Gryszczyńska A., Hacking in the (cyber)space. GIS Odyssey Journal 2022 | Vol. 2, no. 1 | 141:152 https://doi.org/10.57599/gisoj.2022.2.1.141 https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-e50da523-a3b5-48f8-91e3-6369a2d8edf1

[48] Anshori M. F., Db1000n Software as Ukraine's Military Utility to Counter Russian Invasion in 2022. Jurnal Pertahanan 8(2):198-210 https://doi.org/10.33172/jp.v8i2.1683 https://www.researchgate.net/publication/363158743_Db1000n_Software_as_Ukraine's_Military_Utility_to_Counter_Russian_Invasion_in_2022

[49] Vail E., 'We are unstoppable': How a team of Polish programmers built a digital tool to evade Russian censorship, The Record 2022 https://therecord.media/we-are-unstoppable-how-a-team-of-polish-programmers-built-a-digital-tool-to-evade-russian-censorship

innych konfliktów, została przezwyciężona przekazami umęczonego prezydenta Wołodymyra Zełenskiego oraz memami ośmieszającymi rosyjskich agresorów. To między innymi przyczyniło się do popularności internetowych zbiórek gromadzących lekarstwa, umundurowanie, kamizelki kuloodporne a nawet drony Bayraktar czy dronów „kamikaze" takich jak amunicja krążąca Warmate... Tego typu działania z zakresu propagandy, wykorzystujące piosenki, memy, wpisy na portalach społecznościowych czy angażowanie celebrytów pozwoliły Ukraińcom osiągnąć jeden z najbardziej istotnych – zdaniem Autora – celów. Społeczność międzynarodowa przestała być obojętna i żywo zainteresowała się szczegółami konfliktu oferując swoją pomoc.

Niespodziewanie negatywnym skutkiem tych działań stało się jednak podniesienie poziomu bezpieczeństwa rosyjskich podmiotów w cyberprzestrzeni. Chcąc nie chcąc systemy rosyjskiej administracji czy przedsiębiorców musiały zostać zaktualizowane. Także znacząco wzrosła świadomość żołnierzy w zakresie OPSEC i PERSEC, choć może dzięki temu równocześnie ograniczona zostanie ilość popełnianych zbrodni wojennych.

Warto jednocześnie podkreślić, że kolektywy hakerów mieszkających na całym świecie mogą być pożyteczne. Powierzenie im realizacji istotnych zadań zdaniem Autora nie będzie rozsądne, lecz w niektórych sytuacjach sam fakt „siania chaosu" może mieć pozytywne skutki.

Wnioski

Napaść Rosji na Ukrainę pokazała jak mogą wyglądać przyszłe konflikty zbrojne. Jakże tragiczna wojna, ze względu na swój charakter i lokalizację, powinna być szczegółowo analizowana. Cyberataki nie odgrywają w trakcie konfliktu szczególnie istotnej roli z punktu wdziania działań ofensywnych. Jednak są w stanie wprowadzać zamęt, wiązać zasoby oraz oddziałują na morale żołnierzy.

Wielka „cyberwojna", której się spodziewano analizując niszczycielską działalność hakerów z Rosji widoczną na przestrzeni wielu ostatnich

lat[50,51] nie miała miejsca. Pojawiają się analizy dlaczego tak się stało[52],[53] i jedna z możliwych odpowiedzi dotyka tego, że Rosja spodziewała się całkowitego zwycięstwa w czasie kilku dni i nie chciała tym samym niszczyć obszarów, które sama będzie potem odbudowywać[5455].

Ucząc się na tej jakże bolesnej lekcji, należy identyfikować te z działań, które pomogą innym krajom przeciwstawiać się napaściom lub możliwie ją utrudniać. Ponieważ Polska de facto stała się krajem frontowym NATO szczególnie powinno nam zależeć na identyfikacji wszystkich skutecznych sposobów obrony granic. Umiejętność prowadzenia skutecznych działań w cyberprzestrzeni jest tym samym kluczową kompetencją, którą należy rozwijać[56].

Bibliografia

1. An interview with Andrew Boyd, director of the CIA's Centre for Cyber Intelligence Risky.biz https://risky.biz/andrewboyd/
2. Ankel S., Ukrainian hackers created fake profiles of attractive women to trick Russian soldiers into sharing their location, report says. Days later, the base was blown up. Business Insider 2022 https://www.businessinsider.in/tech/news/ukrainian-hackers-created-fake-profiles-of-

[50] Baezner M., Robin P., Cyber and Information warfare in the Ukrainian conflict, Center for Security Studies (CSS), ETH Zürich 2018 https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict

[51] Mohee A., Cyber war: The hidden side of the Russian-Ukrainian crisis DOI: 10.31235/osf.io/2agd3 https://www.researchgate.net/publication/358841316_Cyber_war_The_hidden_side_of_the_Russian-Ukrainian_crisis

[52] Gavrila A., Ukraine's great cyberwar that did not happen . Opinion Paper. IEEE 99/2022 https://www.ieee.es/Galerias/fichero/docs_opinion/2022/dieeeo99_2022_adagav_ucrania_eng.pdf

[53] Maschmeyer L., Cavelty M. D., *op. cit.*

[54] An interview with Andrew Boyd, director of the CIA's Centre for Cyber Intelligence Risky.biz https://risky.biz/andrewboyd/

[55] Dziwisz D., Sajduk B., Rosyjska inwazja na Ukrainę a przyszłość cyberwojny – wnioski w rocznicę „specjalnej operacji wojskowej". Gruszczak A. (red.) THE WAR MUST GO ON. Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski. Wydawnictwo Księgarnia Akademicka 2023 43:52 https://doi.org/10.12797/9788381388801.04

[56] Augustyniak Sz., Wystawiliśmy bitną cyber-armię. Wywiad z gen. Karolem Molendą, IT Wiz 2023 https://itwiz.pl/wystawilismy-bitna-cyber-armie-wywiad-z-gen-karolem-molenda/

attractive-women-to-trick-russian-soldiers-into-sharing-their-location-report-says-days-later-the-base-was-blown-up-/articleshow/94009908.cms

3. Anshori M. F., Db1000n Software as Ukraine's Military Utility to Counter Russian Invasion in 2022. Jurnal Pertahanan 8(2) 198:210 https://doi.org/10.33172/jp.v8i2.1683 https://www.researchgate.net/publication/363158743_Db1000n_Software_as_Ukraine's_Military_Utility_to_Counter_Russian_Invasion_in_2022
4. Ashley, How the food delivery app helped Russian women find torturers in the police station. News Rebeat 2022 https://newsrebeat.com/world-news/96916.html
5. Augustyniak Sz., Wystawiliśmy bitną cyber-armię. Wywiad z gen. Karolem Molendą, IT Wiz 2023 https://itwiz.pl/wystawilismy-bitna-cyber-armie-wywiad-z-gen-karolem-molenda/
6. Baezner M., Robin P., Cyber and Information warfare in the Ukrainian conflict, Center for Security Studies (CSS), ETH Zürich 2018 https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict
7. Battle of Snake Island Русский военный корабль, иди на хуй https://www.youtube.com/watch?v=6_B1m5iNndg
8. Corera G., Russia hacked Ukrainian satellite communications, officials believe, BBC 2022 https://www.bbc.com/news/technology-60796079
9. Coynash H., Belarusians name Russian soldiers caught on camera sending goods plundered in Ukraine to Russia, Kharkiv Human Rights Protection Group 2022 https://khpg.org/en/1608810358
10. Davis B., Speedo-wearing Russian tourist inadvertently reveals location of Putin's artillery in Crimea, Evening Standard 2022 https://www.standard.co.uk/news/uk/russian-tourist-ukraine-war-putin-target-geolocation-crimea-b1020094.html

11. Destructive malware targeting Ukrainian organizations, Microsoft 2021 https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

12. Drążkiewicz A., Lekcja dla nas, poznajemy techniki przeciwnika. Gen. Molenda o działaniach Rosji w cyberprzestrzeni. Polskie Radio 24. 2022 https://polskieradio24.pl/130/4437/artykul/3088678,lekcja-dla-nas-poznajemy-techniki-przeciwnika-gen-molenda-o-dzialaniach-rosji-w-cyberprzestrzeni

13. Druziuk Y., A Citizen-like chatbot allows Ukrainians to report to the government when they spot Russian troops — here's how it works Insider 2022 https://www.businessinsider.com/ukraine-military-e-enemy-telegram-app-2022-4?IR=T

14. Dunhill J., Pentagon Impressed By StarLink's "Eye-Wateringly" Swift Shut Down Of Russian Cyberattack IFLScience 2022 https://www.iflscience.com/pentagon-impressed-by-starinks-eyewateringly-swift-shut-down-of-russian-cyberattack-63401

15. Dziwisz D., Sajduk B., Rosyjska inwazja na Ukrainę a przyszłość cyberwojny – wnioski w rocznicę „specjalnej operacji wojskowej". Gruszczak A. (red.) THE WAR MUST GO ON. Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski. Wydawnictwo Księgarnia Akademicka 2023 43:52 https://doi.org/10.12797/9788381388801.04 https://ruj.uj.edu.pl/xmlui/handle/item/309135

16. Finowie wyśmiewają ruchy wojsk rosyjskich przy granicy. Wysyłają swój "specjalny sprzęt", Onet 2022 https://wiadomosci.onet.pl/swiat/finowie-wysmiewaja-ruchy-wojsk-rosyjskich-przy-granicy-pokazuja-traktory/zysdn71

17. Fog of War. How the Ukraine Conflict Transformed the Cyber Threat Landscape. Mandiant 2023 https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

18. Gavrila A., Ukraine's great cyberwar that did not happen . Opinion Paper. IEEE 99/2022 https://www.ieee.es/Galerias/fichero/docs_opinion/2022/dieeeo99_2022_adagav_ucrania_eng.pdf

19. Hackers play Ukrainian songs https://www.reddit.com/r/UkraineWarVideoReport/comments/wwl1u3/hackers_play_ukrainian_songs_and_watch_the/

20. Haertle A., Tysiące terminali internetu satelitarnego poważnie uszkodzonych w dniu ataku na Ukrainę Zaufana Trzecia Strona 2022 https://zaufanatrzeciastrona.pl/post/tysiace-terminali-internetu-satelitarnego-powaznie-uszkodzonych-w-dniu-ataku-na-ukraine/

21. Hart R., Clearview AI Fined $9.4 Million In U.K. For Illegal Facial Recognition Database. Forbes 2022 https://www.forbes.com/sites/roberthart/2022/05/23/clearview-ai-fined-94-million-in-uk-for-illegal-facial-recognition-database/

22. Italiano L., Orecchio-Egresitz H., Ukraine and Russia have both weaponized facial recognition — in very different ways. Insider 2022 https://www.businessinsider.com/ukraine-russia-have-both-weaponized-facial-recognition-2022-3?IR=T

23. Khatsenkova S., Ukraine war: Backlash after Elon Musk says he can no longer fund Starlink satellites, Euronews 2022 https://www.euronews.com/2022/10/14/backlash-after-elon-musk-says-he-can-no-longer-fund-starlink-in-ukraine

24. Kotowski A., GhostSec zhakował drukarki w Rosji. Zdalnie drukują informacje o wojnie na Ukrainie. Komputer Świat 2022 https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/ghostsec-zhakowal-drukarki-w-rosji-zdalnie-drukuja-informacje-o-wojnie-na-ukrainie/hrsft0c

25. Kowalska-Sendek M., Ukraina na cybernetycznym froncie, Polska Zbrojna 2022 https://polska-zbrojna.pl/home/articleshow/36629?t=Ukraina-na-cybernetycznym-froncie

26. Krzykowski P. Konsekwencje wojny na Ukrainie w wymiarze żywnościowym, ekonomicznym i energetycznym, Roczniki Nauk Społecznych T.15(50) nr 4, Akademia Sztuki Wojennej 2022 https://ojs.tnkul.pl/index.php/rns/article/view/17785/16759

27. Kuśmierek M., Rosjanie nakradli sprzętu rolniczego za 5 mln dolarów. Wywieźli go do Czeczenii i nie potrafią uruchomić Spider's Web

2922 https://spidersweb.pl/2022/05/rosjanie-nakradli-sprzetu-rolniczego-za-5-mln-dolarow-wywiezli-go-do-czeczenii-i-nie-potrafia-uruchomi.html

28. Macias A., UN report details horrifying Ukrainian accounts of rape, torture and executions by Russian troops CNBC 2022 https://www.cnbc.com/2022/10/28/russia-ukraine-war-un-report-details-accounts-of-rape-torture-and-executions.html

29. Maschmeyer L., Cavelty M. D., Goodbye Cyberwar: Ukraine as Reality Check, Policy Perspectives Vol. 10/3, May 2022 Policy Perspectives Vol. 10/3, May 2022 https://doi.org/10.3929/ethz-b-000549252 https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/549252/2/PP10-3_2022-EN.pdf

30. Mazurkiewicz P., „Putin zabija" na rosyjskich paragonach. Anonymous włamali się do drukarek. Rzeczypospolita 2022 https://cyfrowa.rp.pl/bezpieczenstwo/art35915801-putin-zabija-na-rosyjskich-paragonach-anonymous-wlamali-sie-do-drukarek

31. Michalk K., Duch Kijowa - bohater czy miejska legenda?, RMF 2022 https://www.rmf24.pl/raporty/raport-wojna-z-rosja/news-duch-kijowa-bohater-czy-miejska-legenda,nId,5884226#crp_state=1

32. Mohee A., Cyber war: The hidden side of the Russian-Ukrainian crisis DOI: 10.31235/osf.io/2agd3 https://www.researchgate.net/publication/358841316_Cyber_war_The_hidden_side_of_the_Russian-Ukrainian_crisis

33. Olszewski D., Elon Musk udostępnia Starlink na Ukrainie, Computerworld 2022 https://www.computerworld.pl/news/Elon-Musk-udostepnia-Starlink-na-Ukrainie,436628.html

34. Palczewski Sz. Białoruscy Cyberpartyzanci atakują systemy kolejowe. Utrudniają transport rosyjskich wojsk na Ukrainę, Cybersefence24 2022 https://cyberdefence24.pl/armia-i-sluzby/bialoruscy-cyberpartyzanci-pomagaja-ukrainie-utrudniaja-transport-sil-okupacyjnych-

35. Radzewicz Sz., Ukraińcy mają aplikację, przez którą zgłaszają pozycje wojsk rosyjskich. eWróg został użyty już 200 tys. razy Spider's Web 2022 https://spidersweb.pl/2022/03/ewrog-aplikacja-wskazuje-wojska-rosyjskie.html

36. Roth E., Remote lockouts reportedly stop Russian troops from using stolen Ukrainian farm equipment. The Verge 2022 https://www.theverge.com/2022/5/2/23053944/russian-troops-steal-millions-farm-equipment-ukraine-disabled-remotely-john-deere

37. Russia fights back in information war with jail warning, Reuters 2022 https://www.reuters.com/world/europe/russia-introduce-jail-terms-spreading-fake-information-about-army-2022-03-04/

38. Russian Soldiers Phone Calls https://www.nytimes.com/interactive/2022/09/28/world/europe/russian-soldiers-phone-calls-ukraine.html

39. Satter R., Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official, Reuters 2022 https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/

40. Smith A., Anonymous news – live: Russian TV hacked with Ukraine footage in 'biggest op ever seen'. Yahoo News 2022 https://news.yahoo.com/anonymous-news-live-russian-tv-090008311.html

41. Stodolak S., Zbiór pożytecznych idiotów jest coraz większy. Dlaczego uwierzyli Putinowi? Dziennik Gazeta Prawna 2022 https://www.gazetaprawna.pl/magazyn-na-weekend/artykuly/8413199,pozyteczni-idioci-putina-rosja-stone-kusturica-rourke.html

42. Stokel-Walker C., Russia and Ukraine are both weaponising mobile phones to track troops, New Scientist 2022 https://www.newscientist.com/article/2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/

43. Štrucl D., Russian aggression on Ukraine: cyber operations and the influence of cyberspace on modern warfare. Contemporary Military Challenges 2022(2):103-123 2022. https://doi.org/10.33179/BSV.99.SVI.11.CMC.24.2.6 https://www.researchgate.net/publication/361569176_russian_aggression_on_ukraine_cyber_operations_and_the_influence_of_cyberspace_on_modern_warfare

44. Szpor G., Gryszczyńska A., Hacking in the (cyber)space. GIS Odyssey Journal 2022 | Vol. 2, no. 1 | 141:152 https://doi.org/10.57599/gisoj.2022.2.1.141 https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-e50da523-a3b5-48f8-91e3-6369a2d8edf1

45. Ukraine 2022 na cyfrowym froncie. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzenie, 2023 https://www.wojsko-polskie.pl/woc/u/4c/d1/4cd11eaf-3567-405d-994f-f88b6b45ad0b/ukraina_2022_na_cyfrowym_froncie.pdf

46. Ukraine hits Russian Wagner mercenary HQ in east, BBC 2022 https://www.bbc.com/news/world-europe-62547403

47. Ukrainians use phone app to spot deadly Russian drone attacks The Guardian 2022 https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo

48. Vail E., 'We are unstoppable': How a team of Polish programmers built a digital tool to evade Russian censorship, The Record 2022 https://therecord.media/we-are-unstoppable-how-a-team-of-polish-programmers-built-a-digital-tool-to-evade-russian-censorship

49. Vasilyeva N., Beatings and psychological torture: The fate that awaits Russian dissidents like Marina Ovsyannikova, The Telegraph 2022 https://www.telegraph.co.uk/world-news/2022/03/15/beatings-psychological-torture-fate-awaits-russian-dissidents/

50. Vicens A., A year of cyberwar' with Russia: An inside look from a top Ukrainian cybersecurity officialm Cyberscoop 2023 https://cyberscoop.com/victor-zhora-ukraine-russia-cyber-war-one-year/

Abstract

CYBER OPERATIONS DURING HYBRID CONFLICTS - LESSONS FROM THE WAR IN UKRAINE

Summary: The paper presents selected aspects of IT usage that could be observed during Russia's war with Ukraine in 2022. The

analysis of events allows conclusions to be drawn about the effectiveness of various cyber activities in future conflicts. Conclusions can be made in the area of ensuring secure communications, cyber attacks destroying physical infrastructure elements, the use of cell phones, OSINT and also the effectiveness of disinformation and propaganda activities.

Keywords: cybersecurity, hybrid conflicts, Ukraine

Rozdział 11

Winnti: Is the gaming industry in actual danger? Analysis of the operation of the largest organised cybercriminal syndicate targeting video game producers

Marek Piotr STOLARSKI[1]

Video games are becoming more and more popular every year. Novelty or variety keeps life fun, interesting and engaging. Video games give players the opportunity to do something different and they have the capacity to do so because there are over a million games on the market today. As with other software, games also involve multiple types of cyber risks, threats and vulnerabilities and their growing number gains the interest of cybercriminals.

- ***The gaming industry is estimated to exceed $200 billion for the first time[2]***
- ***Gamers to hit the 3.09 billion mark worldwide***

These two numbers characterising the condition of the gaming industry are well known in the cybercrime world. But, at the same time, cybercriminals are aware of the growing numbers, which will reach $203.1 billion through consumer spending.[3] Such stakes connected to the internet, where detecting hostile hacking operations is highly difficult, draw the attention of specialised and subsidised hacker groups.

---

[1] E-mail: marek.stolarski@techland.pl; ORCID:0000-0002-3027-135X

[2]Tom Wijman, *The Global Games Market Will Exceed $200 Billion For The First Time as the US Overtakes China, https://newzoo.com/insights/articles/games-market-revenues-will-pass-200-billion-for-the-first-time-in-2022-as-the-u-s-overtakes-china*(retrieved June. 2022)

[3] Ibid.

One of the primary hacker groups attracted to the expanding gaming industry is Winnti, a Chinese group that the world hasn't been able to deal with for almost a decade. The Group's evolving tactics are like a mutating cybercrime octopus, often targeting game developers.

How do you steal the real stakes in virtual reality?

The cybersecurity community knew as early as 2013 that the main purpose of the Winnti group's malware family was to steal the source code of online games. In particular, Winnti focused more on certificates, which they would steal from software vendors and game developers in Asia. The Group would then plant the source code signed with these certificates at suitable targets. After that, with its false identity, it would circulate to the victim's servers to execute and open further stages of the heist.[4]

One of Winnti's preferred attack methods was to penetrate the infrastructures, beginning with the servers, then steal intellectual property, including projects, ideas, designs and others that ensured the developer's market position.[5]

Origins of the international criminal organisation

The Winnti cybercrime syndicate can be traced back to 2013, when multiple players reported a Trojan had infected their computers. The Trojan would spread through genuine updates from the game vendors' official servers. Initially, security researchers hypothesised that the developer had foul, spying intentions. Still, it later turned out that the malicious code was dedicated to the developer itself as part of a major market crime operation.[6]

The operation targeted two US developers, two from Germany, two from Russia, and fourteen from South Korea. The MMORPG (massively multi-player online role-playing games) sector became a high-yield target because many users constantly connect to the developers' servers through regular subscriptions. Also, the gaming market's nature was a contributing factor

---

[4] [Kaspersky Lab official report] *Winnti. More than just a game,* p. 2 https://media.kaspersky-contenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf (retrieved June. 2022)

[5] Ibid.

[6] Ibid.

– business partners often share servers, contracts and resources, forming a linked network that could be compromised.[7]

What was behind this?

The 2011 Trojan turned out to be a DLL library for 64-bit Windows. It was equipped with a valid certificate and contained an additional driver. The library served as a Remote Administration Tool (RAT) that permitted attackers to control the victim's computer remotely. The certificate's validity aroused suspicion when it led to another victim - a South Korean MMORPG developer from which it was stolen. More certificate thefts targeted South Korean, Japanese, and Chinese companies in one and a half years, including ESTsoft, MGAME, and KOG. The incidents led to a pattern that enabled the identification of the perpetrators' attacks.[8]

Comparing the captured code with the source code exposed a characteristic collection of backdoor programs, both for 32 and 64-bit versions. As a result, the authors responsible for the captured code were dubbed the Winnti group.[9] Further investigations of the incidents based on the software pattern traced the hackers' operations to 2009. For two years, the hackers were able to conduct operations targeting over 35 business targets connected through supply chains (with access to networks through which the malware spread) in Asia (9 countries), Europe (Belarus, Russia, Germany), Brazil, Peru and the USA.[10] In total, the Winnti group included almost 500 criminal subdomains in 2011.[11]

It turned out that the cybercrime group created a dedicated program for each target, with all programs totalling over 100 items. Each program was assigned its command and control (C&C) centre behind a second-level domain

---

[7] Mark Hatchman, *"Winnti" Attacks on Online Gaming Servers Dissected*, https://insights.dice.com/2013/04/11/winnti-attacks-on-online-gaming-servers-dissected/ (retrieved June 2022)

[8] Michael Mimoso, *Winnti Cyberespionage Campaign Targets Gaming Companies*, https://threatpost.com/winnti-cyberespionage-campaign-targets-gaming-companies-041113/77717/ (retrieved June 2022)

[9] [Kaspersky Lab] *Winnti. More than just a game...*, pp. 3-4

[10] Ibid., p. 5

[11] Ibid., pp. 87- 95

without any DNS. Some domains had names deceptively similar to the game developers, only with a different suffix, e.g., .us instead of .com. The discovered subdomains were assigned to target countries or name abbreviations. So ru.domain_name.com would mean the C&C server was for victims in Russia, while fs.domain_name.com was the designation of a specific company.[12]

> *A C&C centre is a server for communicating with malware that has penetrated the victim's network in a targeted attack. It creates a command and control centre which sends commands and queries to be executed on the other side. Hackers use C&Cs in centralised, P2P and random models.[13] After establishing communication, the malware sends a situation report and then awaits instructions. Next, hackers use C&Cs to execute data theft, DDoS attacks, and remote control of compromised machines.[14]*

The Winnti hackers were also interested in implementing C&Cs on computers not connected to the network as the malware spread through a company's internal networks. This was revealed by some servers being assigned to local IP addresses. In such cases, an additional intermediate control site was necessary. A backdoor on a victim's computer with access to deeper layers of the compromised corporate network was used to establish the intermediate control site.[15]

Investigators then used brute-force techniques on the twelve subdomains, revealing 227 third-level domains, including identifying six email addresses with which they were registered. Four of the email addresses were from Gmail. Additionally, some criminal domains had registration details identical to Google Inc.[16]

---

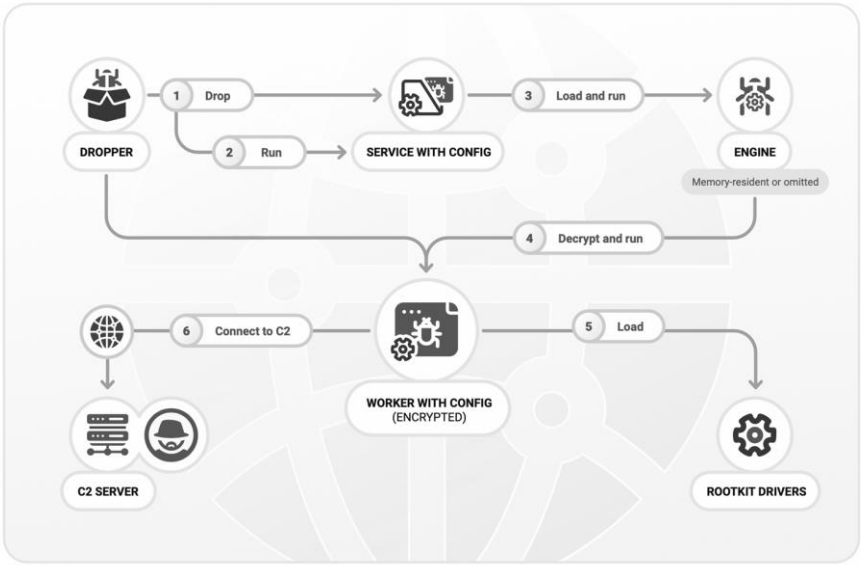
[12] Ibid., p. 6

[13] [Official TrendMicro definition] Command and Control [C&C] Server, https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server (retrieved June 2022)

[14] [Official Cyberpedia definition] *Command-and-Control Explained*, https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained (retrieved June 2022)

[15] [Kaspersky Lab] *Winnti. More than just a game..*, p. 7

[16] Ibid., p. 8



Źródło: Own study based on Kaspersky Raport.
Figure 1. Winnti Execution Flow

The registration details were enough to trace the Winnti Group to 2007 and link it to fake antivirus distribution, even before the command & control servers configured for bots attacking game developers appeared (in 2010).[17]

Modus Operandi

The primary motivation of the Winnti Group's attacks was to steal virtual currency from a game and then convert it to real money. These actions were aided by a malicious code that exploited weak points in the software to

[17] Ibid., p. 8

compromise a victim's computer. A beneficial side benefit of acquiring the source code was the ability to set up their illegal game servers.[18]

The adversaries began their operation by designing a version of the malware dedicated to the service of a specific company. This would identify the target process on the server and inject code to identify vulnerable spots to hide different portions of the malware code, which intercepted and modified processes, generating additional currency for the hackers. The entire operation had to be concealed from the game vendor and the players since detecting the scam would reduce interest in the game, cutting the hackers' profits. As a result, Winnti's secret operations on servers of unsuspecting companies could survive for years.[19]

The general modus operandi of the Winnti Group as of 2013 included[20]:

- Mass theft of certificates - for use against the intended victims and indirect acquisition of additional certificates.
- Use of a rootkit in the kernel of a 64-bit system
- Controlling bots by publishing commands for them on commonly accessible sites
- Commercialising the stolen certificates regardless of a customer's purposes
- Aiming attacks at computer game developers to steal intellectual property

Targeted operation sequences

The starting point is the DLL library underlying the Group's attacks. It imitates an actual component of the Windows system - winmm.dll or apphelp.dll. The components are responsible for basic system functions, such as multimedia. They are chosen as cover since they are widely used by internal and third-party software - such as game vendor clients.[21] The library loading pattern prioritises the one that belongs to the application's folder. Therefore, the original library waiting at the system level will be ignored if the program identifies an identical one in its resources.

---

[18] Ibid., p. 9
[19] Ibid., p. 9
[20] Ibid., p. 80
[21] Dmitri Tarakanov, Winnti 1.0 - Analiza techniczna, https://securelist.pl/analysis/7192,winnti_1_0_analiza_techniczna.html (retrieved June 2022)

Using a RAT backdoor and a C&C server, the hackers could remotely install a false library in a location on the victim's computer. A common location was the %WINDIR% folder, used during system booting. The location ensured the malicious DLL was launched as early as possible.[22]

Furthermore, if some program needed to access the entire library, the false winmm.dll served as a proxy. The AheadLib program, normally dedicated to security administrators for dynamic analysing of malicious code, was also involved in the procedures.[23] Its feature provides any DLL library for which the C code working on the functions contained in the file is created, producing a new library to work as a proxy. Normally, this enables analysing the behaviour of malicious code. Finally, a library template was prepared in a C file using its flexibility, and winmm.dll was inputted as the parameter.[24]

Reaching deeper, another overt library, (PlusDLL).dll, crucial for controlling the entire mechanism, was discovered. Once it was loaded into memory, winmm.dll would send a packet with the bot's settings. Later on, these settings were placed in the header or hidden.[25]

The driver mentioned earlier was also part of the embedded library. Therefore, once it was registered and used as a service, its file would be removed, along with any registration traces. This way, a rootkit functionality was obtained, as the implemented driver, using the address base stored in the embedded library, hid the activity of the malicious DLL, including its internet communications.[26] Furthermore, using a stolen certificate, this driver would pass the trustworthiness test run by the Windows system. In 2013, there were 11 such certificates in use, ensuring protection from antiviruses.[27]

Initially, the PlusDLL library contained information about the victim's system (disk, OS, application that used the hostile library, network adapter MAC address and session data), and each attribute was assigned an ID. The criminals would use this data to send through the C&C plugins to

[22] Ibid.
[23] [Kaspersky Lab] *Winnti. More than just a game..*, p. 10
[24] Dmitri Tarakanov, Winnti 1.0 ...,
[25] [Kaspersky Lab] *Winnti. More than just a game..*, p. 15
[26] Ibid., p. 16
[27] Ibid., p. 18

build the remote control system (using the TCP protocol and LZMA algorithm.[28]). Ultimately, during each system reboot, another such file was downloaded and loaded directly and solely to the operating memory, eliminating the risk of detection or leaving traces. [29]

In short, the entire communication procedure [bot on the victim's computer]<=>[C&C server] was as follows:

> ***Bot:*** *initiation signal =>* ***C&C****: available plugins =>* ***Bot:*** *single query about plugins =>* ***C&C:*** *sent =>* ***Bot:*** *confirms received and goes to standby confirmed every 1 second with „empty" signal.*[30]

In 2013, eight known control plugins enabled control over the command line, file system, processes, services, and internet traffic. For example, the TransPlus plugin was enough to control the victim's disk resources and run programs remotely.[31]

After the false DLL libraries were detected, they were broken down into virus lists called Backdoor.Win32.Winnti[32] and Backdoor.Win64.Winnti[33], while the drivers they used were classified in similar lists with a Rootkit prefix.[34]

2019: The might of Winnti 10 years later

Based on 250 Winnti malware samples studied by Moritz Contag (IT security specialist at Bochum University {RUB}) and an interview with Costin Raiu (Kaspersky Lab analyst team lead)[35], the following can be surmised:

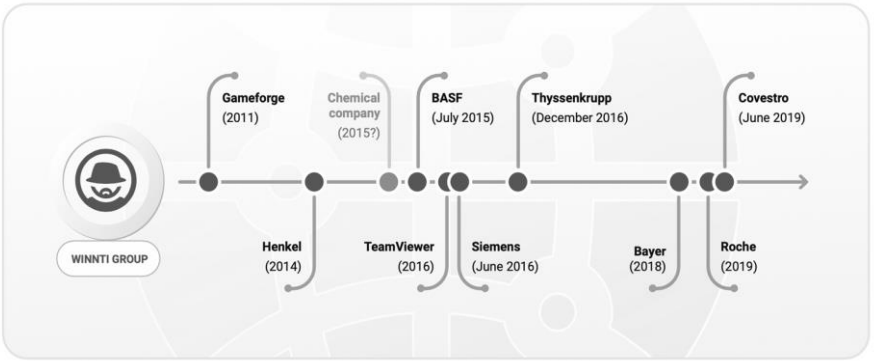
---

[28] Ibid., p. 23
[29] Ibid., p. 21
[30] Ibid., p. 25
[31] Ibid., p. 21
[32] [Microsoft database] *Win32/Winnti,* https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Win32/Winnti (retrieved June 2022)
[33] [Microsoft database] *Backdoor:Win64/Winnti.A!dha,* https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win64/Winnti.A!dha&ThreatID=-2147255939 (retrieved June 2022)
[34] [Kaspersky Lab] *Winnti. More than just a game..*, p. 23.
[35] Hakan Tanriverdi, Svea Eckert, Jan Strozyk, Maximilian Zierer, Rebecca Ciesielski, *Attacking the Heart of the German Industry,* https://web.br.de/interaktiv/winnti/english/ (retrieved June 2022)

- As a malware family, Winnti is now used by two teams extensively, one being responsible for operations in Germany and conducted on a massive scale.
- Since 2014, the Group has expanded its scope of interests, evolving from the gaming industry to other high-profit organisations. Competences in cryptocurrency manipulation have grown into industrial cyber espionage. Their interests have also extended beyond Asia, where Winnti had enjoyed comfortable conditions for years, to perpetrate attacks in France, the USA and Germany (international companies located in Dusseldorf).
- Hackers from this cybercriminal organisation are considered particularly ruthless, consistent, perfectionist and persistent in action, striving to comprehensively study the entire infrastructure of their victim's network to pick the best possible spot to deploy malware. As a result, it is difficult to root Winnti out of the network even when detected.
- When getting to know their victim, the hackers are interested in the structure, and the range of programs used in cyberspace to identify those where substituting files with malicious code can bring the best results.
- The group codes in the names of the companies it intends to attack in its malware. These are large international organisations.
- The cybernetic operations are goal-oriented, even at the cost of detection.
- They use a characteristic string of characters hiding commands: daa0 c7cb f4f0 fbcf d6d1.
- When decoded, the string shows the path to the Windows system.

News reports also indicate that attacks on game developers have resumed. Again, Winnti's special operations spread along with the supply chain network. This time, the same software-infecting code has been identified in three cases. As of 2011, the malicious code launches when the victim's computer begins booting and activates a backdoor in the memory before any other

application code. The backdoor contains an RC4 key encrypted with the XOR 0x37 operation, which is used to decode the DLL library.[36]



Źródło: Own study.

Figure 2. Timeline of the attacks committed by the Winnti Group

The configuration contains the URL address of the C&C server, a variable (t) for hibernation time between tasks, an ID of a given operation, and executable file names (each one identified as active stops the code). In 2018, 5 versions of this malware were identified. Like past versions, the domains for the command and control servers were prepared with a strong reference to actual game publishers and developers. Hitting such domains resulted in redirection to a real website of the victim or its address in social media, while subdomains led directly to the C&C.[37]

Also, the data collected by the bot on the victims' computers corresponded to Winnti's interests in 2011 - including the user, computer name, OS version and language.[38]. Communications encrypted in XOR were conducted using the same key "*&b0i0rong2Y7un1".

The backdoor itself has only four commands:

- for downloading files to the victim's computer (DownUrlFile),
- for downloading and running (DownRunUrlFile),

[36] Marc-Etienne M.Léveillé, *Gaming industry still in the scope of attackers in Asia*, https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/ (retrieved June 2022)

[37] Ibid.

[38] Ibid.

- for running files in memory (RunUrlBinInMem),
- and for hibernating the malicious code (UnInstall).

The files downloaded to the victim's computer (from api.goall-bandungtravel.com) include the following libraries: *cscsrv.dll, dwmsvc.dll, iassrv.dll, mprsvc.dll, nlasrv.dll, powfsvc.dll, racsvc.dll, slcsvc.dll, snmpsvc.dll, sspisvc.dll*.

Everything is the work of a piece of malware designated by ESET as Win64/Winnti.BN. Additionally, the latest versions can automatically update themselves by downloading data from http://checkin.travelsanignacio.com[39].

Current industries of interest to Winnti40:

a) Video games,
b) Aeronautics,
c) Pharmaceuticals,
d) Technology,
e) Telecommunications,
f) Software.

This range of targets may indicate a complex structure of subgroups and ties to a larger number of criminal groups. Still, however, the primary area of attack is Asia and South Korea. In addition, the current motives of the Winnti Group have also included cryptocurrency mining using captured computers since 2018[41].

Flagship hacker tools

1. A characteristic packer[42]

[39] M.Léveillé, *Gaming industry still in the scope...*
[40] Ionut Arghire, *Researchers Find New Backdoor Used by Winnti Hackers*, https://www.securityweek.com/researchers-find-new-backdoor-used-winnti-hackers (retrieved June 2022)
[41] Marc-Etienne M.Leveille, Mathieu Tartare, *Connecting the Dots. Exposing the arsenal and methods of the Winnti Group*, p. 5 https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf (retrieved June 2022)
[42] Ibid., p. 7

The tool for creating virtual machines, which the Group uses to embed a PE file in the game software, is distinguished by:

- The above-mentioned PE file
- RC 4 key:
  - encrypted with the XOR 0x37 instruction,
  - made up only of digits,
  - intended to decrypt the PE file, its name and file path.
- The value of unpacking the code can be of type 1 or 2.
- The packer has a 32 and 64-bit version.

2. PortReuse modular backdoor

The name corresponds to the study results. The Winnti backdoor uses an already active TCP port, connecting itself to the reception function (as an intermediary, without side effects for legal traffic) and waiting for a pre-determined packet that gives the signal to act.[43] The backdoor only needs to save one launch file to function- the other modules exist only in operating memory[44]. The file on the disk can therefore be:

- part of a .NET application,
- part of a VB script invoking and deserialising a .NET object, which in turn launches the shell code,
- an executable file with the shell code directly at the entry point.

Initially, **PortReuse** uses the InnerLoader.dll components.[45] The earlier discovery of the Winnti packer enabled its metadata analysis, where the complete file path from the moment of packing is visible. The path includes the project folder, the "PortReuse".

- The task of **InnerLoader** is to inject two payloads into the target process - NetAgent and SK3. If it serves a role in a .NET application, the version that has been studied looks for the GameServer_NewPoker.exe process, while the VB script targets the DNS - port 53.
- **NetAgent** is then responsible for gaining access to the TCP function so the backdoor can listen. When the right message arrives from the C&C server, it redirects traffic from the C&C to the SK3 module. A version of this payload is additionally tasked with sabotaging the

[43] M.Leveille, Tartare, *Connecting the Dots*, p. 8
[44] Ibid., p. 9
[45] Ibid., pp. 9- 13

ETW of the Windows system by patching the beginning of the function by tracking its process with a value returning an ETW result of "0".

- **SK3** decrypts traffic from the above payload and forwards it. It can execute 13 different commands, such as determining the current folder, listing its contents, copying, moving and deleting data, launching systeminfo.exe, reading and modifying files, including their timestamps, killing processes, and closing connections. Windows supports these commands as standard.
- Modules subordinate to SK3 are **UserFunction** and **ProcTran.** They execute commands in processes with specific PIDs (delivered as arguments) and are responsible for forwarding traffic based on IDs.

There have been variants of PortReuse where both modules, NetAgent and SK3, were combined to function together based on Windows Server API. PortReuse itself also has different versions designed for different jobs. Some look for ports below 22; others target one specific number. Some are interested in one specific process where they are to hide; others pick the one that first launches a given service. Some versions of this backdoor are intended to hook into port 80 and imitate a Windows network service - IIS 10.0.

In 2018, in files with the .mui extension loaded by Win64/Winnti.BN, the use of the known Winnti packer was discovered, but this time the executable files were part of the XMRig program, available online for free and used for cryptocurrency mining.[46] In 2019, the VMProtetct launcher, Winnti's custom packer, the InnerLoader mentioned above, and a framework targeting the sqllang.dll library were discovered.[47]

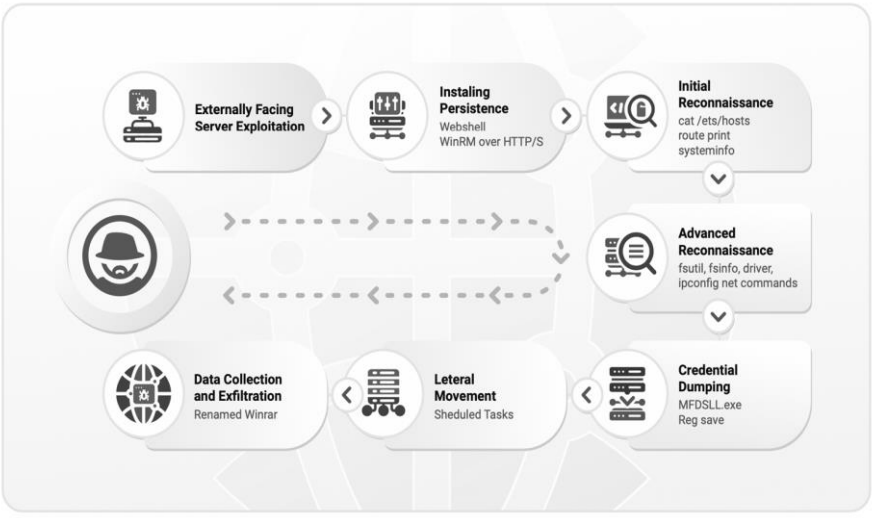
Who are the Winnti

The criminals would download the ff._exe program to the victim's computer, which looks for Microsoft Office and Adobe and HTML and txt files. Analysis revealed GBK coding with simplified Chinese characters, which formed an action report. The interface of the AheadLib program and

[46] M.Leveille, Tartare, *Connecting the Dots.*, p. 22

[47] Dr Subramanian Gurubaran, *Winnti Hacker Group Uses New Malware to Hack Microsoft SQL Servers,* https://gbhackers.com/microsoft-sql-servers/ (retrieved June 2022)

the content of the CmdPlus.dll plugin also pointed to a Chinese origin. In addition, one certificate contained a Korean word, revealing the system's language from where it came.[48]



Źródło: Own study.
Figure 2. Winnti action chain

Tracing the Winnti Group members began in 2013 by collecting keywords that could indicate the team names or the hackers' pseudonyms. One such name was "ydteam". An online search returned a strong presence in the Middle Kingdom. The word popped up on the Chinese internet - including forums and personal blogs - close to pseudonyms "zhikou", "b4che10r", "Shalyse", and "killer". The hacker group also had an official website at the ydteam.cn address, which was up for a year until October 2010, when it was discontinued. In its registration data, the wn6805@126.com email address was found.[49]

[48] [Kaspersky Lab] *Winnti. More than just a game..*, p. 52
[49] Ibid., p. 53

Path to the owner[50]

- The email trail led to a site in the Chinese search engine Baidu, which offered to help with cheap shopping - most likely an attempt to obtain payment details illegally. It was now possible to link the email address with a specific user name and a QQ ID.
- Another website where the same address was used revealed the owner's birth date – 21.12.1992 and marital status. Another - his sex. Yet another - three papers written during school education and published in 2008 and 2009. The same domain yielded another QQ number and confirmed the birth date.
- The next step was to verify the newly acquired information. The QQ number led to a blog where the personal phone number of the owner was provided.
- Finally, it was determined that the ydteam domain belonged to Zheng Wenlong from June 2009 to 22 August 2011.
- Despite privacy protection, the Domaintools.com web page preserved screenshots from the hacker site (from 2010), which contained the nicknames of some members of the Group that ran a forum there.
- The next point of interest was the IP address: 118.142.11.114, associated with the posts, which led to its sources - domains pad62.com and ru.pad62.com. Ji Shao registered the former in June 2011, and it continued to operate without subsequent changes. Moreover, it displayed an actual Chinese address and contact details of the site administrator, including his email address. Based on this information, nine more domains owned by **Ji Shao** were revealed.
- The source of the module downloading files to victim computers using the C&C server was also inspected, which was located under the address tank.hja63.com. Once again, the name Ji Shao popped up.

More hackers from the Winnti Group[51]**:**

---

[50] Ibid., pp. 54- 57

[51] [Kaspersky Lab] *Winnti. More than just a game..*, pp. 58-66

- The investigators also came into possession of the c_20100.nls file. The nicknames it hid were present on the internet on public subsites of Google groups, which contained messages for bots standing by on infected computers. They were often accompanied by encrypted command and control addresses.
- Such messages contained new email addresses, this time from the Gmail and yahoo domains, used as forum user names.
- Additionally, the word **"awertase"** emerged, which led to yet another forum, where an identical bot-message template was found.
    - The email associated with the user was "awertasegfae@yahoo.com"
    - It was connected to the blog of hacker **mere4en7y**, which turned out to be a net denizen active in the hacker community, as searching his nickname returned almost 5.5 thousand results. These included a reveal of a vulnerability detected in the system of a bank from the Weihai city. Mer4en7y also had an active QQ microblog with public comments to video content on programming viruses, creating botnets and developing backdoors.
    - With the search results, the hacker named above could be linked to another one - d4nr4n - who posted on a social media site that he was going with mer4en7y to a programming workshop. Another contact of the active hacker was **"mayuan"** - a graduate of a Chinese forensic police school with a publicly viewable image.
    - Further scrutiny of the results revealed the city of origin - Nanjing - and the authors of the exploit that was used to attack the FTP server of a national radio station. In this case, the email address came from the website of another group - the 90sec hackers' team, and there, a reply of his to a public job offer was found.

However, the bot message IDs came from a larger number of hackers. They used nicknames in various parts of the web, including **"Wz", "Run", and "Jimmycocowell".** The latter created two messages on his blog, with the second one using XOR with BASE64 coding, the same as the new Winnti backdoor - c_201000.NLS. Additionally, a link to this hacker's blog was found on the blogger profile of user "bitgodgod". The next lead was provided by a malicious code fragment from a victim's computer, which pointed to the address of a C&C server at the mail.7niu.com website, registered to Xibei Iiad

with the email address bit_bugbug@tom.com. This address could be found on Chinese websites concerning real estate.[52]

Yang is another hacker associated with the Winnti Group, just as active online as mere4en7y. Yang also published commands for bots on his blog with the subdomain "yang8559420", and this word entered in a search engine enabled him to be identified as the author of maps for the ArcGIS app, which was also selling its source code. His business profile acquainted the investigators with his Aliexpress certificate.[53]

A copy of the bot management code, shared by Yang, was used in the message of user "Lovemeyang", whose nickname in the search engine returned an information noise of inconclusive results, but the links point to a double identity.[54] Other names from the same Group can be found in reports by companies from the IT Security sector:

Axiom

Subgroups BARIUM (targets the gaming industry) + LEAD (focused on stealing sensitive information)

- Group 72
- Blackfly
- Suckfly
- APT41

[55]The last name is also used by the company FireEye, which lists an additional database of malware in use:

- ACEHASH – A Trojan stealing authentication data. Publicly available.
- ADORE.XSEC – A backdoor for Linux works together with a dedicated rootkit.
- ASPXSPY – A publicly available network shell.
- BEACON – A backdoor, an element of the Cobalt Strike platform, sold as a tool for penetration tests.
- CHINACHOP – a network shell for injecting and launching .NET code, made up of a small portion of code on a server, communicating

[52] Ibid., p. 72
[53] Ibid., p. 74
[54] Ibid., p. 79
[55] [FireEye official report], *Doube Dragon. APT41, a dual espionage and cyber crime operation,* p. 57-62 https://content.fireeye.com/apt-41/rpt-apt41/ (retrieved June 2022)

with a C&C. Using HTTP POST commands, it can download files, and launch programs, gain access to databases and file folders.

- COLDJAVA – A backdoor delivering shell code and payload to a victim's Windows register.
- CRACKSHOT is a program with available statuses active/standby, which downloads, installs, and runs files from the disk and operating memory.
- CROSSWALK – A modular backdoor for system penetration and implementation as part of Command & Control orders.
- CROSSWALK.bin – Is a kernel driver that implements filters at the firewall level, enabling it to transmit data without being noticed.
- DEADEYE – Another downloader which uses RC5 encryption when downloading and installing packets from a C&C.
- DOWNTIME – A backdoor that can get directly and exclusively to operating memory or to any place on the disk as a PE file. Its executive phase is a DLL that manages plugins of other libraries.
- EYESIGHT – A loader program, usually working in the presence of programs such as HIGHNOON.
- ENCRYPTORRAAS – Ransomware that encrypts files on the disk based on a pre-determined extension list. The encryption is a combination of public and symmetric keys and RC6 - in the latter case, the key is RSA-encrypted. It can be recognised based on the notifications it leaves in every folder where it encrypts files with a given extension. The note is then named "readme_liesmich_encryptor_raas.txt". This program has been in use since the RaaS operation, conducted in 2015-16 when it was shared in the Tor network.
- FRONTWHEEL – A driver working for the HIGHNOON.bin backdoor.
- GEARSHIFT – A dropper working only in operating memory, its job is to replace two fax DLLs for keyloggers in the form of such libraries.
- GH0ST - A RAT that captures screenshots, audio samples and camera access, comprehensive process, register and file control, and command shell use on the hacker's request.
- GOODLUCK – A DLL library that steals authentication details. It launches when a user logs in to the system, thanks to previously breaking into the register, and saves the captured data in a file on the disk.

- HIGHNOON – A modular backdoor - it can contain a loader and a DLL library with a rootkit. The packet is delivered as a whole to the victim's computer and works under the guise of a Windows service.
- HIGHNOON.bin – A redesigned Windows DLL (apphelp.dll) that loads into memory by replacing it in the search order used by a program.
- HIGHNOON.lite – A standalone HIGHNOON that downloads the necessary modules from the C&C, so they are run in operating memory.
- HIGHNOON.linux – A backdoor with a rootkit for Linux. The kit provides a persistent, hidden connection with the C&C for an SSHD client.
- HIGHNOON.pasteboy – A backdoor using legitimate websites, where it stores C&C addresses encrypted with BASE64.
- HKDOOR – A RAT in DLL form, working standalone as a service or running together with rundll32.exe. Its main function is to install a kernel rootkit, and additionally, it enables remote controlling of processes and files, connecting to URL addresses and shutting down the system.
- HOMEUNIX – Launches downloaded plugins waiting in a memory buffer directly in this memory without passing through the disk. One reason for saving is protection against loss when the system is shut down, and loading immediately after the system is booted, without connecting to the C&C.
- HOTCHAI – A backdoor retrieving the C&C address by decoding an XOR-encrypted DNS message.
- JUMPALL – A dropper for components of the HIGHNOON family.
- LATELAUNCH – Works with the hacker by decoding and loading a file the hacker demands in the command line.
- LIFEBOAT – A backdoor for communicating with the C&C through HTTP.
- LOWKEY – Passively intermediates in concealed communication TCP socket <=> specific pipe.
- NJRAT – An intensively developed RAT, created by Kuwaiti hiding behind the nickname "njq8".

- PACMAN – A backdoor working as a service that connects to the C&C to enable disk recognition, full file and folder control, and stealing data from the Internet Explorer.
- PHOTO – A DLL hides a backdoor sending carrier, folder and file lists. Enables comprehensive management of processes, files and registry keys and captures screenshots. Registers not only audio/video but also logins and passwords - even from protected sources.
- POISONPLUG – A modular backdoor that receives plugins, with a characteristic function of storing coded C&C commands on social media websites. Responsible for continuous service registering and network transmissions. If necessary, it can delete itself.
- POISONPLUG.shadow – A backdoor similar to the above but working in stages. The first stage reports to the C&C that malicious shell code is present inside a legitimate file. The second accepts the plugins suitable in a given situation.
- PORTROAST – Another backdoor enabling communication with C&C to download, install and launch requested applications and code. Creates a reverse shell for this purpose.
- ROCKBOOT – A non-malicious program that moves below the OS and file system - in the firmware. This way, it can activate even before Windows boots, regardless of the boot sequence. Its job is to write the payload in the same layer, giving malware the same privileges.
- SAGEHIRE – Malware decoding subsequent stages of an operation, additionally equipped with a keylogger feature.
- SWEETCANDLE – Another downloader whose sole task is to receive malicious code from the C&C and launch it.
- SOGU – A backdoor sending and downloading files, launching processes, managing the file system, service settings and shell access. It can provide a hacker with a graphical interface by implementing a VNC/RDP protocol.
- TERA – A backdoor that downloads C&C settings through services such as Google Translate or Yahoo!. Works using a rootkit, and once communication is established, provides control over IOCTL queries.
- TIDYELF – A dropper for the WINTERLOVE backdoor, targeting the inside of the iexplorer.exe process. Next, a registry key for a RAT is created, which contains settings for this backdoor's modules.
- WIDETONE – A backdoor intermediating code execution and collecting data on files/folders.

- XDOOR – A comprehensive RAT with a plugin structure. It can be used to capture audio and video materials and key presses to send files to the victim's computer, steal data about the system, establish a reverse shell, and implement malicious DLLs and operations that use commands.
- XMRIG – A cryptocurrency excavator available as an OS, which can be targeted at a CPU or an NVIDIA or AMD GPU.
- ZXSHELL – A backdoor spread by Chinese hacker platforms. It can scan ports, launch keylogging, take screenshots, establish proxies, and send, launch, and delete files. Furthermore, it blocks machines with a packet flood (SYN flood) and creates reverse shells. Even in its basic version, this malware has its own GUI for the hacker to communicate with other backdoors.

Can you defend yourself?

Attacking software developers allows the Winnti group to mass spread malware through regular updates from a single point, a single C&C, and within a specific, single operation.[56] Analyses of Winnti malware indicate that the tools cease their operation if they detect that the infected system is Chinese or Russian.

On the other hand, the Group's real targets are predominantly in Thailand (55%), followed by Taiwan and the Philippines (13% each), with the following countries not exceeding 5%. There is a likelihood that one of the affected game developers is still sending out malware, which leads to an estimation that victims can still number several dozen/hundred thousand.[57]

One of the breakthrough discoveries was the Winnti Group's modus operandi, in which every data packet began with the string "0xdeadface", which enabled corporate IPS/IDS systems to detect the threat in advance and block access.[58] In response, the Group implemented data encryption.

[56] M.Léveillé, *Gaming industry still in the scope ...*
[57] Ibid.
[58] M.Leveille, Tartare, *Connecting the Dots.*, p. 23

A further problem with detecting Winnti is the character of their software, which only activates when requested. In its hibernation phase, the malicious code is difficult to notice. It can wait indefinitely to be awakened and be - rapidly and very effectively - an operation to provide the Winnti Group with remote control.[59]

In 2017, Microsoft filed a civil lawsuit against the owners of six domains: *bafyvoruzgjitwr.com, jkvmdmjyfcvkf.com, nyIalobghyhirgh.com, ribotqtonut.com, tczafklirkl.com,* and *xmpoiunzmxkxkh.com,* (substitute identity terms John Does 1-2 were used), which participated in cybercrime operations targeted at the company's software.*[60]*

In 2018, federal lawyers in the USA filed another suit that contained the names of Chinese citizens charged with cyber intrusions in the years 2010-15 with an intent to steal companies' intellectual property from the aeronautic and high-tech industries. It is known that the attack included the use of Winnti malware and the server name replacement tactic.[61]

At present, the biggest challenge is detecting Winnti malware by the end-users. Forced to regularly download updates, which may be infected with malicious code secured by stolen valid certificates, they cannot rely on antiviruses, which on the one hand, accept software-based on certificates, and on the other, often have programmed automatic acceptance based on patterns, to minimise the risk of false alarms. [62]

Therefore, the most effective solution is a meticulous, time-consuming analysis of owned programs and services, which requires specialist knowledge. This is why the information is drawn from investigations conducted for major companies. The focus of their cybercrime operations works both ways, though - just as comprehensively as the Winnti introduce malicious codes into updates sent by software vendors, so does the problem disappear when detected.[63]

---

[59] Hakan Tanriverdi, Svea Eckert, Jan Strozyk, Maximilian Zierer, Rebecca Ciesielski, *Attacking the Heart of the German Industry,* https://web.br.de/interaktiv/winnti/english/ (retrieved June 2022)

[60] [Lawsuit at a court in Virginia] https://www.noticeofpleadings.net/barium/files/COMPLAINT_AND_SUMMONS/Summons_John_Doe_1_PACER.pdf

[61] M.Leveille, Tartare, *Connecting the Dots.*, p. 5

[62] Marc-Etienne M.Léveillé, *Gaming industry still in the scope...*

[63] Ibid.

2017: ShadowPad (case study)

A malware family forming modular systems for attacking networks and establishing remote control was detected during an investigation at the NetSarang company. The investigation was initiated after Kaspersky Lab specialists discovered unusual DNS queries in the network of a partner company in the finance sector. The source of these queries was the former company, which has developed proprietary network infrastructure maintenance and server management solutions since 1997. [64] An analysis of the NetSarang software showed a hidden modification: a coded payload ready to be remotely activated from outside.[65]

Pattern of operations[66]

- During the first two stages, a legitimate library nssock2.dll with useful content would get to a computer. Then, however, it was expanded with malicious first stage shell code and subordinate second stage code with the associated plugins.
- This library was launched by NetSarang programs, such as Xshell and Xmanager.
- During the launch, the first stage malicious code reports readiness to Command & Control and downloads configuration data for the particular operation - often redirecting communication to another server dedicated to the operation.
- The second stage began with loading a file from the plugin library and creating a remote control system with a DNS protocol. Again, the plugins worked directly in the process memory, similar to 2011-2013.

[64] [Kaspersky Lab AMR (Anti-Malware Research) and GReAT (Global Research & Analysis Team) official report], *ShadowPad in corporate networks*, https://securelist.com/shadowpad-in-corporate-networks/81432/ (retrieved June 2022)

[65] Ibid.

[66] [Kaspersky Lab official report], *ShadowPad: popular server management software hit in supply chain attack*, p. 2 https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/08/07172148/ShadowPad_technical_description_PDF.pdf (retrieved June 2022)

The following plugins were used in the attack on NetSarang: *API support, configuration, communication, and DNS transmission*,[67] and *the nylalobghyhirgh.com domain*, registered to the email abuse@namesilo.com.[68]

However, before the malware was triggered, it routinely, every 8 hours, contacted its list of C&C domains, sending a report on the environment it penetrated - user, hardware, OS, or domain. The decision to take advantage of the situation or not depended on the hackers. The NetSarang proprietary software is used by several hundred global companies, which put the victim on the Winnti target list, as the Group uses supply chains in their operations.[69]

Immediately after the situation was reported, the vendor responded with an update. The backdoor was, in turn, added to the virus database under the name *Backdoor.Win32.ShadowPad.a*.[70]

2018: Operation ShadowHammer (case study)

Kaspersky Lab discovery[71]

- In January 2019, a successful hacker attack aimed at the major Taiwanese computer hardware manufacturer ASUS was brought to light.
- The malware was detected in the official software updates - ASUS Live Update Utility - that the company provided.
- The attack used an installer version from 2015, although with an up to date manufacturer's key.
- The update files at all times originated from the ASUS official website.

---

[67] Ibid., pp. 7- 11

[68] Ibid., p. 3

[69] [Kaspersky Lab press release] *ShadowPad: jak atakujący ukrywają szkodliwy kod w oprogramowaniu użytkowanym przez setki dużych firm na całym świecie,* https://www.kaspersky.pl/o-nas/informacje-prasowe/2845/shadowpad-jak-atakujacy-ukrywaja-szkodliwy-kod-w-oprogramowaniu-uzytkowanym-przez-setki-duzych-firm-na-calym-swiecie (retrieved June 2022)

[70] Ibid.

[71] Adam Haertle, *Setki tysięcy komputerów ASUS-a zarażonych, także w Polsce,* https://zaufanatrzeciastrona.pl/post/setki-tysiecy-komputerow-asusa-zarazonych-takze-w-polsce/ (retrieved June 2022)

- Normally, any attempt to tamper with the manufacturer's executables should invalidate the digital signature, but this did not happen. Instead, hypotheses suggested a stolen certificate (supplanted after it expired in mid-2018[72]).
- Furthermore, it turned out that as early as June 2018, users of the Reddit forum were discussing the behaviour of their hardware manufacturer's firmware. Their messages urged an immediate critical update. However, their vigilance (as well as that of the antivirus software) was lulled by the legitimacy of the certificates.[73]

The direction of the investigation[74]

- At first, an ASUS setup.exe file with updates was discovered, whose protections were broken by Winnti.[75]
- Kaspersky Lab gathered 200 code samples, which pointed to the operation's persistent, targeted, and multi-staged character. In addition, the samples contained heavily coded MD5 values, which concealed the MAC addresses of network adapters.[76]
- The malware was programmed to search for a specific pool of MAC addresses in the infected network as part of an overall, 5-month operation (June-November 2018). The number of devices that had to be located exceeded 600, the incident affected 57 000 users for certain, and the final tally may have been several hundred thousand.[77]
- It was established that 18% of the infected computers were under the protection of Kaspersky software in Russia. Symantec stated that another 15% were their users from the US.[78]

---

[72] Kim Zetter, *Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers* https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers (retrieved June 2022)

[73] Ibid.

[74] [Kaspersky Lab AMR (Anti-Malware Research) and GReAT (Global Research & Analysis Team) official report], *Operation ShadowHammer: a high-profile supply chain attack*, https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/ (retrieved June 2022)

[75] Ibid.

[76] Kim Zetter, *Hackers Hijacked ASUS Software*...

[77] Haertle, *Setki tysięcy komputerów...*

[78] Kim Zetter, *Hackers Hijacked ASUS Software*...

- It is known that when the criminals had control over the update system, both legitimate and infected packets were sent. However, the former had a higher-class certificate.[79]
- A side effect for users outside the Winnti interest list was that the backdoor would potentially enable the criminals to take control over any of the hundreds of thousands of computers at any time. Unfortunately, this number included new computers with factory-installed Asus Live Update Utility, which became vulnerable to attack the moment they were first turned on.[80]

Winnti tactics and technique

- The attackers were able to replace the WinMain function in the binary with one that copied the backdoor's executable code to memory, and then the assigned code attempted to launch it. The entire replacement was finalised without changing the size of the original file.
  - The executables carried a payload that downloaded a Trojan. The attackers overwrote the ASUS Live Updater with their custom PE executable created in Microsoft Visual C++ 2010. It had a subroutine waiting to be called by WinMain or another implemented code from the same application.
  - The code used the import function with an assigned algorithm, which enabled it to scan all MAC addresses available in the network and then compare MD5 hashes with its list of 55 items. The list could vary depending on the version.
  - Based on the results, the malicious software would then decide which of the two subdomains to download the binary file from, moving to the next phase. It then sent compliant hashes for identifying the victim, and in exchange, an executable shell script then arrived from the server to be run in memory. The investigation revealed 230 such codes assigned to different MAC addresses.

The ASUS reaction[81]

[79] Ibid.
[80] Kim Zetter, *Hackers Hijacked ASUS Software...*
[81] Sam Medley, *Asus releases a patch to fix Operation ShadowHammer vulnerability in Live Update Utility,* https://www.notebookcheck.net/Asus-releases-patch-to-fix-Operation-ShadowHammer-vulnerability-in-Live-Update-Utility.415142.0.html (retrieved June 2022)

- Several dozen hours following the discovery and the report, a teleconference was held between Kaspersky Lab and ASUS, and then the software vendor received all versions of the update tool published since 2018.[82]
- Despite the talks with Kaspersky lab, ASUS customers were not warned, and the manufacturer continued to officially use the certificates utilised in the attack for another month.[83]
- When the media became interested in the subject in March 2019, the company issued an update for Asus Live Update Utility (3.6.8) to patch the exploits and vulnerabilities. In addition, it contained improved end-to-end encryption and stronger verification.[84]
- Additionally, a tool testing the system for malware presence was shared with the users.
- For its part, Kaspersky Lab provided a website for users to check if an owned MAC address is on the list coded in the malware.[85]

2019: Attack on German publicly listed companies (case study)86

Karlsruhe-based GameForge became a target most likely due to its sales revenue on the order of 140 million euros annually and its operations in the gaming industry, where Winnti has the most experience. Additionally, this company's games have a virtual currency that can be acquired or purchased. The history of the incident was as follows:

- One of 700 employees opened an infected mail back in 2011, triggering a malicious program in the background. It was noted that several gamers suddenly became extremely rich in virtual currency.

---

[82] [AMR / GReAT official report] *Operation ShadowHammer...*

[83] Adam Haertle, *Setki tysięcy komputerów...*

[84] Paweł Maziarz, *ShadowHammer - potężny atak na użytkowników komputerów firmy ASUS [AKT.],* http://www.benchmark.pl/aktualnosci/shadowhammer-przestepcy-zainfekowali-nawet-milione-komputerow-fir.html (retrieved June 2022)

[85] Adam Haertle, *Setki tysięcy komputerów...*

[86] Hakan Tanriverdi, Svea Eckert, Jan Strozyk, Maximilian Zierer, Rebecca Ciesielski, *Attacking the Heart of the German Industry,* https://web.br.de/interaktiv/winnti/english/ (retrieved June 2022)

- Hacking the company's servers to change the amounts on the players' accounts were considered.
- The game's servers were reinstalled - the situation did not change.
- According to observations, the players were unaware of the scam.
- Kaspersky software proved ineffective, so a delegation of the vendor was summoned to Karlsruhe.
- In 2011 the matter was not reported to the police, as their experience in investigating cybercrime was deemed useless.
- Specialists thoroughly observed the company network and encountered suspicious files immediately taken for examination.
- The malware revealed that the hackers impersonated the GameForge administrators. At the time of detection, the captured access had reached as many as 40 servers.

Henkel[87] was another lucrative target for the Winnti Group, as in addition to its prominent presence in the FMCG sector, an annual ~10 billion Euro - half the company's total revenue - comes from the industrial binder market which replaced traditional welding.

- Winnti successfully attacked the corporation 2014, which was betrayed by the presence of 3 files with the names of the company's website and captured server.
- The hackers listened to all the traffic that went through it and reached regions in the network that were not directly connected to the internet.
- Despite this, the victim declares that no data was stolen.

Covestro, a producer of chemicals belonging to the Bayer Group - reported in 2019 a serious, in its internal assessment, breach into two systems, although without evidence that any data had been stolen.

Bayer, the pharmaceutical giant, is also directly mentioned on the target list of this Chinese hacker group. According to reports, it has been on the list since 2018. [88]

BASF officially reported an attempted breach in 2015, when the hackers were only stopped at the second cyber protection layer.

---

[87] Matteo Iaiani, Alessandro Tugnoli,Valerio Cozzani, *Analysis of Cybersecurity-related Incidents in the Process Industry*, Reliability Engineering & System Safety, January 2021

[88] Scott Ikeda, *Winnti Malware Rampages Through Major International Companies*, https://www.cpomagazine.com/cyber-security/winnti-malware-rampages-through-major-international-companies/ (retrieved June 2022)

Siemens has confirmed that it was targeted by Winnti in 2016, although the attack was successfully defeated.

Teamviewer, a German vendor of remote computer control software installed on over 1 billion PCs worldwide, admitted that the Group caused a necessity to replace the entire IT infrastructure and costly - multi-million worth - operations to eliminate Winnti from the company's network in 2016.

In response to an attack in 2016, ThyssenKrupp prepared specialist software that impersonated Winnti, sending triggering data packets to corporate networks, which the malicious code is intended to recognise and reveal itself. Before this happened, the hackers were able to acquire fragments of data concerning factory construction works, although - according to the company - the data were of little importance.

I*n 2016, faced with cybernetic attacks, German listed companies pooled together their resources and established the DCSO - German CyberSecurity Organisation. It is tasked with thoroughly investigating cybernetic crime groups for their motives, interests and capabilities.*

The DCSO determined in the course of its investigations that Winnti tracks:

- Lead to China as a source,
- Indicate a mercenary character of the Group, operating at the government's instruction.
    - The thesis of political espionage is confirmed by instances of breaches with the use of Winnti malware in government servers in Hong Kong and in a telecommunication supplier in India, near the headquarters of the Tibetan Government in Exile (a file named CTA was found there, dedicated for an attack on Tibet).
    - Other cases confirming this motive are attacks on the global hotel chain Marriott and Lion Air airways, where the only logical motive was to acquire personal details revealing complete travel histories, including overnight stays. Combined with the point above, travellers may have been spied on also during physical movement, thanks to triangulation. There are several telecommunication companies known to have been penetrated by Winnti.

Additionally, the German intelligence agency BND received a budget of 300 million Euros to establish, among others, a cybernetic investigation system with the specific aim of identifying and preventing incursions by this pathway in German territory.

Conclusion

The Winnti Group continues to operate, expanding its branches following the example of global business. The failures to stop their operations and location in the Middle Kingdom - and most likely also cooperation with the Chinese government - form a solid support base for Winnti and ensure their safety (current Winnti goals and motives correspond to the Chinese government's priorities).[89]

From 2009 to 2019, the Group has changed its appearance and capabilities. They no longer focus on a single industry now, as the versatility of malware, similarities between network structures around the world and their complexity levels allow them to attack adversaries much larger than themselves and remain hidden for a long time.

As can be seen, Winnti is a hacker group specialising in persistent, targeted attacks (APT) on game developers. The way this and similar industries function in itself brings many benefits. The primary target is the supply chain and the interconnected networks, which allow access to multiple companies with a presence in the same environment. Furthermore, mass online distribution of software gives Winnti the privilege of reaching large numbers of users with their malware at a low cost.

Sharing computer networks is a strategic practice applied not only by cooperating third-party entities but also by major corporations that create virtual international environments. This common denomination, which is of the greatest interest to Winnti and which the Group has proven capable of picking apart on multiple occasions, makes any company in the world with a significant stake and worth attacking a target. Regardless of the industry or country of origin.

Therefore, the answer to the question of whether the gaming industry is in real danger is - in the age of globalisation, the entire technological international business is in real danger.

Bibliography/References

[89] Scott Ikeda, *Winnti Malware Rampages Through Major International Companies*, https://www.cpomagazine.com/cyber-security/winnti-malware-rampages-through-major-international-companies/ (retrieved June 2022)

1. Matteo Iaiani, Alessandro Tugnoli,Valerio Cozzani, Analysis of Cybersecurity-related Incidents in the Process Industry, Reliability Engineering & System Safety, January 2021
2. Tom Wijman, The Global Games Market Will Exceed $200 Billion For The First Time as the US Overtakes China, https://newzoo.com/insights/articles/games-market-revenues-will-pass-200-billion-for-the-first-time-in-2022-as-the-u-s-overtakes-china (retrieved June. 2022)
3. [Kaspersky Lab official report] Winnti. More than just a game, p. 2 https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf (retrieved June. 2022)
4. [Kaspersky Lab AMR (Anti-Malware Research) and GReAT (Global Research & Analysis Team) official report], ShadowPad in corporate networks, https://securelist.com/shadowpad-in-corporate-networks/81432/ (retrieved June 2022)
5. [Kaspersky Lab official report], ShadowPad: popular server management software hit in supply chain attack, p. 2 https://media.kaspersky-contenthub.com/wp-content/uploads/sites/43/2017/08/07172148/ShadowPad_technical_description_PDF.pdf (retrieved June 2022)
6. [Kaspersky Lab press release] ShadowPad: jak atakujący ukrywają szkodliwy kod w oprogramowaniu użytkowanym przez setki dużych firm na całym świecie, https://www.kaspersky.pl/o-nas/informacje-prasowe/2845/shadowpad-jak-atakujacy-ukrywaja-szkodliwy-kod-w-oprogramowaniu-uzytkowanym-przez-setki-duzych-firm-na-calym-swiecie (retrieved June 2022)
7. Mark Hatchman, "Winnti" Attacks on Online Gaming Servers Dissected, https://insights.dice.com/2013/04/11/winnti-attacks-on-online-gaming-servers-dissected/ (retrieved June 2022)
8. Michael Mimoso, Winnti Cyberespionage Campaign Targets Gaming Companies, https://threatpost.com/winnti-cyberespionage-campaign-targets-gaming-companies-041113/77717/ (retrieved June 2022)

9. [Official TrendMicro definition] Command and Control [C&C] Server, https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server (retrieved June 2022)
10. [Official Cyberpedia definition] Command-and-Control Explained, https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained (retrieved June 2022)
11. Dmitri Tarakanov, Winnti 1.0 - Analiza techniczna, https://securelist.pl/analysis/7192,winnti_1_0_analiza_techniczna.html (retrieved June 2022)
12. [Microsoft database] Win32/Winnti, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Win32/Winnti (retrieved June 2022)
13. [Microsoft database] Backdoor:Win64/Winnti.A!dha, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win64/Winnti.A!dha&ThreatID=-2147255939 (retrieved June 2022)
14. Hakan Tanriverdi, Svea Eckert, Jan Strozyk, Maximilian Zierer, Rebecca Ciesielski, Attacking the Heart of the German Industry, https://web.br.de/interaktiv/winnti/english/ (retrieved June 2022)
15. Marc-Etienne M.Léveillé, Gaming industry still in the scope of attackers in Asia, https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/ (retrieved June 2022)
16. Ionut Arghire, Researchers Find New Backdoor Used by Winnti Hackers, https://www.securityweek.com/researchers-find-new-backdoor-used-winnti-hackers (retrieved June 2022)
17. Marc-Etienne M.Leveille, Mathieu Tartare, Connecting the Dots. Exposing the arsenal and methods of the Winnti Group, p. 5 https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf (retrieved June 2022)
18. Dr Subramanian Gurubaran, Winnti Hacker Group Uses New Malware to Hack Microsoft SQL Servers, https://gbhackers.com/microsoft-sql-servers/ (retrieved June 2022)
19. [FireEye official report], Doube Dragon. APT41, a dual espionage and cyber crime operation, p. 57-62 https://content.fireeye.com/apt-41/rpt-apt41/ (retrieved June 2022)

20. [Lawsuit at a court in Virginia] https://www.noticeofpleadings.net/barium/files/COMPLAINT_AND_SUMMONS/Summons_John_Doe_1_PACER.pdf
21. Adam Haertle, Setki tysięcy komputerów ASUS-a zarażonych, także w Polsce, https://zaufanatrzeciastrona.pl/post/setki-tysiecy-komputerow-asusa-zarazonych-takze-w-polsce/ (retrieved June 2022)
22. Kim Zetter, Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers (retrieved June 2022)
23. [Kaspersky Lab AMR (Anti-Malware Research) and GReAT (Global Research & Analysis Team) official report], Operation ShadowHammer: a high-profile supply chain attack, https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/ (retrieved June 2022)
24. Sam Medley, Asus releases a patch to fix Operation ShadowHammer vulnerability in Live Update Utility, https://www.notebookcheck.net/Asus-releases-patch-to-fix-Operation-ShadowHammer-vulnerability-in-Live-Update-Utility.415142.0.html (retrieved June 2022)
25. Paweł Maziarz, ShadowHammer - potężny atak na użytkowników komputerów firmy ASUS [AKT.], http://www.benchmark.pl/aktualnosci/shadowhammer-przestepcy-zainfekowali-nawet-milione-komputerow-fir.html (retrieved June 2022)
26. Scott Ikeda, Winnti Malware Rampages Through Major International Companies, https://www.cpomagazine.com/cyber-security/winnti-malware-rampages-through-major-international-companies/ (retrieved June 2022)

Rozdział 12

Czy polski ekosystem prawny jest przyjazny dla stworzeń mitycznych i bytów nadprzyrodzonych?

Wojciech PILSZAK

Pod tym nieco przewrotnym i enigmatycznym tytułem znajdziecie Państwo rozważania oparte na aktach prawnych - zarówno obowiązujących jak i ich projektach - jak również własnym doświadczeniu nabytym zarówno podczas służby w Policji oraz w trakcie pełnienia funkcji biegłego sądowego, a dotyczące funkcjonowania w polskim systemie prawnym narzędzi do tzw. inwazyjnej inwigilacji elektronicznej, w szczególności pojawiających się tendencji do prezentowania takich rozwiązań jako kontrola operacyjna.

Na wstępie należy zaznaczyć, iż przedmiotowe opracowanie nie jest w żaden sposób powiązane z jakąkolwiek aktywnością polityczną, jak również nie ma na celu spowodowania jakichkolwiek działań, w szczególności o charakterze politycznym lub prawnym – stanowi on własną analizę zastanego stanu prawnego oraz zawiera wnioski o charakterze ogólnym związane z prawdopodobnym – bo do dnia przygotowania niniejszego opracowania w żaden sposób oficjalnie nie potwierdzonym - wykorzystaniem omawianego rodzaju narzędzi przez instytucje państwowe w Polsce.

Podjęcie decyzji o przygotowaniu wystąpienia poruszającego tą problematykę, w ramach IV Konferencji Naukowej Przestępczość Teleinformatyczna XXI organizowanej przez Akademię Marynarki Wojennej w Gdyni, wyprzedziło, o co najmniej kilka miesięcy, działania podjęte przez polityków zarówno na szczeblu państwowym jak i europejskim. Powołanie w Parlamencie Europejskim komisji śledczej ds. wykorzystania Pegasusa i innych programów szpiegujących, której pierwsze posiedzenie odbyło się 10 kwietnia 2022 r., jak i działania, rozpoczęte nieco wcześniej przez senacką Komisję Nadzwyczajną do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb

specjalnych*, powołaną w na podstawie decyzji Senatu Rzeczypospolitej Polskiej podjętej w głosowaniu w dniu 12 stycznia 2022 r. stały się dodatkowym bodźcem do przygotowania niniejszego opracowania.*

Zaznaczyć należy, iż z uwagi na obszerność tematu, skoncentrowano się jedynie na możliwościach funkcjonowania w krajowym obrocie prawnym, rozwiązań do inwazyjnej inwigilacji elektronicznej typu „Pegasus", „Phantom" czy też „RCS", ograniczając do niezbędnego minimum wszelkie aspekty uboczne. Wbrew powszechnej, obiegowej opinii, wdrożenie tego rodzaju rozwiązań do stosowania przez służby specjalne nie jest związane jedynie ze zdarzeniami, które miały miejsce w ostatnim czasie, lecz dotyczy okresu od roku 2012, a więc dziesięciu ostatnich lat. Ponieważ jednak - z założenia – służby specjalne nie lubią rozgłosu, dopiero wydarzenia z roku 2021, związane z medialnym nagłośnieniem zastosowania potencjalnej inwigilacji elektronicznej wobec osób w różnym zakresie „niewygodnych" dla sprawujących władzę, skierowały zainteresowanie opinii publicznej (a przynajmniej jej bardziej świadomej części) na wykorzystanie takiego oprogramowania w codziennej pracy organów ścigania, w szczególności na jego zgodność z obowiązującym aktualnie prawem.

Ponieważ, do chwili obecnej, nie doczekaliśmy się w polskim systemie prawnym ustawy regulującej formy, metody i środki pracy operacyjnej, poruszać będziemy się w dużej części w sferze domysłów, albowiem wszelkie szczegółowe regulacje są z niezrozumiałych powodów umieszczane w dokumentach niższego rzędu niż ustawa, nierzadko o różnym stopniu niejawności – np. uchylone Zarządzenie nr pf–634 Komendanta Głównego Policji[1]. Należy tutaj zauważyć, iż autor jest zwolennikiem pojawiającej się w innych opracowaniach koncepcji, w myśl której jawne powinny być wszelkie metody formy i środki w zakresie, który obejmuje ich definicje oraz warunki i okoliczności, w jakich są one stosowane, natomiast informacje o charakterze niejawnym powinny dotyczyć jedynie osób bądź okoliczności, w których metody, formy i środki pracy operacyjnej zostały wykorzystane[2]. W ten sposób wyeliminowana zostałaby z tzw. obrotu prawnego niepewność co do okoliczności, czy określone rozwiązanie może być w obowiązującym stanie prawnym dopuszczalne, czy też nie. Oczywiście, w tym miejscu wyłącznie informacyjnie, należy zauważyć, iż w 2016 roku poprzez zmiany Ustawy - Kodeks

[1] Zarządzenie nr pf–634 Komendanta Głównego Policji z dnia 30 czerwca 2006 r. w sprawie metod i form wykonywania przez Policję czynności operacyjno-rozpoznawczych.

[2] Por. Tadeusz Hanausek, *Kryminalistyka: poradnik detektywa*, Katowice 1993, s. 94

postępowania karnego[3], ustawodawca zabezpieczył się w zakresie wykorzystania dowodów pozyskanych z naruszeniem prawa, jednakże temat ten poruszony zostanie w dalszej części niniejszego opracowania. Jako jeden z punktów odniesienia do rozważań, wykorzystany zostanie projekt Ustawy o czynnościach operacyjno-rozpoznawczych[4], który do chwili obecnej pozostaje jedyną próbą ustawowego uregulowania tej problematyki. Można odnieść wrażenie, iż brak dalszego procedowania tego projektu jest celowym zabiegiem - niezależnym od aktualnej sytuacji politycznej - mającym pozostawić szersze pole do działania organom ścigania, poprzez brak rzeczywistej kontroli – w tym w zakresie ich stosowania – nad czynnościami operacyjno-rozpoznawczymi. Zapoznając się z projektem Ustawy o czynnościach operacyjno-rozpoznawczych znajdziemy w niej definicję pracy operacyjnej, określonej jako zespół przedsięwzięć, jawnych i niejawnych prowadzonych wyłącznie w celu:

- rozpoznania, zapobiegania i wykrywania przestępstw,
- odnajdywania osób ukrywających się przed organami ścigania lub wymiarem sprawiedliwości oraz osób zaginionych, jeżeli zachodzi uzasadnione podejrzenie, że ich zaginiecie jest wynikiem przestępstwa, a także odnajdywanie rzeczy utraconych w wyniku przestępstwa lub mających związek z przestępstwem,
- ustalenia tożsamości osób i zwłok, w przypadku uzasadnionego podejrzenia przestępczego działania[5].

Co do zasady, bardzo podobną definicję pracy operacyjnej odnajdziemy w uchylonym Zarządzeniu nr pf–634 Komendanta Głównego Policji. Określono ją w nim jako wszystkie jawne i niejawne czynności oraz przedsięwzięcia taktyczne i techniczne, oparte na przepisach prawa, podejmowane w związku z realizacją ustawowych zadań Policji w celu rozpoznania, zapobiegania oraz wykrywania czynów zabronionych, a także ścigania ich sprawców[6].

---

[3] Konkretnie od 15 kwietnia 2016 r. przepis art. 168a k.p.k. obowiązuje w brzmieniu nadanym mu ustawą z dnia 11 marca 2016 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw - *Dz.U. z 2016 r. poz. 437.*

[4] Projekt Ustawy o czynnościach operacyjno-rozpoznawczych (Druk nr 353 z dnia 7 lutego 2008 r.).

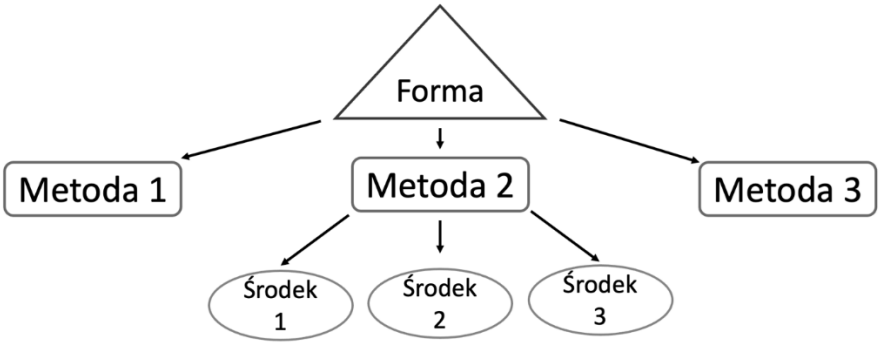
[5] *Ibidem*, art. 2.

[6] § 1 pkt 18 Zarządzenia nr pf–634 Komendanta Głównego Policji z dnia 30 czerwca 2006 r.

Ciekawostką jest, iż w definicji znajdującej się w Zarządzeniu uwypuklono znaczenie przepisów prawa przy prowadzeniu pracy operacyjnej, natomiast w definicji znajdującej się w projekcie Ustawy, ten aspekt został pominięty.

Pomijając ten drobny szczegół, zauważyć należy, iż obie przedstawione powyżej definicje, w sposób wystarczający uwypuklają istotne aspekty czynności operacyjno-rozpoznawczych.

W ramach pracy operacyjnej możemy wyróżnić formy, metody, środki i zasady. Nie rozwodząc się nad szczegółami, które z uwagi na niejawność obowiązujących aktualnie przepisów w tym zakresie mogą odbiegać od wiedzy, jaką dysponuje autor niniejszej publikacji, możemy stwierdzić - stosując bardzo ogólne rozróżnienie – iż **formy** – to kategorie spraw, **metody** – zespół wykorzystywanych środków, a same **środki** – narzędzia, jak na poniższej infografice.



Zgodnie z projektem Ustawy o czynnościach operacyjno-rozpoznawczych, wśród form pracy operacyjnej możemy wyróżnić:

1. **Sprawdzenie** – to czynności zmierzające do wstępnej weryfikacji jednostkowej informacji także na podstawie sprawdzeń w zbiorach kartotecznych i archiwalnych;
2. **Rozpoznanie** – to zespół czynności operacyjno-rozpoznawczych mających na celu uzyskanie, gromadzenie i sprawdzanie niezbędnych do wykonywania zadań służb państwowych informacji o osobach, przedsiębiorstwach lub instytucjach, środowiskach, zdarzeniach, zjawiskach oraz przedmiotach, obiektach lub miejscach;

3. **Rozpracowanie** – to zespół zaplanowanych i systematycznie realizowanych czynności operacyjno-rozpoznawczych wobec osoby fizycznej lub prawnej albo grupy osób w związku z przypuszczeniem lub stwierdzeniem przygotowywania, usiłowania lub dokonania określonego przestępstwa albo nieustalonego rodzaju działalności przestępczej;
4. **Poszukiwanie** – to zespół czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych lub administracyjno-porządkowych, których celem jest zatrzymanie lub ustalenie miejsca pobytu osoby objętej zainteresowaniem procesowym lub operacyjnym uprawnionych organów względnie odnalezienie rzeczy utraconej w wyniku przestępstwa lub mającej z nim związek[7].

Zastosowany w tym projekcie aktu prawnego, regulującego problematykę pracy operacyjno-rozpoznawczej, podział został przytoczony jedynie w celu wskazania rodzaju czynności jakie kryć się mogą pod sformułowaniem „formy pracy operacyjnej".

Każda z powyższych form wymaga zastosowania metod lub metody pracy operacyjnej. Metoda to zespół powiązanych ze sobą jawnych i niejawnych przedsięwzięć i środków zastosowanych w sposób mający doprowadzić do osiągnięcia wyznaczonego celu lub wykonania określonego założeniami zadania[8]. W ramach nieobowiązującego już zarządzenia nr pf-634 KGP jako metody pracy operacyjnej wymieniono: współpracę z osobowymi źródłami informacji, przedsięwzięcia werbunkowe, kombinację operacyjną, operację specjalną, działania maskujące, kontrolę operacyjną, zakup kontrolowany, kontrolowane wręczenie lub przyjęcie korzyści majątkowej, przesyłkę niejawnie nadzorowaną, obserwację, wywiad operacyjny, zasadzkę i analizę kryminalną[9]. Szerszy katalog metod pracy operacyjnej znajdziemy w projekcie Ustawy o czynnościach operacyjno-rozpoznawczych. Wymieniono w nim wywiad, penetrację terenu, zasadzkę, eksperyment, analizę operacyjną, obserwację osób, miejsc i środków transportu, pułapkę, współpracę z osobami fizycznymi, kontrolę korespondencji, wykorzystanie środków technicznych (podsłuch rozmów telefonicznych, podsłuch i podgląd pomieszczeń

[7] Art. 4 Projektu Ustawy o czynnościach operacyjno-rozpoznawczych.
[8] Definicja wynikająca z § 1 pkt 11 Zarządzenia nr pf–634 Komendanta Głównego Policji.
[9] *Ibidem*, § 7 ust. 1.

i osób, podsłuch techniczny środków łączności przewodowej i radiowej, nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu, nadzór elektroniczny środków łączności przewodowej i radiowej), zakup kontrolowany, przesyłkę niejawnie nadzorowaną, obiekty specjalne, kombinację operacyjną, grę operacyjną oraz operacje specjalne[10].

Analizując zapisy tego projektu można odnieść wrażenie, iż jego twórcy umieścili w obrębie jednego terminu – przynajmniej częściowo - zarówno metody jak i środki pracy operacyjnej, jak również dokonali rozbicia na elementy metody pracy określanej w Zarządzeniu nr pf–634 Komendanta Głównego Policji jako „kontrola operacyjna", poprzez określenie w odrębnych artykułach podmiotów uprawnionych i okoliczności jej stosowania – wprost kopiując zapisy z aktów prawnych omówionych poniżej[11]. Zastosowanie takiego rozwiązania może wydawać się kontrowersyjne i zaciemniające sam projekt ustawy, jednakże badanie tej kwestii nie jest przedmiotem niniejszego opracowania.

Przed rozpoczęciem analizy mającej na celu, między innymi, ustalenie z jakimi działaniami na gruncie czynności operacyjno-rozpoznawczych mamy do czynienia przy stosowaniu inwazyjnych metod inwigilacji elektronicznej, oraz czy znajdują one odzwierciedlenie w obowiązujących normach prawnych, należy tytułem krótkiego wprowadzenia wymienić instytucje uprawnione do prowadzenia działań operacyjno-rozpoznawczych o typie i charakterze wymienionych w art. 19 Ustawy z dnia 6 kwietnia 1990 r. o Policji[12], czyli kontroli operacyjnej. W ramach niniejszego opracowania Ustawa o Policji została potraktowana jako dokument bazowy, dla wszelkich odpowiadających jej innym ustawom dotyczących instytucji państwowych dysponujących zbliżonymi lub takimi samymi uprawnieniami jak w niej omawiane. Na chwilę przygotowywania niniejszego opracowania, interesującymi z punktu niniejszych rozważań uprawnieniami dysponują następujące instytucje, dalej nazywane podmiotami uprawnionymi:

- Policja[13];
- Straż Graniczna[14];

---

[10] Art. 2 ust. 3 Projektu Ustawy o czynnościach operacyjno-rozpoznawczych.
[11] *Ibidem*, art. 14 i art. 15.
[12] t.j. Dz. U. z 2021 r. poz. 1882 z późn. zm.
[13] Art. 19 Ustawy z dnia 6 kwietnia 1990 r. o Policji, t.j. Dz. U. z 2021 r. poz. 1882 z późn. zm.
[14] Art. 9e Ustawy z dnia 12 października 1990 r. o Straży Granicznej, t.j. Dz. U. z 2022 r. poz. 1061 z późn. zm.

- Żandarmeria Wojskowa[15];
- Agencja Bezpieczeństwa Wewnętrznego[16];
- Agencja Wywiadu (za pośrednictwem Szefa ABW)[17];
- Centralne Biuro Antykorupcyjne[18];
- Służba Kontrwywiadu Wojskowego[19];
- Służba Wywiadu Wojskowego (za pośrednictwem SKW lub ABW odpowiednio do kompetencji)[20];
- Służba Celno-Skarbowa w ramach Krajowej Administracji Skarbowej[21];
- Inspektor Nadzoru Wewnętrznego Biura Nadzoru Wewnętrznego MSWiA[22];
- Służba Ochrony Państwa[23].

Jak widać z powyższego zestawienia wachlarz instytucji uprawnionych mogących korzystać z możliwości jakie daje kontrola operacyjna jest bardzo szeroki: od służb specjalnych, poprzez organy ścigana po instytucje skarbowe.

Kontrola operacyjna wydaje się być jedyną metodą pracy operacyjnej, której zakres przynajmniej częściowo pokrywa się z możliwościami narzędzi w rodzaju „Pegasusa". Przyjrzyjmy się więc warunkom, w jakich może być

---

[15] Art. 31 Ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, t.j. Dz. U. z 2022 r. poz. 655 z późn. zm.

[16] Art. 27 Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, t.j. Dz. U. z 2022 r. poz. 557 z późn. zm.

[17] Art. 6 ust. 3 Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, t.j. Dz. U. z 2022 r. poz. 557 z późn. zm.

[18] Art. 17 Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, t.j. Dz. U. z 2022 r. poz. 1900.

[19] Art. 31 Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, t.j. Dz. U. z 2022 r. poz. 502, z późn. zm.

[20] Art. 6 ust. 3 Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, t.j. Dz. U. z 2022 r. poz. 502, z późn. zm.

[21] Art. 118 Ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej, t.j. Dz. U. z 2022 r. poz. 813 z późn. zm.

[22] Art. 11n Ustawy z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych, t.j. Dz. U z 2022 r. poz. 1488 z późn. zm.

[23] Art. 42 Ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, tj. Dz. U. z 2019 r. poz. 828 z późn. zm.

ona zastosowana oraz zweryfikujmy czy użycie takich narzędzi, jak wymienione powyżej mieści się w ramach jej stosowania.

W celu omówienia procedury wymaganej przy zastosowaniu kontroli operacyjnej, w głównej mierze wykorzystane zostaną zapisy zawarte w Ustawie o Policji. Jak już wspomniano wcześniej, zapisy dotyczące innych podmiotów uprawnionych, zawarte w regulujących ich działanie aktach prawnych są w znacznej mierze przeniesione z zapisów cytowanej ustawy, w bardzo wielu przypadkach dosłownie.

Pierwszym i niezbędnym warunkiem determinującym możliwość zastosowania kontroli operacyjnej jest działanie w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw z zamkniętego katalogu wymienionego w Ustawie[24]. Nie jest dopuszczalne stosowanie kontroli operacyjnej w zakresie przestępstw innych niż wskazane. Na tym tle podsłuchiwanie polityków czy prokuratorów prezentujących stanowisko odmienne od reprezentowanego przez aktualnie rządzącą partię, może wydawać się co najmniej dyskusyjne. Kolejnym bardzo ważnym elementem, determinującym możliwość zastosowania kontroli operacyjnej jest wyczerpanie innych rozwiązań. Ustawodawca określa to stwierdzeniem „gdy inne środki okazały się bezskuteczne albo będą nieprzydatne" dając jednoznacznie do zrozumienia, iż decyzję o złożeniu wniosku o zastosowaniu kontroli operacyjnej powinna poprzedzić co najmniej analiza obejmująca możliwość wykorzystania innych rozwiązań (lub raczej ich brak). Niejako domyślnie można przyjąć, iż analiza ta powinna zostać przedstawiona właściwemu organowi (Sądowi) wraz z wnioskiem o zastosowanie kontroli operacyjnej. Niestety, praktyka wskazuje, że bardzo często mamy do czynienia z pewnym pójściem na skróty i „automatyzacją" wniosków o kontrolę operacyjną. Wnioskodawca wykorzystuje formułę o nieprzydatności lub braku wystarczalności innych środków, a Sąd bez weryfikacji przyjmuje ją do wiadomości. Warto także zwrócić uwagę na samo określenie zakresu kontroli operacyjnej. Ustawowo zdefiniowana kontrola operacyjna prowadzona jest niejawnie i polega na:

1. uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;
2. uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;

[24] Art. 19.1 Ustawy z dnia 6 kwietnia 1990 r. o Policji.

3. uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;
4. uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;
5. uzyskiwaniu dostępu i kontroli zawartości przesyłek[25].

Każda z powyższych czynności stanowi inny rodzaj kontroli operacyjnej, o czym świadczy także fakt, iż w dalszych zapisach tego samego artykułu znajdziemy wymóg wskazania we wniosku o zastosowanie kontroli operacyjnej jej rodzaju[26]. Niedopuszczalne zatem jest interpretowanie zapisu art. 19 ust. 6 Ustawy o Policji łącznie, jako czynności dopuszczalnych w ramach jednej kontroli operacyjnej. W kontekście bardzo ogólnego przedstawienia możliwości rozwiązań typu „Pegasus" i pokrewne, należy zauważyć, iż dysponują one między innymi takimi możliwościami jak:

- Podsłuch urządzeń w czasie rzeczywistym;
- Pozyskiwanie zawartości urządzeń;
- Podsłuch i podgląd otoczenia urządzeń w czasie rzeczywistym;
- Podejmowanie aktywności „w imieniu" urządzenia;

Porównanie możliwości tego rozwiązania z zakresem kontroli operacyjnej prowadzi do jednoznacznego wniosku, iż nawet gdyby przyjąć, że pojedyncza kontrola operacyjna może obejmować jednocześnie wszystkie działania określone w ustawie, co jak wykazano powyżej jest niedopuszczalne, to możliwości systemów takich jak „Pegasus" wykraczają znacznie poza wskazane w ustawie.

Kolejnym – chyba najbardziej istotnym – elementem związanym z procesem stosowania kontroli operacyjnej jest zarządzanie jej przez Sąd na wniosek instytucji uprawnionej. W teorii powinno to gwarantować, iż wnioskujący nie będą nadużywali tej metody pracy operacyjnej. Taki tryb zarządzania kontroli operacyjnej daje pewność podmiotom współpracującym, iż działają w ramach obowiązującego prawa. Należy pamiętać, że niezbędnym elementem kontroli operacyjnej jest współpraca - przedsiębiorca telekomuni-

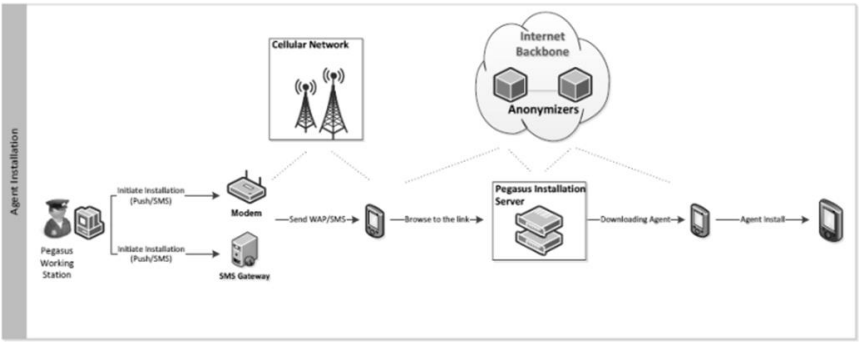
[25] *Ibidem*, Art. 19 ust. 6.
[26] *Ibidem,* Art. 19 ust. 7 pkt 5.

kacyjny, operator pocztowy oraz usługodawca świadczący usługi drogą elektroniczną są obowiązani do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej[27]. W tym miejscu należy wspomnieć o możliwości zarządzenia kontroli operacyjnej nie uzyskując zgody Sądu. Jest to możliwe tylko w dwóch przypadkach, z których pierwszy ma miejsce w sytuacji, jeśli opóźnienie mogłoby to spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa. Wówczas wnioskodawca może zarządzić, po uzyskaniu pisemnej zgody właściwego prokuratora, kontrolę operacyjną, zwracając się jednocześnie do właściwego miejscowo Sądu okręgowego z wnioskiem o wydanie postanowienia w tej sprawie. W razie nieudzielenia przez Sąd zgody w terminie 5 dni od dnia zarządzenia kontroli operacyjnej, organ zarządzający wstrzymuje kontrolę operacyjną oraz dokonuje protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania[28]. Należy jednakże pamiętać, iż zniszczenie materiałów nie jest tożsame z utratą informacji pozyskanych w trakcie pięciu dni kontroli prowadzonej bez zgody Sądu. Drugi z takich przypadków to tzw. czynności inwigilacyjne, zastrzeżone wyłącznie dla Agencji Bezpieczeństwa Wewnętrznego, które mogą trwać nie dłużej niż 3 miesiące i tylko wobec osoby nie będącej obywatelem Rzeczpospolitej Polskiej[29].

Prześledźmy teraz proces infekowania urządzenia przez oprogramowanie typu „Pegasus", przedstawione na poniższym schemacie pochodzącym z opisu produktu[30].

---

[27] *Ibidem*, Art. 19 ust. 12.
[28] *Ibidem*, Art. 19 ust. 3.
[29] Art. 9 ust. 1 Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. Dz. U. z 2019 r. poz. 796, z 2021 r. poz. 464, 815).
[30] *https://ia801005.us.archive.org/1/items/nso-pegasus/NSO-Pegasus.pdf* - data dostępu 26.11.2022 r., s. 13.



Jak wynika z powyższego schematu operator systemu, przy wykorzystaniu ogólnodostępnej infrastruktury telekomunikacyjnej, inicjuje proces instalacji wysyłając wiadomość z zainfekowanym linkiem, po kliknięciu w który, przy wykorzystaniu infrastruktury anonimizującej, następuje połączenie z serwerem instalacyjnym Pegasusa i zainfekowanie urządzenia ofiary. Ten, z założenia uproszczony, opis pozwoli na wykazanie, iż całkowicie bezpodstawnym jest traktowanie działań z wykorzystaniem tego rodzaju rozwiązań jako kontroli operacyjnej. Przypomnijmy, iż warunkami niezbędnymi dla zaistnienia kontroli operacyjnej, oprócz zdefiniowania określonego jej zakresu, jest kontrola sądowa oraz współpraca z podmiotami prywatnymi, mającymi zapewnić infrastrukturę niezbędną do jej realizacji. Podmioty korzystające z rozwiązań typu „Pegasus", uzyskują dostęp do arsenału możliwości znacznie większych niż określone ustawowo ramy kontroli operacyjnej. Nie muszą także liczyć się ze zgodą Sądu na zastosowanie posiadanych rozwiązań – tylko od ich woli zależy czy poinformują Sąd o zastosowaniu systemu. Nie potrzebują także współpracy z wymienionymi w ustawie przedsiębiorcami, bo korzystają z ogólnodostępnej infrastruktury – jedynym podmiotem, z którym współpraca, przynajmniej w zakresie korzystania z rozwiązania może być niezbędna, jest dostawca lub ewentualnie producent zastosowanego rozwiązania. I nie jest to konieczność wynikająca z potrzeby zapewnienia wykorzystania systemu w sposób ograniczający możliwość naruszania praw obywatelskich – jest to konieczność czysto techniczna związana ze szkoleniami, aktualizacjami i bieżącą obsługą systemu.

Na zakończenie tej części opracowania pozostaje do wyjaśnienia jeszcze jedna, bardzo ważna, kwestia. W powyższych rozważaniach, poprzez porównanie aktualnego stanu prawnego z dostępną wiedzą o zakresie

możliwości oprogramowania do inwazyjnej inwigilacji elektronicznej, wykluczyliśmy możliwość funkcjonowania tych rozwiązań w ramach metody pracy operacyjnej określanej jako kontrola operacyjna. Aby – przynajmniej hipotetycznie – określić w jakiej kategorii metod pracy operacyjnej powinno znaleźć się zastosowanie oprogramowania typu „Pegasus", powinniśmy sięgnąć do źródeł historycznych.

W latach 1970-1989, Służba Bezpieczeństwa PRL stosowała poznawczą metodę pracy operacyjnej o nazwie Inwigilacja operacyjna[31]. Była to metoda pracy operacyjnej polegającą na stałym lub okresowym kontrolowaniu zachowania i działania osób, które, zdaniem funkcjonariuszy, mogły w sprzyjających okolicznościach podjąć działalność antysystemową. Tym samym była ona metodą profilaktyczną, pozwalającą na utrzymanie inicjatywy przez służby. Umożliwiała uchwycenie momentu rozpoczęcia działalności uznawanej za wrogą. Ponadto materiały gromadzone w jej trakcie - stanowiące najczęściej obszerny zasób wiedzy wyjściowej o figurancie - dawały możliwość niezwłocznego podjęcia działań[32]. Porównując możliwości oprogramowania do inwazyjnej inwigilacji elektronicznej w rodzaju omawianego, z definicją inwigilacji operacyjnej, można odnieść nieodparte wrażenie, iż zakresy obu się nakładają, czyli stosowanie oprogramowania pokroju „Pegasusa" jest tożsame ze stosowaniem inwigilacji operacyjnej. Jedynym „problemem" jaki pojawia się przed stosującymi tego rodzaju rozwiązania, jest brak jakiegokolwiek ich umocowania w systemie prawnym obowiązującym w chwili obecnej w Rzeczpospolitej Polskiej, czyli - w największym uproszczeniu – ich nielegalność. Jak już wspomniano wcześniej, ustawodawca, poprzez zmianę przepisów Ustawy - Kodeks postępowania karnego, zabezpieczył się w zakresie wykorzystania dowodów pozyskanych z naruszeniem prawa, ograniczając możliwość odrzucenia takiego dowodu wyłącznie z uwagi na fakt pozyskania go z naruszeniem przepisów postepowania lub za

[31] Filip Musiał, *Podręcznik bezpieki. Teoria pracy operacyjnej Służby Bezpieczeństwa w świetle wydawnictw resortowych Ministerstwa Spraw Wewnętrznych PRL (1970-1989)*, Wydanie IV Kraków-Warszawa, s. 326.

[32] *Ibidem*, s. 341.

pomocą czynu zabronionego, jednakże – niezależnie od oceny dopuszczalności dowodów pozyskanych w ten sposób[33] – w odrębnym obszarze należy rozpatrywać odpowiedzialność funkcjonariuszy pozyskujących dowody[34], zarówno w kontekście przestępstwa przekroczenia uprawnień określonego w art. 231 § 1 Kodeksu karnego, jak i jego postaci kwalifikowanej, określonej w § 2 tego artykułu.

Konkludując, a jednocześnie odpowiadając na postawione - w żartobliwej formie - w tytule pytanie, stwierdzić należy, iż w chwili obecnej obowiązujący w Rzeczpospolitej Polskiej „ekosystem prawny" w żadnym zakresie nie jest przyjazny dla rozwiązań określanych nazwą występującego w mitologii greckiej uskrzydlonego konia (Pegasus), jak i innych bytów nadprzyrodzonych, do nazw których z takim upodobaniem sięgają twórcy inwazyjnych rozwiązań do inwigilacji elektronicznej. Jako przyczynę tego stanu wskazać należy:

1. Nieczytelne i niejasne uregulowania prawne, w tym brak ustawy precyzującej działania dozwolone, które mogą być podejmowane w ramach czynności operacyjno-rozpoznawczych – prace na taką ustawą zostały przerwane i nic nie wskazuje na to, aby ktokolwiek był zainteresowany ich wznowieniem. Ponadto część regulacji prawnych związanych z pracą operacyjną umieszczona jest dokumentach wewnętrznych podmiotów uprawnionych, i jest traktowana jako informacje niejawne, co powoduje, iż zamiast ukrywać tylko informacje co do osób bądź okoliczności, w których metody, formy i środki pracy operacyjnej zostały wykorzystane, niejawne są także wszelkie metody formy i środki w zakresie, który obejmuje ich definicje oraz warunki i okoliczności, w jakich są one stosowane. Zgromadzenie wszystkich informacji dotyczących zasad i okoliczności stosowania pracy operacyjnej w jednym, jawnym akcie prawnym najwyższego rzędu zakończyłoby większość spekulacji związanych z jej stosowaniem.

---

[33] Problematyka dopuszczalności dowodu w kontekście, który wydaje się istotny w trakcie rozważań nad inwazyjnymi metodami inwigilacji elektronicznej, została m. in. poruszona w publikacji Sebastiana Brzozowskiego, *Dopuszczalność dowodów uzyskanych z naruszeniem przepisów postępowania w kontekście art. 168a k.p.k.*, Palestra 1-2/2017.

[34] Por. art. 231 Ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2022 r. poz. 1138 z późn. zm).

2. Kontrola sądowa takich rozwiązań jak Pegasus nie istnieje – umiejscowienie po stronie podmiotu uprawnionego wszystkich istotnych elementów systemu powoduje, że tylko od niego zależy czy poinformuje Sąd o zastosowaniu systemu;
3. Chociaż możliwości, jakie daje inwazyjna inwigilacja elektroniczna, są wyjątkowo zbieżne z metodą pracy określaną jako inwigilacja operacyjna, to ta ostatnia została oficjalnie usunięta z podręczników pracy operacyjnej na początku lat 90-tych XX wieku, i nic nie wskazuje na to, iż miałaby do nich powrócić. Być może przywrócenie do łask tej metody pracy z jednoczesnym dostosowaniem jej do aktualnych realiów i wymogów prawnych, byłoby w pewnym zakresie remedium na coraz bardziej wyrafinowane i skuteczne metody komunikacji wykorzystywane przez grupy przestępcze i organizacje terrorystyczne. W definiowaniu na nowo inwigilacji elektronicznej jako elementu inwigilacji operacyjnej, należałoby szczególny nacisk położyć na dostęp inwazyjny do urządzeń - realizowany zarówno poprzez przełamanie lub ominiecie zabezpieczeń jak i wykorzystanie błędów oprogramowania.

Na zakończenie podnieść należy, iż w związku z dynamicznym rozwojem przestępczości oraz adaptowaniem na potrzeby zorganizowanych grup przestępczych nowoczesnych rozwiązań umożliwiających zabezpieczenie komunikacji[35], zastosowanie rozwiązań do inwazyjnej inwigilacji elektronicznej powoli staje się koniecznością a nie fanaberią. Odpowiedzialne państwo powinno jednak stworzyć warunki, aby zasady ich wykorzystania były jasno i czytelnie określone w jawnych i powszechnie dostępnych dla obywatela uregulowaniach prawnych. W przeciwnym wypadku będziemy mieli do czynienia z sytuacją podobną do tej, gdy jeden z absolwentów Wyższej Szkoły Oficerskiej SB MSW im. F. Dzierżyńskiego w Legionowie starał się uzasadniać, że stosowanie techniki operacyjnej nie narusza praw osób inwigilowanych, ponieważ:

- *osoba inwigilowana nie jest w stanie odczuć żadnej dolegliwości związanej z inwigilacją, jako że z uwagi na tajność tych działań nie jest świadoma, że aparat ścigania kontroluje jej zachowanie; [...]*

---

[35] **Wojciech Pilszak, Analiza urządzenia typu Encrophone wykorzystywanego do bezpieczne komunikacji w grupie przestępczej [w:]** Piotr Chlebowicz, Paweł Łabuz, Tomasz Safjański [red.], **Antykryminalistyka. Taktyka i technika działań kontrwykrywczych, Warszawa 2022, s. 90 i nast.**

- *w przypadku stwierdzenia nietrafnego zastosowania inwigilacji organa MSW odwołują ją dyskretnie bez potrzeby naprawiania szkód wobec obywatela niesłusznie podejrzewanego, gdyż szkód takich przy prawidłowo realizowanej inwigilacji być nie mogło;*
- *mimo że środki T[echniki] O[peracyjnej] są w stanie rejestrować nie tylko działalność przestępczą, lecz i fakty z życia prywatnego osoby inwigilowanej, to jednak z uwagi na nieprzydatność tych ostatnich do ścigania karnego, jak i ustawowy obowiązek zachowania tajemnicy — SB nie jest zainteresowana w ujawnianiu szczegółów związanych z życiem osobistym obywateli, którymi się interesuje*[36].

O tym, jakie tego rodzaju rozumowanie niesie konsekwencje, w szczególności w obszarze budowania zaufania obywateli do państwa, chyba nie trzeba nikogo uświadamiać.

Literatura:

1. Tadeusz Hanausek, *Kryminalistyka: poradnik detektywa*, Katowice 1993,
2. Filip Musiał, *Podręcznik bezpieki. Teoria pracy operacyjnej Służby Bezpieczeństwa w świetle wydawnictw resortowych Ministerstwa Spraw Wewnętrznych PRL (1970-1989)*, Wydanie IV Kraków-Warszawa 2020.
3. Sebastian Brzozowski, *Dopuszczalność dowodów uzyskanych z naruszeniem przepisów postępowania w kontekście art. 168a k.p.k.*, Palestra 1-2/2017.
4. Piotr Chlebowicz, Paweł Łabuz, Tomasz Safjański [red.], *Antykryminalistyka. Taktyka i technika działań kontrwykrywczych*, Warszawa 2022.
5. Paweł Łabuz, Jacek Kudła, Tomasz Safjański [red.], *Czynności operacyjno-rozpoznawcze polskich służb ochrony prawa w prawie krajowym i międzynarodowym,* Warszawa 2022.
6. Michał Gabriel-Węglowski, *Działania Antyterorystyczne. Komentarz*, Warszawa 2018.

Źródła w internecie:

[36] Filip Musiał, *Podręcznik bezpieki…* s. 184.

1. *https://ia801005.us.archive.org/1/items/nso-pegasus/NSO-Pegasus.pdf* - data dostępu 26.11.2022 r.

Akty prawne (obowiązujące, uchylone i projekty):

1. Ustawa z dnia 6 kwietnia 1990 r. o Policji, t.j. Dz. U. z 2021 r. poz. 1882 z późn. zm.
2. Ustawa z dnia 12 października 1990 r. o Straży Granicznej, t.j. Dz. U. z 2022 r. poz. 1061 z późn. zm.
3. Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, t.j. Dz. U. z 2022 r. poz. 655 z późn. zm.
4. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, t.j. Dz. U. z 2022 r. poz. 557 z późn. zm.
5. Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, t.j. Dz. U. z 2022 r. poz. 1900.
6. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, t.j. Dz. U. z 2022 r. poz. 502, z późn. zm.
7. Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej, t.j. Dz. U. z 2022 r. poz. 813 z późn. zm.
8. Ustawa z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych, t.j. Dz. U z 2022 r. poz. 1488 z późn. zm.
9. Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, tj. Dz. U. z 2019 r. poz. 828 z późn. zm.
10. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. Dz. U. z 2019 r. poz. 796, z 2021 r. poz. 464, 815).
11. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2022 r. poz. 1138 z późn. zm).
12. Zarządzenie nr pf–634 Komendanta Głównego Policji z dnia 30 czerwca 2006 r. w sprawie metod i form wykonywania przez Policję czynności operacyjno-rozpoznawczych.
13. Projekt Ustawy o czynnościach operacyjno-rozpoznawczych (Druk nr 353 z dnia 7 lutego 2008 r.).

Rozdział 13

Genealogia na usługach oszustów i wymiaru sprawiedliwości

Joanna LUBIERSKA[1]

Badania genealogiczne polegają na poszukiwaniu osób w celu odtworzenia powiązań rodzinnych. Zajmują się nimi hobbyści, regionaliści oraz naukowcy, a poszukiwania mogą dotyczyć nie tylko ustalenia koligacji osoby poszukującej, ale i osób w żaden sposób niespokrewnionych z szukającym. Genealogia, jako nauka pomocnicza historii, w ostatnich latach stała się niezwykle popularna wśród różnych grup społecznych, bez względu na wiek, czy wykształcenie. Na wzrost zainteresowania badaniami relacji rodzinnych wpłynęło kilka czynników, m.in.: dostępność dokumentów archiwalnych. Pierwszym z nich jest digitalizacja zbiorów pochodzących z zasobów archiwów państwowych, uczelni wyższych i muzeów oraz umieszczanie ich w Internecie, spowodowało, że poszukiwania z roku na rok cieszą się coraz większym zainteresowaniem. Możliwość przeglądania w dowolnym miejscu i czasie dokumentów, książek czy gazet sprawiła, że przestały mieć znaczenie kwestie związane z przygotowaniem wyjazdu do archiwum (takie jak dostosowanie się do godzin pracy danej instytucji, dojazd do innego miasta, nocleg, umiejętność korzystania z katalogów podręcznych, poruszanie się po archiwum, etc.). drugim powodem jest indeksowanie przez wolontariuszy ksiąg metrykalnych wybranych parafii i stworzenie wyszukiwarek umożliwiających szybsze wyszukiwanie dokumentu dotyczącego określonej osoby (najczęściej metryki chrztu, ślubu lub zgonu).
Do najczęstszych motywów podejmowania poszukiwań genealogicznych należą m.in.:

- chęć poznawcza wynikająca z ciekawości, pojawiająca się niekiedy po stracie bliskich,

[1] Uniwersytet im. Adama Mickiewicza w Poznaniu, Stowarzyszenie Polscy Profesjonalni Genealodzy, joanna.lubierska@amu.edu.pl, ORCID iD: 0000-0001-7422-7724

- konieczność odtworzenia historii rodzin na potrzeby publikacji regionalnych lub naukowych,
- chęć uregulowania spraw majątkowych (zbycie nieruchomości obciążonej służebnościami) i spadkowych (nabycie prawa do spadku),
- snobistyczne (wykazanie przynależności do określonego stanu, najczęściej szlacheckiego lub chęć udowodnienia powiązań ze znaną osobą lub rodziną).

Obok pozytywnych motywów skłaniających do podjęcia badań genealogicznych, mogą pojawić się także „negatywne", wynikające z wielu pobudek, wśród których mogą być i powody z punktu widzenia organów ścigania określane jako przestępcze. Celem tego tekstu jest przedstawienie kilku, wybranych przykładów właśnie takiego wykorzystania genealogii.

Przypadek 1. „Jak stworzyć drzewo genealogiczne za milion złotych"

Wiosną 2018 roku w poznańskiej prasie, a później w ogólnopolskich gazetach dziennikarze zaczęli opisywać sprawę 50-letniego Krzysztofa G., ps. Gering, który za stworzone przez siebie fikcyjne drzewo genealogiczne udowadniające prawa do atrakcyjnych nieruchomości w kilku polskich miastach, w ciągu kilku lat otrzymał od brytyjskiego małżeństwa milion złotych. Ze wstępnych ustaleń śledczych wynikało, że Krzysztof G., posiadający wykształcenie podstawowe, podawał się za znanego łódzkiego prawnika, zajmującego się m.in. badaniami genealogicznymi. Był bardzo starannie przygotowany: stworzył fikcyjną historię rodziny pokrzywdzonych – inżyniera z Wielkiej Brytanii oraz jego żony – według której mieli być oni potomkami zamożnej rodziny posiadającej przed II wojną światową na terenie Łodzi, Poznania i innych miast majątek utracony w wyniku powojennych wywłaszczeń. Krzysztof G. był też bardzo przekonujący, systematycznie dostarczał swoim klientom sfałszowane dokumenty dotyczące utraconych majątków, a także przedstawiał fałszywe wyniki badań genealogicznych. W trakcie śledztwa okazało się, że przygotował prawie pięćset dokumentów.

Krzysztof G. powoływał się na wpływy w sądach w Łodzi, Poznaniu i Koninie i obiecywał pośrednictwo w uzyskaniu zwrotu nieruchomości lub pozyskaniu odszkodowania za nie. Przekonani o swoim polskim pochodzeniu pokrzywdzeni regularnie przelewali na konto bankowe podejrzanego określone sumy pieniężne.

Na poczet przyszłego spadku oraz kosztów związanych z jego odzyskaniem Krzysztof G. wyłudził od swoich ofiar przez sześć lat prawie milion złotych. Zdobyte w ten sposób pieniądze przeznaczał na zakup przedmiotów

kolekcjonerskich. W toku śledztwa okazało się, że był kolekcjonerem i rekonstruktorem, ze szczególnym zamiłowaniem zbierał eksponaty z czasów II wojny światowej (stąd pseudonim „Gering"). Podczas przeszukania w jego mieszkaniu policjanci znaleźli między innymi wyrzutnię granatów i pocisk przeciwlotniczy. Do oskarżenia o oszustwo dodano więc jeszcze zarzut nielegalnego posiadania broni.

> Działania CBŚP wsparte zostały przez saperski patrol rozminowania JW w Tomaszowie Mazowieckim, ponieważ w mieszkaniu podejrzanego znajdował się niemal arsenał pochodzący z okresu II wojny światowej. W jego lokalu był pocisk artyleryjski 75 mm, pocisk przeciwlotniczy kal. 37 mm, mechanizm zapalnika z układem ogniowym grupy zapalników AZ, dwa pociski podkalibrowe kal. 46 mm, pocisk podkalibrowy kal. 76 mm, granat odłamkowy garłacz, wyrzutnia 10 mm granatu przeciwpancernego, 4 szt. amunicji do broni 7,92 mm z prochem[2].

W miejscu zamieszkania podejrzanego Krzysztofa G. na poczet przyszłych kar zabezpieczono mienie o wartości prawie 300 tysięcy złotych oraz dokumenty, na podstawie których podejrzany oszukiwał pokrzywdzonych. Razem z Krzysztofem G. zatrzymano 51-letnią Monikę D., podejrzaną o składanie fałszywego oświadczenia notarialnego, czym pomagała podejrzanemu w legalizowaniu środków wyłudzonych od pokrzywdzonej rodziny. Krzysztofowi G. postawiono zarzut „popełnienia oszustwa, podrabiania dokumentów, powoływania się na wpływy oraz prania pieniędzy". Za zarzucane mu czyny groziła mu kara do 12 lat więzienia. Ostatecznie w 2019 roku sąd skazał go na 4 lata pozbawienia wolności[3].

Budowa czteropiętrowej kamienicy na warszawskiej Ochocie przy ulicy Joteyki 13 rozpoczęła się w 1939 roku, ale przed II wojną światową powstał tylko parter. Dopiero po zakończeniu wojny dobudowane zostały kolejne piętra i od tego momentu aż do 2008 roku budynek należał do Skarbu Państwa, a następnie został zreprywatyzowany. Zarządzanie kamienicą po decyzji Samorządowego Kolegium Odwoławczego (w skrócie: SKO), stołeczny Ratusz przekazał w 2010 roku spadkobiercom dawnych właścicieli, czyli braciom Kaplan oraz Aleksandrowi Piekarskiemu. Kuratorem tego ostatniego

---

[2] Źródło: http://cbsp.policja.pl/cbs/aktualnosci/156793,CBSP-zatrzymalo-Geringa.html (dostęp: 22.02.2020).

[3] Źródło: https://www.forbes.pl/finanse/oszustwo-falszywe-drzewo-genealogiczne-prawa-do-przedwojennego-majatku/nmfwpg1 (dostęp: 22.02.2020).

w 2008 roku ustanowiono Bogumiłę Górnikowską, która następnie przed sądem zeznała, zwrócił się do niej adwokat Roman Porwisz, reprezentujący synów współwłaścicielki wspomnianej nieruchomości i zapytał, czy nie zostałaby kandydatem na kuratora drugiego współwłaściciela, Aleksandra Piekarskiego. O Piekarskim nie wiedziano nic, ani gdzie mieszkał, ani kiedy i gdzie się urodził. Założono więc, że trzeba będzie sprawdzić około stu Aleksandrów Piekarskich, czym miał się zająć wynajęty archiwista.

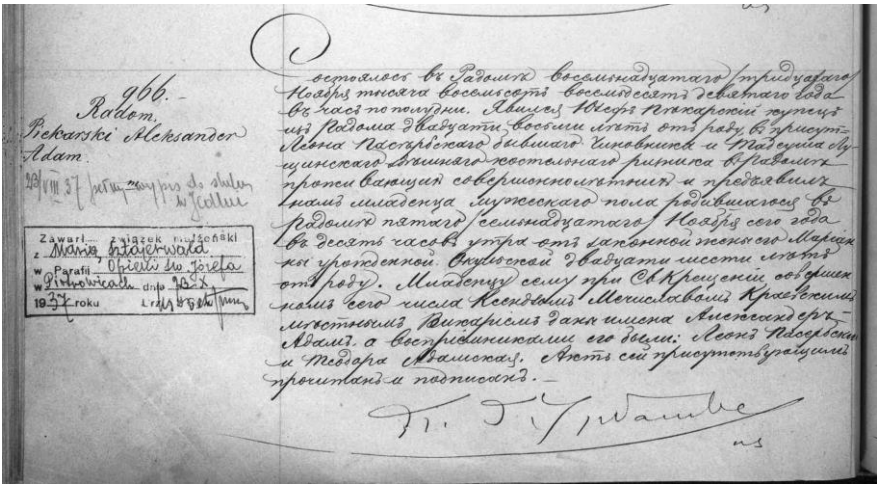
Źródło: Centralne Biuro Śledcze Policji, https://cbsp.policja.pl/cbs/aktualnosci/156793,CBSP-zatrzymalo-Geringa.html (dostęp: 20.02.2020).

Rysunek 3. Zabezpieczone pociski w mieszkaniu Krzysztofa G. oraz zdjęcie z zatrzymania Geringa

Przypadek 2. Historia warszawskiej kamienicy i jej długowiecznego współwłaściciela

Zaniepokojeni lokatorzy kamienicy przy ulicy Joteyki 13 przeprowadzili własne śledztwo, w trakcie którego ustalili rok urodzenia przedwojennego właściciela Aleksandra Piekarskiego. Nadto, sprawą – po ich interwencji

– zainteresowało się „Stowarzyszenie Miasto Jest Nasze”[4], a następnie gazeta „Fakt”. W jednym z artykułów zarzucono Bogumile Górnikowskiej wprost, iż działała niezgodnie z przepisami prawa, ponieważ urodzony w 1889 roku Aleksander Piekarski, w momencie reprywatyzacji miałby 118 lat, a dodatkowo budynek nie został ukończony przed wojną, dlatego nie powinien znaleźć się na liście dóbr do zwrócenia.



Źródło: https://www.familysearch.org/ark:/61903/3:1:S3HT-XC94-XY5?fbclid=IwAR12sOku80YRUwNLwJInAToCm4foedLTJUdSEzc8bgIP5Vv3buaLv1bkmEM&i=74&wc=9TM3-923%3A21713801%2C48550701%2C49969501&cc=1407440 (dostęp: 20.02.2020).

Rysunek 2. Akt urodzenia Aleksandra Adama Piekarskiego, Archiwum Diecezji Radom-skiej, Akta par. św. Jana Chrzciciela w Radomiu, nr aktu 966/1889

[4] Warszawskie stowarzyszenie Miasto jest Nasze powstało w październiku 2013 roku jako sprzeciw mieszkańców wobec polityki stołecznego ratusza m.in. na: „prowadzenie chaotycznej polityki przestrzennej, bierność wobec reprywatyzacji budynków użyteczności publicznej, placówek edukacyjnych i parków, traktowanie urzędów jak prywatnych folwarków, nepotyzm czy wreszcie ignorowanie głosu mieszkańców przy podejmowaniu kluczowych decyzji inwestycyjnych i prowadzenie konsultacji społecznych w sposób fasadowy”. Organizacja skupia ponad dwustu członków niezwiązanych z partiami politycznymi i jest obecnie największym ruchem miejskim w Warszawie, źródło: https://miastojestnasze.org/mjn/historia/ (dostęp: 17.10.2021).

Mecenas Roman Porwisz który składał wniosek o ustanowienie kuratora dla Aleksandra Piekarskiego, twierdził, że nie wiedział, iż Piekarski urodził się w 1889 roku, a zmarł, jak ustalono w trakcie kwerendy, w 1959 roku. Adwokat tłumaczył, że gdy tylko dowiedział się o jego śmierci, wystąpił do sądu o zniesienie kurateli, która została uchylona w 2011 roku i od tego czasu kuratora w tej sprawie nie było.

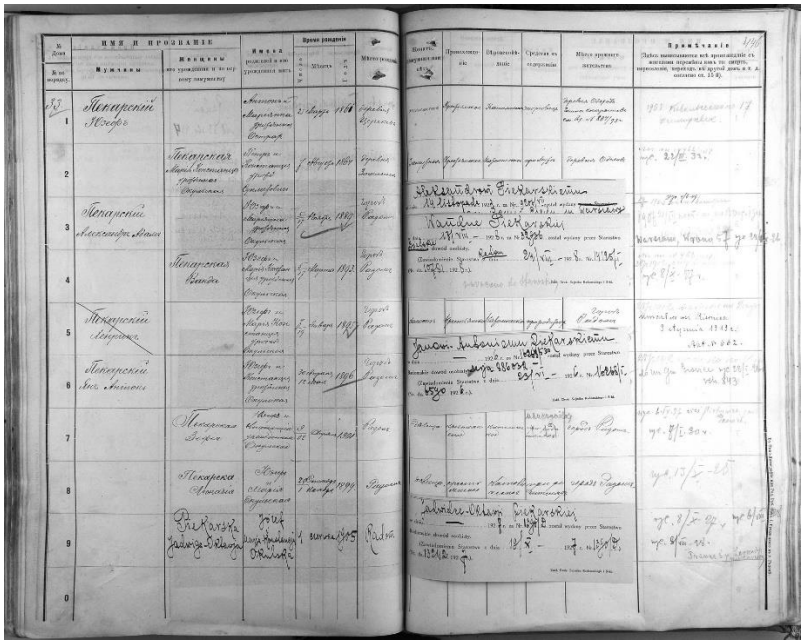
Reprywatyzacją kamienicy przy ulicy Joteyki 13 zajmował się m.in. Naczelny Sąd Administracyjny. Zgodnie z wyrokiem, który jest ostateczny, uchylona została decyzja SKO z 2008 roku. Na jej podstawie spadkobiercy otrzymali odszkodowanie oraz prawo do zarządzania nieruchomością na Ochocie. Prokuratura Okręgowa w Warszawie potwierdziła, że prowadzone było śledztwo dotyczące przekroczenia uprawnień lub niedopełnienia obowiązków służbowych przez działających w celu osiągnięcia korzyści majątkowej na rzecz spadkobierców nieruchomości, urzędników SKO w Warszawie oraz funkcjonariuszy publicznych z urzędu m. st. Warszawy w związku z wydawanymi przez nich decyzjami administracyjnymi[5].

W trakcie kwerendy genealogiczno-archiwalnej okazało się, że istnienie stu Aleksandrów Piekarskich w przedwojennej Warszawie jest niemożliwe. Ustalenie danych właściwego Aleksandra Piekarskiego zajęło kilka godzin, z wyjazdem do Radomia poszukiwania zajęły jeden dzień. Kluczowe dla tej sprawy ustalenia, które przeprowadził Adam A. Pszczółkowski[6], były następujące: Aleksander Adam Piekarski urodził się 17 listopada 1889 roku w Radomiu, jako syn Józefa kupca radomskiego i Marii-Konstacji z Okulskich. Wraz z rodzicami i rodzeństwem: Wandą, Henrykiem, Janem-Antonim, Zofia, Leokadią, Jadwigą-Oktawią mieszkał w Radomiu pod numerem hipotecznym 33. Po powstaniu niepodległego państwa polskiego w 1918 roku wyjechał do Warszawy, gdzie otrzymał dowód osobisty dnia 11 listopada 1923 roku o numerze 9206/VII. W 1926 roku był zameldowany przy ulicy Wroniej 57 w Warszawie. Zawód urzędnik. W 1930 roku pod tym samym adresem wymieniony już został jako przemysłowiec. Wkrótce przeprowadził się na

[5] Źródło: https://wiadomosci.com/warszawa-kamienice-przy-joteyki-13-oddano-zarzad-wspolwlascicielowi-ktory-zyl-50/ (dostęp: 22.02.2020).

[6] Adam Antoni Pszczółkowski – genealog, heraldyk specjalizujący się w badaniach nad szlachtą północnego Mazowsza, autor licznych opracowań, konsultant genealogiczny Związku Szlachty Polskiej, członek Sekcji Demografii Historycznej Komitetu Nauk Demograficznych PAN.

Wspólną 36. Dnia 23 października 1937 roku w kościele św. Józefa Oblubieńca w Jedlni-Letnisko (pod Radomiem) wziął ślub z Marią Sztajerwald. Po ślubie przeniósł się do warszawskiej kamienicy przy ulicy Złotej 9, podczas okupacji niemieckiej (1940 rok) – adres uległ zmianie – odtąd numer 7. Zmarł 17 listopada 1959 roku, dokładnie w siedemdziesiąte urodziny, pod adresem Kniewskiego 7[7], a więc w tym samym miejscu, w którym mieszkał przed wojną. W „Życiu Warszawy" z dnia 24 listopada 1959 roku żona i rodzina złożyła podziękowała za uczestnictwo w pogrzebie.



Źródło: fot. Adam A. Pszczółkowski.

Rysunek 3. Księga ludności stałej miasta Radom, Archiwum Państwowe w Radomiu, Kniga postojannago narodonaselenija goroda Radoma s nr 24 po nr 36, 1901–1928, sygn. 9816, k. 446

W trakcie kwerendy ustalono w jakich okolicznościach Aleksander Piekarski nabył nieruchomość w ówczesnej kolonii we wsi Czyste - posesję

[7] Ówczesna nazwa ulicy Złotej.

przy ulicy Joteyki 13. Ówczesna właścicielka gruntu Kaplanowa nie miała wystarczających środków na postawienie kamienicy, dlatego odstąpiła Piekarskiemu część praw do gruntu. Piekarski, jako producent skrzyń i właściciel wielu tartaków był majętnym człowiekiem. W 1939 roku rozpoczął budowę kamienicy, która została ukończona po II wojnie. Wedle „Spisu właścicieli domów w Mieście Stołecznym Warszawie" z końca 1938 roku – funkcjonowały przy tej ulicy tylko budynki o numerach 4, 6 i 8.

Biblioteka Narodowa w Warszawie ma w swoim zasobie m. in. słowniki biograficzne (nawet osób zasłużonych dla niewielkich miejscowości), archiwalne książki telefoniczne, kartoteki personalne ułożone alfabetycznie, zbiory nekrologów, wycinki prasowe, etc. Wśród nich jest rozpoczęty w 1935 roku i nigdy niedokończony „Polski Słownik Biograficzny" (w skrócie: PSB), który znajduje się w każdej bibliotece – mają go w swoich zasobach te ważniejsze warszawskie, i krakowskie, i wrocławskie, jest również dostępny w Miejskiej Biblioteki Publicznej w Radomiu, która sąsiaduje z Sądem Okręgowym w Radomiu. W 1981 roku redakcja PSB rozpoczęła zbieranie materiałów dla osób i rodzin, których nazwiska zaczynają się na Pie- i przy tej okazji zainteresowała się rodzeństwem Piekarskich. Opracowano więc biogramy Jadwigi i Wandy Piekarskich, dodając przy okazji informacje o pozostałych członkach rodziny. Wtedy okazało się, że wszystkie dzieci Józefa Piekarskiego i Marii-Konstancji z Okulskich brały udziały w dziele niepodległościowym i konspiracyjnym. I tak:

1. Aleksander (*1889) – żołnierz AK,
2. Wanda (*1893 +1972) – AK, więźniarka Ravensbrück,
3. Henryk (*1895 +1919) – wedle ustaleń zginął w walkach z Ukraińcami, w bitwie pod Kiernicą,
4. Jan (*1896 +1942) – AK, zamordowany w Auschwitz,
5. Leokadia (*1899),
6. Zofia (*1901 +1941) – AK, rozstrzelana przez Niemców w Pińczowie,
7. Jadwiga (*1905 +1944) – AK, sanitariuszka w powstaniu warszawskim, zginęła.

Henryk ma teczkę odznaczeniową w Wojskowym Biurze Historycznym (niegdyś Centralne Archiwum Wojskowe), Wanda ma teczkę odznaczeniową (Virtuti Militari) i personalną. Jest również teczka personalna Aleksandra, ale prawdopodobnie nikt do niej nie zajrzał, a nawet nie sprawdził, że zachowała się.

Piatkowska Janina Eisenwarenhdlg. Hafenstr 143a 834 27
Piatkowska Karolina Schreibwaren Szembek-Pl 6 10 26 66
Piatkowska Kazimiera Beamtin Ropienstr 36 216 73
Piatkowska Maria Seifengesch. Wspolnastr 31 941 75
Piatkowska Maria Dingastr 25 11 23 69
Piatkowska-Chrzanowska Melania Em.-Plater-Str 25 884 82
Piatkowska Regina Kozmirskastr 2 980 51
Piatkowska Stanislawa Zuckerwarenladen Kazimierz-Wielki-Pl 2 695 16
Piatkowska Stefania Nordsüdallee 227/233 932 35
Piatkowska Walentyna Asfaltowastr 6 442 11
Piatkowski Adam Moniuszkostr 4 244 90
Piatkowski Antoni Wein- und Spirituosenhdlg. Skaryszewskastr 13 10 06 70
Piatkowski Antoni Grottger-

Piechnikowa Henryka Damen u. Herrenkonfektion fr. Irena Trzaska Musikinstrumente Marschallstr 91 966 63
Piechocki Adam Ein- u. Verk. v. Flaschen u. versch. Abfällen Litzmannstadt Str 82 217 19
Piechocki Adam Eugeniusz Miedzianastr 14 682 16
Piechocki Czeslaw Spedition Wilanowskastr 8 895 05
Piechocki Lukasz Szopskastr 7 10 54 90
Piechocki Wawrzyn + Vulkanisieranstalt Bahnhofstr 31 523 98
Piechorowska Zofia Seifenwarenhdlg. Zlotastr 44 350 87
Piechorowski Stanislaw Zlotastr 16 590 81
Piechotko Kazimierz Maciej Nieporetskastr 4 10 13 04
Piechotowa Janina Schneiderin Litewskastr 9 702 20
Piechowiak Brunon Wasserstoffallee 77 10 34 87
Piechowicz Aleksander Obstladen Mlynarskastr 20 306 78
Piechowicz Jozef Advokat Se-

Piekarska Zofia Wysockistr 58a 10 19 35
Piekarski A. & Co. GmbH Kreuzstr 30 636 86
Piekarski Aleksander Pappe- u. Papierfabrik Nalewkistr 2a 12 14 20
Piekarski Aleksander Ostendstr 142 10 02 12
Piekarski Aleksander Zlotastr 7 320 07
Piekarski Czeslaw Ludwikastr 6 203 32
Piekarski Israel Siennastr 29 222 95
Piekarski Konstanty Wolskastr 74 444 33
Piekarski Ludwik Glaswarenlbr. u. Lager Marschallstr 132 336 21
Piekarski Ludwik Franciszek Wirtschaftler Kruczastr 8 879 75
Piekarski Romuald Mlodkastr 14 10 11 68
Piekarski St. Wlodkowski K. Gemüse u. Obstverk. Mirowskastr 9 332 73
Piekarski Stefan + Gartenarbei-

Pienkowski Jan Galanterie Radomer Str 31 859 51
Pienkowski Jan Küchengeräte Ogrodowastr 62 327 58
Pienkowski Jan Torpl 3 212 98
Pienkowski Konstanty Litewskastr 4 701 66
Pienkowski Marian Dr. Kinderarzt Szopenstr 6 999 47
Pienkowski Mieczyslaw Essenwarengesch. Kilinskistr 1 11 54 43
Pienkowski Stanislaw Bankbeamt. Marschallstr 25 823 39
Pienkowski Stefan Prof. Dr. Hozastr 69 963 67
Pienkowski Wladyslaw Baumat. u. techn. Art. Kalkverkaufspunkt Neue Burgstr 69a 705 01
Pienkowski Wladyslaw Kalk Zement u. Gipslager Neue Welt 59 592 61
Pieprzycki Piotr Schreibmasch. Neue Burgstr 3 710 75
Piernikarska Maria Jadwiga Koszykowastr 79a 994 12

Pietkiewicz Kazimierz K bildhauer Dzieanikarskastr 12 6
Pietkiewicz Zofia II Mark halle 461 51
Pietkiewiczowa Barbara Zahnarzt Wspolnastr 16 88
Pietkiewiczowa Helena arztin Pius-XI-Str 46 87
Pietkowska John Halina arzt Wspolnastr 26 88 96
Pietkowski Radzimir Ing. str 1 90
Pietnik Marceli Eisgrubens 26
Pietnik Maria Eisenstr 43 58
Pietos Ludwik Ogrodowas 22
Pietowski Ksawery Techn Mokotowskastr 29 73
Pietowski Stefan Mechan. zisionslbr. Konopackastr 19 Direktion 10 5
Verw. Techn. u. Handelsbu
Werkst. 10 5
10 3

Źródło: zb. Mazowieckiej Biblioteki Cyfrowej.

Rysunek 4. Amtliches Fernsprechbuch für den Distrikt Warschau 1942 = Urzędowa Książka Telefoniczna dla Dystryktu Warschau 1942, s. 134

Zastanawiające było, gdzie znajduje się grób przywróconego do życia przez Sąd Okręgowy w Radomiu Aleksandra Piekarskiego. W dostępnych warszawskich wyszukiwarkach cmentarnych nie występował żaden Aleksander Piekarski, choć w Warszawie miało być ich przecież stu. W rozwikłaniu zagadki nie pomogła wdowa po Piekarskim – ponieważ dziękując w „Życiu Warszawy" za uczestnictwo w pogrzebie, nie wspomniała, gdzie ten pogrzeb się odbył.

W Polskim Słowniku Biograficznym wspomniano o grobie rodzinnym Piekarskich w Jedlni-Letnisko. Tamtejszy cmentarz znajdujący się na przedmieściach Radomia, nie należy do małych, nie jest też zinwentaryzowany. Udało się jednak odszukać grób całej rodziny Piekarskich (rodzice, dzieci i dwie synowe), a wszyscy zostali zapisani z datami dziennymi zgonów. Grób Aleksandra Piekarskiego znajduje się 14 kilometrów od Sądu Okręgowego w Radomiu, który wydał dokument o zmartwychwstaniu Aleksandra Piekarskiego w 2010 roku.

Kolejnym budynkiem sąsiadującym z Sądem jest Urząd Stanu Cywilnego, w którym znajdują się dokumenty dotyczące tej rodziny. Dalsze archiwalia (w tym metryki chrztu Aleksandra i jego rodzeństwa) można znaleźć w budynku oddalonym od Sądu o ponad kilometr (15 minut piechotą). Warto również dodać, że w Jedlni-Letnisko jest ulica Rodziny Piekarskich.

Źródło: fot. Adam A. Pszczółkowski

Rysunek 5. Grób rodziny Piekarskich w Jedlni-Letnisko

Przypadek 3. Genealogia genetyczna czyli sprawa Golden State Killera

Ten przypadek z oszustwami nie ma nic wspólnego; to sprawa kryminalna dotycząca kilkunastu zabójstw, które wydarzyły się w Stanach Zjednoczonych w latach 70. i 80. XX wieku. Mordercę złapano po wielu latach dzięki genealogicznemu serwisowi internetowemu. Genealogia w tym wypadku przysłużyła się społeczeństwu amerykańskiemu, a nie stała narzędziem oszustów.

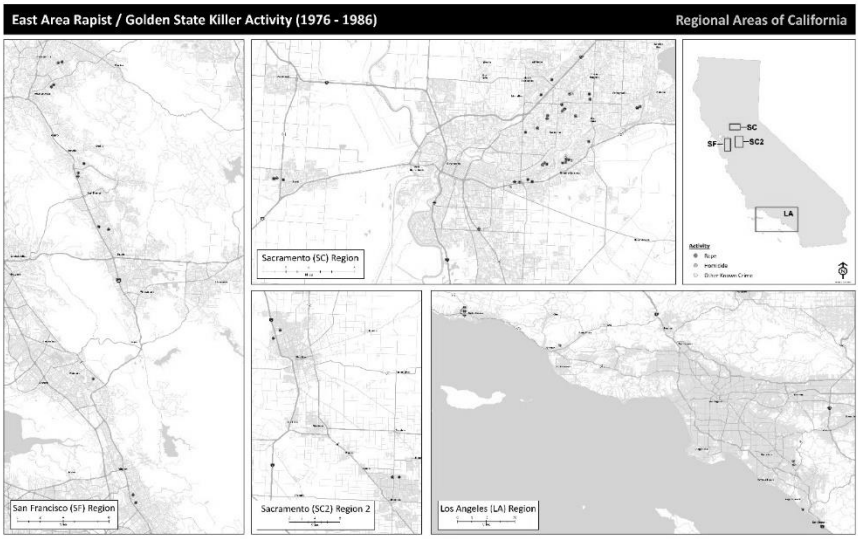
13 morderstw, 51 gwałtów, jedna próba podwójnego morderstwa oraz szereg włamań zostało dokonanych w Sacramento w latach 1976-1986. Śledztwo trwało ponad 40 lat, zebrano tysiące dowodów, przesłuchano setki podejrzanych, za każdym razem drobiazgowo zbierano dowody, zabezpieczano ślady, zachowano DNA sprawcy i sporządzono dokładny portret psychologiczny, ale przestępca wciąż pozostawał nieuchwytny.

Źródło: https://en.wikipedia.org/wiki/Joseph_James_DeAngelo (dostęp: 3.10.2021)

Rysunek 6. DeAngelo jako funkcjonariusz policji w Exeter w 1973 roku

Joseph James DeAngelo Jr., pracował w policji jako szeregowy funkcjonariusz. Uczestniczył w patrolach, nie brał udziału w śledztwach. Był przeciętny pod każdym względem, nie wyróżniał się niczym, miał żonę, psa i był fanem amerykańskiego baseballu. W 2018 roku policja z Sacramento odnalazła go, siedemdziesięciodwuletniego, wówczas już emerytowanego policjanta, za pośrednictwem genealogicznych serwisów internetowych. To serwisy dzięki którym można odkryć nieznaną sobie, bliższą i dalszą rodzinę. W jednym z nich zarejestrował się daleki krewny DeAngelo. Uruchomiło to całą sekwencję zdarzeń, która doprowadziła do zatrzymania niczego nie spodziewającego się J.J. DeAngelo.jr Porównano m.in. wciąż przechowywane DNA z miejsc zbrodni, sprawdzono drzewa genealogiczne, porównano inne zebrane dane, zawężając tym samym grupę podejrzanych.

Do identyfikacji sprawcy zbrodni potrzebna jest próbka DNA pobrana z miejsca przestępstwa oraz materiał porównawczy. Gdy nie można sprawdzić DNA bezpośrednio podejrzanego, wtedy można porównać profile DNA nawet nieżyjącej osoby, ale spokrewnionej z podejrzanym lub z DNA żyjącego krewnego, który dobrowolnie udostępnił swoje DNA w internecie.



Źródło: https://en.wikipedia.org/wiki/Joseph_James_DeAngelo (dostęp: 3.10.2021)

Rysunek 7. Mapa ataków przypisywanych Golden State Killerowi

J. J. DeAngelo Jr. wiedział, że nie figuruje w żadnym rejestrze, dlatego wiele lat pozostawał bezkarny. Prawdopodobnie zdawał sobie sprawę ze swojej rzadkiej genetycznej cechy – był tzw. *non-secretor*. To właściwość charakterystyczna dla ok. 20% populacji. *Non-secretor* (nie-wydzielacz) nie ma w wydzielinach ciała antygenów swojej grupy krwi. Warto tu również dodać, że badania DNA, dzięki którym można było ustalić sprawcę przestępstw, opracowano dopiero w 1985 roku[8].

J.J. DeAngelo Jr. został skazany na karę dwunastokrotnego dożywocia bez możliwości zwolnienia warunkowego, którą odsiaduje od 2021 roku w kalifornijskim więzieniu stanowym w Corcoran.

Zaznaczyć jednak trzeba, że genealogia jest nauką, która jak każda wiedza może być wykorzystana w pozytywnym lub negatywnym celu, stąd nie można jej samej traktować jako przestępczego narzędzia. To ludzie nadużywają zaufania do nauki, jak w wypadku genealogii, tworząc fałszywe i nieistniejące powiązania rodzinne między osobami w przestępczym celu.

[8] Źródło: https://zaufanatrzeciastrona.pl/post/golden-state-killer-zly-policjant-ktory-nie-przewidzial-rozwoju-technologii/ (dostęp: 22.02.2020).

Współczesna genealogia coraz mniej wiąże się ze żmudnym przeglądaniem ksiąg w archiwach miejskich czy kościelnych. Wiele dokumentów, drzew genealogicznych, zinwentaryzowanych nagrobków czy profili DNA zostało zdeponowanych w różnego typu bazach danych w ogólnodostępnej sieci Internet. Można nie tylko samemu odkrywać rodzinne historie, poszukiwania można zlecić firmom genealogicznym o sprecyzowanych profilach działania (np. są firmy poświęcone genealogii żydowskiej, firmy przeprowadzające poszukiwania na wybranym terenie, czy specjalizujące się w odszukiwaniu praw do dawnego majątku). Status zawodu genealoga nie jest uregulowany żadnymi przepisami, dlatego warto, przed podjęciem jakichkolwiek działań przeprowadzić research, który zawęzi krąg wybranych biur genealogicznych.

Zawodowi genealodzy mogą dziś współpracować z policją, prokuraturą, kancelariami prawnymi czy sądami. Dostępność źródeł, umiejętność odczytywania dokumentów, metodyka poszukiwań oraz wiedza poparta wieloletnią praktyką mogą okazać się niezwykle przydatne przy ustaleniu stanu faktycznego w sprawach spadkowych czy majątkowych. Z tą myślą powstało w 2019 roku Stowarzyszenie Polscy Profesjonalni Genealodzy, do którego należy kilkanaście firm genealogicznych z całej Polski. Jego celem nadrzędnym jest nie tylko dbałość o standardy etyczne w środowisku, ale i kreowanie dobrego wizerunku w taki sposób, by genealogia nie kojarzyła się z „drzewami za milion złotych".

Rozdział 14

Narzędzia hackerskie – aspekty karne i techniczne

Filip RADONIEWICZ[1]

Artykuł 269b § 1, typizujący czyny zabronione dotyczące tzw. narzędzi hackerskich został wprowadzony do kodeksu karnego[2] w związku z dostosowywaniem polskiego prawa[3] do Konwencji Rady Europy z dnia 23 listopada 2001 r. o cyberprzestępczości[4], która w art. 6 ust. 1 lit. a [5] przewiduje zakaz rozpowszechniania narzędzi hackerskich, polegający przede wszystkim na zakazie udostępniania ich w Internecie, skąd mogą być łatwo pobrane oraz – ze względu na fakt, iż wiele z nich jest bardzo łatwych w obsłudze – zostać wykorzystane art. do poważnego zakłócenia funkcjonowania sieci oraz podłączonych do niej komputerów nawet przez osobę nieposiadającą zbyt wysokich umiejętności (dla określenia takich osób stworzono pojęcie *script kiddies* – dzieciaki skryptowe). Rozszerza się w ten sposób zakres kryminalizacji cyberprzestępstw również na czynności przygotowawcze do ich popełnienia. Warto jednak odnotować w tym miejscu stanowisko A. Adamskiego, wskazującego, że zakaz ten w rzeczywistości jest

---

[1] Dr Filip Radoniewicz, Akademickie Centrum Polityki Cyberbezpieczeństwa ASzWoj, e-mail: f.radoniewicz@akademia.mil.pl, ORCID: 0000-0002

[2] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2022 r. poz. 1138 ze zm.), dalej jako KK.

[3] Ustawa z dnia 18 marca 2004 r. o zmianie ustawy - Kodeks karny, ustawy - Kodeks postępowania karnego oraz ustawy - Kodeks wykroczeń (Dz. U. Nr 69, poz. 626), dalej jako Nowelizacja z 2004 r.

[4] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728).

[5] Analogiczną (ale nie identyczną) regulację przewidziano w art. 7 dyrektywy Parlamentu Europejskiego i Rady 2013/40/ UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE L 218 z 14.08.2013 r., s. 8); zob. szerzej F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 262-263.

„skierowany przeciwko ostentacyjnemu publikowaniu w Internecie symboli i rekwizytów podkultury hackerskiej" i wprowadzenie tego rozwiązania może wywołać reakcje obronne tego środowiska, doprowadzając do lepszego ukrycia zasobów (lepszy kamuflaż, umieszczenie na serwerach położonych poza zasięgiem jurysdykcji państw-stron Konwencji o cyberprzestępczości) czy powstania „czarnego rynku" z narzędziami hackerskimi. W efekcie może nie przynieść efektów zamierzonych przez twórców Konwencji o cyberprzestępczości[6]. Wątpliwości co do zasadności penalizacji czynów dotyczących narzędzi hackerskich miała również D. Denning, która wskazywała, że egzekwowanie zakazu produkcji i rozpowszechniania takich programów jest przedsięwzięciem kosztownym i być może należałoby się zastanowić, czy rozwiązaniem korzystniejszym nie byłoby przeznaczenie choć części środków do tego wykorzystywanych na prewencję, wykrywanie i obronę przed incydentami zagrażającymi bezpieczeństwu sieci[7]. Moim zdaniem, nie zmienia to faktu, że omawiana regulacja jest potrzebna. Nawet niewielkie ograniczanie dostępności narzędzi hackerskich w sieci (zarówno przez zmniejszenie ich liczby, jak i utrudnienie ich uzyskania) będzie rzutować na ograniczenie liczby ataków i wzmocnienie bezpieczeństwa, co obecnie jest niezwykle istotne z uwagi na fakt, iż cyberprzestrzeń stała się globalnym rynkiem wymiany towarów i usług, a Internet – głównym medium wymiany informacji[8]. Ponadto przyjęte rozwiązanie umożliwia organom ścigania walkę ze sprzedażą urządzeń i świadczeniem usług związanych z łamaniem różnego rodzaju zabezpieczeń elektronicznych[9]. Nie można również tracić z oczu oczywistego faktu, że brak jakiejkolwiek regulacji kwestii produkcji i rozpowszechniania narzędzi hackerskich wzmacnia poczucie bezkarności sprawców nadużyć komputerowych, a jednocześnie zachęca ich do dalszego eksperymentowania z programami tego typu[10] (co stanowi niezwykle częsty motyw działania sprawców cyberprzestępstw)[11].

---

[6] Por. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2001, s. 37–38.

[7] D. Denning, *Reflections on Cyberweapons Controls*, Computer Security Journal 2000, vol. XVI, nr 4, http://faculty.nps.edu/dedennin/publications/reflections_on_cyberweapons_controls.pdf, data wejścia 1.12.2022 r.

[8] A. Adamski, *Przestępczość w cyberprzestrzeni...*, s. 42–44; K. Gienas, *Prawnokarne aspekty „narzędzi hackerskich",* M. Praw. 2005, nr 2 – dodatek Prawo Mediów Elektronicznych, s. 37.

[9] Por. A. Adamski, *Przestępczość w cyberprzestrzeni...*, s. 38.

[10] Tamże, s. 44.

[11] F. Radoniewicz, *Odpowiedzialność karna…*, s. 186-187.

Przepis art. 269b § 1 KK penalizuje szeroko pojęte czynności przygotowawcze do przestępstw wymienionych w jego dyspozycji. Kryminalizuje on wytwarzanie, pozyskiwanie, zbywanie, udostępnianie urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstw określonych w art. 165 § 1 pkt 4 KK. (sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach poprzez zakłócanie, uniemożliwienie lub wywarcie w inny sposób wpływu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych), art. 267 § 3 (nielegalny podsłuch i inwigilacja za pomocą urządzeń technicznych i programów komputerowych), art. 268a § 1 albo § 2 w związku z § 1 (naruszenie integralności danych, utrudnianie dostępu do danych oraz zakłócanie ich przetwarzania), art. 269 § 1 lub 2 (sabotaż komputerowy) albo art. 269a (zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej), a także haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, teleinformatycznym lub w sieci teleinformatycznej. Jak widać, ustawodawca nie uwzględnił w wyliczeniu zawartym w treści art. 269b k.k. przepisów art. 267 § 1 i § 2 KK[12], a także art. 268 § 2 k.k.[13].

Z „wytwarzaniem" mamy do czynienia wówczas, gdy sam sprawca tworzy narzędzia hackerskie lub przystosowuje w tym celu urządzenia i programy stworzone do innych, nieprzestępnych celów. „Pozyskanie" to każde działanie, wskutek którego sprawca uzyskuje dostęp do takich narzędzi (oraz możliwość ich użycia), a przeniesienie własności egzemplarzy narzędzi hackerskich na inne osoby stanowić będzie „zbycie". W przypadku programów komputerowych niezwykle rzadko będzie się ono wiązało z fizycznym przeniesieniem własności nośnika (np. płyty CD).

---

[12] „Art. 267. § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego."

[13] Brak w katalogu art. 268 § 2 KK. nie stnaowi takiego problemu jak brak.art. 267 § 1 i 2, gdyż przepis ten generalnie jest zbędny, a jeo roę może pełnić art. 268 § 1 i 2 (Zob. szerzej F. Radoniewcz, *Odpowiedzialność karna*…, s. 460)..

W przeważającej większości wypadków przybierze formę umożliwienia pobrania takiego narzędzia z Internetu po uiszczeniu opłaty (np. za pomocą wysłania płatnej wiadomości SMS). Z kolei przez „udostępnienie" rozumieć należy umożliwienie korzystania z narzędzi osobom trzecim (zarówno konkretnym, jak i innym, bliżej nieokreślonym), bez utraty władztwa nad nimi lub dostępu do nich[14]. W przypadku programów komputerowych czy haseł dostępu przykładem takiego działania będzie umieszczenie ich na witrynie internetowej (precyzyjniej – na serwerze – na witrynie znajduje się tylko link) lub serwerze FTP, udostępnienie za pośrednictwem sieci *peer-to-peer*[15]. Natomiast zamieszczenie na stronie internetowej linka, czyli odnośnika do strony, niebędącej własnością sprawcy, za której pośrednictwem można je uzyskać, pod warunkiem, iż osoba go umieszczająca zdaje sobie sprawę z jej zawartości, można zakwalifikować jako pomocnictwo[16]. W zasadzie tym, co różni udostępnienie narzędzia hackerskiego w postaci hasła lub programu komputerowego od zbycia jest odpłatność tej ostatniej formy rozpowszechniania[17].

Wśród znamion czasownikowych czynu z art. 269b § 1 k.k. nie przewidziano „posiadania" (na co pozwalają państwom-stronom postanowienia Konwencji o cyberprzestępczości z uwagi na trudności związane z ewentualnym udowodnieniem sprawcy, że posiadał narzędzie z zamiarem wykorzystania go do późniejszego popełnienia przestępstwa[18]). Jest to jednak iluzoryczne ograniczenie zakresu kryminalizacji z uwagi na jednoczesną karalność pozyskiwania.

---

[14] Por. P. Kozłowska-Kalisz [w:] *Kodeks karny. Komentarz aktualizowany*, red. M. Mozgawa, LEX/el. 2023, komentarz art. 269b; W. Wróbel, D. Zając [w:] *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d*, red. A. Zoll, Warszawa 2017, komentarz do art. 269b.

[15] Por. A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne,* St. Praw. 2005, nr 4, s. 61; K. Gienas, *Uwagi do przestępstwa stypizowanego w art. 269b kodeksu karnego,* Prokurator 2005, nr 1, s. 82; Zob. też J. Barta, R. Markiewicz, *Odpowiedzialność za odesłania w Internecie* (w:) J. Barta, R. Markiewicz (red.), *Handel elektroniczny*, Kraków 2005, s. 485 i n.

[16] Zob. W. Wróbel, D. Zając [w:] *Kodeks karny…..* Podobnie A. Sakowicz (w:) *Kodeks karny. Tom I–II. Komentarz, red. M. Królikowski, R. Zawłocki*, komentarz do art. 269b.

[17] F. Radoniewicz, *Odpowiedzialność karna*…, s. 331.

[18] Karalności posiadania nie przewiduje również np. regulacja niemiecka [§ 202c kodeksu karnego (Strafgesetzbuch – StGB) z dnia 15 maja 1871 r.] czy brytyjska (sekcja 3A Computer Misuse Act 1990), a kryminalizuje np. francuska [art. 323-3-1 Kodeksu karnego (*Code pénal*) Republiki Francuskiej z 22 lipca 1992 r.)] i czeska (§ 182 Kodeksu karnego Republiki Czeskiej z dnia 8 stycznia 2009 r.

Mimo że ustawodawca użył liczby mnogiej w stosunku do przedmiotów wykonawczych, penalizacją objęte jest np. zbycie tylko jednego programu czy udostępnienie tylko jednego hasła. Odnośnie do tej kwestii panuje zgodność w doktrynie i orzecznictwie. Natomiast, jak zauważa A. Marek, dyskusyjna jest interpretacja, zgodnie z którą do wypełnienia znamion czasownikowych zbywania lub udostępniania wystarcza dokonanie tych czynności wobec jednej osoby[19]. Uważam, że należy się zgodzić z P. Kozłowską-Kalisz, że gdyby wystarczające było dopuszczenie się czynności sprawczej określonej w omawianym przepisie wobec jednej tylko osoby, ustawodawca posłużyłby się liczbą pojedynczą, tak jak np. w art. 267 § 4 czy art. 265 § 1 k.k.[20] W sytuacji bowiem gdy sprawca dokonuje jednej z wymienionych w dyspozycji przepisu czynności względem konkretnej osoby, co najmniej licząc się z możliwością, że wykorzysta ona dany program czy hasło do popełnienia określonego czynu zabronionego, jego zachowanie należy kwalifikować jako pomocnictwo do przestępstwa popełnionego przez kupującego (czy też osobę, której narzędzie udostępniono).

Programami[21] służącymi do popełnienia przestępstwa z art. 267 § 3 KK[22] są w szczególności sniffery - (ang. *sniffing* – węszenie, *sniffer* – „wąchacz", szperacz), przechwytujące dane przesyłane siecią. Ich rolę mogą pełnić programy służące administratorom sieci tzw. monitory sieci (analizatory protokołów), używane do analizowania ruchu w sieci w celach diagnostycznych. Poza programami przynajmniej z założenia przeznaczonymi dla administratorów, jak Network Monitor czy CommView, *tcpdump* i *wireshark* (dawniej *ethereal*), istnieje wiele snifferów powstałych jako „narzędzia hackerskie", takich jak *Sniffer Pro* czy *Esniff.c*. Należy również wskazać programy wysoko wyspecjalizowane, takie jak opracowany przez amerykańskie Federalne Biuro Śledcze (FBI) *Carnivore* (pol.

---

[19] A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, s. 576.

[20] P. Kozłowska-Kalisz (w:) *Kodeks karny...*,.

[21] W zasadzie wszystkie omówione w tym artykule programy należą do grupy *malware* - ang. *malicious software* – oprogramowanie złośliwe, W prezentacji programów umożliwiających popełnienie przestępstw wymienionych w art. 269b § 1 KK, pominięto służące popełnieniu przestępstwa z art. 165 § 1 pkt 4 KK, gdyż jest ono zamachem na integralność danych komputerowych oraz systemu informatycznego, a w związku z tym sprawcy korzystają z tych samych narzędzi, jak w przypadku czynów z art. 268a, 269 i 269a KK.

[22] „Art. 267 § 3 KK Tej samej karze (co w § 1, tj. grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 - FR) podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem."

mięsożerca), *dSniff* czy *Cain i Abel*. Generalnie programy tego typu umożliwiają filtrowanie przechwytywanych pakietów pod kątem poszukiwanych danych. Sniffer musi być zainstalowany na komputerze podłączonym do sieci lokalnej, w której znajduje się komputer mający być celem ataku. Obecnie zdecydowana większość sieci składa się z wielu segmentów „oddzielonych" od siebie koncentratorami[23] lub switch'ami[24](przełącznikami). W tym pierwszym wypadku możliwe jest przechwycenie danych, ale tylko w ramach danego segmentu, natomiast w drugim wypadku nie jest to nawet możliwe, gdyż przełączniki filtrują dane w ten sposób, że do danego komputera trafiają jedynie dane doń skierowane. Nie można w tym wypadku działać całkowicie z zewnątrz – z innego segmentu sieci, a tym bardziej z Internetu. Istnieją oczywiście inne metody pozwalające na podsłuchiwanie również w sieciach z przełącznikami[25]. W ostatnich czasach w związku z rozwojem sieci bezprzewodowych WLAN (ang. *Wireless Local Area Network* – bezprzewodowe sieci lokalne) można mówić o swego rodzaju renesansie techniki snifingu klasycznego. W sieciach tych medium są fale radiowe. Korzystają z nich przede wszystkim urządzenia przenośne (m.in. laptopy, palmptopy, telefony komórkowe, jak również sieci łączące komputery i urządzenia peryferyjne w biurach czy domach). Podłączyć się do niej może każde urządzenie wyposażone w interfejs WLAN. Ponieważ medium transmisji (fale radiowe) może być wspólne nie tylko dla urządzeń podłączonych do niej, ale i urządzeń z innych sieci bezprzewodowych, każdy może podsłuchiwać transmisję danych w sieci bezprzewodowej, której brak odpowiedniego zabezpieczenia bądź ma je bardzo słabe, co ma miejsce zwłaszcza w sieciach domowych, do których dostęp często nie jest chroniony hasłem, bądź wprawdzie jest nim

---

[23] Koncentrator (hub) – sieciowe urządzenia wieloportowe, które poza łączeniem segmentów sieci (tzw. koncentratory pasywne – jedynie łączą kable), mogą wykonywać dodatkowe zadania (np. koncentratory aktywne – wzmacniają sygnał, stąd czasami nazywane wieloportowymi wzmacniakami, a tzw. smart hubs mogą monitorować transmisję). Ponieważ przesyłają sygnały elektryczne z jednego portu (gniazda) na wszystkie pozostałe, transmitowane dane trafiają do wszystkich komputerów do nich podłączonych;

[24] Przełącznik (ang. switch) –sieciowe urządzenie łączące segmenty (podsieci) sieci. Ponadto umożliwiają tworzenie wirtualnych sieci lokalnych (VLAN – ang. Virtual Local Area Network) – sieci urządzeń wydzielonych logicznie w ramach innej większej sieci fizycznej. Urządzenia tworzące sieć VLAN, niezależnie od swojej fizycznej lokalizacji (mogą znajdować się w różnych segmentach sieci), mogą się ze sobą komunikować, tak jakby były w jednej wspólnej sieci lokalnej.

[25] Zob. F. Radoniewicz, *Odpowiedzialność karna*…, s. 90-91.

zabezpieczony, ale jest ono mało skomplikowane lub fabryczne (ustalone przez producenta sprzętu i niezmienione przez nieświadomego istnienia takiej konieczności użytkownika)[26].

Do programów służących inwigilowaniu systemów komputerowych służą w szczególności takie programy jak trojany, *back door'y* (furtki, tylne drzwi) oraz oprogramowanie *spy-ware*. Trojan (koń trojański) - nieszkodliwy na pierwszy rzut oka program (np. skrypt wykonywalny na witrynach internetowych; kiedyś najpopularniejszą formą były wygaszacze ekranu), w których zapisano dodatkowe instrukcje. Wykonują one działania, których użytkownik nie jest świadomy. Służą one do obejścia zabezpieczeń systemu. Po zainstalowaniu trojana sprawca może uzyskiwać dostęp do danych. Ponadto sam trojan może wykonywać pewne czynności, takie jak usuwanie danych lub ich modyfikacja czy przesyłanie plików do napastnika. Pojęcie *back door* („tylne drzwi", „furtka") można rozumieć dwojako: po pierwsze, jako program, który zainstalowany w systemie użytkownika (zarówno w zwykłym komputerze, jak i na serwerze) – oczywiście bez jego wiedzy– umożliwia osobie, która go umieściła, wchodzenie do niego z pominięciem zabezpieczeń. Może być on pozostawiony przez sprawcę po przeprowadzonym przez niego ataku w celu umożliwienia mu powrotu do systemu bez konieczności ponownego łamania zabezpieczeń lub umieszczony przez niego w jakikolwiek inny sposób. W zasadzie można przyjąć, że w tym wariancie jest to typ trojana (najsłynniejszym trojanem tego typu był „Back Orifice", który mógł zostać zakamuflowany jako komponent dowolnego innego programu). Po drugie – i jest to pierwotne znaczenie tego terminu – jako furtka świadomie pozostawiona przez autora programu[27] .

Natomiast *spyware* (czyli oprogramowanie szpiegujące) programy zbierające dane w komputerze użytkownika (np. dane osobowe, numery kart płatniczych, hasła, adresy odwiedzanych stron internetowych). Mogą zostać umieszczone w systemie ofiary w wyniku uzyskania przez sprawcę nieuprawnionego dostępu do niego (czyli włamania) albo za pomocą trojana lub za pomocą programu „tylne drzwi", czy przy pomocy „furtki". Wśród innych metod instalacji należy wskazać przesłanie takiego programu pocztą

---

[26] D. Lisiak, M. Tomaszewski (w:) D. Lisiak, I. Politowska, M. Szmit, M. Tomaszewski, *13 najpopularniejszych ataków na twój komputer – wykrywanie, usuwanie skutków, zapobieganie*, Gliwice 2011, s. 18–20.

[27] D.L. Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci,* Gliwice 2004, s. 283; M. Tomaszewski (w:) D. Lisiak, I. Politowska, M. Szmit, M. Tomaszewski, *13 najpopularniejszych ataków*..., s. 78.

elektroniczną jako załącznik do e-maila (po otwarciu którego program instaluje się w systemie),. Zdarza się, że niektóre programy spyware są rozpowszechniane wraz z programami użytkowymi (tak było w przypadku np. komunikatora AOL czy KaZaa – popularnego klienta sieci p2p). Zebrane dane są przekazywane osobie (czy firmie), która go umieściła, w różny sposób. Przede wszystkim mogą być przesyłane bezpośrednio za pośrednictwem Internetu. Jeżeli jednak atakujący ma dostęp do infiltrowanego systemu, może pobierać je „osobiście" poprzez „wchodzenie" do niego co pewien czas celem ich odbioru. Podobnie w przypadku, gdy program został zamontowany w wyniku włamania – sprawca może zapewnić sobie możliwość powrotu do zaatakowanego systemu (np. pozostawiwszy sobie furtkę do niego) i odebrać dane. Nie należy zapominać, iż poza inwigilowaniem systemu umieszczenie programu spyware może umożliwić uzyskanie atakującemu uprawnień administratora systemu (jeżeli uda się przechwycić jego hasło), co wiąże się z przejęciem pełnej kontroli nad nim[28].

Warto jeszcze wspomnieć o *keyloggerach*. Są to programy lub urządzenia odczytujące i zapisujące wszystkie znaki wpisywane przez użytkownika za pomocą klawiatury. W ten sposób gromadzi cenne informacje, np. hasła. Niektóre *keyloggery* mają także możliwość przechwytywania danych zapamiętanych w przeglądarce internetowej w celu automatycznego wypełniania przez nią różnego rodzaju formularzy, okien logowania itp.; Zaletą programowych *keyloggerów* jest brak konieczności uzyskania fizycznego dostępu do inwigilowanego komputera. Wadą – brak możliwości zapisu loginu i hasła do systemu, gdyż włącza się on po jego uruchomieniu. *Keylogger* sprzętowy zwykle ma postać przejściówki pomiędzy kablem klawiatury, a portem do którego jest wpięta. To druga z jego zasadniczych wad. O pierwszej w zasadzie była mowa – konieczność uzyskania dostępu do komputera ofiary (natomiast odbiór przechwyconych danych często następuje droga radiową) – jest on widoczny. Czasami jednak spotkać można *keyloggery* zamontowane w klawiaturze, która zostaje podłączona w miejsce klawiatury ofiary.

Zamachom na integralność danych komputerowych (ich kasowanie, modyfikacja, unicestwianie), a więc czynom kryminalizowanym przez

[28] Por. C. Easttom, J. Taylor, *Computer Crime, Investigation, and the Law*, Boston 2011, s. 176–178.

przepisy art. 268a § 1 i 2 KK[29] są przede wszystkim wirusy - programy instalujące się bez wiedzy użytkownika. Wykonują różne działania, które mogą polegać na zakłócaniu pracy systemu (np. wyświetlają różne komunikaty) lub na niszczeniu danych. Mogą się klonować (replikować własny kod) oraz atakować inne komputery czy to poprzez zapisywanie się na fizycznych nośnikach, na których są potem przenoszone przez użytkowników, czy przez sieć, przesyłając się jako załączniki do e-maili. Czasami pozostają uśpione przez jakiś czas, by zaatakować wraz z nadejściem określonego dnia (bomba czasowa) lub w przypadku wykonania przez użytkownika określonej czynności, np. uruchomienia kolejny raz zainfekowanego programu (bomba logiczna). Wirusy mogą ulegać mutacji. Oczywiście nie jest ona w pełni samoczynna (chociaż niektóre z nich są w stanie replikować się w ten sposób, że powstałe kopie różnią się kodem, sprawiając wrażenie pewnego rodzaju mutacji; nie jest to jednak proces zamierzony, ma raczej charakter losowy, a ponadto nie wiąże się ze zmianą funkcji poszczególnych instrukcji). Miesięcznie pojawia się co najmniej kilkaset wirusów[30].

Zamachom na integralność danych służą również programy typu *ransomware* (termin pochodzi od ang. ransom „okup" i software „oprogramowanie" - oprogramowanie, które blokuje dostęp do zasobów systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (zwykle poprzez ich zaszyfrowanie), w celu uzyskania okupu przez osobę, która nim się posługuje w zamian za przywrócenie stanu pierwotnego.

Nie należy zapominać, że umieszczenie przez sprawcę jakiegokolwiek programu w cudzym systemie komputerowym wiąże się z modyfikacją danych na dysku twardym czy innym nośniku danych komputerowych (np. karcie pamięci w przypadku smartfonów), a co za tym idzie – stanowi czyn zabroniony z art. 268 § 2 lub 3 KK, 268a §1 lub 2 KK albo 269 § 1 lub 2 KK, co ma istotne znaczenie (zob. dalsze uwagi).

Istnieje cała grupa programów służących sianiu chaosu w sieci – zakłócaniu, blokowaniu bądź uniemożliwianiu jej funkcjonowania, a zatem

---

[29] „Art. 268a.§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5."

[30] S.W. Brenner, *Cybercrime and the Law. Cheallenges. Issues, and Outcomes*, Boston 2012, s. 36–37;.

czynów stypizowanych w art. 268a § 1 i 2 KK, 269 § 1 i 2 KK[31] oraz 269a KK[32]. Wśród nich w pierwszej kolejności należy wskazać robaka – samoreplikujący się program, który , w przeciwieństwie do wirusów, jest samodzielny – nie jest powiązane z innym programem. Robaki często powielają się i pocztą elektroniczną (mailery i mass-mailery) w postaci załączników wysyłane są przez nieświadomych użytkowników. Głównym celem działania robaków jest sianie chaosu w sieci, niekoniecznie jednak wiążącego się z niszczeniem danych. Pierwszym robakiem, jaki pojawił się w Internecie, był Internet Worm (lub Morris Worm), stworzony w 1988 r. przez R.T. Morrisa Jr. (wówczas był studentem informatyki na uniwersytecie w Cornell, obecnie jest profesorem w Massachusetts Institute of Technology) w celu wykazania wadliwości zabezpieczeń systemów operacyjnych i anonimowo wypuszczony do Internetu., unieruchamiając w ciągu kilku godzin 6000 komputerów podłączonych do Internetu (wówczas stanowiło to ok. 10% ogółu)[33]. Inne, służące zakłócaniu pracy sieci programy, to wabbity (ang. *wabbits*) i króliki (ang. *rabbits*) czynią to poprzez atak odmowy usługi (zob dalsze uwagi), polegający na rozmnożeniu procesów, a w konsekwencji zablokowaniu tablicy procesów systemu operacyjnego (stąd nazwa tego ataku tzw. *fork-bomb* – fork to funkcja systemowa służąca tworzeniu nowych procesów). Efekt ten zostaje osiągnięty poprzez gwałtowną ich replikację.

Wspomniane wyżej ataki DoS (ataki odmowy usługi, *Denial of Service*) to działania mające zazwyczaj na celu zakłócenie pracy sieci (łącznie z jej zablokowaniem). Mogą również stanowić wstęp do innych działań (np. przejęcia sesji - *session hijacking*). Z uwagi na mechanizm działania wyróżnia

---

[31] „Art. 269 § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych."

[32] „Art. 269a. Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5."

[33] Zob. szerzej S.W. Brenner, *Cybercrime and the Law. Challenges. Issues, and Outcomes*, Boston 2012, s. 38–39; D.J. Loundy, *Computer crime, information warfare, and economic espionage*, Durham 2003, s. 57 i n.

się dwa zasadnicze rodzaje ataków odmowy usług: ataki powodujące zawieszenie się usług (pochłaniania zasobów) oraz ataki przepełnienia (pochłaniania pasma)[34]. Bez zagłębiania się w szczegóły, w zasadzie można przyjąć, że polegają na wywołaniu dużego ruchu sieciowego lub ruchu określonego rodzaju, prowadzącego do zawieszenia serwera, przeciążenia routera lub innych urządzeń sieciowych. Mogą być również skierowane przeciw konkretnym komputerom, uniemożliwiając im komunikację z serwerem. Ich „wzmocnionym" wariantem są ataki DdoS (rozproszone ataki DoS, ang. *Distributed Denial of Service*), wykorzystujące botnety, czyli sieci systemów komputerowych (zwykle komputerów, a obecnie również smartfonów, czy innych urządzeń sieciowych np. routerów bądź innych urządzeń podłączonych do sieci, np. inteligentna lodówka, autonomiczny samochód) stworzonych przez sprawcę bez wiedzy ich użytkowników, po przejęciu nad nimi kontroli. Są to tzw. zombie lub agenci. W tej sytuacji wykrycie sprawcy jest trudne, gdyż w ataku mogą uczestniczyć tysiące komputerów z całego świata, które zdalnie uruchamiane są w określonym momencie i za ich pomocą przeprowadzany atak. Ponieważ możliwe jest wykorzystanie ogromnej liczby komputerów rozsianych po całym świecie, prawdziwe źródło ataku pozostaje nieznane. Obecnie służą już nie tylko do przeprowadzania rozproszonych ataków odmowy usługi (dDoS), ale innym celom, w szczególności rozsyłaniu spamu, okradaniu posiadaczy rachunków bankowych i handlowaniu nielegalnie uzyskanymi informacjami pochodzącymi z zainfekowanych komputerów-zombie. W ciągu 10 dni botnet składający się ze 183 tys. komputerów jest w stanie zgromadzić 310.000 rekordów danych (numerów rachunków bankowych, kart płatniczych oraz loginów i haseł dostępu)[35]. W Internecie można uzyskać zarówno programy do przeprowadzenia ataków DoS (i dDoS), jak i „gotowe" botnety. Można również wynająć botnet na określony czas.

Użyte w przepisie 269b § 1 KK sformułowanie „hasła komputerowe i kody dostępu" to przykładowe wyliczenie danych – zwykle w postaci ciągu znaków – umożliwiających uzyskanie dostępu do informacji przechowywanych w systemach informatycznych. Jak wskazuje W. Wróbel, z tej też przyczyny pod pojęciem danych należy rozumieć również dane

[34] F. Radoniewicz, *Odpowiedzialność karna*…, s. 108-112.

[35] A. Adamski, *Botnety jako zagadnienie prawno-kryminologiczne na tle doświadczeń amerykańskich*, Prok. i Pr. 2013, nr 11, s. 68–69.

biometryczne[36]. Trudno jednak wyobrazić sobie nieuprawnione wykorzystanie takich danych (tj. przez osobę, której nie charakteryzują, gdyż jest to np. tęczówka oka czy linie papilarne). Natomiast nie zawierają się w danych w rozumieniu przepisu art. 269b § 1 KK numery seryjne oprogramowania komputerowego[37]. Wynika to z ich przeznaczenia. Służą bowiem do uzyskania możliwości korzystania z programu komputerowego (gdy podanie numeru wymagane jest do jego zainstalowania czy uruchomienia) bądź dalszego używania go po zakończeniu okresu próby lub uzyskania dostępu do wszystkich jego funkcji (np. w programach *shareware*[38]). Podobnie nie są na podstawie omawianego przepisu kryminalizowane zachowania dotyczące *cracków*. Są to niewielkie programy, zwykle w formie analogicznej, jak tzw. łata (ang. *patch*[39]), pozwalające na ominięcie zabezpieczeń programu, takich jak wymóg podania numeru seryjnego czy klucza. Crack zazwyczaj zastępuje plik wykonywalny (o rozszerzeniu .exe) danego programu (lub go modyfikuje). Na marginesie nadmienić należy, że udostępnienie numeru seryjnego czy *cracka* osobie trzeciej (np. poprzez umieszczenie na stronie internetowej czy forum internetowym) nie będzie karalne również na podstawie art. 267 § 4 KK, gdyż uzyskanie ich zwykle nie następuje na skutek popełnienia przestępstwa z art. 267 § 3 KK. Nie możliwe będzie zakwalifikowanie go jako czynu z art. 118[1] ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[40]. Ustęp 1 tego artykułu penalizuje bowiem wytwarzanie urządzeń lub ich komponentów przeznaczonych do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed

---

[36] W. Wróbel, D. Zając [w:] *Kodeks karny…..*

[37] Por. K. Gienas, *Uwagi do przestępstwa..*, s. 79–80; W. Wróbel, D. Zając [w:] *Kodeks karny…..*

[38] Programy na licencji *shareware* są rozpowszechniane nieodpłatnie w celu umożliwienia ewentualnemu nabywcy zapoznania się z ich możliwościami. Zwykle użytkownik nie może korzystać ze wszystkich funkcji takiego programu (by mieć dostęp do jego pełnej wersji, musi zakupić pełną licencję i otrzymać klucz programu lub numer seryjny) albo ma taką możliwość, ale – jeżeli jest to tzw. wersja *trial* – jedynie przez pewien okres, ograniczony przez liczbę uruchomień (np. 60) lub upływ czasu (np. 30 dni). Następnie przestaje on działać, a użytkownik może zakupić „pełną" wersję i aktywować program przez wpisanie numeru seryjnego lub klucza.

[39] Łata, łatka (ang. *patch*) – poprawka, rzadziej uaktualnienie, do programu, zwykle służy do usunięcia pewnych problemów czy błędów lub uaktualnieniu programu.

[40] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r. poz. 2509).

odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych, obrót takimi urządzeniami lub ich komponentami albo reklamowanie ich w celu sprzedaży lub najmu. W ust. 2 natomiast zakazano posiadania, przechowywania lub wykorzystywania takich urządzeń lub ich komponentów. Takiej interpretacji sprzeciwia się choćby treść art. 269b § 1 k.k., w którym urządzenie jest wymienione obok programu. Nie jest również możliwe przyjęcie, że *crack* (o numerze seryjnym czy kluczu nie wspominając) jest komponentem urządzenia. Jak zostało wskazane, jest on samodzielnym programem, który ma służyć umożliwieniu korzystania z zabezpieczonego programu komputerowego. Nie można go uznać za element systemu komputerowego, bowiem poprzez umieszczenie na dysku twardym nie staje się jego częścią.

Cracki nie są jedynymi programami, które znalazły się poza zakresem kryminalizacji przepisu art. 269b § 1 KK. Wśród nich w pierwszej kolejności należy wskazać programy służące do uzyskiwania dostępu do systemu komputerowego, a więc hackingu, czyli czynu kryminalizowanego przez niewymienione w art. 269b § 1 KK przepisy art. 267 § 1 i 2 KK. Będą to np. programy do łamania haseł (w ich przypadku będzie jednak na podstawie art. 269b § 1 KK karalne użycie takiego programu w celu uzyskania hasła).

Nie jest również zakazane produkowanie, posiadanie czy rozpowszechnianie skanerów portów, czyli programów służących – jak sama nazwa wskazuje - skanowaniu portów, czyli „miejsc" przyporządkowanych każdej usłudze lub aplikacji miejsce, z którego i do którego docierają „jej" dane. Skanowanie portów polega na sprawdzeniu, które z nich w danym systemie są otwarte. Używane do tego są programy nazywane po prostu skanerami. Pozwalają one na ustalenie, które urządzenia w sieci są podatne na atak, jakie usługi są uruchomione, a następnie na zbadanie ich pod kątem luk w zabezpieczeniach. Skaner podejmuje czynności prowadzące do nawiązania połączenia, wysyłając pakiety danych do wszystkich portów w systemie, i oczekuje na odpowiedzi – jeżeli port nasłuchuje, czyli jest otwarty – odpowiada. Jest to najprostsza i najbardziej wiarygodna metoda skanowania, jednak działanie to naraża sprawcę na wykrycie. Poza tym od momentu nawiązania połączenia komputer ofiary protokołuje adresy IP. Istnieją bardziej skomplikowane sposoby skanowania pozwalające tego uniknąć. Skanowanie jest niekaralną w polskim prawie (zresztą w zdecydowanej większości państw jest podobnie, wyjątek stanowi Zjednoczone Królestwo) fazą przygotowawczą do ataku.

Na pierwszy rzut oka nie są karalne na podstawie art. 269b § 1 KK czyny dotyczące innych programów zaliczanych do tzw. *malware*, wśród

których wypada wskazać programy takie jak:

- *adware* (ang. advertising software) – jest to zarówno oprogramowanie rozpowszechniane za darmo, ale „w zamian" za tolerowanie przez użytkownika wyświetlających się reklam, będących źródłem dochodów producenta (są to programy na licencji typu *adware*), jak i takie, które instalują się bez zgody użytkownika i wyświetlają je w natarczywy sposób. Programy tego typu z reguły monitorują również strony WWW odwiedzane przez użytkownika i w ten sposób dostosowują treści reklam do konkretnych zainteresowań. W związku z tym nie tylko zajmują pasmo transmisyjne, ale przede wszystkim naruszają prywatność użytkownika. Często jednocześnie inwigilują jego komputer, przesyłając swojemu producentowi zebrane tą drogą dane[41].
- *Browser Hijacker* – program modyfikujący ustawienia przeglądarki internetowej użytkownika, co może oznaczać np. zmianę domyślnej strony startowej;
- *rootkity* - program (a w zasadzie zestaw programów) wykorzystywany do uzyskania pełnego dostępu do systemu typu unix/linuks (użytkownik root to odpowiednik administratora w systemach Microsoftu) oraz ukrycia faktu ataku (poprzez np. ukrywanie plików, procesów czy zalogowanych użytkowników) oraz obecności sprawcy. Rootkity zazwyczaj rozpowszechniane są w formie trojanów, backdoorów i innego rodzaju złośliwych kodów, udających zwykłe programy lub biblioteki systemowe. Niektóre wersje uzyskują kontrolę nad jądrem systemu, co znacznie utrudnia ich usunięcie (wpływają na działania administratora, mające na celu ich wykrycie), a nawet potrafią zagnieździć się w pamięci BIOS płyty głównej czy karty graficznej, przez co nawet reinstalacja systemu czy formatowanie dysku twardego nic w takiej sytuacji nie pomogą.

Wskazane wyżej programy są umieszczane w systemie komputerowym ofiary, co wiąże się – jak była już mowa – z modyfikacją

---

[41] Por. M. Tomaszewski (w:) D. Lisiak, I. Politowska, M. Szmit, M. Tomaszewski, 13 najpopularniejszych ataków …, s. 80.

zawartości nośnika pamięci, a zatem realizacją znamion czynu z 268a § 1 KK. Co za tym idzie – można przyjąć, że służą również popełnieniu przestępstwa z tego przepisu.

Natomiast z pewnością nie są kryminalizowane na mocy przepisów kodeksu karnego czyny dotyczące takich programów jak

- *web bug* – program umieszczony na stronie internetowej, zbierający dane dotyczące odwiedzających (np. czas wejścia na stronę, adres IP, typ używanej przeglądarki);
- *web crawler* (inne nazwy to web spider, web robot, web bot, natomiast po polsku: robot indeksujący, robot internetowy, pająk) – program zbierający informacje o strukturze, stronach i treściach znajdujących się w Internecie; zakres zbieranych danych jest różny. Mogą np. skanować strony internetowe w poszukiwaniu adresów e-mail, tworząc z nich bazy danych, wykorzystywane następnie przez spamerów do rozsyłania niechcianych maili;
- większość tzw. *botów* –„bot" to skrót od „robot"; jest to program wpuszczony do Internetu i w sposób automatyczny wykonujący zadania, do jakich został stworzony. Jego przykładem jest wspomniany wyżej *web crawler*. Obecnie jednak najczęściej termin ten używany jest dla określenia programów służących do przejmowania komputerów, a następnie tworzenia z ich udziałem botnetów, a jego produkcja, rozpowszechnianie, udostępnianie jest karalne na podstawie art. 269b § 1 KK.
- *exploity*, czyli programy służące do wykorzystania luk w protokołach sieciowych i oprogramowaniu w celu wniknięcia do systemu komputerowego

Na zakończenie tej części rozważań wypada jeszcze odnieść się do kwestii poruszonej przez K. Gienasa. Autor ten uważa, że nie stanowi przestępstwa z art. 269b § 1 KK udostępnianie kodów źródłowych programów, ponieważ jest to jedynie zapis ciągu symboli i komend, który dopiero po skompilowaniu do postaci kodu wynikowego (maszynowego) staje się wykonywalny – czytelny dla komputera. Podkreśla, że aby tego dokonać, trzeba posiadać pewną wiedzę z zakresu informatyki oraz dysponować odpowiednim programem. Wskazuje jednak, że udostępnienie programu w postaci kodu źródłowego wraz z instrukcją, w jaki sposób należy go skompilować, można zakwalifikować jako usiłowanie popełnienia

przestępstwa[42]. Uważam, że z uwagi na to, iż kod źródłowy jest jedną z postaci programu, jego kompilacja jest obecnie procesem w pełni zautomatyzowanym, przebiegającym bez ingerencji człowieka. Należy przyjąć, że udostępnienie kodu źródłowego stanowi realizację znamion czynu zabronionego z art. 269b § 1 KK[43].

Omawiane przestępstwo można popełnić w zasadzie przez działanie. Istnieje jednak możliwość udostępniania wymienionych narzędzi przez zaniechanie, pod warunkiem zaistnienia przesłanek określonych w art. 2 KK[44]. Przykładem może być sytuacja, gdy osoba, na której ciąży szczególny obowiązek utrzymania kodów dostępu do danych informatycznych lub systemu informatycznego, nie dopełni tego obowiązku[45].

Występek określony w art. 269b § 1 KK. jest przestępstwem materialnym. Do jego znamion należy skutek w postaci stworzenia urządzenia lub programu (przy wytwarzaniu), objęcia władztwa nad nim (lub nad nośnikiem danych, na którym jest zapisany), uzyskania doń dostępu (w przypadku pozyskania), przeniesienia władztwa nad nim (lub nad nośnikiem danych, na którym jest zapisany) na osoby trzecie (zbycie)[46] lub uczynienia dostępnym dla osób trzecich (w przypadku zbycia za pośrednictwem sieci lub udostępniania). Jest to przestępstwo powszechne. Popełnić je można tylko umyślnie. Strona podmiotowa obejmuje obie postaci umyślności (zamiar bezpośredni i ewentualny).

Przepis art. 269b § 1 KK stanowić miał – jak był mowa wyżej - panaceum na problem powszechnej dostępności w Internecie narzędzi hackerskich, umożliwiającej dokonywanie ataków i innych działań destrukcyjnych nawet osobom dysponującym zaledwie elementarną wiedzą z dziedziny informatyki. Jednak jest on wadliwie skonstruowany. Pierwsza z wad została wyżej opisana – jest nią brak wskazania w jego treści hackingu (zarówno nieuprawnionego uzyskania informacji z art. 267 § 1 k.k., jak i nieuprawnionego dostępu do systemu informatycznego z art. 267 § 2 k.k.). Co się tyczy innych, to, po pierwsze, w przepisie tym mowa jest o programach

---

[42] K. Gienas, *Uwagi do przestępstwa*..., s. 79

[43] F. Radoniewicz, *Odpowiedzialność karna*…,

[44] W świetle art. 2 KK odpowiedzialności karnej za przestępstwo skutkowe popełnione przez zaniechanie podlega ten tylko, na kim ciążył prawny, szczególny obowiązek zapobiegnięcia skutkowi.

[45] B. Kunicka-Michalska (w:) *System prawa karnego. Tom 8. Przestępstwa przeciwko państwu i dobrom zbiorowym*, red. L. Gardocki, Warszawa 2018, s. 1051.

[46] Por. P. Kozłowska-Kalisz (w:) *Kodeks karny*....

„przystosowanych" do określonych działań. Istnieje zatem problem, jak ocenić działanie twórcy programu spełniającego kilka funkcji (tzw. programy o podwójnej naturze)[47], użytego następnie przez osobę trzecią w celach przestępczych, których autor by sobie nie życzył[48]. W celu zachowania *ratio legis* wprowadzenia tego przepisu i uniknięcia zbyt szerokiej kryminalizacji W. Wróbel zaproponował jego interpretację nawiązującą do definicji karalnych czynności przygotowawczych z art. 16 § 1 k.k., wymagając tym samym od sprawcy wytwarzającego lub pozyskującego wymienione w przepisie narzędzia zamiaru bezpośredniego (w przypadku zbywania i udostępniania poprzestając na wymogu zamiaru ewentualnego)[49]. Moim zdaniem dla przypisania sprawcy winy wystarczy – jak sygnalizowałem wyżej – by działał on w zamiarze ewentualnym[50]. Przyjęcie przez ustawodawcę

---

[47] Np. monitory sieciowe, inaczej nazywane analizatorami protokołów, umożliwiające administratorom analizę ruchu w sieci, mogą zostać wykorzystane przez przestępców jako sniffery. Programy do odzyskiwania haseł mogą zostać wykorzystane do ich łamania.

[48] Por. A. Adamski, *Cyberprzestępczość – aspekty...*, s. 60.

[49] W. Wróbel, D. Zając [w:] *Kodeks karny…*.

[50] Tak też A. Adamski, *Cyberprzestępczość – aspekty...*, s. 61; K. Gienas, *Uwagi do przestępstwa...*, s. 81–82*;* O. Górniok (w:) O. Górniok i in.*, Kodeks karny, t. II, Komentarz do art. 117–363*, Gdańsk 2005, s. 369–370; M. Kalitowski (w:) *Kodeks karny. Komentarz,* red. M. Filar, Warszawa 2012, s. 1214; P. Kozłowska-Kalisz (w:) *Kodeks karny*.... Stanowisko, iż wytwarzania i pozyskiwania można się dopuścić jedynie z zamiarem bezpośrednim, prezentują W. Wróbel i D. Zając (o czym była mowa wyżej) oraz J. Piórkowska-Flieger, *Kodeks karny. Komentarz,* red. T. Bojarski, Warszawa *2012,* s. 713), A. Sakowicz (*Kodeks karny…*, komentarz do art. 269b), R. Hałas (*Kodeks karny. Komentarz,* A. Grześkowiak, K. Wiak, Warszawa 2015, s. 1242). Natomiast B. Kunicka-Michalska uważa, że trudno wyobrazić sobie wytwarzanie, pozyskiwanie czy zbywanie bez zamiaru bezpośredniego sprawcy [zob. B. Kunicka-Michalska (w:) *System prawa...*, s.1053], a zdaniem A. Marka czynności sprawcze wymienione w przepisie art. 269b § 1 k.k. mogą być popełnione jedynie w zamiarze bezpośrednim, zamiarem zaś ewentualnym może być objęte przeznaczenie urządzeń, programów, haseł, kodów dostępu i innych danych (zob. A. Marek, *Kodeks karny...*, s. 576). Jacek Giezek, krytycznie odnosząc się do stanowiska, iż wytwarzania i pozyskiwania dopuścić się można jedynie w zamiarze bezpośrednim, podkreśla wręcz, iż bardziej prawdopodobne wydaje się popełnienie tego przestępstwa w zamiarze ewentualnym, gdy sprawca jedynie godzi się na to, że swoim zachowaniem wypełni znamiona przestępstwa, gdyż zwykle sytuacja będzie przedstawiać się w ten sposób, iż nie tyle chce wytworzyć, pozyskać, zbyć lub udostępnić określone urządzenia lub programy komputerowe, lecz że z pewnym jedynie prawdopodobieństwem zakłada, że okażą się one przystosowane do popełnienia jednego z określonych w komentowanym przepisie przestępstw, godząc się, że tak właśnie będzie. Autor ten sugeruje wręcz, że owa „niepewność diagnozy" np. co do przystosowania urządzeń lub programów pozwala przyjąć, że mamy w takim przypadku do czynienia jedynie z zamiarem ewentualnym [L Giezek [w:] D. Gruszecka, K. Lipiński, G. Łabuda, A. Muszyńska, T.

takiego rozwiązania stwarza możliwość ścigania zarówno osób, które wytwarzają i udostępniają w Internecie programy służące do działań destrukcyjnych (ich autorów, webmasterów umieszczających na swoich witrynach internetowych owe narzędzia lub linki do stron, na których są one dostępne), jak i administratorów oraz osób zajmujących się bezpieczeństwem systemów informatycznych, którzy wymieniają się w sieci wiedzą na ten temat lub używają tego typu programów do testowania zabezpieczeń systemów[51]. Barbara Kunicka-Michalska stoi na stanowisku, że wobec takich osób, jako działających w ramach praw i obowiązków, ma miejsce wyłączenie odpowiedzialności karnej[52], a W. Wróbel podkreśla, że brak w treści przepisu art. 269b § 1 k.k. klauzuli wskazującej, że sprawca podlega karze tylko wówczas, gdy podejmuje wymienione w nim działania bez uprawnienia, należy uznać za przeoczenie ustawodawcy[53]. Moim zdaniem należy w tej kwestii sięgnąć do źródeł, tj art. 6 Konwencji o cyberprzestępczości. Autorzy Konwencji nie dość, że wprowadzili wymóg braku uprawnień po stronie sprawcy, to jeszcze – uznając jak widać ten zabieg za niewystarczający – podkreślili w przepisie art. 6 ust. 2, że „niniejszego artykułu nie należy interpretować jako mającego na celu pociągnięcie do odpowiedzialności karnej w przypadku, kiedy produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucja lub inne udostępnianie lub posiadanie, o którym mowa w ustępie 1 niniejszego artykułu, nie jest dokonywane w celu popełnienia przestępstwa określonego zgodnie z artykułami 2-5 niniejszej konwencji, jak w przypadku dozwolonego testowania lub ochrony systemu informatycznego".

Podsumowując, dla bytu przestępstwa przewidzianego w art. 6 Konwencji musi zostać spełnionych szereg przesłanek, mających na celu ograniczenie nadmiernej kryminalizacji. Po pierwsze musi być spełniony po

---

Razowski, J. Giezek, Kodeks karny. Część szczególna. Komentarz, Warszawa 2021, komentarz do art. 269b].

[51] Artykuł 6 Konwencji o cyberprzestępczości przewiduje wyłączenie w takim wypadku karalności. Podobną klauzulę należałoby wprowadzić w tym przepisie.

[52] B. Kunicka-Michalska (w:) System prawa..., s.1054.

[53] W. Wróbel [w:] *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-277 k.k.*, red. A. Zoll, Warszawa 2013, komentarz do art. 269b. Wymóg, by działanie sprawcy było nieuprawnione wprowadzono art. 1 pkt 8 lit. a ustawy z dnia 23 marca 2017 r. (Dz.U. z 2017 r. poz.768' dalej jako Nowelizacja z 2017 r.), ale jedynie w przypadku uzyskiwania dostępu do danych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej przy użyciu hasła komputerowego, kody dostępu lub innych danych umożliwiających ów dostęp.

stronie sprawcy wymóg braku uprawnienia. Po drugie, sprawca musi mieć zamiar, by narzędzie zostało użyte do popełnienia przestępstwa określonego w art. 2–5, a więc czynu musi dopuścić się w zamiarze kierunkowym. Po trzecie urządzenia i programy komputerowe muszą być zaprojektowane lub przystosowane głównie (ang. *primarily*) do popełnienia któregoś z przestępstw określonych w Konwencji o cyberprzestępczości (oba te rozwiązania przyjmuje dyrektywa 2013/40 dotycząca ataków na systemy informatyczne). Po czwarte nie może to być osoba działająca w celu dozwolonego testowania lub ochrony systemu informatycznego.

Nowelizacją z 2017 r. w celu likwidacji wyżej opisanych mankamentów przepisu art. 269b § 1 KK i dostosowania go do postanowień Konwencji o cyberprzestępczości, dodano przepis art. 269b § 1a KK, przewidujący kontratyp. W jego świetle nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia. Należy się zgodzić z W. Wróblem i Dominikiem Zającem, że zakres przyjętego rozwiązania powinien zostać rozszerzony także na zachowania służące ochronie przed innymi zagrożeniami (incydentami sieciowymi) niż wskazane w przepisie art. 269b § 1 KK (np. bezpośrednim włamaniem do systemu), analogicznie jak w art. 269c[54]. Osobiście uważam, że wskazane byłoby użycie (abstrahując od konieczności – o czym była już mowa - umieszczenia przepisów kryminalizujących hackimg, tj. art. 267 § 1 i 2 KK w katalogu w art. 269b § 1 KK) właśnie ogólnego sformułowania w rodzaju „działania wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia" (jak to ma miejsce właśnie w art. 269c KK[55]) zamiast odwoływania się do katalogu przepisów z art. 269b § 1 KK.

Uważam, że przyjęte rozwiązanie – po uwzględnieniu wyżej wskazanych uwag – należałoby uznać za trafne. Trudno w związku z tym zgodzić się z tezą zawartą w opinii prawnej Fundacji Frank Bold

---

[54] W. Wróbel, D. Zając [w:] Kodeks karny…..

[55] „Art. 269c. Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody"

i Krakowskiego Instytutu Prawa Karnego w sprawie odpowiedzialności karnej uczestnika programu bug bounty (na gruncie polskiego Kodeksu karnego) [56], że przepis ten jest zbędny, gdyż wyszukiwanie błędów w systemach/sieciach teleinformatycznych lub informatycznych w obu wskazanych w przepisie 269b § 1 przypadkach nie powinno być uznawane za realizację znamion czynu zabronionego. Zachowanie osoby, która zajmuje się wyszukiwaniem luk i słabości systemu informatycznego nie godzi w dobro prawne właściciela systemu – co więcej należy je ocenić jako społecznie dodatnie w przypadku, gdy podjęte jest w celu zapewnienia bezpieczeństwa danego systemu, tj. ujawnienia i przekazania informacji o stwierdzonych nieprawidłowościach osobie uprawnionej. Oczywiście, sama czynność wyszukiwania luk jest oczywiście bezkarna w takim wypadku bezkarna. Problem pojawia się jednak, gdy osoba tego dokonująca używa do tego programu hackerskiego. Uważam, że wypełnia ona wówczas znamiona czynu zabronionego z art. 269b § 1 KK i udzielone przez administratora systemu uprawnienie, a nawet zastosowanie kontratypu zgody pokrzywdzonego nie jest w stanie tego zmienić.

Na zakończenie zwrócić należy uwagę, że nowelizacją z 2017 r. podwyższono górną granicę kary grożącej za przestępstwo z art. 269b § 1 KK do 5 lat pozbawienia wolności, co uzasadniono jedynie koniecznością umożliwienia zastosowania wobec sprawcy tego czynu instytucji tzw. przepadku rozszerzonego, przewidzianego w art. 45 § 2 k.k.[57] Spotkało się to ze słuszną krytyką[58], zwłaszcza, że już wcześniej w doktrynie podnoszono, że kara przewidziana za czyny z art. 269b jest za wysoka. Zachowania nim kryminalizowane stanowią bowiem – jak wskazano wyżej – swego rodzaju czynności przygotowawcze do popełnienia dalszych przestępstw. Jednak w żadnym wypadku – poza przestępstwem art. 269 § 1 i § 2 - czyn zakwalifikowany z tego

---

[56] Opinia prawna Fundacji Frank Bold i Krakowskiego Instytutu Prawa Karnego w sprawie odpowiedzialności karnej uczestnika programu bug bounty (na gruncie polskiego Kodeksu karnego), sporządzona przez M. Małeckiego i B. Kwiatkowskiego, http://blog.frankbold.pl/wp-content/uploads/2016/12/Frank-Bold-KIPK-opinia-prawna-bug-bounty.pdf, data wejścia 1.12.2022 r.

[57] Uzasadnienie rządowego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, druk nr 1186, pkt 4.6.

[58] *O (braku) odpowiedzialności karnej za szukanie luk w systemach i sieciach informatycznych* – opinia prawna Fundacji Frank Bold i Krakowskiego Instytutu Prawa Karnego, http://blog.frankbold.pl/bug-bounty/).

przepisu nie będzie mógł, z uwagi na wysokość sankcji – zostać tak potraktowany i zakwalifikowany jako czyn współukarany uprzedni. Z uwagi na dysproporcję sankcji np. między 267 § 3 i 269b, można byłoby w zasadzie przyjąć, że czyn zakwalifikowany z tego pierwszego przepisu, stanowi czyn współukarany następczy. A zatem mamy do czynienia z sytuacja kuriozalną[59]. W związku tym należy przyjąć, że są to oddzielne przestępstwa, czego konsekwencją będzie wymierzenie kary łącznej. Wskazane byłoby obniżenie grożącej za występek 269b sankcji i to do wysokości niższej niż pierwotna (tj. 3 lat pozbawienia wolności), gdyż już ona rodziła problemy[60].

Wśród krajów Unii Europejskich polski kodeks karny przewiduje zdecydowanie najwyższą karę za tego rodzaju czyn zabroniony. Przykładowo:

- Art. 197 ter i 264 ter Kodeksu karnego Królestwa Hiszpanii (*Código Penal*) – grzywna lub kara pozbawienia wolności do 2 lat,
- § 202c StGB – grzywna lub kara pozbawienia wolności do roku,
- §201 norweskiej ustawy o karze (Kodeksu karnego) (*Lov om straff – Straffeloven*) z dnia 20 maja 2005 r. –(ustawa nr 28 z 2005 r.) – grzywna lub kara do roku pozbawienia wolności,
- art. 323-3-1 *Code pénal*- zastosowano nietypowe rozwiązanie. Sprawcy grozi kara przewidziana za czyn, do którego popełnienia „narzędzie hackerskie" może posłużyć. Jeżeli może ono znaleźć zastosowanie w przypadku kilku przestępstw – sprawca podlega karze najsurowszej. A kary za te czyny mają porównywalna wysokość jak w innych krajach UE, w tym w Polsce.

Z krajów europejskich jedynie w albańskim kodeksie karnym (jest on wyjątkowo surowy, jeden z typów kwalifikowanych zabójstwa zagrożony jest karą pozbawienia wolności w wysokości nie niższej od 40 lat lub dożywotnim pozbawieniem wolności) za podobne przestępstwo przewidziano tak wysoką sankcję [od 6 miesięcy do 5 lat pozbawienia wolności - § 293ç. Kodeksu karnego Republiki Albanii z dnia 27 stycznia 1995 r.(ustawa nr 7895 z 1995 r.)].

---

[59] W. Wróbel, D. Zając [w:] Kodeks karny…..

[60] Zob. F. Radoniewicz, *Odpowiedzialność karna…*, s. 348.

Rozdział 15

Credential stuffing

Kamil KOŁODZIEJCZYK[1]

STRESZCZENIE: Przedstawione w tym rozdziale informacje opisują atak typu credential stuffing. Wyjaśniają jego pojęcie oraz porównują go z innymi zbliżonymi działaniem atakami. Zaprezentowano także algorytm jego działania na podstawie skryptu w języku Python3, symulującego testowanie odporności serwisu internetowego na ten atak. Omówione zostają także najlepsze praktyki zabezpieczenia systemów przed tego rodzaju atakiem, a także odpowiedzialność karna za jego nielegalne przeprowadzenie. Opracowanie ma za zadanie szczegółowo wyjaśnić administratorom i użytkownikom ten rodzaj ataku oraz zaprezentować najlepsze wskazówki dla zabezpieczania swoich kont oraz systemów.

Słowa kluczowe: credential stuffing, upychanie poświadczeń, combolista, bezpieczeństwo systemów komputerowych.

Wstęp

Współcześnie niemal każda witryna, aplikacja, usługa udostępniająca zasoby swoim użytkownikom wymaga posiadania konta w swoim portalu. Dotyczy to zarówno portali informacyjnych, aplikacji bankowych, a nawet w ostatnim czasie gier komputerowych. Doprowadza to w efekcie do tego, że każdy użytkownik usług informatycznych posiada od kilku do nawet kilkudziesięciu kont różnych serwisach internetowych. Autentykacja dla kont użytkownika opiera się najczęściej na zastosowaniu loginu i hasła znanych wyłącznie właścicielowi danego konta.

Duża ilość kont przypadająca na jedną osobę w skorelowaniu z identyczną liczbą wykorzystywanych loginów i haseł oraz „ludzkim lenistwem" powoduje, że użytkownicy wykorzystują te same poświadczenia do wielu lub nawet do wszystkich swoich serwisów internetowych. Logicznym jest, że

[1] Mgr inż., Zarząd w Warszawie Centralnego Biura Zwalczania Cyberprzestępczości, ul. Puławska 148/150, 02-624 Warszawa, Polska

dużo łatwiejsze jest zapamiętanie jednego hasła do trzydziestu kont niż trzydziestu różnych haseł dla każdego z nich. Z reguły nie dotyczy to loginu, ponieważ najczęściej jest nim używany przez użytkownika adres email. Bardzo często spotykane są osoby chwalące się posiadaniem różnych haseł do wszystkich serwisów, lecz gdy przyjrzeć się temu bliżej okazuje się, że owszem jest to za każdym razem inne hasło, ale z tym samym rdzeniem. Np. do portalu onet.pl hasło brzmi: „ja!GOda342onet", a do serwisu bankowości mBANK: „ja!GOda342mBANK". Na pierwszy rzut oka wyglądają one na trudne hasła, ale znając jedno z nich nie problem jest domniemywać haseł do innych serwisów.

Taka sytuacja stała się bardzo atrakcyjną dla cyberprzestępców, którzy posiadają świadomość, że hasła skradzione z jednego miejsca mogą postawić przed nimi otworem inne konta tych samych użytkowników.

Według ostatnich badań Digital Shadows Research Team w 2022 roku zespół badawczy Photon odkrył ponad 24 miliardy wykradzionych danych uwierzytelniających[2]. Sytuacja ta ma efekt samonapędzającej się spirali, ponieważ większa liczba skompromitowanych haseł znajdujących w sieci Internet powoduje wzrost przeprowadzanych ataków z ich wykorzystaniem.

Jednym z takich ataków polegających na wykorzystaniu loginów i haseł do serwisów jest właśnie *credential stuffing.* W samym 2020 roku firma Akamai zaobserwowała ponad 193. miliardy tego rodzaju ataków[3].
Celem niniejszego opracowania jest wyjaśnienie czym jest atak *credential stuffin*g. Omówiona będzie także anatomia jego przeprowadzenia. Dalej zostanie zaprezentowane działanie podstawowych narzędzi na podstawie skryptu w języku Python3 symulującego testowanie odporności serwisu na ten atak. Wskazane będą najlepsze praktyki zabezpieczania przed nim. Na zakończenie, ku przestrodze omówiona zostanie odpowiedzialność karna za jego nielegalne przeprowadzenie.

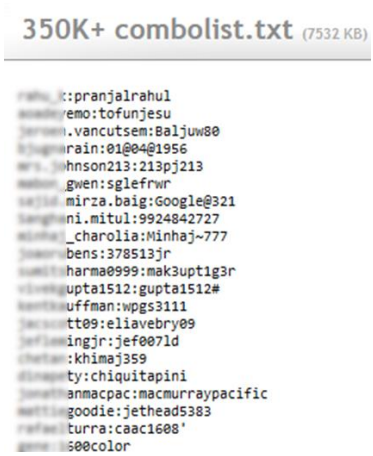
---

[2] Digital Shadows Photon Research Team: *Account Takeover in 2022. The 24-billion password problem*, https://resources.digitalshadows.com/whitepapers-and-reports/account-takeover-in-2022, 2022.
[3] Akamai, *Phishing for finance*, https://www.akamai.com/site/en/documents/state-of-the-internet/soti-security-phishing-for-finance-report-2021.pdf, 2021.

Credential stuffing – co to jest?

Credential *stuffing* jest to jedna z metod cyberataku polegająca na wykorzystaniu skompromitowanych poświadczeń użytkowników (najczęściej w postaci loginów i haseł) celem uzyskania dostępu do systemu. Opiera się on na założeniu, że użytkownicy wykorzystają to samo hasło w innych serwisach. Cechą tego ataku jest to, że nie jest on wykonywany ręcznie, lecz przy wykorzystaniu skryptów, programów bądź botów automatyzujących tę czynność.

Combolisty są to bazy specjalnie przygotowanych loginów i haseł, które najczęściej wyciekły ze skompromitowanych serwisów internetowych. Są one powszechnie dostępne na wielu portalach w sieci Internet. Posiadają one z reguły ustandaryzowaną formę „login:hasło" Na rysunku numer 1 został przedstawiony fragment combolisty składającej się z 350 tysięcy haseł ujawnionej w serwisie www.chomikuj.pl.



Źródło: www.chomikuj.pl.

Rysunek 1. Fragment przykładowej combolisty znalezionej w sieci Internet

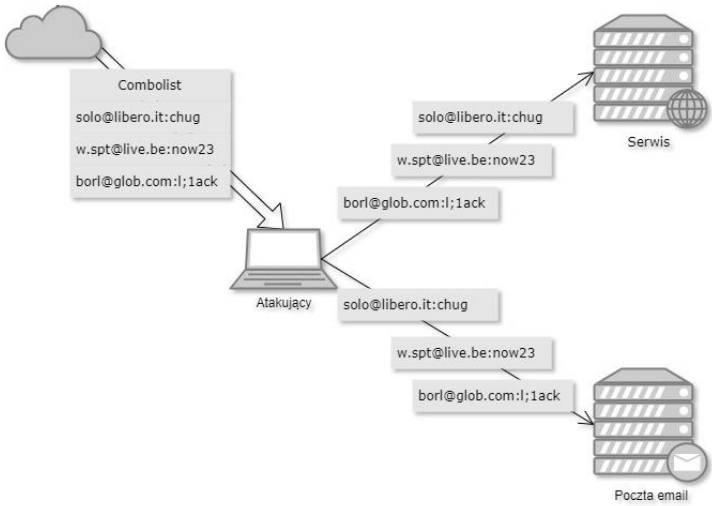
Interesującym miejscem umożliwiającym zweryfikowanie czy dane konta wyciekły z jakiegokolwiek serwisu jest witryna: www. haveibeenpwned.com. Dzięki niej, na podstawie adresu email bądź numeru telefonu zweryfikować można czy konkretne konto, a raczej jego dane prawdopodobnie znajdują się w którejś z combolist dostępnych w sieci. Strona wyświetli informacje na temat wycieków, w których dane konto brało udział. Jeśli hasło do konta nie było zmieniane od czasu incydentu koniecznym jest jego zmiana.

Cyberprzestępcy wykorzystują tę witrynę do identyfikacji combolist, w których znajdować się mogą poświadczenia ich celu (szczególnie w przypadku spersonalizowanych ataków na konkretną osobę lub witrynę).

Algorytm ataku *credential stuffing* sprowadzić można do czterech kroków:

1. Pozyskanie combolisty – polega na pobraniu odpowiedniej bazy danych loginów i haseł najczęściej z sieci Internet.
2. Załadowanie combolisty do odpowiedniego narzędzia automatyzującego atak i jego konfiguracja. Ponadto narzędzie to musi zostać odpowiednio skonfigurowane w taki sposób, aby podejmowało próbę ominięcia zastosowanych przez cel zabezpieczeń.
3. Wskazanie witryny lub witryn do ataku – w tym kroku wskazywany jest wprost adres do strony logowania, gdzie mają być testowane kolejne pary poświadczeń.
4. Uruchomienie i zbieranie wyników – Atak zbiera informacje na temat pomyślnych logowań. Mogą być one wykorzystane do prowadzenia w późniejszym czasie spersonalizowanych ataków, sprzedaży skompromitowanych kont innym cyberprzestępcom lub uzyskiwania prywatnych informacji z serwisów. Informacje te mogą zostać wykorzystane w przyszłości do prowadzenia ataków phishingowych jak np. *spear phishing*.

Na rysunku numer 2 został zaprezentowany schemat takiego ataku.



Źródło: opracowanie własne.

Rysunek 2. Schemat ataku credential stuffing

Narzędzia do prowadzenia ataków credential stuffing

Ciekawym pomysłem może być zweryfikowanie odporności własnej witryny internetowej na tego rodzaju atak. Jest to jedna z najlepszych form budowania bezpiecznego systemu. Oczywiście powinno zostać to zweryfikowane w trakcie prowadzenia testów penetracyjnych. Jednak atak ten jest na tyle prosty w wykonaniu, że można go przeprowadzić na własnym systemie bez dodatkowych kosztów.

Do przeprowadzenia ataku wykorzystać można gotowe narzędzia utworzone specjalnie do tego celu. Jednym z najpopularniejszych jest narzędzie: OpenBullet, które pozwala na prowadzenie tego typu ataków. Jego minusem jest dość skomplikowana konfiguracja dla początkującego użytkownika. Posiada ono własne forum, gdzie użytkownicy wymieniają się najlepszymi jego konfiguracjami pozwalającymi na prowadzenie bardziej nierozpoznawalnych działań. Poprzednikami tego narzędzia działającymi na tej samej zasadzie są: Sentry MBA Mods, Vortex, SNIPR. Minusem wykorzystywania gotowych rozwiązań są najczęściej ograniczone konfiguracje, znane systemom wykrywania i zapobiegania włamaniom jak IDS (ang. *Intrusion Detection Systems*) oraz IPS (ang. *Intrusion Prevention Systems*). Przez to już po kilku próbach atak może być niemożliwy do dalszego prowadzenia.

Nieco lepszym rozwiązaniem może być stworzenie własnego narzędzia, którego działanie wprowadzi w błąd wspomniane wyżej systemy. W tym wypadku do takiego prostego ataku wystarczy przykładowy skrypt napisany w języku Python3, przedstawiony na rysunku numer 3.

```
from time import sleep
from random import uniform
from selenium import webdriver
from selenium.webdriver.common.by import By

target="https://celAtaku.com"

browser= webdriver.Firefox(executable_path=r'C:\ ... \geckodriver.exe')
browser.get(target)
browser.maximize_window()

f=open("combolist.txt",'r')

for line in f:
        a = line.split(':')
        element_login = browser.find_element(By.ID,('user_login'))
        element_login.send_keys(a[0])

        element_pass = browser.find_element(By.ID,('user_password'))
        element_pass.send_keys(a[1])

        sleep(1)

        element_pass.submit()
        time.sleep(uniform(0.1, 5.0)))

browser.close()
```

Źródło: opracowanie własne.

Rysunek 3. Fragment skryptu pozwalającego na prowadzenie ataków credential stuffing

Skrypt przedstawiony na rysunku numer 3 oczywiście nie jest kompletnym programem pozwalającym na prowadzenie pełnowymiarowego ataku credential stuffing. Nie zbiera on wyników działania ani także nie waliduje poprawnych trafień danych. Wymaga to wprowadzenia kilku zmian w jego algorytmie. Posłużyć on może w głównej mierze do przetestowania odporności własnego systemu na ten atak. Jego prezentacja w niniejszym opracowaniu ma jednak za zadanie wyłącznie przedstawić prostotę narzędzi potrzebnych do realizacji tego typu testów:

1. W liniach od 1 do 4 importowane są niezbędne funkcje i biblioteki języka python:
   - „`sleep`” – funkcja biblioteki „`time`”, która pozwala na wstrzymanie działania programu. Np. w oczekiwaniu na załadowanie witryny/serwisu, które mają zostać zaatakowane.
   - „`uniform`” - funkcja biblioteki „`random`”. W skrypcie została zaimplementowana jedna z możliwych technik omijania systemów wykrywania i zapobiegania włamaniom. Mianowicie losowy czas generowania żądań kierowanych do witryny. Wysyłanie zapytań do serwisu w stałym czasie może zostać w prosty sposób zidentyfikowane jako atak. Wysyłanie ich co pewien odstęp czasu wydłuża prowadzenie ataku, ale tym samym może wprowadzać w błąd wyżej opisane systemy.
   - „`selenium`” – jest to biblioteka przeznaczona do prowadzenia automatycznych testów aplikacji internetowych. Funkcja „`webdriver`” odpowiada za interakcję z przeglądarką internetową. Zaś funkcja „`By`” odpowiada za lokalizację elementów na stronie. Wykorzystanie biblioteki `selenium` nie jest najefektywniejszą metodą prowadzenia ataku jednak na potrzeby niniejszego opracowania jej użycie świetnie prezentuje działanie ataku. Wykorzystanie biblioteki `selenium` pozwala natomiast uzyskać w logu przeglądarki autentyczny jej *fingerprint*.
2. W linii 6 wskazywana jest witryna pozostająca celem ataku. Istnieje możliwość rozbudowy skryptu o możliwość importowania listy witryn do prowadzenia testów.
3. W liniach od 8 do 10 skrypt otwiera przeglądarkę Mozilla Firefox (przy wykorzystaniu sterownika geckofriver.exe), a następnie przechodzi na wskazaną w linii 6 stronę internetową. Dalej maksymalizuje okno.
4. W linii 12 otwiera comboliste ze swojego katalogu (została ona tam umieszczona wcześniej).
5. W liniach od 14 do 25 program wykonuje w pętli do momentu, aż skończą się pozycje w comboliście, następujące działania:
   - rozdziela login od hasła z formy login:hasło,
   - odnajduje pole nazwy użytkownika na stronie i wpisuje w to miejsce login,
   - odnajduje pole hasła na stronie i wpisuje w to miejsce hasło,
   - czeka 1 sekundę (ustawione w celu prezentacji wypełnionych pól),

- zatwierdza logowanie (tożsame z wciśnięciem klawisza Enter),
- czeka losowy okres czasu zanim wykona sprawdzenie kolejnej pary loginu i hasła.

6. Po wykonaniu pętli zamyka przeglądarkę .

W skrócie, program ten wywołuje stronę internetową, a następnie wprowadza kolejno loginy i hasła. W celu zwiększenia efektywności programu testującego odporność na atak credential stuffing warto zastanowić się nad dodaniem dodatkowych funkcji jak np. generowanie losowego odcisku przeglądarki, rotowanie adresów IP, wielowątkowość itd.

Wiele z takich „niestandardowych" narzędzi znaleźć można w repozytoriach witryny www. github.com.

Credential stuffing a inne ataki

Credential stuffing jest bardzo często mylony z innym bardzo podobnym atakiem: „*password spraying*". Polega on na wykorzystaniu już znanej i zweryfikowanej nazwy użytkownika na wielu kontach łącząc to z popularnie stosowanymi hasłami. W tym wypadku atak odbywa się na hasła użytkownika. *Credential stuffing* opiera się zaś na ponownie wykorzystywanych loginach i hasłach użytkownika w wielu serwisach.

Credential stuffing może także przerodzić się w atak DDoS (ang. *Distributed Denial of Service*) jeśli będzie wykonywany z dostateczną częstotliwością z odpowiednio dużej liczby urządzeń. W takiej sytuacji nie dość, że weryfikowane są loginy i hasła użytkowników to dodatkowo strona pozostaje niedostępna dla swoich użytkowników.

Upychanie poświadczeń jest także w swoim działaniu zbliżone do ataków *brute force*. Jednak nie jest to to samo. Metoda *brute force* usiłuje odgadnąć dane bez kontekstu przy wykorzystaniu losowych znaków lub ich ciągów. Ponadto nie bazuje ona na danych pochodzących z poprzednich wycieków.

Zabezpieczenie przed atakami credential stuffing

Istnieje wiele sposobów ochrony przed tego rodzaju atakami. Do najpopularniejszych z nich należą:

- Umożliwienie wykorzystania adresu email oraz zwykłej nazwy jako loginu użytkownika – ten sposób raczej nieznacznie zwiększa bezpieczeństwo konta użytkownika. Jednak w sieci Internet

o wiele częściej znaleźć można combolisty w postaci „email:hasło" niż „nazwa użytkownika: hasło". Kombinacja tych dwóch rodzajów autentykacji nieznacznie komplikuje generowanie combolisty (jednak atakującemu nic nie stoi na przeszkodzie, aby jednym poleceniem rozdzielić nazwę od domeny w adresie email).

- Ograniczenie liczby logowań w czasie – na przykład w sytuacji kilku niepoprawnych logowań na konta użytkowników w krótkim odstępie czasu, ustawienie pewnego czasu oczekiwania przed kolejną próbą.
- Blokowanie tzw. bez nagłówkowych przeglądarek – takimi przeglądarkami będą przeglądarki nieposiadające środowiska graficznego jak na przykład PhantomJS. Wykorzystywane są one głównie do prowadzenia automatyzacji jakichś czynności np. zwiększenia licznika wyświetlanych reklam lub prowadzenia ataków DDoS. Zablokowanie dostępu do strony takiej przeglądarce wymusi na atakujących wykorzystanie np. klasycznych przeglądarek. W efekcie obniży to efektywność ataku.
- Czarna lista adresów IP – atakujący z reguły wykorzystują ograniczoną pule adresów IP. Dobrym rozwiązaniem jest ograniczenie bądź blokowanie adresów IP, które podejmują próbę logowania do wielu kont użytkownika w krótkim okresie.
- Czarna lista odcisków palców urządzeń – Najczęstszą kombinacją tworzenia odcisków palców urządzeń jest zbieranie informacji o systemie operacyjnym, przeglądarce, geolokalizacji oraz języku. Na tej podstawie, podobnie jak przy czarnej liście adresów IP, jeśli identyczna grupa parametrów wykona wiele prób logowania do kont użytkowników wskazywać to może na atak *credential stuffing*.
- Korzystanie z CAPTCHA – ma ona za zadanie wymusić na użytkowniku wykonanie jakiejś akcji, aby udowodnili, że są ludźmi logującymi się do systemu. Warto metodę tą połączyć z blokowaniem bezgłowych przeglądarek z uwagi na możliwość ominięcia go przez wykorzystanie właśnie takich narzędzi. Wymuszenie wykonania takiej akcji „znalezienie autobusu na zdjęciach" spowoduje znaczne ograniczenie tempa ataku.
- MFA (*ang. Multi-Factor Authentication*) – Jest to jedna z najlepszych metod ochrony konta użytkownika. W założeniu przy jej wykorzystaniu użytkownik chcący zalogować się do swojego

konta musi zweryfikować się co najmniej na dwa różne sposoby (wtedy 2FA). Np. hasło/pin/kod wysłane na urządzenie mobilne użytkownika lub dane biometryczne jak na przykład odcisk palca. Metoda ta jest najskuteczniejsza również z innego powodu. Użytkownik, wobec którego podejmowana jest próba uzyskania dostępu do konta, jest informowany o tym fakcie. Niespodziewany sms z prośbą o potwierdzenie logowania do danej witryny powinien być wystarczającym alarmem dla użytkownika, że ktoś usiłuje uzyskać dostęp do jego danych

Najlepszym rozwiązaniem pozostaje stosowanie kombinacji wielu powyższych metod zabezpieczenia przed atakami. Ponadto w celu wprowadzenia dezinformacji u prowadzącego atak warto jest zastanowić się nad wprowadzeniem generowania fałszywych odpowiedzi sugerujących pomyślne logowanie do konta. Spowodować to może pewnego rodzaju zamieszanie w środowisku atakującego.

W przypadku stwierdzenia ataku w systemie komputerowym przez administratora niezbędnym jest wymuszenie resetu haseł dla użytkowników oraz uniemożliwienie wprowadzania tego samego hasła ponownie.

Administrator może podejmować próby ochrony swoich użytkowników poprzez wprowadzanie zabezpieczeń jednak to użytkownik powinien zrozumieć niski poziom niebezpieczeństwa jaki zapewnia sobie w przypadku stosowania tego samego hasła w wielu serwisach.

Credential stuffing w prawie polskim

Na terenie Polski w 2021 roku miał miejsce głośny atak *credential stuffing*, którego celem stał się System Dostawcy Tożsamości Profil Zaufany. 27-latek za pomocą tej metody włamał się do konta 239 użytkowników tego serwisu. W następstwie tego ataku udostępniał on dalej zweryfikowane poświadczenia na swoim forum internetowym. Mężczyzna został zatrzymany przez funkcjonariuszy Wydziału do walki z Cyberprzestępczością Komendy Stołecznej Policji. Jak się okazało przeprowadzał on identyczne ataki na inne serwisy w sieci Internet. Potwierdzonymi „trafieniami" dzielił się z innymi osobami[4].

[4] Niebezpiecznik.pl, *To on włamywał się na Profile Zaufane. Został aresztowany na 2 miesiące, ale grozi mu 8 lat*, https://niebezpiecznik.pl/post/wlamywal-sie-na-profile-zaufane-zostal-aresztowany-na-2-miesiace-ale-grozi-mu-8-lat.

Zgodnie z obowiązującym prawem w Polsce mężczyźnie przedstawiono następujące zarzuty:

– art. 269b kk, którego treść brzmi: „*Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 sprowadzenie niebezpieczeństwa powszechnego § 1 pkt 4, art. 267 bezprawne uzyskanie informacji § 3, art. 268a niszczenie, uszkadzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych § 1 albo § 2 w związku z § 1, art. 269 niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu § 1 lub 2 albo art. 269a zakłócanie pracy systemu informatycznego, teleinformatycznego lub sieci teleinformatycznej, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5*”[5]. Tym artykułem objętych może być kilka czynów. W pierwszej kolejności pozyskiwanie programów komputerowych przystosowanych do popełnienia przestępstwa. W swoim podstawowym brzmieniu dotyczy on wszystkich narzędzi, które można wykorzystać do popełnienia przestępstwa. Ze względu jednak na absurdalność tego przepisu stosowany on jest wobec narzędzi, które zostały stworzone z zamiarem popełnienia przestępstw. W rezultacie nie jest on stosowany wobec narzędzi posiadających wiele funkcji[6]. Przecież program Wireshark może być wykorzystywany do podsłuchu pakietów sieciowych, a jest doskonałym narzędziem pracy na przykład administratorów sieciowych.

  Drugim czynem jaki może zostać objęty tym artykułem jest pozyskiwanie oraz udostępnianie danych umożliwiających dostęp do informacji przechowywanych w sieci informatycznej, czyli loginy i hasła. Przekładając atak *credential stuffing* na ten czyn mowa tu o combolistach, które powstały z zamiarem popełnienia

[5] Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny.
[6] Michał B. i in, Bezpieczeństwo aplikacji webowych, Securitum, 2019.

przestępstwa. Ich pobieranie, a także udostępnianie już zweryfikowanych poprawnych combolist (umożliwiających dostęp do kont użytkowników) powodować będzie stanowić wyczerpanie znamion czynu opisanego w tym artykule.

– art. 267 kk, który posiada następujące brzmienie: „*Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2*”[7]. Czyn opisany w tym artykule dotyczy udanych prób uzyskania dostępu do kont użytkowników. Na przykładzie zatrzymanego sprawcy ataków, objęło to wszelkie konta, do których uzyskał dostęp, w tym te, na które się zalogował oraz dane, które udostępnił innym osobom. Istotnym w tym artykule jest fakt, że nie musi dojść do zapoznania się z informacją nieprzeznaczoną przez sprawcę. Wystarczające jest stworzenie takiej możliwości. Usiłowanie stworzenia takiej możliwości może zostać potraktowane jako usiłowanie dokonania tego przestępstwa o czym mowa poniżej.
– art 13 kk w zw. z art 267 kk – dotyczy on usiłowania popełnienia przestępstwa określonego w art. 267 kk. Artykułem tym objęte zostały wszelkie nieudane próby dostępu do kont użytkowników. Czyli te próby, które nie zakończyły się poprawnym logowaniem do strony.

Powyższe przepisy karne bezpośrednio dotyczą ataku credential stuffing. Wobec powyższego osoby podejmujące się takich praktyk muszą się liczyć z konsekwencjami swoich działań w przypadku zatrzymania przez organy ścigania i udowodnienia winy.

W sytuacji, gdy atak ten przerodzi się w DDoS sprawca odpowiadać może z art. 269a kk, którego brzmienie jest następujące: „*Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5*”[8]. Przepisem o podobnym

[7] Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny.
[8] ibidem.

brzmieniu jednak zagrożonym większa karą jest art. 269 § 1 kk: „*Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8*”[9]. Różnica pomiędzy przepisami art. 269a kk oraz 269 kk tkwi w rodzaju danych. Mianowicie te w art. 269 § 1 kk dotyczą danych krytycznych oraz istotnych dla funkcjonowania państwa. Można to na przykład porównać do ataku DDoS przeprowadzonego na wieżę kontroli lotów.

Podsumowanie

Na podstawie informacji zawartych w niniejszym opracowaniu uznać można, że z reguły banalny do przeprowadzania atak jakim jest *credential stuffing* stanowić może poważne zagrożenie dla administratorów systemów oraz użytkowników serwisów internetowych. Anatomia jego prowadzenia jest niezwykle banalna i oparta na wykorzystaniu gotowych lub własnych narzędzi. Nie jest konieczne posiadanie skomplikowanej wiedzy technicznej ani informatycznej, aby móc wieczorem, w domu uruchomić taki atak na serwerze VPS i rano zebrać jego wyniki.

Wobec powyższego istotne jest niebagatelizowanie tego rodzaju ataku przez użytkowników oraz administratorów systemów. W niniejszym opracowaniu wskazano najpopularniejsze techniki zabezpieczenia systemów przed tym atakiem. Warto jednak zaznaczyć, że ogromną rolę w bezpieczeństwie w tym wypadku odgrywa świadomość użytkownika. W przypadku wykorzystywania tego samego hasła we wszystkich serwisach w połączeniu z brakiem MFA, w myśl popularnego powiedzenia „okazja czyni złodzieja” naraża użytkownika w istotnym stopniu na utratę danych w ten sposób.

Tym samym, jeśli jest taka możliwość należy łączyć te dwie techniki (MFA oraz różne hasła w różnych serwisach) w celu zabezpieczenia swojego konta. Zastosowanie nadto innych technik opisanych w niniejszym opracowaniu dodatkowo poprawia bezpieczeństwo użytkownika.

[9] ibidem.

Bibliografia

1. Digital Shadows Photon Research Team: *Account Takeover in 2022. The 24-billion password problem*, https://resources.digitalshadows.com/whitepapers-and-reports/account-takeover-in-2022, 2022.
2. Akamai: *Phishing for finance*, https://www.akamai.com/site/en/documents/state-of-the-internet/soti-security-phishing-for-finance-report-2021.pdf, dostęp: 10.10.2022.
3. Niebezpiecznik.pl, *To on włamywał się na Profile Zaufane. Został aresztowany na 2 miesiące, ale grozi mu 8 lat*, https://niebezpiecznik.pl/post/wlamywal-sie-na-profile-zaufane-zostal-aresztowany-na-2-miesiace-ale-grozi-mu-8-lat, dostęp: 14.10.2022.
4. Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny.
5. Michał B. i in, *Bezpieczeństwo aplikacji webowych*, Securitum, 2019.

Abstract

CREDENTIAL STUFFING

Summary: The information in this chapter describes a credential stuffing attack. They explain its concept and compare it with other similar attacks. The algorithm of its operation based on a script in Python3 simulating the resistance of a website to this attack was also presented. The best practices for securing systems against this type of attack are also discussed, as well as criminal liability for its illegal conduct. The study is designed to explain in detail to administrators and users this type of attack and indicate the best tips for securing their accounts and systems.

Keywords: credential stuffing, combolist, security of computer systems.

Załącznik

Operations Analysis of Crypto-assets in Terrorist Financing

CFLW Intelligence Services[1]

Disclaimer and Disclosure Statement

Legal Disclaimer

This study is conducted and the report written as part of the Anti-FinTer project, which has received funding from the European Union's ISFP-2020-AG-TERFIN program under the Grant Agreement No. 101036262. This document reflects only the views of the author(s). The European Commission

---

[1] Contact the authors via: dr Mark van Staalduinen, Managing Director, CFLW Cyber Strategies, Mark.vanStaalduinen@CFLW.com, CFLW.com

is not in any way responsible for any use that may be made of the information it contains. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Disclosure Statement

This report is a property of the Anti-FinTer Consortium partner who developed this property, and it shall not be reproduced, disclosed, modified, or communicated to any third parties without the prior written consent of the abovementioned entities.

1 Introduction

1.1 Purpose of the Report

This report is prepared as part of Anti-FinTer1, a project convened in 2022 to develop expertise at European Union (EU) level in emerging terrorist financing (TF) threats by providing risk analysis, best practices, and policy recommendations. The purpose of this report is to provide an overview of modi operandi in TF exploiting crypto-assets, new payment products and services (NPPS), social media, Dark Web activities, and crowdfunding, with a view to identifying the corresponding gaps as well as good practices in the operational and counter-terrorism pipelines of the respective law enforcement agencies (LEAs).

As investigators, we cannot see what we cannot see. Our biases get in the way, giving rise to blind spots, incomplete perspectives, and inaccurate interpretations of data [1] [2]. Because of the role we play and the importance of fairness and neutrality, we must start by identifying our own knowledge gaps and recognizing how they can impair our investigative work.

1.2 Scope and Intended Audience

This report examines and analyses in detail the current modi operandi in TF activities supported by recent technological advancements, like crypto-assets, Dark Web, etc. It pays particular attention towards examining, defining, and formalizing innovative investigation techniques that are likely to lead

to successful attempts in the actual operational setting, where the overall objective is to exploit "non-financial" information (for example from the Dark Web) in the investigation process. Specifically, the report extends on the widely adopted "follow the money" approach, so as to incorporate the concept of "parallel investigations" (i.e. jointly performing financial and conventional criminal analysis of cases) introduced by the Financial Action Taskforce (FATF) recommendations [3] and ending up with the introduction of possible investigation practices on "follow the actor", where the overall goal is to identify the common group of criminal actors that are behind multiple cases of the same or different operational fields.

Short-term beneficiaries of this report include project partners and affiliated parties to national Financial Intelligence Units (FIUs). Medium-term beneficiaries include national authorities, LEAs, FIUs, the judiciary system, research organizations, and financial institutions (FIs). Long-term beneficiaries include all EU member states and associated countries, the European Anti-Cybercrime

Technology Development Association (EACTDA), the European Network of Law Enforcement Technology Services (ENLETS), Europol, the European Border and Coast Guard Agency (FRONTEX), and the European Union Agency for Law Enforcement Training (CEPOL).

1.3 Structure of the Report

The report consists of the following sections:
Section 1: Introduces this report.
Section 2: Provides an overview of TF and recent technological advancements.
Section 3: Describes current TF modi operandi.
Section 4: Explains the challenges and gaps in countering the financing of terrorism (CFT).
Section 5: Introduces the concept of "parallel investigations" and other good practices.
Section 6: Details the "follow the money" and "follow the actor" approaches.
Section 7: Concludes with some areas for further focus going forward.

1.4 Referenced Documents

In drafting this report, an extensive literature review was conducted of close to 200 different publications, scholarly works, and news reports on terrorist organizations, TF, and crypto-assets. In particular, this report drew heavily from well-established guidelines in the field such as INTERPOL's

Guidelines on the Darknet and Cryptocurrencies, FATF's Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, Europol's annual EU Terrorism Situation and Trend Report (TE-SAT), Egmont group published materials, etc.

2 Overview of Terrorist Financing and Recent Technological Advancements

2.1 Key Concepts

2.1.1 Money Laundering vs Terrorist Financing

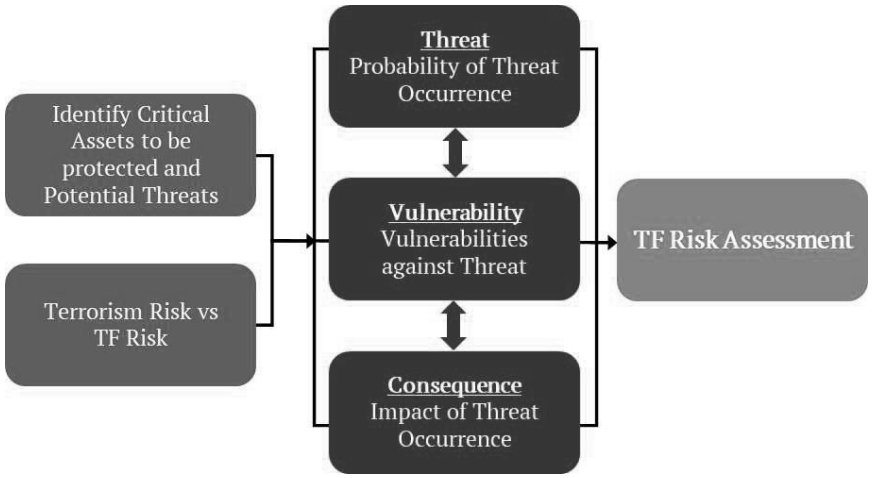
Money laundering (ML) and TF activities appear as interrelated; however, nuanced differences exist between these two distinct offences. Not all ML is TF—but most TF is ML. While ML derives from illegal proceeds, TF may derive from both legitimate and illegitimate sources. In ML, generation of funds may be an end in itself with the purpose of laundering to conceal their illicit origin and transmit them to a legitimate enterprise. In TF, the end is to support acts of terrorism, and for that reason the funds must ultimately be transferred to terrorist actors. Another important distinction is that ML investigation tends to be enforcement-led and focused on gathering evidence to prosecute perpetrators of already-committed crimes. TF investigations, on the other hand, are required by the nature of the threat to be preventive in nature and intelligence-led [4].

Although there may be some overlap between ML and TF, the motive, threat, and risk indicators differ. While a low volume funds transfer may be low risk for ML, it may pose a higher risk for TF when considered along with other factors, for example, terrorist financiers have been known to use low-limit prepaid cards for their purposes despite them being considered lower risk for ML.

The primary goal of entities involved in TF is therefore not necessarily to conceal the sources of funds, but to conceal both the funding activity and the nature of the funded activity [5].

2.1.2 Key Terms Relevant to Assessing Terrorist Financing Risk

A TF risk can be seen as a function of threat, vulnerability, and consequence. It involves the risk that funds intended for terrorists are being raised, moved, stored, or used in or through a jurisdiction, in the form of legitimate or illegitimate assets [4]. The relationships between these terms are depicted as follows:



Źródło: C.-L. Liu and J. Quek, "Enhancing building security for embassies along the Maritime Silk Road against terrorist attacks," Journal of Infrastructure, Policy and Development, vol. 3, no. 1, pp. 115-128, 2019.

Figure 1. Key concepts and terms relevant to assessing terrorist financing risk

2.1.2.1 Threat

A threat is an actor with the potential to cause harm by raising, moving, storing, or using funds for terrorist purposes. Such threats may include domestic or international terrorist organizations and their facilitators, funds, and past, present, and future TF activities, as well as individuals and populations sympathetic to these organizations.

2.1.2.2 Vulnerability

The concept of vulnerability comprises things that can be exploited by the threat or that may support or facilitate its activities. They may include features of a particular sector, a financial product, or type of service that makes them attractive for TF, weaknesses in anti-money laundering/countering the financing of terrorism (AML/CFT) controls, or a jurisdiction's contextual features such as a large informal economy or porous borders. There may be overlap in vulnerabilities exploited for both ML and TF.

2.1.2.3 Consequence

Consequence refers to the impact that a threat may cause if realized. This includes the effect on domestic or institutional financial systems, as well

as the economy and society at large. Consequences for TF are likely to be more severe than for ML or other types of financial crime. Given the challenges in assessing consequences, countries need not take a scientific approach when considering them, and instead may want to start with the presumption that consequences of TF will be severe and consider whether there are any mitigating factors.

2.1.2.4 Terrorist Financing Risk Assessment

A TF risk assessment is a systematic process to identify, analyse, and understand TF risk, serving as a first step in addressing it. It should generally cover all aspects of raising, moving, storing, and using funds or other assets such as goods, vehicles, or weapons to meet terrorist needs. This should go beyond fundraising and address terrorist procurement and terrorist facilitation networks, including Foreign Terrorist Fighters (FTFs).

2.1.2.5 Terrorism Risk vs Terrorist Financing Risk

Terrorism risk and TF risk are often, but not always, interlinked. For example, a TF risk assessment will consider domestic and foreign terrorist threats. If a jurisdiction has active organizations operating domestically, this increases the probability of TF. But in light of the cross-border nature of TF, a jurisdiction facing low terrorism risk may still face significant TF risk. A low terrorism risk implies that terrorists are not using funds domestically but may still raise funds domestically or move funds through the jurisdiction.

2.2 Types of Terrorism

Terrorism, in its broadest sense, is the use of violence and fear to achieve an ideological aim. There are various definitions of terrorism, with no universal agreement about it. Terrorism is a charged term. It is often used to connote that something is "morally wrong". Governments and non-state groups use the term to denounce opposing groups. When terrorism is perpetrated by nation states, it is not considered terrorism by the state conducting it, making legality a grey area [7].

The following definitions are drawn from Europol's annual EU Terrorism Situation and Trend Report (TE-SAT) [8]. Europol categorizes terrorists by their motivation—however, many groups have a mixture of motivating ideologies, although one ideology or motivation usually dominates. The categories are not necessarily mutually exclusive.

2.2.1 Jihadist

Jihadism aims to create an Islamic state governed exclusively by Islamic shari'a law, as interpreter by them. Major representatives are the Al-Qaeda network and Islamic State of Iraq and Syria (ISIS). Jihadists legitimise the use of violence with reference to classical Islamic doctrines on jihad, a term which literally means 'striving' or 'exertion', treating it as religiously sanctioned warfare. Sunni Islam is believed to be under attack from a global non-Muslim alliance, comprising Christians, Jews, and people of other religions such as Buddhists and Hindu, as well as secularists. Muslim governments who ally with 'enemies of Islam', such as by enrolling as members of the United Nations (UN), are declared non-Muslims and therefore, legitimate targets. Some jihadists even regard Shi'is, Sufis, and other Muslims as their enemies.

2.2.2 Extreme Right-Wing/Ethnically or Racially Motivated

Right-wing terrorism refers to the use of violence by right-wing groups, such as neo-Nazi, neofascist, and ultranationalist formations. They seek to force political, social, and economic systems into following an extremist right-wing model. One of their core concepts is supremacism, the idea that certain people sharing a common nation, race, or culture, etc. are superior to all others, giving them the right to rule over the rest of the population. Their ideologies feed off sub-cultures that resist social diversity and equal rights of minorities. Racist behaviour, authoritarianism, xenophobia, and hostility to LGBTQ+ communities and immigrants, are commonly found attitudes in such groups. The terms Extreme Right-Wing (ERW) terrorism & Ethnically or Racially Motivated (EoRM) terrorism are used interchangeably [9].

2.2.3 Left-Wing and Anarchist

Left-wing and Anarchist (LWA) terrorism, as an umbrella term, is used to describe violence promoting the absence of authority as a societal model. Such groups pursue a revolutionary, anticapitalist and anti-authoritarian agenda. Examples are the Italian 'Informal Anarchist Federation' or the Greek 'Conspiracy of Cells of Fire'.

2.2.4 Ethno-Nationalist and Separatist

Ethno-nationalist and separatist terrorist groups are motivated by nationalism, ethnicity, and/or religion. Separatist groups seek to carve out a state for themselves from a larger country, or annex territory from one country to that of another. The Irish Republican Army (IRA), Euskadi Ta Askatasuna

(ETA) in the Basque Country, and the Kurdish Partiya Karkerên Kurdistan (PKK) organisations fall into this category.

2.2.5 State-sponsored

State-sponsored terrorism is violence carried out with the active support of national governments provided to non-state actors. States can sponsor terrorist groups in several ways such as funding their organizations, providing training, supplying weapons, providing other logistical and intelligence assistance, and hosting groups within their borders.

2.2.6 Single issue

Single-issue or special-interest terrorism tends to focus on specific issues such as animal rights or environmentalism, in the belief that violence will compel a society to change its attitudes toward their cause. They are largely limited to online campaigns and nonviolent demonstrations by decentralised groups without strong cohesion.

2.3 Impact of Technological Advancements on Terrorist Financing

2.3.1 What is the Dark Web, and who uses it?

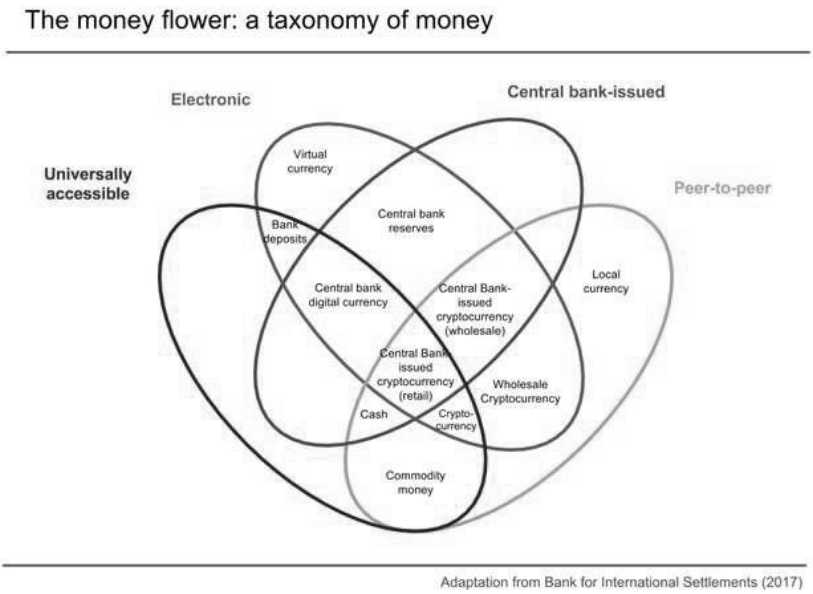
Due to a rapidly evolving cyber landscape, the Internet has become a source for open intelligence collection by law enforcement investigators, as well as a tool that can be abused for terrorist purposes. Social media sites and general web presence have facilitated efforts by terrorist actors to obtain financing worldwide. The internet has also facilitated their attempts to acquire weapons, materials, and knowledge, recruit, as well as spread their ideology without much financial outlay or government intrusion. Furthermore, the use of encrypted and anonymous tools provided by the Dark Web obfuscates their presence and hinders law enforcement. Nonetheless, understanding the methods that terrorists use in the Dark Web will enable law enforcement to act accordingly. It is important to note that not only terrorists, criminals, and law enforcement use the Dark Web, but also whistle-blowers, dissidents, activists, and intelligence organizations [10].

The Dark Web is the World Wide Web counterpart that exists on darknets, which are overlay networks that use the Internet but require specific software, configurations, or authorization to access. Such darknets include small peer-to-peer (P2P) networks, as well as large, popular networks such as Tor, Freenet, Invisible Internet Project (I2P), and Riffle, which are operated by public organizations and individuals. Through the Dark Web, private computer networks can communicate and conduct business anonymously without

divulging identifying information, such as a user's location or IP address. The Tor onion services uses the traffic anonymization technique of onion routing under the network's top-level domain suffix .onion [11].

2.3.2 Crypto-assets and Peer-to-peer transactions/Decentralized Finance

The use of encryption has been the most significant change to affect investigators – in particular, the use of encrypted assets or crypto-assets [10], which are purely digital assets that use public ledgers over the internet to prove ownership. They use cryptography, P2P networks, and a distributed ledger technology such as blockchain to create, verify, and secure transactions. Cryptoassets such as Bitcoin or Ethereum have various characteristics enabling them to be used as a medium of exchange, store of value, or for other business purposes.



Źródło: Bank for International Settlements, "Central bank digital currencies," Mar 2018. [Online]. Available: https://www.bis.org/cpmi/publ/d174.htm. [Accessed 14 Mar 2022].

Figure 2. The money flower: a taxonomy of money

The above figure illustrates the four key properties of money: issuer (be it central bank or otherwise); form (be it digital or physical); accessibility (be it public or restricted); and technology (be it account-based or token-based).

Crypto-assets have changed how illegal goods and services are traded in the Dark Web and transformed the financial world. As of March 2022, there were more than 9,000 crypto-assets trading in the marketplace [13]. Governments are now starting to regulate them, and FATF has imposed stringent Know Your Customer (KYC) requirements on exchanges that move crypto into fiat currencies. By doing so, they hope to make transactional records identifiable to real persons so as to lessen their anonymity.

P2P transactions appear to present high risks because they do not involve the presence of regulated entities, occurring outside the supervisory sphere. Despite the FATF's attempts at greater clarity, some decentralized finance (DeFi) models may remain in a grey area [14].

2.3.3 Social Media

Social media platforms are widely used by terrorists to spread propaganda and fund attacks worldwide. Recent attacks have showcased social media's role in radicalizing and recruiting individuals as well as screening their violent footage. The Christchurch mosque attacks in March 2019 that killed 51 people were announced on 8chan, live-streamed on Facebook, and then reposted repeatedly on various social media channels. These attacks were designed to "go viral", so as to garner support for more attacks and create a TF campaign. Investigations found that the "lone wolf" actor had made multiple donations to ERW entities overseas, transferring funds via crypto. Although the Christchurch video was subsequently removed from the internet, it can still be viewed from within the Dark Web.

Given the accessibility, reach, and anonymity afforded by these platforms, TF is often hidden in plain sight. Social media facilitates virality by offering instant and wide reach, opening the door for sympathizers to donate in small amounts, but the sheer volume results in significant amounts raised. Since calls for donations are often disguised as charitable causes, donors are tricked into becoming unwitting pawns.

Accounts raising funds on social media might try to vet prospective donors in online conversation first. Financial details are then exchanged using private messages sent via encrypted platforms involving exchange of credit card numbers, prepaid card details, bank account information, or digital wallet addresses. Payment instructions may be embedded in images or videos which

are hard to detect through standard search engines. Funds are sometimes moved through a chain of electronic transfers and then withdrawn in cash to be further transported by couriers, so as to layer and conceal the source of funds and final beneficiaries.

Relevant social media platforms include Facebook, YouTube, Twitch, Telegram, and Gab, while image boards include 4chan, 8chan/8kun, Endchan, and Meguca. Social media platforms themselves are not complicit in terrorism financing, but generally cooperate with authorities in providing information, or closing and blocking of such accounts. Crowdfunding platforms and payment processors can provide valuable information to an investigation when misconduct is suspected, such as personal identification, transaction details, IP addresses, and account information [15].

2.3.4 New Payment Products and Services

NPPSs utilise innovations to initiate payments through, or to extend the reach of, traditional markets. They provide an alternative for clients to the products and services that are commonly offered by traditional regulated FIs, such as banks. One of their greatest positive impacts has been the inclusion of individuals from developing countries in which basic financial services have not previously been sufficiently available. Their development allows for increased access to financial services for a wider population, creating new markets.

NPPSs are increasingly interconnected, not only between themselves but also with traditional payment methods. FinTechs, prepaid cards, mobile payment services, internet-based payment services and virtual currencies, internet-based loans, and alternative remittance services are manifestations of this trend. Simultaneously, however, methods of ML and TF have also evolved to circumvent legal protections in this area. Many NPPSs are anonymous by design, rendering tchem vulnerable to exploitation for ML/TF, particularly in jurisdictions with weaker AML/CFT laws. NPPSs both enhance existing financial services and create entirely new ones. They may be used to co-mingle illicit cash with legitimate business takings, move illicit funds across borders, or conceal criminal proceeds and send them offshore [16]. For example, low-value transactions via PayPal have been linked to terrorist suspects [15].

2.3.5 Crowdfunding

Crowdfunding has become particularly popular, with specialized websites allowing people to easily set up a fundraising page and collect donations. Although the vast majority of such activity is legitimate, it is vulnerable to exploitation because of how easy it is to mask the true funding purpose.

One of the underlying factors is the terrorists' presence in social media, forums, gaming chatrooms, and other internet platforms. Reliance on crowdfunding models also allows terrorists to extend their reach internationally.

Financiers can remain anonymous by simply publishing their crypto wallet number for donors to transfer funds to.

Jihadist financiers often disguise their true intent to avoid drawing attention from the fundraising platform or public authorities. Instead, they claim legitimate aims such as assistance to refugees. On the other hand, ERW actors often do not conceal their activities, especially if the group is not officially banned or designated as terrorist.

For example, the above figure shows an advertisement retrieved from the Dark Web by the Dark Web Monitor (DWM). The Daily Stormer is an American far-right, neo-Nazi, and white supremacist message board website that advocates for a second genocide of Jews, and the screenshot shows tchem soliciting for donations.

In addition, crowdfunding can be used to transfer funds abroad by avoiding regulated financial entities. Canada has seen instances where terrorist suspects who are under investigation have used crowdfunding websites prior to their attempts to leave the country [15].

Źródło: Daily Stormer, "Daily Stormer – The Most Censored Publication in History," 2022. [Online]. Available: http://stormer5v52vjsw66jmds7ndeecudq444woadhzr2plxlaayexnh6eqd.onion. [Accessed 4 May 2022].

Figure 3. Screenshot of The Daily Stormer 's advertisement on the Dark Web

2.3.6 Non-fungible Tokens

Non-fungible tokens (NFTs) are digital tokens on a blockchain that represent ownership of images, videos, audio files, and other forms of media or ownership of physical or digital property. The tokens represent and verify the ownership of a unique digital asset, such as a piece of digital art. Because the NFTs are on a blockchain, they are publicly verifiable, auditable, and digitally unique. But unlike crypto-assets on a blockchain with fluctuating exchange rates, such as Bitcoin or Ether, the value of each NFT in theory depends on the individual exchange between a buyer and seller and the subjective valuation the parties place on the NFT.

Although the U.S. Department of the Treasury recently concluded that "the art market should not be an immediate focus for the imposition of comprehensive AML/CFT requirements," they highlighted the explosive growth

of the NFT market as an area of potential concern [18]. In particular, smart contracts allow artists to be paid every time an NFT is sold, which incentivizes selling the piece several times with the possibility that no due diligence is completed on the purchaser [19]. NFT marketplaces and other intermediaries in NFT transactions should pay careful attention to the ways in which otherwise legitimate platforms can be abused for ML or TF purposes.

3 Current Terrorist Financing Modi Operandi

3.1 Types of Organizations and their Uses of Funds

Terrorist actors vary in size, structure, operational reach, motivations, recruitment, and capabilities. Despite their differences, they share a common need for financial means to transform plots into terrorist acts [15].

3.1.1 Terrorist Organizations

Terrorist organizations utilize funds according to the following broad functional categories.

3.1.1.1 Operations

Operationally, funds are needed to carry out attacks and undertake pre-operational surveillance. This includes travel to and from the objective, vehicles and other machinery, and equipment ranging from light assault weapons to improvised explosive devices (IEDs). Funds are also required for fake identification and basic living expenses.

3.1.1.2 Propaganda and Recruitment

The Internet provides a less expensive way to initiate recruitment but following up requires additional costs. Indeed, exploitation of social media for such purposes has become a priority CFT issue. More complex organizations are investing in sophisticated propaganda operations including magazines and newspapers, internet domains, websites, and television and radio outlets.

3.1.1.3 Training

Funds are needed for training of operatives in weapons, bomb-making, and ideology. Terrorist groups often acquire land or buildings to be used as training facilities.

3.1.1.4 Salaries and Member Compensation

Funds are also needed to pay salaries of leadership and members. Providing financial security and incentives to group members can secure commitment to the organisation's goals and ideology. They may also provide long-term financial support to the families of jailed or deceased operatives.

3.1.1.5 Social Services

Lastly, funds are needed to establish or subsidize social institutions that provide health, social, and educational services. Terrorists do this to undermine the credibility of the official governments – by providing services that they say the state is neglecting – and to build support within local populations.

3.1.2 Foreign Terrorist Fighters

Foreign terrorist fighters (FTFs) are defined by FATF as "individuals who travel to a state other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training" [20]. They are pivotal to terrorist groups and remain a significant threat. Their needs are modest and include basic living expenses. Prior to entering the conflict zone, they might need to purchase weapons. Their funding may also occur informally, through family networks. It is often difficult to determine the real end use of the transfers since most of the funding from source to conflict zones is for legitimate family support or humanitarian reasons.

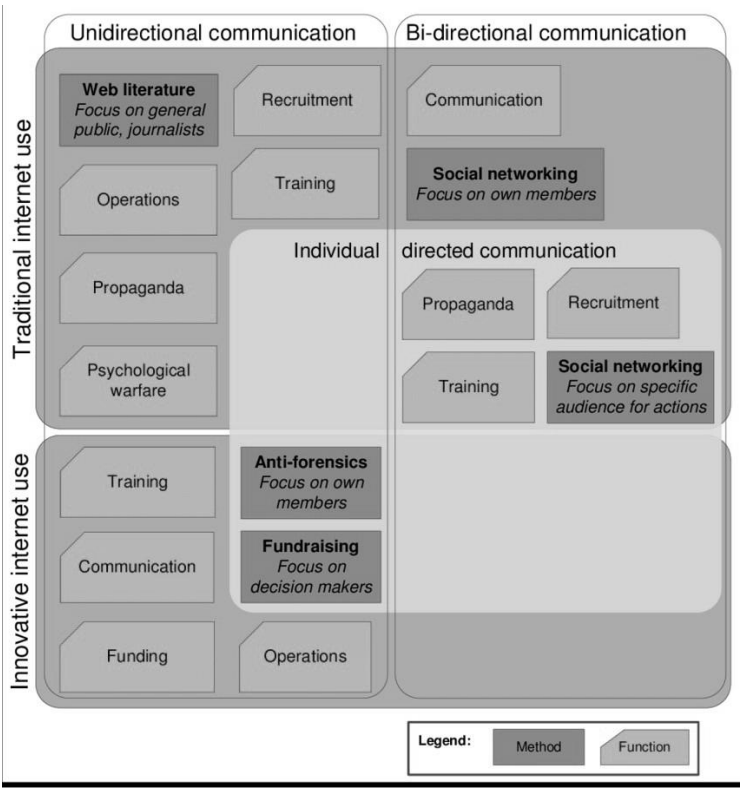
3.1.3 Lone Actors and Small Cells

In contrast to large organizations, lone actors and small cells have only minor financial needs since the costs of their attacks are low. They do not control territory, field conventional militias, or operate checkpoints. That said, they must have the means to provide for their own basic needs, communication, and materials for their attacks. According to a Norwegian Defence Research Establishment report, three out of four European small cell terrorist plots that took place between 1994 and 2013, cost less than USD10,000 each. The bulk of expenses is incurred by the lethal component, such as assault rifles or explosives.

3.1.4 Extremist Online Communities

Online social networks have a formative influence on individuals' behaviour due to their inherent socialising, recruitment, and decision shaping

functions. This is exacerbated by the international character of digital environments, the search for belonging, amusement, and heroic masculinity, the promotion of violence through memetic irony, and the gamification and "memeification" of terrorism. In ERW online communities, conspiracy narratives often claim malicious intent behind societal events. Members of an online community can contact one another, forming both online and offline bonds. The most potent combination involves online identification with the terrorist group coupled with offline engagement in physical activities [21].



Źródło: N. Veerasamy and M. Grobler, "Terrorist Use of the Internet: Exploitation and Support through ICT infrastructure," Jan 2011. [Online]. Available: https://www.researchgate.net/publication/266173850_Terrorist_Use_of_the_Internet_Exploi tation_and_Support_through_ICT_infrastructure/. [Accessed 25 Feb 2022].

Figure 4. The Internet as terrorist supporting mechanism

The above figure shows the complexity of Internet usage as both traditional communication and information gathering tool, via innovative new ways. The Internet is also used for both unidirectional and bi-directional communications.

3.2 Sources of Funds

Terrorist actors rely on numerous sources of income comprising both inherently criminal as well as legitimate activities [15].

3.2.1 Private Donations

Private donations come from a wide range of sources. An analysis of TF-related prosecutions in the US since 2001 found that approximately one-third of cases involved direct financial support from individuals to terrorist networks. The trend for newer organizations is to look for small-scale sources especially though social media.

3.2.2 Abuse/Misuse of Non-Profit Organizations

Particularly during COVID, terrorist organizations have falsely claimed to be non-profit organizations (NPOs) so as to raise funds online, by diverting donations, abusing program delivery to support the terrorist organization, and creating fake NPOs through misrepresentation and fraud. Charities at highest risk of abuse are those engaged in services operating close by to active terrorist threats.

3.2.3 Proceeds of Criminal Activity

Criminal proceeds are another source of funds. Terrorists have engaged in credit card fraud, insurance and loan fraud, tax crimes, drug trafficking, smuggling of goods and associated tax fraud, illicit tobacco trade, smuggling of antiques and cultural artefacts, as well as armed robberies.

3.2.4 Extortion of Groups and Businesses

Extortion of local populations is a way for terrorists to sustain their activities. Revenue streams include so-called taxation of illegal drugs, protection and arbitration taxes, human trafficking, and cigarette smuggling.

3.2.5 Kidnapping for Ransom

Kidnapping for ransom is another growing source of revenue. Paid ransoms are reported to range from EUR600,000 to EUR8 million per ransom. The trail of funds can be complicated if a kidnapping occurs in one jurisdiction and ransom payment in another.

3.2.6 Legitimate Commercial Enterprise

Revenue can be channelled from a commercial enterprise, such as a used car dealership or restaurant franchise, to support a terrorist organisation. ERW terrorists also raise funds through concerts and events, and sale of merchandise.

3.2.7 State Sponsorship

Many public sources and governments have also claimed that certain terrorist groups are statesponsored.

3.2.8 Self-funding

Last but not least, small attacks can be effectively self-funded by individuals and their suport networks using savings, credit, or proceeds of businesses under their control.

3.3 Traditional Channels for Movement of Funds

Terrorist actors employ a range of methods to move funds, often internationally, to their end point without being detected [15].

3.3.1 Banking Sector

The banking sector continues to be attractive for TF because of the speed and ease at which it can move funds within the international financial system, especially using the bank accounts of NPOs to move funds to terrorist organisations. Such transactions are often small-scale and hard to distinguish from the large number of legitimate daily transactions. Although AML/CFT controls are making it harder to move funds through this sector, the risk remains.

3.3.2 Remittance Sector/Money Service Businesses

The remittance sector is also vulnerable to TF. The term money services business (MSB) is used to describe businesses that transmit or convert money, encompassing non-bank FIs. In countries where banking access is limited and terrorist groups operate, MSBs may be the primary means for cross-border funds transfers. The biggest threat involves agents or employees who knowingly facilitate such transfers on behalf of terrorist groups, falsifying transaction reporting to obfuscate or anonymise details.

3.3.3 Hawala and Similar Providers

Unregulated hawala are a traditional money transfer mechanism operating extensively in South Asia, the Middle East, and Africa due to geography, culture, and lack of banking access. They are money transmitters which arrange for low-value funds transfers between receiving and pay-out agents through non-bank methods such as trade and cash, and net settlement over a prolonged period, mostly operating near migrant communities. Please refer to Annex I for a detailed exploration of how hawala works.

3.3.4 Cash

Cash continues to play a major role in TF. While funds may be raised in many ways, they are often converted into cash to be brought into conflict zones, facilitated by porous borders, difficulty in detecting small amounts, and lack of regulations. The rise of bulk cash smuggling between conduit countries and high-risk areas has also been observed.

3.3.5 Prepaid Cards

Prepaid cards can be loaded domestically and inconspicuously carried cross-border without any declaration. Upon arrival, the funds are then converted back to cash through offshore ATM withdrawals. Any person can access the stored value using the accompanying personal identification number (PIN).

3.3.6 Online Payments

Online payments appear to be linked to online equipment and clothing purchases before travel to conflict zones, rather than direct payments to fund terrorist activities. The use of such payments reflects their prevalence in the financial system, rather than their vulnerability to TF.

3.4 Movement of Funds via Crypto-assets

Terrorists are seeking operational security and convenience—particularly those networks trying to promote safe and easy methods of funds transfer to prospective donors online. Their opportunism is also evident from how they leverage financial infrastructure and businesses under their control, as we will later see in the case of Al-Qaeda. In this regard, terrorists are looking for crypto-assets that offer anonymity for both users and transactions, quick transmission, low volatility, widespread adoption, and reliability.

3.4.1 Pros and Cons

Pros	Cons
Used as alternative if other funds transfer methods are banned	Requires internet access, expertise, and access to vendors/exchanges
Allow for anonymous cross-border funds transfers	Volatility
	Evidentiary nature of blockchain data
Useful for fundraising, strategic procurement, online infrastructure	Not preferred for purchasing arms, explosives, or weapons due to lack of widespread acceptance

Table 1: Pros and cons of moving funds via crypto-assets

On the one hand, the advantages of using crypto-assets such as Bitcoin to move funds include its availability as a means of last resort if other methods of transferring money are banned. For example, the Danish branch of the Nordic Resistance Movement, a Nazi group, lost their bank account in October 2020 based on the bank's terms of service, and thus switched to crypto [9]. Crypto-assets also allow for anonymous cross-border funds transfers. After fiat has been converted into crypto, subsequent decentralized crypto transfers can be challenging to investigate. Furthermore, crypto is useful for fundraising, strategic procurement, and online infrastructure.

On the other hand, the disadvantages of using crypto-assets include the need for internet access, people who understand the basics of using crypto, and access to vendors who accept crypto-assets and exchanges that can convert them into cash. As a result, terrorist networks using crypto-assets in Syria tend to be more consolidated or centralized than the traditional, non-crypto

networks operating in the country. Moreover, crypto-assets are volatile, and coins with low adoption and market value are even more so. Increased volatility invites the risk of a quick loss of value as assets are stored, especially with delays in converting to real currency. Such realities may reduce the appeal of crypto-assets. Additionally, blockchain data might not be suitable for criminals because of its evidentiary nature, given that it is documented, immutable, and cannot be manipulated. Finally, crypto-assets are also not the preferred currency for purchasing arms, explosives, or weapons, due to the lack of widespread acceptance [23].

3.4.2 Assessment of Suitability of Crypto-assets for Terrorist Financing

With regard to assessing the suitability of crypto-assets for TF, the RAND Corporation examined five financial activities (fundraising, illegal drug and arms trafficking, remittance and transfer of funds, attack funding, and operational funding) and evaluated the importance of six cryptocurrency properties in facilitating these activities, namely anonymity, usability, security, acceptance, reliability, and volume, as shown in Figure 5. They found that no cryptocurrency uniformly offers these features to terrorist actors; in particular, security is probably inadequate for terrorist needs [24].

Assessment of Terrorist Finance Activities with Respect to Cryptocurrency Properties

	Fundraising	Illegal Drug and Arms Trafficking	Remittance and Transfer	Attack Funding	Operational Funding
Anonymity	Moderate importance	Critical importance	Moderate importance	Critical importance	Lesser importance
Usability	Critical importance	Lesser importance	Lesser importance	Lesser importance	Lesser importance
Security	Moderate importance	Critical importance	Critical importance	Critical importance	Critical importance
Acceptance	Lesser importance	Lesser importance	Lesser importance	Moderate importance	Moderate importance
Reliability	Lesser importance	Moderate importance	Critical importance	Critical importance	Moderate importance
Volume	Moderate importance	Lesser importance	Critical importance	Lesser importance	Critical importance

Źródło: RAND Corporation, "Terrorist Use of Cryptocurrencies – Technical and Organizational Barriers and Future Threats," 2019. [Online]. Available: https://www.rand.org/pubs/research_reports/RR3026.html. [Accessed 2 Mar 2022].

Figure 5. Assessment of terrorist financing activities with respect to cryptocurrency properties

All in all, crypto-assets are not replacing other methods of TF. Instead, terrorists often use cryptoassets in conjunction with other MSBs and transfer methods. Many unlicensed MSBs have incorporated crypto-assets as another means of transferring funds. Terrorists taking crypto-asset donations rely heavily on them because they need to convert their crypto-assets into cash but cannot turn to services that follow the regulations. Disturbingly, many of these businesses do not bother with KYC, and continue to grow in volume of legitimate transactions while allowing terrorist groups to abuse them [25].

3.5 Crypto-related Business Models/Activities that may Facilitate Terrorist

Financing The following are some crypto-related business models and activities that may facilitate TF [26].

3.5.1 Crypto Exchanges

Crypto exchanges are companies and individuals that offer fiat to crypto-asset exchange services to the public. Exchange services are often just one aspect of a full spectrum of often unregulated financial services offered by Virtual Asset Service Providers or VASPs (in FATF terminology).

3.5.2 P2P Exchangers and Platforms

P2P exchangers and platforms facilitate transfers of value for the public, including the buying and selling of crypto directly without a central operator. In practice, many fail to comply with regulatory requirements or conduct customer due diligence (CDD). They usually charge higher percentage fees and accept a wide variety of payment methods.

3.5.3 Crypto Kiosks

Crypto kiosks, commonly referred to as "Bitcoin ATMs," are standalone machines that allow users to convert fiat to and from crypto-assets using a customer's mobile device, thus offering convenient physical access to crypto-asset exchange services. In practice, many fail to comply with regulatory requirements or conduct CDD.

3.5.4 Crypto Casinos

Crypto casinos facilitate various forms of betting denominated in crypto-assets. Traditional brickand-mortar casinos generally do not accept crypto; however, online gambling sites do.

3.5.5 Anonymity-Enhanced Cryptocurrencies (AECs)/Privacy Coins

The acceptance of AECs or privacy coins—such as Monero, Dash, and Zcash-by MSBs and darknet marketplaces has increased their usage. They obscure transactions on their blockchain to maintain the anonymity of users and their activity, thus undermining regulatory AML/CFT controls. The advanced encryption techniques used by AECs constitute a formidable challenge to identifying those responsible for such transactions.

3.5.6 Mixers, Tumblers, and Chain Hopping

"Mixers" and "tumblers" are entities that attempt to obfuscate the source of crypto units by mixing crypto from several users before delivery. For a fee, a customer can send crypto to an address controlled by the mixer. The mixer then commingles this crypto with funds received from other customers before sending it to the requested address. "Chain hopping" is when criminals move between different types of crypto-assets to shift the trail from one blockchain to another.

3.5.7 Jurisdictional Arbitrage and Compliance Deficiencies

Finally, the lack of consistent AML/CFT rules and crypto regulation across jurisdictions impedes law enforcement's ability to prevent crypto-asset enabled crime. For example, illicit financial flows may move to jurisdictions which lack the record-keeping necessary to support investigations.

4 Challenges and Gaps in Countering the Financing of Terrorism

4.1 Broad Challenges

The following are some of the broad challenges and gaps that jurisdictions face in combating TF [9].

4.1.1 Different Legal Regimes

Differing legal regimes across jurisdictions can determine which agencies investigate the underlying terrorist activity and its financing. For example, some actors might be classified as criminals and prosecuted under non-terrorism-related charges, while others might be viewed as national security threats and charged under terrorism-related charges. Investigation of TF activity may not be available for certain types of crime, and terrorists might exploit these loopholes for regulatory arbitrage.

4.1.2 Growing Transnational Links

Growing transnational links have resulted from terrorist groups using the internet and social media to share propaganda and recruit supporters from around the world. They may also forge financial links and collaborate in paramilitary or other specialized training. Individuals have travelled to conflict zones to network, recruit, and acquire combat experience.

4.1.3 Foreign Terrorist Fighters

Information on FTFs is often highly confidential, making the sharing of such information challenging. To obtain a full picture of their activity, data from FIUs needs to be combined with contextual and de-sensitised information from operational and intelligence authorities as well as private sector entities. As such, arrangements for interagency collaboration need to be established.

4.1.4 Lone Actors

Lone actors are not directly affiliated with a terrorist organization. They typically do not rely on an extensive network of entities that provide operational support or leave a financial trail. Authorities and FIs may see fewer opportunities for financial disruption of these attacks and place less emphasis on them.

4.1.5 Social Media

Social media may show the relationships between individuals but may not provide sufficient clues to distinguish between sympathisers, supporters, and actual terrorists. Also, the challenges in proving TF or obtaining evidence on the use of internet fund transfers have been noted [15]. Social media information could be better leveraged for investigative and prosecutorial purposes. Further discussion could be on defining reporting obligations for crowdfunding platforms and improving regulations on digital payments. Online spaces must be understood as an extension of society, and it is important to enhance digital literacy, raise awareness of extremist radicalization, and promote responsible online behaviour [21].

4.1.6 Exploitation of Natural Resources

The natural resource sector may be exploited for TF in countries which lack effective controls. The gas, oil, timber, diamonds, precious metals, wildlife, and charcoal sectors are profitable sources of revenue, leading to extortion, smuggling, theft, illegal mining, kidnapping for ransom, corruption and other environmental crimes. Such crimes are often complex and require

extensive financial analysis. In view of the vast sums that can be generated, we must consider how public and private sectors can collaborate together with actors outside of the traditional AML/CFT regime [15].

4.2 Challenges and Gaps Specific to fighting Extreme Right-Wing terrorism

ERW terrorism is a complex and growing phenomenon that encompasses a wide range of actors. These range from "lone wolves" to small and medium organizations, as well as transnational movements. This type of terrorism faces some specific challenges.

4.2.1 Lack of National Designations

Designation as a terrorist or terrorist organisation results in an entity having its assets frozen and it being prohibited from transactions. However, there is no international designation regime targeting ERW groups. Furthermore, these groups cannot be designated if they operate as loose networks of affiliated individuals and fail to meet the criteria for potential terrorist activity or lack an identifiable command and control structure. Some jurisdictions may face legal constraints in curbing non-violent activity or face domestic political challenges in acting against groups which are affiliated with political parties.

4.2.2 Public-Private Partnerships and Information Sharing

Many jurisdictions have public-private partnerships that focus on Jihadist TF, including forums to share threat specific information. These could be applied to ERW groups. Contextual indicators to help FIs identify possible terrorist activity may also be extended to ERW threats.

4.2.3 Inclusion of Extreme Right-Wing Groups in National Risk Assessment Process

Countries which are vulnerable to ERW groups should also include them in their national risk assessments (NRAs). Although national authorities have a good grasp of transnational sharing of ideological propaganda, they have yet to capture sufficient data on transnational fundraising activity.

4.3 Impact of COVID-19

The UN has warned of increased terrorist and TF activity while government attention is focused on COVID-19 [27] [28]. In general, the pandemic and ensuing economic and social crises have contributed to polarisation in society, causing attitudes to harden. As many individuals suffered financial

losses, they looked to blame their misfortune on governments, foreigners, or ethnic and racial minorities. At this same time, the drop in international travel temporarily restricted terrorists' freedom of movement, limiting opportunities for physical meetings and shifting their networking activities online [8].

4.3.1 Increased Fraud

Terrorists have attempted to profit from the pandemic through increased fraud, with scams to appeal to individuals who may have lost their jobs or suffered a loss in income. Fraudsters may impersonate government officials with the intent of obtaining personal banking information or physical cash from individuals. Such cases are likely to increase as governments disburse grants and tax relief payments to their citizens.

There has also been a significant increase in online scams involving counterfeiting of medical supplies, personal protective equipment (PPE), and pharmaceutical products. The fraudsters claim to represent businesses, charities, and international organisations offering masks, testing kits and other products, requesting credit card information for payment but never delivering the goods. In addition, terrorists posing as charities circulate emails requesting donations for COVID-related research, victims, and/or products. Recipients of these emails are then directed to provide credit card information or make payments through the fraudster's secure digital wallet.

The economic crisis has also led to an increase in investment scams, such as promotions falsely claiming that products or services of publicly traded companies can prevent, detect or cure COVID- 19. Microcap stocks, typically issued by the smallest companies, are vulnerable to such schemes due to the limited availability of public information on these companies.

4.3.2 Changing Financial Behaviours

COVID has also led to significant changes in financial behaviours and patterns. Some banks have closed physical branches, reduced opening hours or restricted the services available in-person.

Customers are carrying out more transactions remotely. There has been a shift to online banking, including remote customer on-boarding and identity verification. However, this may have reduced the effectiveness of CDD.

Certain population segments such as the elderly, low-income, and remote or indigenous communities may be less familiar with using online banking platforms, and therefore more susceptible to fraud. Furthermore, as has been seen during past downturns, those with financing needs may seek out unlicensed lenders, which may include terrorist groups.

4.3.3 Increased Financial Volatility

This period of increased financial volatility has also led to exploitation of new vulnerabilities. In an economic downturn, terrorists may seek to invest in real estate or troubled businesses to generate cash and mask illicit proceeds. They can also introduce illicit proceeds into the financial system by restructuring existing loans. In addition, corporate insolvency proceedings can free up illicit cash contained in businesses whilst masking the funds' origins.

Recent swings in securities values are resulting in individuals liquidating their portfolios and withdrawing large amounts of banknotes. Increased physical cash transactions can mask TF activities in several ways. For example, banknotes can be used to purchase safe haven assets such as gold, which are less easily traceable.

Stockpiling of crypto-assets also increases when there are general concerns over the state of the economy. For example, crypto-assets may be used for payments in fraud schemes linked to the pandemic. In one recent case, the US Justice Department reported that an individual used cryptoassets to launder proceeds earned from selling fraudulent COVID medicine [29].

5 "Parallel Investigations" and Other Good Practices

5.1 "Parallel Investigations"

To discover all relevant actors in the network, it is important to conduct parallel investigations on the terrorism and TF offence at the same time. This combines complementary expertise from both disciplines and ensures offences are systematically and holistically investigated. Since financing is an integral part of the overall activity cycle, a TF investigation can identify targets early, allowing more time for disruption. TF should not just be evidence-based but also intelligence-led [3].

5.1.1 Involvement of All Relevant Competent Authorities

A thorough assessment of TF risks will involve many key public authorities including intelligence and security agencies, police and border security, prosecution authorities, the FIU, customs, the national authority in charge of financial sanctions, supervisory and regulatory authorities, and foreign counterparts. Other agencies may hold relevant information, such as tax authorities, social welfare administrations, and civil aviation authorities.

Assessment will also involve non-government stakeholders such as FIs, designated non-financial businesses and professions (DNFBPs), and NPOs.

Also, it is essential to collaborate with foreign counterparts, for example by conducting a joint investigation or providing them information so that they can conduct a parallel investigation.

5.1.2 Collection of Wide Range of Quantitative and Qualitative Information

It will be necessary to collect a wide range of quantitative and qualitative information, including on the general criminal environment, TF and terrorism threats, TF vulnerabilities of specific sectors and products, and the jurisdiction's general CFT capacity. While relationships are revealed from financial information, intelligence value can be derived from "non-financial" information such as phone numbers, email addresses, passport numbers, etc. contained in financial documents.

5.1.3 Identify All Parties and Assets Involved

Investigators should identify all parties involved in a timely manner as well as all assets which might be subject to confiscation. As much financial investigation as possible should occur before the terrorist becomes aware he is being investigated, including tracing of assets and liabilities, net worth analysis, and understanding of income and expenditures.

5.1.4 Overcoming Challenges Faced

Many jurisdictions face challenges with the investigative capacity to conduct parallel investigations [30].

5.1.4.1 Integration of Parallel Investigations

Often, financial investigations are not pursued if the underlying terrorist activity appears to be selffunded or sums involved are small. Good practices include ensuring that a TF investigation can be launched without an underlying terrorism case, and that the TF investigation can continue even where the corresponding terrorism investigation has already been concluded. Another useful practice is to issue manuals and procedures for identifying and investigating TF.

5.1.4.2 Information-sharing

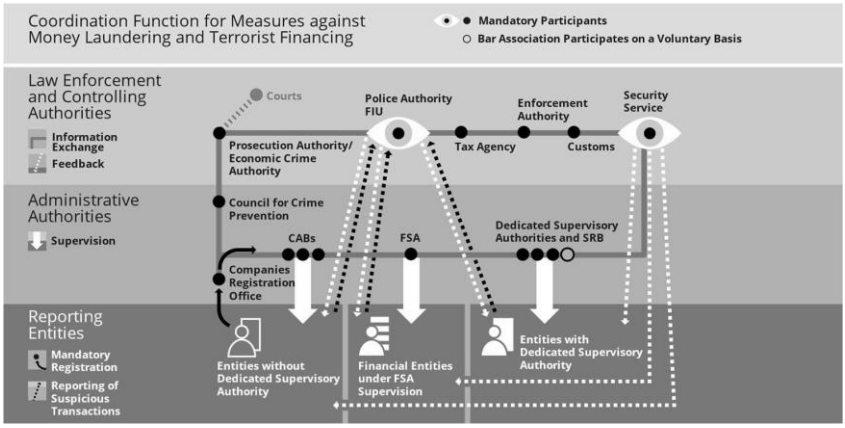
The sensitive nature of related information can pose information sharing challenges. As such, the lead agency must be able to segregate the handling of sensitive and non-sensitive information by ensuring all participants have appropriate security clearance, and innovative mechanisms must be established, such as through redacted or sanitized reports, extracts of cases, 'closed' briefings, use of anonymized or aggregated statistics, or use of proxy organisations to validate information.

5.1.4.3 Time-sensitivity

TF cases are often time-sensitive and there is a fine balance between allowing the TF activity to continue, so as to gather further evidence, and disrupting the activity to prevent a possible attack. Many jurisdictions have opted to disrupt the activities early instead of pursuing a TF prosecution. This is often done in the interest of public safety, or where there is insufficient evidence to suport a TF prosecution. 5.2 Example of Swedish System for AML/CFT In the example of Sweden, CFT takes place globally, on the EU level, as well as nationally. Several LEAs and administrative agencies, together with large parts of the private sector, have obligations in this area. Since 2014, Sweden has a national strategy for an effective regime to combat ML and TF. The strategy is based on available knowledge on the threats, vulnerabilities, and risks that Sweden is exposed to. Its purpose is to define the goals, priorities, and measures necessary in the short and somewhat longer term. There is also a national counter-terrorism strategy which complements the CFT work [31].

5.2 Example of Swedish System for AML/CFT

In the example of Sweden, CFT takes place globally, on the EU level, as well as nationally. Several LEAs and administrative agencies, together with large parts of the private sector, have obligations in this area. Since 2014, Sweden has a national strategy for an effective regime to combat ML and TF. The strategy is based on available knowledge on the threats, vulnerabilities, and risks that Sweden is exposed to. Its purpose is to define the goals, priorities, and measures necessary in the short and somewhat longer term. There is also a national counter-terrorism strategy which complements the CFT work [31].



Źródło: Government Offices of Sweden, "Combatting money laundering and terrorist financing," 26 Sep 2019. [Online]. Available: https://www.government.se/government-policy/financialmarkets/combatting-money-laundering-and-terrorist-financing/. [Accessed 15 Jun 2022].

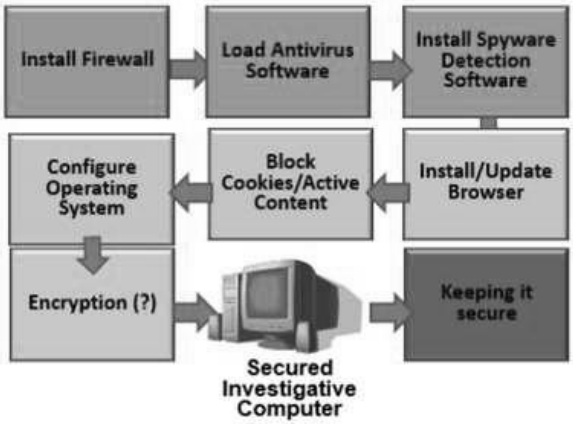
Figure 6. Schematic of the Swedish system for anti-money laundering/countering financing of terrorism

5.3 Operational Guidance for Dark Web Investigations

Accessing any area of the Dark Web requires investigators to consider their general safety, even on computers. The application of good technical practices and practical operational tips will help to prevent investigators from being identified or their computer systems from being breached [10].

5.3.1 Good Technical Practices

Accessing the Dark Web requires investigators to consider their general safety, even on computers. This requires an effective process to secure their systems. Computers should be free of references to investigators or their agency. Investigators should arrange to purchase Internet access from an independent source. A VPN confers another layer of protection. The investigator is advised to consider local regulations and laws when designing online access and computer investigations.



Źródło: INTERPOL, "Guidelines on the darknet and cryptocurrencies," INTERPOL Innovation Center, Singapore, 2020.

Figure 7. Process for securing the investigative computer

The Tor Browser constitutes a basic level of protection for the investigator. Building a multi-layered defence helps to protect against the target being led to the investigators' real IP, role, or identity. Software known as Virtual Machines (VMs) add an additional layer of security by allowing users to boot another operating system (OS) within the existing system. A useful suggestion is to create a master environment with all the tools, updating it as required and cloning a new copy of this environment for each investigation.

5.3.2 Practical Operational Tips

Investigators should have already built certain personae into their investigative plans. Due to the nature of darknet markets, vendors and users are wary of new users, which is why access often requires a username and password. The longer the identity has been around, the more likely the persona will be accepted. Another good practice is to use a separate identity for each investigation. Creating multiple profiles is a good practice, ensuring that the case is not totally lost if one identity is inadvertently disclosed.

When investigating a site with an accompanying forum, it is good practice to login to the forum with the same persona used on the market. Building credibility through comments and questions on the forum helps build the overall credibility of the persona. Forums can be an excellent source of intelligence to obtain information about the market's administrators and vendors.

All user identification information should be unique to the persona being built because we do not know who is able to see the user's data on the back end. The reuse of something as simple as the same PIN might identify the investigator as a law enforcement officer. Likewise, the e-mail address should be unique to the persona. Be sure to use a "zero-knowledge" e-mail provider or an e-mail service from within the Tor network. Investigators also need to prepare Pretty Good Privacy (PGP) keys ahead of time, generating a new pair of keys for each identity assumed.

5.4 Availability and Admissibility of Evidence

Many of the challenges in TF cases relate to the availability and admissibility of evidence [30].

5.4.1 Elements of Offence that are Challenging to Prove

Some particular challenges related to proving the elements of the TF offence include:

- Having to prove that the defendant intended or knew that the funds were to be used for a terrorist act – especially where the defence claims the funds were meant for personal expenses;
- Having to prove that the recipient is a terrorist, especially where they have not been officially designated as such, or before a terrorist attack is committed; and
- And having to prove TF when the funds are sent overseas or may not ever be actually used to finance an attack.

5.4.2 Challenges in using Classified Intelligence as Admissible Evidence

TF cases may rely on classified intelligence. The defendant may also be privy to information that is classified, and thus pose a disclosure risk to the national authorities. Challenges in "converting" classified intelligence into admissible evidence include:

- Prosecution having to find a way to recreate information otherwise only found in classified material;
- Prosecution finding itself in a position where it would have to reveal secret information, and therefore, dismissing the case;
- The inadmissibility of some evidence leading to partial sentencing;
- The burden of steps required to keep the sources and methods of intelligence gathering confidential; and
- Differing levels of security clearance amongst different officials, complicating inter-agency cooperation.

5.4.3 Good Practices

Although gathering and using evidence is challenging, there are also some good practices:

- Having legislation or judicial procedures specifically dealing with how to manage classified intelligence.
- Involving the prosecutor at an early stage to determine admissibility of evidence.
- Steering the investigation such that confidential intelligence is supplemented with admissible evidence.
- Developing jurisprudence to enable the use of circumstantial and indirect evidence to prove knowledge and intent.
- Using the defendant's own words and activities, such as on social media, to prove intent.
- Establishing a system of domestic designations or developing jurisprudence which gives weight to foreign designations.
- Using the 24/7 electronic evidence system under the Budapest Convention to offer immediate assistance.
- Having a designated special court to deal with terrorism and TF cases; and
- Using administrative powers to freeze assets based on confidential intelligence that cannot be used to support a prosecution.

5.5 Legal, Professional, Ethical, and Societal Considerations

When mounting a Darknet investigation, the investigator must bear in mind the following considerations [10].

5.5.1 Legal Challenges

Legal challenges to investigating crimes on the Dark Web include country-specific laws, and the legality of using crypto in the investigation. The level of active engagement in the Dark Web differs with each case. Dark Web investigations are inherently multinational in nature, requiring the assistance of international counterparts. A good example was in 2017 when AlphaBay and Hansa Market were shut down. FBI decided to quietly terminate AlphaBay without much fanfare and given that the Hansa market did not offer any child abuse material or weapons, the Netherlands police allowed it to continue operating for a few more weeks. This bought precious time for the global law enforcement community to acquire more knowledge and evidence. It is advisable to secure the prosecutor's approval whenever interaction with other Dark Web platform users is required.

5.5.2 Chain of Custody

The chain of custody of evidence documented on the Dark Web is as important as any other evidence collected in the real world. Where it was found, how it was found, how it was documented, where it was stored and who handled the evidence, all typically need to be addressed and documented.

5.5.3 Proper Documentation

Documentation of Dark Web-based evidence found through the Tor Browser is similar to traditional Internet based evidence – it includes the screen capture of the browser as the investigator sees it, downloading and documenting the source code of the hidden service site, as well as the images found on the site. Once all the evidence has been collected from the target web page, the investigator should validate the evidence collected by hashing the files.

5.5.4 Technology Exploits

One approach to identifying Darknet users is to use technology exploits. The defences of a user who rigorously implements and uses anonymization techniques would be challenging to penetrate. Hence, the aim of technology exploits is to social engineer a situation in which targets violate their personal and computer security habits. A momentary violation is long enough to expose the target's true IP address. It is important for the investigator to understand the legal implications for using such exploits.

5.5.5 Ethical Considerations for Data Collection and Use of Analytics Tools

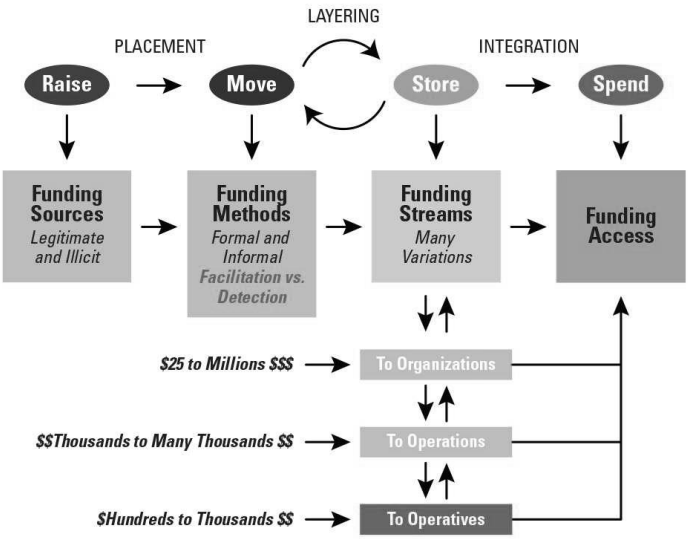
The tools rely on big data and machine learning algorithms to collect, aggregate and analyse data items from Darknet markets, crypto ledgers, and seized devices. Such tools raise significant ethical issues. Appropriate safeguards must be integrated into their design with regard to privacy and data protection, security, data minimization, confidentiality, purpose binding, and transparency constraints. The risk of interference with privacy and other fundamental rights must be balanced with the goal of preventing, investigating, detecting, and prosecuting terrorist-related activities. Nonetheless, such interferences must be minimized, and the tools used in a proportionate manner and for a clearly defined purpose, so as to uphold public security.

6 "Follow the Money" and "Follow the Actor" Approaches

6.1 "Follow the Money"

6.1.1 Tracking the Flow of Money to Identify Suspects

A well-established methodology is the "follow the money" approach, where the fundamental principle is to track the flow of money leading to the identification of suspects behind the illicit activities. This requires collaboration across various functional areas including asset recovery, the use of crypto and fiat currencies, law enforcement and regulatory agencies, foreign counterparts, international authorities, and public-private partnerships. It holistically considers all stages of TF, including raising, moving, and using funds, as well as the different sources, channels, destinations, and origins of terrorist funds [3].



Źródło: D. M. Lormel, "Terrorist Financing: Visualizing Funding Flows," ACAMS Today, 18 Sep 2018. [Online]. Available: https://www.acamstoday.org/terrorist-financing-visualizingfunding-flows/. [Accessed 15 Jun 2022].

Figure 8. The terrorist-funding cycle

6.1.2 Relevant Information and Cross-Border Intelligence

There are many types of information which are relevant to investigators that can be obtained from the banking, remittance, hawala, and NPO sector that include the services offered, types of customers served, nature of TF threats, as well as AML/CFT compliance and awareness within each sector.

When assessing cross-border TF risks, jurisdictions would typically consult information on crossborder elements from existing intelligence, customs experience and confiscations, analysis of crossborder declarations or cross-border wire transfers, and information on international cooperation related to terrorism and TF [4].

6.1.3 Money Laundering/Terrorist Financing Red Flag Indicators Associated with Crypto-assets

In 2020, FATF prepared a list of red flag indicators to assist in identifying potential ML and TF activity involving crypto-assets. These indicators are specific to the nature of crypto-assets and their associated financial activities and should be considered in context, necessitating further investigation where appropriate. The presence of a single indicator does not necessarily confirm terrorist activity. Often, it is the presence of multiple indicators in a transaction with no logical business explanation that raises suspicion of potential terrorist activity [33].

6.2 Crypto-asset Analytics

Although crypto-assets are often deemed as anonymous, all transactions are actually publicly recorded on the blockchain. The main obstacle faced by investigators is that the owner of a specific address often remains unknown. Therefore, investigations aim to attribute addresses to persons so as to de-anonymize crypto usage [10].

6.2.1 Tracing Crypto-asset Transactions to an Exchange and De-anonymizing Users

The goal of tracing crypto transactions is to follow the transactions to a compliant party. At some point, the crypto may be changed to fiat or accessed via an exchange. Customer information at the exchange can be requested through legal services.

Tracing a transaction is complicated and involves substantial numbers of records. Online resources like *www.blockchain.com* allow investigators to

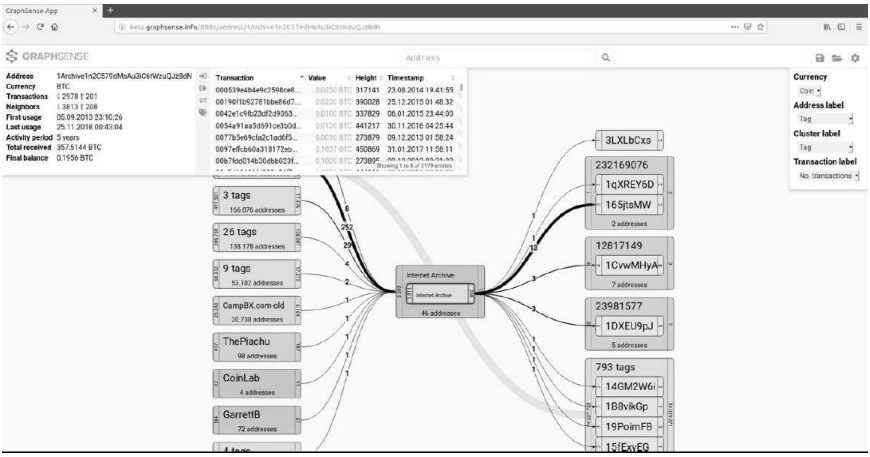
visualize the amount of Bitcoin, the number of transactions occurring with that address, the amount of Bitcoin currently available associated with the address, and the detail of each transaction.

6.2.2 Clustering/Analysing Blockchain Transactions

Various crypto-asset analytics tools are available on the market that help to achieve a better overview of raw transactions, which rely on clustering. The underlying logic is that if two addresses (such as A and B) are used as inputs in the same transaction, these belong to the same person. If address B is then used again in a single transaction with another address (such as C), then the three addresses (A, B and C) must somehow be controlled by the same entity. If the investigators can determine the owner of one of these addresses, they can therefore determine ownership of all of these addresses.

6.2.3 GraphSense

GraphSense is an open-source platform that accesses the Bitcoin blockchain and retrieves relevant data regarding the address entered. The GraphSense user can go through the transactions to and from the address entered and locate potential clusters of addresses that belong to the same entity. GraphSense obtains data from multiple sources that have tagged addresses. As GraphSense users trace through transactions, they will see the identifiable address information, which law enforcement investigators can serve a legal request on, to identify the entity behind the transaction.



Źródło: INTERPOL, "Guidelines on the darknet and cryptocurrencies," INTERPOL Innovation Center, Singapore, 2020.

Figure 8. GraphSense address identification

6.2.4 Other Crypto-asset Analytics Providers

Over the past few years, several other commercial companies have developed tools to provide information about many known addresses (such as exchanges), as well as graphical interfaces to analyse transactions more easily. They also assist law enforcement in case investigations, by tracing transactional records. The following are examples of such companies:

- Chainalysis (https://www.chainalysis.com/)
- Elliptic (https://www.elliptic.co/)
- Blockseer (https://www.blockseer.com/)
- Ciphertrace (https://ciphertrace.com/)
- Scorechain (https://www.scorechain.com/)
- Crystal Blockchain (https://crystalblockchain.com/)
- Blockchain Intel (http://blockchainintel.com/)
- Walletexplorer (https://www.walletexplorer.com)

6.3 Case Study: Disruption of Three Global Cyber-Enabled Terrorist Financing Campaigns using Crypto-asset Analytics

In August 2020, the US Department of Justice announced the dismantling of three TF cyber-enabled campaigns involving the Al-Qassam Brigades, Al-Qaeda, and ISIS. They were found to have used cyber-tools to finance their operations, including online solicitation of crypto donations from international supporters. The government has filed three civil forfeiture complaints and a criminal complaint involving the seizure of four websites, four Facebook pages, over 300 crypto accounts, and millions of dollars.

According to the government's complaint, the Al-Qassam Brigades (AQB) posted requests for Bitcoin donations on its social media page and official websites, claiming that such donations would be untraceable and used to support violent causes. The group's websites included videos on how to make anonymous donations using unique Bitcoin addresses. Fortunately, Inland Revenue Service (IRS), Homeland Security Investigations (HSI), and Federal Bureau of Investigation (FBI) personel were able to track and seize the 150 crypto accounts used to launder funds to and from the terrorists' accounts.

The government's investigation also revealed that Al-Qaeda and affiliated terrorist groups operated a Bitcoin ML network using social media platforms and encrypted messaging apps to solicit crypto donations. In some cases, the groups claimed to be acting as charities, while actually soliciting funds for violent attacks. Al-Qaeda and their affiliates used sophisticated techniques in an attempt to conceal their fundraising efforts, but law enforcement was able to identify and seize 155 cryptoasset accounts linked to the groups.

Finally, the government's investigation uncovered a scheme whereby individuals associated with ISIS marketed fake PPE - such as N95 respirator masks—to customers across the globe in an effort to take advantage of the pandemic. The funds from such sales would have been used to suport ISIS's operations [34].

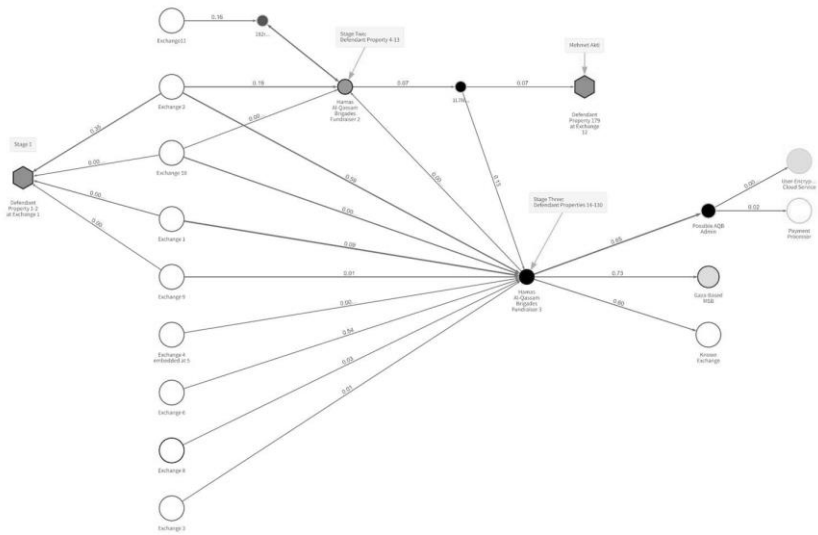
6.3.1 Al-Qassam Brigades' Terrorist Financing Campaign

The AQB are the military wing of Hamas and a designated terror organization in the US. Prospective donors were initially invited to send bitcoin to a static address posted on social media, but within months, the terrorist group constructed a wallet infrastructure that generated a new, unique address for each individual donor, making the funds more difficult to trace.

This donation campaign occurred in three stages, and the Chainalysis Reactor graph in Figure 10 shows the three wallets used by the group throughout its campaign, which unfolded in increasing technological sophistication in real time as the financiers got better at soliciting crypto donations.

On the left, we see donations come in from several addresses, mostly hosted at large, mainstream exchanges, and on the right, we see where crypto donations were moved in an effort to launder and convert them to cash.

Undercover agents emailed the website administrators promoting the campaign and confirmed that donations would be used to purchase weapons for Syrian militant groups. Using blockchain analysis, agents were then able to identify 40 Bitcoin addresses of donors who sent funds to donation addresses across the 3 stages of the campaign. Most of these addresses were hosted at various exchanges.



Źródło: Chainalysis, "Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis," 13 Aug 2020. [Online]. Available: https://blog.chainalysis.com/reports/cryptocurrency-terrorismfinancing-al-qaeda-al-qassam-brigades-bitcointransfer/. [Accessed 15 Jun 2022].

Figure 10. Al-Qassam Brigades' use of cryptocurrency in donation campaigns

The terrorist group used a mainstream crypto exchange, a crypto merchant services provider, and two unlicensed MSBs to convert crypto donations into cash. One of the unlicensed MSBs ran its crypto operation as a nested service, meaning it conducted all transactions using addresses at a mainstream exchange. Agents reached out to the exchange hosting those addresses and

learned that they belonged to a Turkish national. Most of the more than USD1 million worth of crypto-assets seized in this investigation came from his businesses.

Since then, U.S. agents have seized the primary web page promoting the campaign, and the organization hasn't received any new donations since October 2020 [25].

6.3.2 Al-Qaeda's Terrorist Financing Donation and Money Laundering Infrastructure

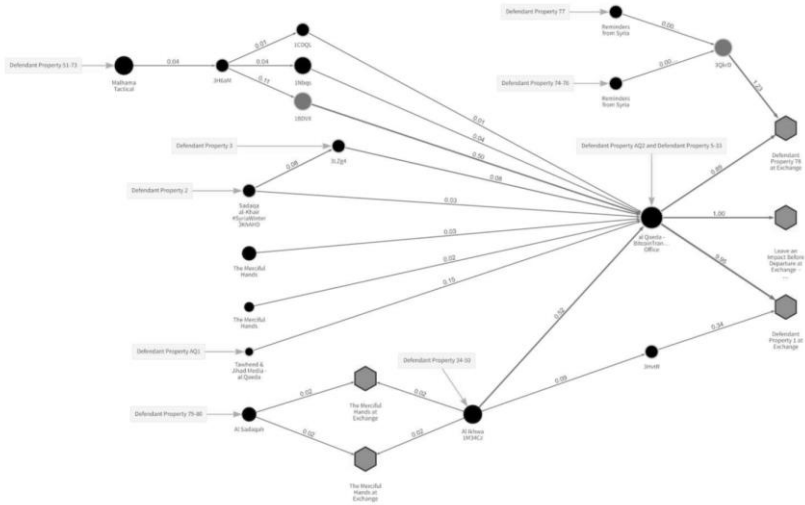
Meanwhile, Al-Qaeda and its related groups launched a crypto-based infrastructure to receive and launder donations for TF. They used multiple layers of transactions to obfuscate movement of donations to a central hub of addresses, from which funds were then redistributed. Blockchain analysis identified the BitcoinTransfer Office in Idlib, Syria as the central hub. BitcoinTransfer purports to be a crypto exchange but appears to be fully under the control of terrorist groups.

While multiple terrorist groups ran their own individual donation pushes, nearly all of tchem followed a similar strategy. The groups presented themselves as charities operating in Syria and solicited Bitcoin donations on social media and messaging platforms like Telegram and Facebook. Despite the facade, these groups publicly indicated that donations would be spent on weapons, as can be seen in the screenshot.

Źródło: Chainalysis, "Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis," 13 Aug 2020. [Online]. Available: https://blog.chainalysis.com/reports/cryptocurrency-terrorismfinancing-al-qaeda-al-qassam-brigades-bitcointransfer/. [Accessed 15 Jun 2022].

Figure 11. Telegram advertisement soliciting for Bitcoin donations

In May 2019, one of the Telegram pages promoted a funding campaign for "bullets and rockets for the mujahideen" with a single Bitcoin address listed. Agents monitored that address as donations came in and noticed the funds being moved to an address hosted at BitcoinTransfer.



Źródło: Chainalysis, "Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis," 13 Aug 2020. [Online]. Available: https://blog.chainalysis.com/reports/cryptocurrency-terrorismfinancing-al-qaeda-al-qassam-brigades-bitcointransfer/. [Accessed 15 Jun 2022].

Figure 12. Al-Qaeda's crypto-based infrastructure

Agents also observed campaigns conducted by other groups affiliated with Al-Qaeda, using similar modus operandi [25].

Despite U.S. efforts to disrupt this activity, new iterations of the BitcoinTransfer office and some groups from the original scheme remain operational today [23].

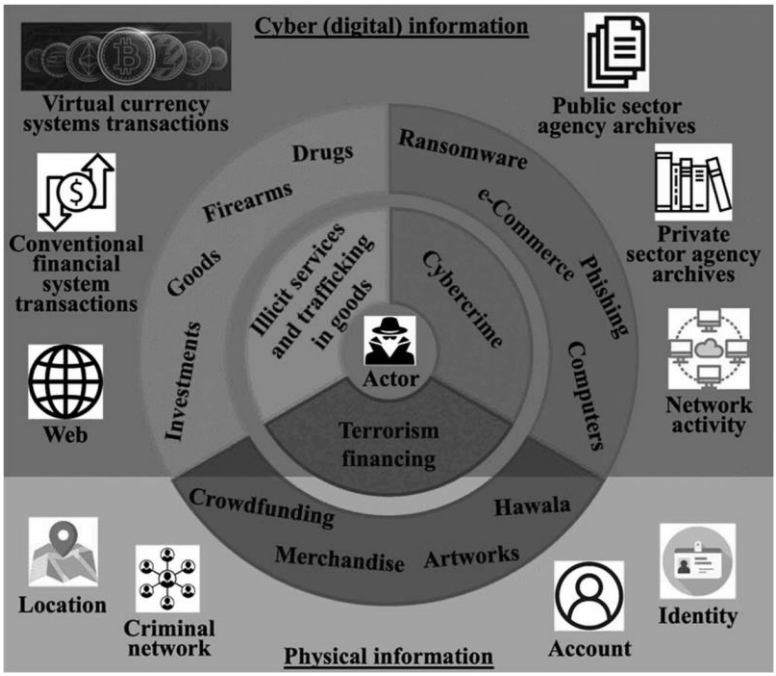
6.4 "Follow the Actor"

The "follow the money" approach alone cannot guarantee an investigation's success. Terrorist organizations tend to compartmentalize their activities, in order to avoid detection. Therefore, a "follow the actor" approach is necessary to identify the suspects, combining both digital and physical information cues. In this regard, we are looking to develop a methodology that jointly analyses several TF cases to identify the common actors who are responsible for multiple incidents [36].

It should be noted that fully disrupting the TF network can be very challenging, especially if the identity of the recipient is unknown and the funds

have been sent to an unstable conflict zone. Even if authorities manage to isolate part of the network, other financiers can still continue to transfer funds to the same recipient.

Investigating and prosecuting TF offences can lead to the discovery and disruption of a wider TF network. It may also uncover criminal activity that generated the funds, or the laundering of the funds.



Źródło: R. King, G. Kioumourtzis and G. Papadopoulos, "Countering Terrorist Financing," ERCIM News, 1 Apr 2022. [Online]. Available: https://ercimnewsercim.eu/en129/special/countering-terrorist-financing. [Accessed 15 Jun 2022].

Figure 13. Proposed "follow the actor" financial investigation strategy

6.4.1 Financial Roles Played by Individuals within Terrorist Organizations

In particular, identifying the financial role that an individual plays within a terrorist organization is the key to strategically disrupting the TF. Financial supporters may be involved in four distinct but interrelated roles [3]:

- Donors are witting or unwitting individuals who support the organization's goals through financial contributions. Their activities usually do not extend beyond monetary support;
- Fundraisers are individuals who actively solicit funds on behalf of the organization, who are often engaged in the movement and concealment of funds;
- Facilitators are directly associated with the organization's leadership and operatives, often directly involved in promoting the agenda, and well apprised of operational plans; and
- Operatives are the individuals who conduct the terrorist attack, procuring the necessary resources to accomplish the mission, either through organizational support or self-funding.

6.4.2 Exploiting "Non-Financial" Information in Dark Web Open-Source Investigations

Law enforcement investigations generally start with a complaint about a specific person, place or thing. Intelligence investigations can start from details about a possible crime or its locality. Although de-anonymizing a target is challenging, targets are nonetheless prone to accidentally leaving behind clues in the Dark Web as to their identity. This includes any monikers, e-mail address, Bitcoin address, and other identifying information. Investigators can combine this information together with open-source intelligence (OSINT) to build a profile of the target [10].

6.4.2.1 HTML

Buried within the HTML source code can be errant bits of information that are potentially actionable intelligence for the investigator, for e.g., tracking code used by the target or Google Analytics codes, which are registered to specific Google users whose identity can be revealed with appropriate legal service.

6.4.2.2 Image Search

Image metadata can provide valuable intelligence. First, the image itself can be searched for and identified from its use elsewhere on the Internet, and second, the data contained in the file that describes when and where the image was taken, which is called Extensible information or Exif data.

If the target website has JPG image files, chances are they will contain additional information about the image.

6.4.2.3 PGP Keys and Monikers

When a PGP key is made, a user is asked for his name and e-mail address. Although neither is necessarily correct, some do follow directions blindly, and this can be used to de-anonymize the target. Users with the same PGP key are likely to be the same person. When the target's website is examined, there will be data which can be used to identify the target, such as moniker, email address, or other items of interest. Darknet users tend to reuse monikers and PGP keys to prove their identity, especially after a Darknet site has been closed down.

6.4.2.4 Other Identifying Information from Clearnet

Using OSINT tools such as Maltego (described in section 6.4.3.2), we can start looking for leads to additional information left on the clearnet, such as communication about Darknet sales or complaints about a vendor. By researching whether a moniker has already been used on social media networks, the investigator can uncover other possible leads.

6.4.2.5 Crypto Addresses

When exploring the target's website or vendor page, investigators will often come across a crypto address used by the vendor. Investigators can then identify any crypto transactions associated with this address.

6.4.3 Commercial Tools

An important part of investigation planning is finding available tools to assist in the investigation. The following are tools that have been found to provide investigators with a positive investigative outcome.

6.4.3.1 Dark Web Monitor

The application of visual analytics applied to Dark Web data will facilitate a "follow the actor" investigative approach by identifying commonalities in the depiction of illicit goods. Dark Web Monitor (DWM) presents operational perspectives to improve attribution in the investigations of Dark Web crimes. As a Google for the Dark Web, DWM collects as many darknet services as possible from Tor, I2P, Zeronet, etc. It typically monitors more than one million Dark Web domains daily, of which more than 130,000 are active to-date. DWM provides access to all crawled and timestamped HTML pages, enabling investigators and researchers to contextualize their findings

based on original and raw data. DWM is also infrastructure-focused and therefore, much less intrusive than alternative dark web monitoring solutions that primarily target individual suspects or specific markets only.

6.4.3.2 Maltego

Maltego is a complementary tool suggested for the investigative toolkit. First, Maltego assists with open-source investigations of names, e-mails, domains, and IP addresses. Second, it has tools to assist with the tracing of bitcoin. To trace an e-mail, Maltego does look-ups on various sites around the Internet for mentions of the e-mail address, and then produces a screen diagram of the relationships between the information it found. When tracing a Bitcoin address, Maltego uses CipherTrace's database of Darknet and crypto references as well as the Bitcoin blockchain [10].

6.4.4 Evidence from Social Media Platforms

Authorities should have a wide variety of investigative techniques at their disposal such as wiretaps, monitoring internet usage, intercepting social media communications, or access to undercover agents. Often, jurisdictions experience challenges in protecting the identity of confidential informants. From time to time, it is often necessary to refresh the sources and find new informants.

6.4.4.1 Challenges Faced

Although social media is an important source of evidence, it poses certain challenges. For example, pre-authorization from the court may be required before intercepting communications, and it can also be challenging to obtain content from overseas. Furthermore, social media content may not be admissible as evidence.

6.4.4.2 Good Practices

Therefore, good practices in collecting such evidence include:

- Investigators creating profiles on platforms, entering closed groups, and communicating with suspects to produce direct evidence such as screenshots;
- Using the law enforcement agent who communicated directly with the suspects as a witness; and
- Engaging with the social media platforms and their law enforcement departments as early as possible, so as to understand the types of information available and how it can be obtained. One example is to use

preservation orders to ensure the social media content is not routinely deleted while the investigation is ongoing [30].

6.5 Case Studies to Illustrate the "Follow the Actor" Approach

6.5.1 Financial Analysis of an Extreme Right-Wing Organization

The Egmont Group has provided an example of a domestic FIU which received a suspicious transaction report (STR) concerning "Association A" after its unlawful activities were reported in the media. The report suggested Association A was collecting funds for illegal purposes. Subsequently, the FIU gathered information through its direct access to the national association register, tax authority database, and bank account register, as well as spontaneous disclosures from counterpart FIUs, enabling it to conduct in-depth financial analysis of Association A's activities.

Furthermore, in the wake of a terrorist attack in Country Z, the FIU proactively checked public information against its own data and realized that Association A had links to a violent ERW organization known for hate ideology, having received donations from the alleged perpetrator of this attack. The FIU reported its findings to national security authorities, citing suspected ERW activities.

The main challenge faced were the delays in accessing information from a foreign FinTech, as well as in obtaining further information from reporting entities.

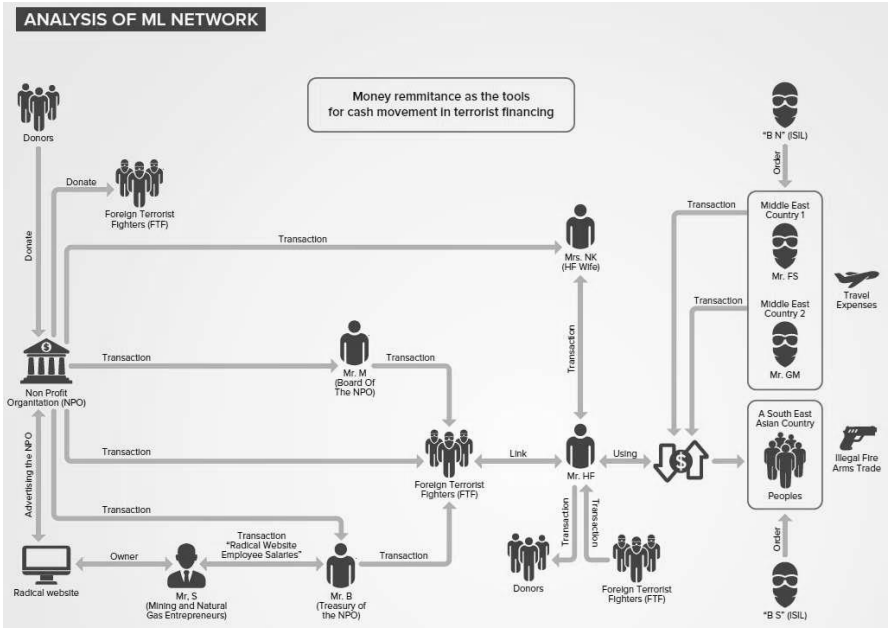
Nonetheless, the FIU's analysis enabled domestic authorities and foreign FIUs to develop knowledge of ERW groups and their activities by mapping their financial supports. Positive and detailed feedback from domestic law enforcement agencies (LEAs) regarding the analysis allowed the FIU to identify links to another network, which prompted a separate investigation [37].

6.5.2 Terrorist Financing through Money Remittance and NPOs (Indonesia)

In 2015, Indonesia conducted an NRA on TF which found that NPOs had become a TF risk. In the same year, the Thamrin bombing attack took place in Jakarta. Indonesia's FIU, the Pusat Pelaporan dan Analisis Transaksi Keuangan (Financial Transaction Reports and Analysis Center of Indonesia) (PPATK), formed a special task force to facilitate parallel investigations, exchanging information with investigators to create maps of TF networks. The task force began focusing on subjects in the network map and NPOs.

In collaboration with LEAs, they identified a NPO whose transactions were not consistent with its mandate. Further investigation revealed the NPO

also had links to a terrorist network, and that it had transacted funds with high-risk countries. Figure



Źródło: Egmont Group of Financial Intelligence Units, "Best Egmont Cases – Financial Analysis Cases 2014–2020," 2021. [Online]. Available: https://egmontgroup.org/wpcontent/uploads/2022/01/2021-Financial.Analysis.Cases_.2014-2020-3.pdf. [Accessed 25 Jan 2022].

Figure 14. PPATK mapping of the terrorist financing network

The parties that received funds from the suspect were identified as FTFs, and the funds were suspected to have bought communication devices used to coordinate the January 2015 bombings. In addition, the FIU obtained open-source information that the suspect committed vandalism during a demonstration for the release of Indonesia's ISIS commander in 2014.

Once the NPO was identified, the task force employed a variety of analytical tools, including onsite examination. Their financial analysis also involved open sources of information and collaboration with domestic and foreign authorities. After mapping the TF network, the FIU proactively shared this intelligence with the National Police.

On a prosecution level, the FIU identified the beneficial owner of those funds, "B N" (ISIL), who was on the designated individuals list and a self-declared ISIS leader for Southeast Asia. The suspect's international transactions involved three other countries, which the FIU alerted. The FIU also exchanged information about this case with international counterparts from other Southeast Asian countries, as well as Australia and New Zealand.

As a result of the parallel investigations, the suspect was charged with terrorism and TF. He was sentenced to six years' prison for illegal weapons possession. This successful pre-emptive action possibly saved hundreds of lives [38].

7 Conclusion

While this report has highlighted recent as well as current trends, jurisdiction experience is continuing to evolve. Likewise, the changing nature of TF threats and vulnerabilities means that relevant information sources for assessing TF risk might change over time. Wherever possible, CFT efforts should include community engagement as well as consider broader criminal networks and activities which terrorist organizations often draw on to raise and move funds. Information sharing initiatives are vital to deepening the understanding of TF risk and going forward there is a need for enhanced information sharing on TF risk within regions which face similar TF threat profiles. In particular, understanding TF risks linked to individual perpetrators as well as larger terrorism organizations often requires scrutinizing copious amounts of financial data. For developed countries with large financial and trade flows, the development of smart solutions to cope with "big data" and the continued development of multi-agency information sharing mechanisms will likely be important in ongoing efforts to identify and assess TF risk [4].

Familiarizing ourselves with existing good practices in LEAs' operational and counter-terrorism pipelines, as well as identifying the corresponding gaps, are crucial in fighting TF associated with emerging technologies. It is hoped that this report brings its readers up to speed in terms of understanding current modi operandi in TF and the challenges and gaps in countering them. Many of the points raised are specific to the inherent characteristics and vulnerabilities associated with emerging technologies and are neither exhaustive nor applicable in every situation. Rather, these are just some of the many elements that contribute to an overall picture of potential TF risk, and it is important that they not be viewed in isolation but in the context of information obtained from relevant authorities.

References

[1]. G. Zack, "Implicit Bias and the Investigation," 14 Jan 2020. [Online]. Available: https://cv.corporatecompliance.org/Portals/1/PDF/Resources/past_handouts/Internal_Investigation/2021/II0721/W03.pdf. [Accessed 15 Jun 2022].

[2]. Wikipedia, "Cognitive bias," 17 May 2022. [Online]. Available: https://en.wikipedia.org/wiki/Cognitive_bias. [Accessed 15 Jun 2022].

[3]. FATF, "Operational Issues - Financial Investigations Guidance," Jun 2012. [Online]. Available: https://www.fatfgafi.org/publications/methodsandtrends/documents/operationalissuesfinancialinvestigationsguidance. html. [Accessed 15 Jun 2022].

[4]. FATF, "Terrorist Financing Risk Assessment Guidance," Jul 2019. [Online]. Available: https://www.fatf-gafi.org/publications//methodsandtrends/documents/Terrorist-Financing-Risk-Assessment-Guidance.html. [Accessed 15 Jun 2022].

[5]. Global Risk Insights, "Countering terrorism financing through anti-money laundering measures," 9 Dec 2015. [Online]. Available: https://globalriskinsights.com/2015/12/countering-terrorism-financing-through-antimoney-laundering-measures/. [Accessed 4 May 2022].

[6]. C.-L. Liu and J. Quek, "Enhancing building security for embassies along the Maritime Silk Road against terrorist attacks," Journal of Infrastructure, Policy and Development, vol. 3, no. 1, pp. 115-128, 2019.

[7]. Wikipedia, "Terrorism," 21 Apr 2022. [Online]. Available: https://en.wikipedia.org/wiki/Terrorism. [Accessed 4 May 2022].

[8]. Europol, "European Union Terrorism Situation and Trend Report," 7 Dec 2021. [Online]. Available: https://www.europol.europa.eu/publications-events/main-reports/europeanunion-terrorism-situation-and-trend-report-2021-tesat. [Accessed 9 Feb 2022].

[9]. FATF, "Ethnically or Racially Motivated Terrorism Financing," Jun 2021. [Online]. Available: https://www.fatfgafi.org/publications/methodsandtrends/documents/ethnically-raciallymotivatedterrorism-financing.html. [Accessed 16 Apr 2022].

[10]. INTERPOL, "Guidelines on the darknet and cryptocurrencies,"INTERPOL Innovation Center, Singapore, 2020.

[11]. Wikipedia, "Dark web," 4 Feb 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Dark_web&oldid=1069929052. [Accessed 4 May 2022].

[12]. Bank for International Settlements, "Central bank digital currencies," Mar 2018. [Online]. Available: https://www.bis.org/cpmi/publ/d174.htm. [Accessed 14 Mar 2022].

[13]. Wikipedia, "Cryptocurrency," 15 Jun 2022. [Online]. Available: https://en.wikipedia.org/wiki/Cryptocurrency. [Accessed 20 Jun 2022].

[14]. Elliptic, "The FATF's Virtual Asset Guidance: What You Need to Know," 4 Nov 2021. [Online]. Available: https://www.elliptic.co/resources/fatf-virtual-asset-guidance-whatyou-need-to-know. [Accessed 11 Nov 2021].

[15]. FATF, "Emerging Terrorist Financing Risks," Oct 2015. [Online]. Available: http://www.fatfgafi.org/publications/methodsandtrends/documents/emerging-terrorist-financingrisks.html. [Accessed 28 Jan 2022].

[16]. D. Goldbarsht, "New Payment Products and Services – Potential anti-money laundering and counter-terrorist financing risks," 24 Apr 2020. [Online]. Available: https://mysecuritymarketplace.com/v2-whitepapers/new-payment-products-and-servicespotential-anti-money-laundering-and-counter-terrorist-financing-risks/. [Accessed 18 Jul 2022].

[17]. Daily Stormer, "Daily Stormer – The Most Censored Publication in History," 2022. [Online]. Available: http://stormer5v52vjsw66jmds7ndeecudq444woadhzr2plxlaayexnh6eqd.onion. [Accessed 4 May 2022].

[18]. US Department of the Treasury, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art," 4 Feb 2022. [Online]. Available: https://home.treasury.gov/news/press-releases/jy0588. [Accessed 15 Jun 2022].

[19]. K. J. Barnett and C. McCrory, "Department of Treasury Releases Study on Money Laundering Risks in Art and NFTs," 22 Feb 2022.

[Online]. Available: https://www.regulatoryoversight.com/2022/02/department-of-treasury-releases-study-on-money-laundering-risks-in-art-and-nfts/. [Accessed 14 Jun 2022].

[20]. FATF, "Guidance on Criminalising Terrorist Financing," Oct 2016. [Online]. Available: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/criminalisingterrorist-financing.html. [Accessed 2 Aug 2022].

[21]. European Commission, "Lone Actors in Digital Environments," Oct 2021. [Online]. Available: https://ec.europa.eu/home-affairs/whatsnew/publications/lone-actors-digitalenvironments-october-2021_en. [Accessed 29 Mar 2022].

[22]. N. Veerasamy and M. Grobler, "Terrorist Use of the Internet: Exploitation and Support through ICT infrastructure," Jan 2011. [Online]. Available: https://www.researchgate.net/publication/266173850_Terrorist_Use_of_the_Internet_Exploitation_and_Support_through_ICT_infrastructure/. [Accessed 25 Feb 2022].

[23]. A. Alexander and T. MacDonald, "Examining Digital Currency Usage by Terrorists in Syria," CTC Sentinel, vol. 15, no. 3, pp. 25-33, 2022.

[24]. RAND Corporation, "Terrorist Use of Cryptocurrencies – Technical and Organizational Barriers and Future Threats," 2019. [Online]. Available: https://www.rand.org/pubs/research_reports/RR3026.html. [Accessed 2 Mar 2022].

[25]. Chainalysis, "The 2021 Crypto Crime Report," 2021.

[26]. US Department of Justice, "Attorney General William P. Barr Announces Publication of Cryptocurrency Enforcement Framework," 8 Oct 2020. [Online]. Available: https://www.justice.gov/opa/pr/attorney-general-william-p-barr-announces-publicationcryptocurrency-enforcement-framework. [Accessed 7 Feb 2022].

[27]. FATF, "COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses," May 2020. [Online]. Available: https://www.fatfgafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html. [Accessed 28 Jan 2022].

[28]. FATF, "Update: COVID-19-Related Money Laundering and Terrorist Financing Risks," Dec2020. [Online]. Available:

https://www.fatfgafi.org/publications/methodsandtrends/documents/updated-covid-19-ml-tf.html. [Accessed 25 Jan 2022].

[29]. US Department of Justice, "Darknet Vendor Arrested on Distribution and Money Laundering Charges," 9 Apr 2020. [Online]. Available: https://www.justice.gov/usaoedva/pr/darknet-vendor-arrested-distribution-and-money-laundering-charges. [Accessed 18 Jul 2022].

[30]. FATF, "FATF President's Paper: Anti-money laundering and counter terrorist financing for judges and prosecutors," Jun 2018. [Online]. Available: https://www.fatfgafi. org/publications/fatfgeneral/documents/aml-cft-judges-prosecutors.html. [Accessed 1 Mar 2022].

[31]. Government Offices of Sweden, "Combatting money laundering and terrorist financing," 26 Sep 2019. [Online]. Available: https://www.government.se/government-policy/financialmarkets/combatting-money-laundering-and-terrorist-financing/. [Accessed 15 Jun 2022].

[32]. D. M. Lormel, "Terrorist Financing: Visualizing Funding Flows," ACAMS Today, 18 Sep 2018. [Online]. Available: https://www.acamstoday.org/terrorist-financing-visualizingfunding-flows/. [Accessed 15 Jun 2022].

[33]. FATF, "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing," 14 Sep 2020. [Online]. Available: https://www.fatfgafi.org/publications/methodsandtrends/documents/virtual-assets-red-flagindicators.html. [Accessed 11 Jan 2021].

[34]. US Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," 13 Aug 2020. [Online]. Available: https://www.justice.gov/opa/pr/globaldisruption-three-terror-finance-cyberenabledcampaigns. [Accessed 5 Mar 2022].

[35]. Chainalysis, "Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis," 13 Aug 2020. [Online]. Available: https://blog.chainalysis.com/reports/cryptocurrency-terrorismfinancing-al-qaeda-al-qassam-brigades-bitcointransfer/. [Accessed 15 Jun 2022].

[36]. R. King, G. Kioumourtzis and G. Papadopoulos, "Countering Terrorist Financing," ERCIM News, 1 Apr 2022. [Online]. Available: https://ercimnews.ercim.eu/en129/special/countering-terrorist-financing. [Accessed 15 Jun 2022].

[37]. Egmont Group of Financial Intelligence Units, "FIUs' Capabilities and Involvement in the Fight Against the Financing of Extreme Right-Wing Terrorism," Jul 2021. [Online]. Available: https://egmontgroup.org/wp-content/uploads/2022/01/IEWG-ERWTF-publicbulletin2.pdf. [Accessed 24 Jan 2022].

[38]. Egmont Group of Financial Intelligence Units, "Best Egmont Cases – Financial Analysis Cases 2014–2020," 2021. [Online]. Available: https://egmontgroup.org/wpcontent/uploads/2022/01/2021-Financial.Analysis.Cases_.2014-2020-3.pdf. [Accessed 25 Jan 2022].

[39]. Al Bawaba, "Mideast's ancient hawala system: follow the flow of migrant money," 28 Jan 2016. [Online]. Available: https://www.albawaba.com/slideshow/mideasts-ancient-hawalasystem-follow-flow-migrant-money-792662. [Accessed 15 Jun 2022].