Rocznik Bezpieczeństwa Morskiego

PRZESTĘPCZOŚĆ TELEINFORMATYCZNA 2021

Pod redakcją:

Jerzego Kosińskiego
Roberta Janczewskiego

Gdynia 2022

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

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

SPIS TREŚCI

Wstęp

Rok 2021 był kolejnym rokiem, w którym pandemia COVID-19 wymusiła wykorzystanie nowych technologii wspierających transformację cyfrową, w szczególności wspomagających zdalną pracę i nauczanie. Jednocześnie niejako potwierdziła od dawną znaną zasadę, iż przestępcy wykorzystując każde zjawisko i zdarzenie mogące budzić jednocześnie powszechny niepokój lub wręcz strach oraz zaciekawienie i nadzieję błyskawicznie dostosowują swoje techniki, taktyki i procedury działania do aktualnych warunków.

Zgodnie z ukształtowaną już tradycją, w murach Akademii Marynarki Wojennej, w 2021 roku odbyła się doroczna, w prawie pełnym wymiarze, kolejna edycja Konferencji Naukowej Przestępczość Teleinformatyczna XXI (PTXXI). Zgromadziła bardzo liczne grono (ponad 300) uczestników, którzy uczestniczyli w wielu tematycznych, poświęconym różnym aspektom cyberprzestępczości sesjach.

Wspomniany w poprzednim akapicie „prawie pełny wymiar" wynikał z rzeczywistych, ściśle związanych z problematyką Konferencji zdarzeń, a właściwie incydentów o podłożu przestępczym. To co się wydarzyło wpisało się niejako w obszar tematyczny praktycznych i naukowych rozważań oraz dyskusji nad cyberprzestępczością. Incydent, o którym mowa miał miejsce w drugim dniu Konferencji i przyczynił się do konieczności przeprowadzenia działań ewakuacyjnych związanych z przesłanym na adres e-mail Komedy Miejskiej Policji w Gdyni ostrzeżeniu o podłożeniu bomby.

Korespondencja, która spowodowała zamieszanie wyglądała następująco:

```
Od: islamista.jihad.gdynia@onet.pl [mailto:islamista.ji-
had.gdynia@onet.pl]
Wysłano: 22 września 2021 15:51
Do: Konferencja Przestępczość Teleinformatyczna XXI
<PTXXI@amw.gdynia.pl>
Temat: [SPAM] Ja zrobiłem bombę w Gdynia

Ja zrobiłem bombę w Gdynia.
Bomba HMTD, miedziankit, ANFO.
Detonator telekomunikacją, ja odpalę, albo auto.
Przyjdzie sms i nie ma ludzi żywych.
```

```
Bomba jest w Biblioteka Główna im. Lecha Kaczyńskiego ul.
Śmidowicza 69
81-127 Gdynia
Teraz dużo ludzie tam w budynku.
Ja zrobiłem zabić wszystkie ludzie tam w budynku.
Wszystkie ludzie zginą zaraz.
Allah jest wielki.
Allah jest wielki.
Nie tęczowa! Nie pogańska!
WIELKA POLSKA MUZUŁMAŃSKA !!!
```

Pomimo, że treść tej korespondencji wydawała się niepoważna, to przybyły do Akademii Marynarki Wojennej patrol policyjny profesjonalnie zareagował na te zdarzenie. Dzięki takiej postawie Policji chwilę po godzinie 16.00 wszczęto procedurę przerwania konferencji, ewakuacji uczestników oraz minerskiego sprawdzenia budynku biblioteki AMW oraz przylegającego do niego terenu parkingu. Ze względu na właściwość miejscową wszystkie prowadzone działania przejęła od Policji Żandarmeria Wojskowa. Przy udziale uczestników konferencji wykonano analizę, która pozwoliła na ustalenie miejsca, z którego został wysłany fałszywy alarm bombowy. Jednocześnie stwierdzono, że ustalony adres IP należy do botnetu[1]. A to mogło oznaczać, że użytkownik powiązany ze zidentyfikowanym adresem IP może nie być autorem owej wiadomości, a tym samym odpowiedzialny za fałszywy alarm bombowy. Po godz. 21.00 podejrzany użytkownik komputera stanowiącego źródło nadesłanej wiadomości, dzięki skutecznemu działaniu żandarmerii, był przesłuchany, a jego sprzęt komputerowy wstępnie przeszukany przez biegłego i zabezpieczony do badań. Kolejnego dnia konferencja była kontynuowana już bez przeszkód.

Sprawne i skuteczne działanie uczestników konferencji, którzy wsparli czynności śledcze potwierdziło, że to cykliczne, naukowe wydarzenie jakim jest Konferencja Naukowa Przestępczość Teleinformatyczna XXI skupia wysokiej klasy naukowców i praktyków w dziedzinie cyberbezpieczeństwa i cyberprzestępczości.

---

[1] Botnet to sieć zainfekowanych komputerów używanych do nielegalnych celów bez wiedzy użytkowników, źródło: https://sjp.pwn.pl/slowniki/botnet.html, dostęp: 12.04.2022 r.

Niestety w czasie PTXXI doszło również do kolejnego incydentu stanowiącego cyberprzestępstwo. Kilka godzin później (o godzinie 21.45) jeden z organizatorów konferencji otrzymał wiadomość e-mail zawierającą groźbę pozbawienia go życia. Treść tej przestępczej korespondencji wyglądała następująco:

```
Od: pedofil.misiaczek@pseudonim.pl [mailto:pedofil.misia-
czek@pseudonim.pl]
Wysłano: 22 września 2021 21:45
Do: j.kosinski@outlook.com
Temat: Jerzy Kosiński, zamorduję cię cwelu

Jerzy Kosiński, zamorduję cię cwelu. To przez ciebie straciłem
całą reputację. 25 lat temu. Pomogłeś mnie namierzyć. Złamane
życie za niewinne obrazki z dzieciakami... Czekałem na zemstę
tyle lat. W końcu przyszedł na nią czas. Stefan Wilmont pokazał
mi, że się da. Rozjebał tego bandytę Adamowicza. Jutro ja roz-
jebię ciebie. Jednym strzałem z czarnoprochowca. Innych na sali
dobiję nożem desantowym. Postaram się zabić jak najwięcej
z was. Jerzy Kosiński, ty skurwielu, żegnaj się z rodziną. Zrób
to dzisiaj. Jutro wrócisz z konferencji nogami do przodu.
Podpisano,
Pedofil Misiaczek
```

W przypadku tego incydentu postępowanie Policji niestety negatywnie obiegało od obsługi incydentu z godziny 15.51. Wszelkie czynności związane z tym zdarzeniem miały zupełnie inny przebieg niż w pierwszym przypadku. Chronologia wygląda następująco. Pokrzywdzony otrzymaną groźbą ze względu na własne miejsce zamieszkania w dniu 24 września złożył w Komendzie Powiatowej Policji (KPP) w Szczytnie zawiadomienie o podejrzeniu popełnienia przestępstwa. Przyjęcia dokonała, w bardzo profesjonalny sposób pani st. sierżant. Dodatkowo pokrzywdzony pocztą elektroniczną (e-mail) przekazał wynik wykonanej analizy i wskazał kogo i o co należy w związku z tą analizą poprosić. Pomimo to Policja niestety nie wykonała żadnych czynności sprawdzających. Główną wykonaną czynnością była próba przekazania do Komendy Miejskiej Policji (KMP) w Gdyni zawiadomienia do realizacji. Próba okazała się jednak nieudana, ponieważ KMP w Gdyni odmówiła przejęcia sprawy mimo, iż pokrzywdzony otrzymał informację, że 10.11.2021 roku w IV Komisariacie Policji w Gdyni wszczęto dochodzenie prowadzone pod nadzorem Prokuratury Rejonowej (PR) w Gdyni.

Dwa miesiące od uzyskania informacji o wszczęciu dochodzenia, czyli w dniu 10.01.2022 roku pokrzywdzony został zaproszony telefonicznie na przesłuchanie w charakterze pokrzywdzonego do Prokuratury Rejonowej w Szczytnie. Tam dowiedział się, że PR w Szczytnie nadzoruje dochodzenie zlecone do prowadzenia KPP w Szczytnie. Dowiedział się również, że nie sprawdzono jeszcze, kto był użytkownikiem adresu IP, z którego wysłano e-maila, ani nie uzyskano informacji, kto zarejestrował i jak używał konto poczty elektronicznej wykorzystane do wysłania groźby. Okazało się także, że PR Gdynia nie zarejestrowała wszczęcia wspomnianego powyżej dochodzenia. W dniu 21.03.2022 roku prokurator PR w Szczytnie zatwierdziła postanowienie o umorzeniu dochodzenia wobec niewykrycia sprawcy przestępstwa. W trakcie prowadzenia dochodzenia Policja potwierdziła jedynie ustalenia przekazane przez pokrzywdzonego w czasie zgłaszania zawiadomienia o popełnieniu przestępstwa.

Przedstawienie reakcji na osi czasu Żandarmerii na pierwsze zdarzenie i Policji na drugie pokazałoby, że Żandarmeria w cztery godziny (4 godz.) wykonała znacznie więcej niż Policja w ciągu 178 dni.

Takie specyficzne, pozorowane „działanie" niektórych, z całą stanowczością należy podkreślić niektórych, jednostek Policji potwierdza również reakcja na zadane w trybie zapytania o informację publiczną pytanie o dane statystyczne dotyczące cyberprzestępczości. Odpowiedzi na identycznie zadane pytania w latach poprzednich Komenda Główna Policji udzielała w ciągu kilku dniu (samo wprowadzenie pytania i uzyskanie odpowiedzi z Krajowego Systemu Informacji Policyjnej zajmuje od kilkunastu do kilkudziesięciu minut). W 2021 roku zajęło to kilkadziesiąt dni, po uprzednim poinformowaniu pytającego, że pytanie jest nieprecyzyjne (przez kilkanaście ostatnich lat identyczne pytanie było wystarczająco precyzyjne) i że na odpowiedź KGP ma 90 dni.

Przyjęta przez Parlament w 2021 roku nowelizacja Ustawy z dnia 6 kwietnia 1990 r. o Policji powołuje do istnienia Centralne Biuro Śledcze Policji (CBŚP), które stanowi jednostkę organizacyjną Policji służby śledczej realizującą na obszarze całego kraju zadania w zakresie rozpoznawania, zapobiegania i zwalczania przestępczości zorganizowanej.

Bardzo pozytywnie należy postrzegać fakt, że zauważono w Policji konieczność innego traktowania specjalistów związanych z technologiami informatycznymi, w zakresie ścieżki kariery (chociaż trudno o takiej mówić w

Policji?) oraz ich płac. Mimo, iż powołanie do życia jednostki policji przeznaczonej do działań w obszarze cyberprzestępczości wydaje bardzo słuszne, nasuwają się wątpliwości:

- czy jeżeli pojawi się więcej przestępstw z użyciem noża, to również zostanie utworzone Centralne Biuro Zwalczania Przestępstw z Użyciem Noża? Cyberprzestepczość jest tylko narzędziem do popełniania przestępstw gospodarczych czy kryminalnych. Przejęcie dostępu do bazy danych może okazać się nie być celem samym w sobie, a tylko środkiem do np. zarobienia pieniędzy;
- jakimi przestępstwami będzie zajmowało się Biuro? W ujęciu wertykalnym (przestępstw, które są specyficzne dla samej cyberprzestrzeni jest zbyt mało, aby tworzyć Biuro) czy horyzontalnym (wykorzystanie technik komputerowych i informatycznych znacznie upraszcza dokonanie przestępstw, co wobec tego stawia pod znakiem zapytania zasadność powoływania takiego Biura). W założeniach ustawy nie przewidziano żadnych mierników mających określić stopień osiągnięcia zamierzonych celów (konieczne zatem wydają się kolejne regulacje wykonawcze). Analiza proponowanych zmian pozwala na wniosek, przyjęto model zwalczania cyberprzestępczości: ludzie + pieniądze = brak cyberprzestępczości;
- tworząc elitarną, w sensie płacowym i ścieżki kariery, grupę funkcjonariuszy można spodziewać się, że funkcjonariusze innych służb policyjnych nie będą chcieli dzielić się z nimi informacjami. A skuteczność działań wykrywczych opartych wyłącznie o rozwiązania techniczne i technologię jest znikoma. Dla osiągania zadowalających rezultatów niezbędna i konieczne są dane i informacje pozyskiwane z innych wydziałów działających w Policji;
- w chwili obecnej w policyjnych wydziałach zajmujących się problematyką cyberprzestępczości pracuje ponad 300 osób, a docelowo ma ich być 1800. Można wręczyć medal byłemu Komendantowi WSPol w Szczytnie, który w tej uczelni doprowadził do rozpadu zakładu zajmującego się cyberprzestępczością i, co jest chyba ewenementem na skalę krajową, likwidacji kierunku informatyka w bezpieczeństwie, który miał przygotowywać funkcjonariuszy do tej służby. Kto i gdzie

będzie szkolił tych policjantów? – podkreślam, że znajomość technologii to za mało. W jaki sposób zapewni się, że po wyszkoleniu policjant pozostanie w Policji, a nie przejdzie np. do SKW albo banku?;

- do Biura zostaną zapewne zwerbowani funkcjonariusze mający jakąkolwiek wiedzę z powiatów – kto będzie realizował sprawy na tym poziomie (już są kłopoty z tym, aby sprawę prowadził policjant, który jest do tego przygotowany),
- wątpliwości budzi również moment ogłoszenia tego działania – masowe fałszywe alarmy bombowe, ataki na klientów bankowości elektronicznej, ataki ransomware nie były wystarczającą podstawą do proponowania takiej struktury, a włamanie na konto pocztowe ważnego polityka i dezinformacja stały się wyzwalaczem do tworzenia Biura. Czy Biuro zatem będzie zajmować się głównie tymi dwoma zagrożeniami?
- proponowany zakres działań operacyjnych (art.19c), który niestety nie wszedł do ustawy (przerażający niektóre osoby, że będzie służył do inwigilacji) powinien być wykorzystywany przez struktury do tego już wytworzone i przygotowane – wydziały WTO, a nie cyber.

Pomimo przedstawionych uwag warto trzymać kciuki za Pełnomocnika do spraw utworzenia Biura, gdyż można spodziewać się, jak to wynika z teorii i praktyki (tworzenie CBŚ), że w pierwszym okresie nastąpi nie poprawa, a pogorszenie zwalczania cyberprzestępczości.

Oddana w państwa ręce monografia składa się 13 zróżnicowanych tematycznie rozdziałów. Zakres tematyczny niniejszej publikacji jest szeroki. Większość z nich nie jest związana z tematem przewodnim planowanej konferencji. W monografii dominuje szerokie 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

Wykorzystanie cyberprzestrzeni w konflikcie hybrydowym

dr hab. inż. Piotr DELA[1]

STRESZCZENIE: W rozdziale przedstawiono najważniejsze elementy wykorzystania cyberprzestrzeni w konflikcie hybrydowym. Uwagę skupiono na istocie cyberprzestrzeni i konfliktu hybrydowego, celach realizowanych w tego typu konfliktach, obiektach i sposobach oddziaływania realizowanych w cyberprzestrzeni.

SŁOWA KLUCZOWE: cyberprzestrzeń, konflikt hybrydowy, teoria walki, bezpieczeństwo, wojna.

Wstęp

Rozważania nad wykorzystaniem cyberprzestrzeni w konflikcie hybrydowym należy rozpocząć od identyfikacji terminów podstawowych związanych z walką, postrzeganą także jako kooperacja negatywna.

Sam termin walka ma wiele znaczeń i definicji, szczególnie współcześnie, kiedy jest on używany potocznie i powszechnie do opisu zarówno walki przymiotnikowej takiej jak *walka zbrojna*, *walka informacyjna*, *walka polityczna* czy też jakikolwiek innej formy rywalizacji. Walka, w tym walka zbrojna, jest kategorią podstawową sztuki wojennej. Także w prakseologii walka i walka zbrojna mają swoje odzwierciedlenie w ogólnej teorii walki i są określane jako kooperacja negatywna [13].

[1] Akademia Kaliska, Morskie Centrum Cyberbezpieczeństwa, p.dela@akademia.mil.pl; ORCID: 0000-0003-3643-3759.

W ujęciu prakseologicznym walka oznacza kooperację, w której wszystkie strony ponoszą czyste straty. Może być ona prowadzona w różnych obszarach, na płaszczyźnie ekonomicznej, energetycznej, militarnej, informacyjnej, jak również ostatnio obserwowanej płaszczyźnie technologicznej. Logika takiego postrzegania walki prowadzi do zwycięstwa najsilniejszego [17].

Mirosław Sułek zauważył, że współczesne stosunki międzynarodowe, ale także stosunki międzyludzkie i społeczne, są syntezą współpracy, rywalizacji i walki w różnych wymiarach, z różnym nasileniem i zaangażowaniem. Nie można bowiem mówić tylko o absolutnej współpracy czy absolutnej walce [17].

Rywalizacja w ujęciu Sułka, postrzegana przez pryzmat cyberprzestrzeni, postrzegana jest jako chęć dominacji w obszarze technologicznym i uzależnieniem innych podmiotów od swoich rozwiązań technicznych i technologicznych. Przez długie lata dominację w cyberprzestrzeni posiadały Stany Zjednoczone, co wynikało jednoznacznie z podstaw technologicznych sieci Internet. Jej początki wywodzą się bowiem od projektu ARPANET realizowanego na zlecenie Departamentu Obrony Stanów Zjednoczonych. Dominacja ta związana była z celowym podejściem uzależniania poszczególnych państw od teoretycznie darmowych technologii i rozwiązań. Przykładami mogą być chociażby upublicznienie architektury komputerów klasy IBM PC i darmowe dostawy oprogramowania MS dla szkół. Przyczyniło się to do powszechnej informatyzacji państw ubogich i mniej zamożnych, niemniej jednak kosztem uzależnienia technologicznego. Dostrzegając zagrożenia technologiczne, najwięksi światowi gracze tacy jak np. Rosja i Chiny, podjęli działania związane z uniezależnieniem się od amerykańskich technologii sieciowych. W przypadku Rosji uniezależnienie polegało na stworzenie autonomicznej sieci RuNet, własnego portalu społecznościowego VK oraz zmuszenie światowych koncernów informatycznych do przechowywania danych o rosyjskich użytkownikach sieci Internet na serwerach umieszczonych na terytorium Rosji. Z kolei Chiny posiadające własny, ogromny potencjał gospodarczy i intelektualny, rozpoczęły rozwój własnych nowoczesnych

technologii cyfrowych, co doprowadziło do dominacji technologicznej w wielu obszarach.

Patrząc na historię wojen i wojskowości, cyberprzestrzeń stała się kolejnym obszarem walki, w tym walki zbrojnej i zarazem walki niezbrojnej, na równi (jeżeli nie ważniejszym) z lądem, wodą, powietrzem i kosmosem. Ludzkość od zarania dziejów doskonaliła narzędzia i sposoby walki rozszerzając obszary konfliktu z lądu aż do przestrzeni kosmicznej. Środowiska te są naturalne, niezależne od człowieka, a dostęp do nich uwarunkowany jest poziomem rozwoju technicznego i posiadanymi technologiami. W przypadku cyberprzestrzeni mamy do czynienia ze środowiskiem antropogenicznym, stworzonym przez człowieka i całkowicie zależnym do człowieka. Dodatkowo, cyberprzestrzeń stała się kluczowym środowiskiem oddziaływania w klasycznie pojmowanej walce zbrojnej poprzez umożliwienie oddziaływanie na pozostałe cztery obszary walki.

W sztuce wojennej istotne znaczenie mają także terminy *konflikt zbrojny* i *wojna*. Można zauważyć, że w tym obszarze badawczym zaszły znaczące zmiany i współczesne konflikty, w tym konflikty zbrojne i wojny, różnią się od wojen i konfliktów z przeszłości. Jest to zgodne z obserwowanym zjawiskiem polegającym na tym, że każda epoka ma swoje wojny, uwarunkowane poziomem rozwoju cywilizacyjnego, posiadaną techniką i technologią, funkcjonującymi formami stosunków międzyludzkich. Obserwowana ekspansja środków przekazu informacji, a cyberprzestrzeń jest jej wyznacznikiem, przewartościowała sposoby i formy funkcjonowania społeczeństw. Dostęp do informacji, możliwość jej szybkiego przekazywania umożliwił społeczeństwom nową jakość życia związaną z realizacją funkcji społecznych, ekonomicznych, edukacyjnych, które jeszcze nie tak dawno były abstrakcyjne. Technologie te pozwalają nie tylko na szybszy rozwój społeczeństw, ale mają również istotny wymiar ekonomiczny i gospodarczy.

Jednoznaczne odróżnienie wojny i konfliktu zbrojnego jest współcześnie niezmiernie trudne. Składają się na to różnego rodzaju czynniki, związane między innymi z przyspieszeniem rozwoju ekonomicznego świata, zwiększeniem populacji ludności, rozwarstwieniami w zamożności społeczeństw,

zmianami klimatycznymi i geopolitycznymi. *Wojna* stała się terminem często używanym przez polityków i decydentów w celu wyrażenia swojego nastawienia do zaistniałej sytuacji. Jest retoryką nastawioną najczęściej na wywarcie konkretnego wrażenia.

Zjawiskiem obserwowanym we współczesnych konfliktach zbrojnych jest ich hybrydowość, rozumiana jako nowe, niemniej jednak znane z przeszłości, podejście poznawcze w nauce o konfliktach zbrojnych [5]. Hybrydowość jest postrzegana jako współwystępowanie zarówno *starych*, jak i *nowych* elementów wojen, klasycznych konfliktów zbrojnych i wojen *ponowoczesnych*; starć zarówno konwencjonalnych sił zbrojnych, jak i konfliktów asymetrycznych, supernowoczesnych technologii wojskowych i prymitywnych narzędzi walki, walki o terytoria i zasoby naturalne oraz sporów o idee, tożsamości i wartości [5]. Zjawisko to uwarunkowane jest jednoczesnym współistnieniem w czasie i w przestrzeni wojen odmiennych generacji, które wzajemnie się przenikają na współczesnym polu walki [5].

Cechą hybrydowości konfliktów zbrojnych jest współistnienie dwóch głównych obszarów konfliktu: klasycznej – postrzeganej przez pryzmat terytorium i nowoczesnej – postrzeganej jako środowisko wirtualne, budowane na bazie nowoczesnych technologii komunikacyjnych. Pierwsza odnosi się do tradycyjnie pojmowanych państw lub grup społecznych stale zamieszkujących dany obszar. Płaszczyzna wirtualna dotyczy z kolei struktury transgranicznej, ponad terytorialnej, umożliwiającej komunikowanie się w obrębie sieci i propagowanie w niej wartości, zasad i idei [5]. Wojny w wymiarze terytorialnym ukierunkowane są najczęściej na rozciągnięcie i utrzymanie kontroli nad danym obszarem, ochronę granic i egzekwowanie norm prawnych w stosunku do ludności zamieszkujących ten obszar. Są one uwarunkowane klasycznym postrzeganiem państwa, w ustalonych i respektowanych granicach, ludnością zamieszkującą w tych granicach i władzą zdolną do kontroli ludności i terytorium. Wojny w wymiarze wirtualnym redefiniują parametry konfliktu i marginalizują takie determinanty, jak: terytorium, zasoby naturalne, porządek publiczny czy nawet państwo. Na płaszczyźnie wirtualnej powstają nowe podmioty, pewnego rodzaju pseudopaństwa, pozbawione

tradycyjnych elementów władzy, mające jednak skuteczne instrumenty pomnażania zasobów finansowych, prowadzące kampanie informacyjne i oddziaływujące na otoczenie, zarówno lokalne, jak i międzynarodowe [5].

Istota cyberprzestrzeni

Cyberprzestrzeń definiowana jest różnorodnie i niejednoznacznie. W literaturze i dokumentach normatywnych można znaleźć wiele definicji cyberprzestrzeni czy też przestrzeni cybernetycznej. Definicje te najczęściej odnoszą się do jej struktury i funkcjonalności i nie postrzegają cyberprzestrzeni jako środowiska kooperacji negatywnej, środowiska walki, określanego inaczej jako infrastruktura walki. W sztuce wojennej infrastruktura walki kojarzona jest zarówno ze środowiskiem naturalnym, geograficznym i demograficznym, jak i wszelkimi wytworami ludzkiej działalności (obiektami antropogenicznymi), znajdującymi się na obszarze działań zbrojnych i przystosowanymi do potrzeb danej walki [14]. Traktując cyberprzestrzeń jako środowisko walki powinniśmy uwzględniać zarówno jej aspekty fizyczne, ekonomiczno-gospodarcze, informacyjne, wirtualne, jak i społeczne, co powinno zostać odzwierciedlone w formach i sposobach oddziaływania w konfliktach hybrydowych

Zidentyfikowanie i wyjaśnienie kluczowego terminu jakim jest *cyberprzestrzeń* powinno uwzględniać aspekty związane z historią powstawania tego środowiska, ideami, które przyświecały jego twórcom. Początki współczesnej cyberprzestrzeni związane są bezpośrednio z powstaniem sieci Internet i sięgają końca lat sześćdziesiątych ubiegłego wieku. Powstanie cyberprzestrzeni związane było z programem zbrojeniowym realizowanym przez RAND Corporation na zlecenie rządowej agencji ARPA (ang. *Advanced Research Projects Agency*). W ramach jednego z programów zbrojeniowych realizowanych w czasach zimnej wojny, RAND Corporation zrealizował projekt rozległej sieci komputerowej ARPANET (ang. *Advanced Research Projects Agency Network*). Wyzwaniem, z którym zmierzyli się jej twórcy, było stworzenie sieci łączności, w której nie występowałyby jednostki

centralne sterujące siecią i która byłaby w stanie samodzielnie korygować błędy i nawiązywać połączenia w przypadku uszkodzenia elementów sieci. W 1969 roku, w sieci złożonej z czterech węzłów, przesłano pierwszy komunikat [9]. W wyniku rozwoju technologii, poprzez łączenie coraz to nowych sieci lokalnych, sieć ta pokryła swoim zasięgiem praktycznie cały obszar kuli ziemskiej i stała się ogólnie dostępna dla większości populacji. Przełomowymi momentami jej rozwoju było opracowanie technologii WWW (ang. *World Wide Web*), VoIP (ang. Voice over Intenet Protocol), pojawienie się portali społecznościowych i smartfonów, które zapoczątkowały rewolucję w dostępie do informacji.

W polskim systemie prawnym definicji cyberprzestrzeni występuje wiele. Jedna z pierwszych definicji cyberprzestrzeni została opublikowana w *Założeniach do Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009-2011*, gdzie cyberprzestrzeń określono jako *przestrzeń komunikacyjna tworzona przez system powiązań internetowych* [6]. W kolejnym *Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016* definicja cyberprzestrzeni uległa lekkiej rozbudowie i przyjęła postać *cyfrowa przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami* [11]. Inną definicję można znaleźć w nowelizacjach ustaw o stanach nadzwyczajnych [21]. *Cyberprzestrzeń* jest określona jako *przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, w rozumieniu art. 3. pkt 3. ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami* [20]. System teleinformatyczny według ustawy o informatyzacji to *zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy Prawo telekomunikacyjne* [19]. Urządzeniem końcowym jest urządzenie telekomunikacyjne przezna-

czone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci. Definicję tą powtórzono w *Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej 2013* przyjętej przez Radę Ministrów w 2013 roku [7]. W *Strategii Cyberbezpieczeństwa RP na lata 2017-2022* [12]. cyberprzestrzeń zdefiniowano jako *przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*. Natomiast w *Ustawie o Krajowym Systemie Cyberbezpieczeństwa* [10] z 5 lipca 2018 roku cyberprzestrzeni nie definiowano.

Cyberprzestrzeń jest definiowana również w środowisku międzynarodowym. Na uwagę zasługują cztery, w ocenie autora, najważniejsze. Pierwszą z nich jest definicja opracowana przez Departament Obrony USA, mówiąca, że cyberprzestrzeń jest *globalną domeną środowiska informacyjnego, składającą się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, a także osadzone w nich procesory i kontrolery* [4]. Definicja odnosi się tylko do sfery technicznej cyberprzestrzeni i nie uwzględnia aspektu społecznego – jej roli i znaczenia dla współczesnych społeczeństw. Z kolei w Unii Europejskiej cyberprzestrzeń jest definiowana jako *wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata* [22]. Podobnie jak w definicji amerykańskiej, sfera użytkownika została tu także całkowicie pominięta. Uwagę należy zwrócić także na definicję zawartą w Tallinn *Manual 2.0* [18]. Cyberprzestrzeń postrzegana jest jako *środowisko utworzone przez fizyczne i nie fizyczne komponenty, cechujące się użyciem komputerów i spektrum elektromagnetycznego do składowania, modyfikowania i wymiany danych przy użyciu sieci komputerowej* [18]. W powyższej definicji uwagę przyciąga określenie *niefizyczne komponenty*, które w takim ujęciu oznaczają najprawdopodobniej informacją, której fizyczną reprezentacją są dane. Centrum w Tallinie, opracowano także inną definicję cyberprzestrzeni, postrzegając ją jako *zależny od czasu zbiór połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcje z tymi systemami* [15]. Można w niej zaobserwować, że użytkownicy są ważnymi elementem cyberprzestrzeni, a tworzone interakcje

mają istotny wpływ na dostęp do informacji i kształtowanie postaw, poglądów, opinii. Znamienne jest także podkreślenie znaczenia czasu, który jest jednym z determinantów skuteczności walki w cyberprzestrzeni.

Jak już wspomniano, cyberprzestrzeń różni się od innych domen operacyjnych tym, że w całości została stworzona przez człowieka i przez niego może być dowolnie kontrolowana, kształtowana i modyfikowana. Stwierdzenie to jest o tyle istotne, że w odróżnieniu do innych domen operacyjnych, podatności i zagrożenia występujące w cyberprzestrzeni mogą być eliminowane poprzez zarządzanie samą domeną. Próba rozstrzygnięcia, czym jest cyberprzestrzeń postrzegana jako domena operacyjna, powinna uwzględniać, że środowisko to stało się sferą umożliwiającą zarówno jednostkom, jak i całym społeczeństwom, tworzenie nowych form relacji i funkcjonowania. Najważniejszym elementem cyberprzestrzeni, a zarazem jej istotą, jest informacja. Bez informacji cyberprzestrzeń jest tylko nic nieznaczącym zbiorem urządzeń sieciowych połączonych ze sobą sieciami teleinformatycznymi. Patrząc na zagrożenia występujące w cyberprzestrzeni, można dostrzec, że wszystkie one są związane z informacją, jej zdobywaniem, modyfikowaniem, blokowaniem, niszczeniem, myleniem. Odmienne są natomiast cele tej szkodliwej, wrogiej lub też złośliwej działalności. Złodziej kradnący pieniądze z banku internetowego potrzebuje najczęściej informacji dotyczących nazwy banku, loginu, hasła i sposobu autoryzacji transakcji. Haker wykradający poufne informacje, potrzebuje informacji na temat struktury organizacyjnej atakowanego podmiotu, systemu zabezpieczeń, przyjętych rozwiązań technicznych, osób zajmujących kluczowe pozycje w organizacji, sposobu komunikowania, loginów i haseł umożliwiających dostęp do zasobów. Zdobyte (przejęte) informacje mogą być wykorzystywane do blokowania i niszczenia systemów teleinformatycznych i krytycznych, działania z pozycji dodatniej, do dyskredytacji lub szantażu decydentów i organizacji. Propagandyści z kolei, chcąc osiągnąć przyjęte cele prowadzonych kampanii propagandowych, muszą posługiwać się odpowiednio spreparowanym przekazem informacyjnym, co wymaga informacji na te-

mat uwarunkowań społeczno-historycznych i kulturowych danego społeczeństwa, sytuacji ekonomicznej, bieżących nastrojów i istniejących podziałów. Dodatkowo, w wyniku celowego oddziaływania informacyjnego podziały w społeczeństwach mogą być pogłębiane lub tworzone. Informacja jest krytycznym elementem rywalizacji i walki w cyberprzestrzeni, odmienne są cele i sposoby oddziaływania. Cyberprzestrzeń posiada także swój wymiar fizyczny, co powoduję, że jej elementy mogą zostać unieszkodliwione (zniszczone) na drodze oddziaływania kinetycznego.

Patrząc przez pryzmat użytkowników cyberprzestrzeni, możemy środowisko to zdefiniować jako **przestrzeń aktywności ludzkiej, z wykorzystaniem urządzeń elektronicznych, związaną z operacjami na informacji.** Należy zauważyć, że aktywność ta ma zazwyczaj charakter kooperacji w trzech głównych relacjach: człowiek - człowiek, człowiek - cyberprzestrzeń i cyberprzestrzeń - człowiek. W pierwszym przypadku cyberprzestrzeń umożliwia wymianę informacji pomiędzy jej użytkownikami. To przede wszystkim usługi telefonii internetowej, komunikatorów sieciowych, portali społecznościowych i poczty elektronicznej. Kooperacja negatywna, w tego typu relacjach, jest ukierunkowana na blokowanie usług oraz przekazywanie dezinformacji i propagandy. W drugim przypadku kooperacji człowiek – cyberprzestrzeń, człowiek tworzy własny świat wirtualnej rzeczywistości. Składową tej rzeczywistości są w głównej mierze gry sieciowe, dające użytkownikom poczucie funkcjonowania w nowym wymiarze, pozwalającym odgrywać role, które w rzeczywistym świecie są niemożliwe do spełnienia. Niesie to za sobą istotne zagrożenia społeczne, ponieważ wirtualizacja środowiska ma ogromny wpływ na kształtowanie jednostki. Pojawienie się treści i bodźców ukierunkowanych na konkretne zachowanie użytkowników świata wirtualnego może stanowić zagrożenie nawet dla bezpieczeństwa państwa. Trzeci przypadek kooperacji związany jest z wykorzystaniem sztucznej inteligencji jako elementu cyberprzestrzeni zdolnego do samodzielnego rozwiązywania problemów postawionych przez użytkowników. To w głównej mierze systemy eksperckie i różnego rodzaju *asystenci internetowi*, wspierający użytkowników

w ich codziennym życiu. Coraz większego znaczenia w tego typu relacjach nabierają boty - wyspecjalizowane programy wspierane elementami sztucznej inteligencji, wykorzystywane do powielania komunikatów, głównie w portalach społecznościowych. Są to narzędzia wykorzystywane także do szerzenia dezinformacji i propagandy. Istotnego znaczenia nabiera, nie wymieniona wcześniej, relacja cyberprzestrzeń – cyberprzestrzeń. Jej zaistnienie może okazać się końcem znanego nam świata, co związane będzie najprawdopodobniej z usamodzielnieniem i uniezależnieniem się sztucznej inteligencji. Człowiek w tym wypadku przestanie być wyłącznym twórcą cyberprzestrzeni.

Próbując zdefiniować cyberprzestrzeń z poziomu podmiotów bezpieczeństwa, które ją wykorzystują w swojej codziennej działalności, należy w powyżej definicji zamienić słowa *aktywności ludzkiej* na słowa *kooperacji podmiotów bezpieczeństwa* i wpisać jako cel takiej działalności *realizację własnych interesów*. W przypadku podmiotu jaki jest państwo będą to interesy narodowe. Tym samym cyberprzestrzeń staje się polem współdziałania, rywalizacji i walki, w myśl postulatów Mirosław Sułka. Wziąwszy powyższe pod uwagę, możemy **cyberprzestrzeń** zdefiniować jako **przestrzeń kooperacji podmiotów bezpieczeństwa, z użyciem urządzeń elektronicznych, związaną z realizacją własnych interesów.** W zaproponowanej definicji użyto określenia *urządzenia elektroniczne*, które tworzą środowisko operowania na zbiorach informacji. Zdefiniowanie urządzenia elektronicznego może być z jednej strony proste, z drugiej zaś niezmiernie skomplikowane. W najprostszej definicji to *urządzenie działające dzięki elektronicznym układom cyfrowym* [8]. Chodzi tutaj o te wszystkie urządzenia, które są używane przez ludzi do operowania na informacji. Zasadnym jest pytanie, czy można *urządzenia elektroniczne* zastąpić określeniem *środowisko cyfrowe lub środowisko elektroniczne*?

Cele działań w cyberprzestrzeni

Wskazanie celów wymaga zidentyfikowania, czym w swojej istocie jest cel działania i jakie podmioty mogą go realizować. Zgodnie z definicjami encyklopedycznymi, celem jest tym: *do czego się dąży, co się chce osiągnąć* [16]. W prakseologii termin *cel* jest rozumiany jako planowany wynik racjonalnego działania. Jest on określany przez podmiot działania i w zależności od przyjętego przez niego systemu wartości może być określany jako *stopniowalny* lub *niestopniowalny* [1]. Przytoczony podmiot działania jest postrzegany różnie, w zależności od sposobu zorganizowania i jego umiejscowienia w systemie bezpieczeństwa. Podmiotami mogą być zarówno poszczególni ludzie, społeczność, grupy formalne lub nieformalne, związki, stowarzyszenia, organizacje, firmy, służby, siły zbrojne, państwa, sojusze i inne organizacje międzynarodowe. Każdy z nich ma swój system wartości, tym samym cele działania mogą być niezwykle odmienne. Będą one pochodną rodzaju kooperacji, w której uczestniczą, ukierunkowanej na współdziałanie, rywalizację i walkę.

Cele wyznaczone przez podmioty prowadzące walkę w cyberprzestrzeni mogą być różne, podyktowane możliwościami samych podmiotów i funkcjonującymi, tak jak wspomniano, systemami wartości [3]. Dla podmiotów, jakimi są państwa, cele mogą wynikać z obowiązujących polityk i strategii, przyjętych doktryn i sposobów realizacji interesów narodowych. Większość państw prowadzi defensywną politykę, ukierunkowaną na zwiększenie bezpieczeństwa na drodze pokojowej, realizowaną poprzez rozbudowę potencjału odstraszania, zawierania koalicji i sojuszy. Istnieją też państwa, które dążąc do realizacji swoich celów, osiągają interesy narodowe na drodze agresywnej, poprzez rozwój ofensywnych zdolności, prowadzenie agresywnych kampanii informacyjnych, destabilizację wybranych obszarów, generowanie podziałów pomiędzy państwami i społeczeństwami. Do tego dochodzą także różne grupy interesów, jak chociażby separatyści, fundamentaliści, terroryści czy też korporacje. Każdy z nich może wyznaczać swoje cele, uwarunkowane posiadanym potencjałem. Uwagę przykuwają zwłaszcza

korporacje międzynarodowe, szczególnie związane z nowoczesnymi technologiami informacyjnymi. Ich zasoby ekonomiczne i informacyjne pozwalają na skuteczną rywalizację z podmiotami bezpieczeństwa takimi jak państwa czy też wspólnoty państw. Tym samym stają się one podmiotami mogącymi skutecznie realizować swoje cele poprzez generowanie problemów politycznych, społecznych czy też ekonomicznych, zarówno na poziomie lokalnym, jak również w skali globalnej.

Na pierwszy plan realizowany w kooperacji negatywnej wysuwa się *cel polityczny*, pojmowany jako oczekiwany efekt postępowania w sferze politycznej [3]. To rezultat wzajemnych powiązań i oddziaływań pomiędzy wszystkimi uczestnikami życia politycznego. Są nimi partie polityczne, społeczeństwa, elity, lobbyści, ośrodki władzy formalnej i nieformalnej, grupy nacisku czy nawet związki wyznaniowe. Działania związane z realizacją celów politycznych są ukierunkowane na wzmocnienie, utrzymanie lub osłabienie poszczególnych podmiotów polityki. W walce działania te mogą prowadzić, w stosunku do podmiotu politycznego, zarówno do osamotnienia, zdezawuowania, zmuszenia, destabilizacji, zmiany, jak i upadku. Wszystkie powyżej wyartykułowane cele są ukierunkowane na osłabienie lub wręcz zniszczenie podmiotu politycznego. Są podyktowane własnymi interesami, przeciwstawnymi do interesów atakowanego podmiotu. Największe znaczenie odgrywa tutaj oddziaływanie informacyjne, szantaż, dyskredytacja, dezinformacja i propaganda, ukierunkowane zarówno na obiekt oddziaływania, jak również na jego otoczenie. Do osiągnięcia celu politycznego mogą być wykorzystane także elementy oddziaływania informatycznego i kinetycznego, zgodnie z zasadą synergii, zespolenia działań kierunkowych na maksymalizację efektów. Droga do osiągnięcia celu jakim jest zmiana lub upadek państwa może być wielostopniowa i rozłożona w długim okresie. W pierwszej kolejności agresor będzie oddziaływał informacyjnie na społeczeństwo w celu jego skłócenia, pogłębienia istniejących podziałów i budowania nastrojów niezadowolenia w stosunku do aktualnej sytuacji i władzy. Jednocześnie wśród społeczności międzynarodowej będzie realizowana kampania informacyjna ukierunkowana na osłabienie wizerunku państwa i jego społeczeństwa. Będą

szerzone nieprawdziwe informacje na temat atakowanego społeczeństwa, bazujące zazwyczaj na stereotypach i uprzedzeniach. Faza takiego oddziaływania może trwać latami, do momentu, aż agresor uzna, że nadszedł czas do dalszej eskalacji agresji, polegającej na wprowadzeniu elementów oddziaływania informatycznego i kinetycznego. Zniszczenie lub obezwładnienie kluczowych elementów infrastruktury krytycznej w połączeniu z oddziaływaniem kinetycznym, noszące znamiona skrytobójstwa, dywersji i sabotażu, może być przysłowiowym zapalnikiem do wywołania masowych protestów, strajków lub też a skrajnych przypadkach zamachu stanu. Wszystko zależy od przyjętych celów agresora, siły jego oddziaływania i odporności atakowanego państwa.

Kolejnym celem walki realizowanym w cyberprzestrzeni może być *cel ekonomiczny,* związany z aktywnością podmiotu w sferze gospodarczej, jego wiarygodnością finansową, efektywnością ekonomiczną i posiadanymi zasobami [3]. Dla podmiotów takich jak państwo cele ekonomiczne są najczęściej podyktowane zrównoważonym rozwojem kraju, rozwojem gospodarki, wzrostem zamożności społeczeństwa, a jego wymiernymi znacznikami są: produkt krajowy brutto, dług publiczny, zdolność kredytowa, stosunek eksportu do importu, poziom zamożności społeczeństwa, posiadane rezerwy finansowe. Sprostanie takim wyzwaniom wymaga od państwa posiadania i ciągłego rozwijania: zasobów materiałowych, ludzkich, energetycznych, kluczowych technologii, silnego przemysłu, stabilnego systemu finansowego i prawnego. Tym samym w kooperacji negatywnej, ukierunkowanej na cele ekonomiczne, można oddziaływać między innymi na: zasoby, ludzi, technologie, przemysł, system finansowy i prawny. Istnieją państwa, których działalność w cyberprzestrzeni jest ukierunkowana na kradzież technologii, co pozwala im skuteczniej rozwijać własną gospodarkę i potencjał ekonomiczny. Znane są przypadki wrogiej działalności w stosunku do zasobów, mających kluczowe znaczenie. Zasobami tymi są chociażby surowce energetyczne czy kluczowe technologie. W odniesieniu do zasobów ludzkich sterowanie przekazem informacyjnym szkalującym dane społeczeństwo, powielającym stereotypy i uprzedzenia, może być ukierunkowane na wystraszenie emigrantów

chcących podjąć pracę w atakowanym kraju. Generowanie podziałów i niepokojów społecznych może także skutkować zwiększeniem emigracji zarobkowej, tym samym pozbawieniem atakowanego państwa rąk do pracy. Szerzenie fałszywych informacji na temat sytuacji gospodarczej i ekonomicznej danego państwa może doprowadzić do obniżenia ratingów zdolności kredytowej tego państwa, tym samy do jego głębokiej zapaści ekonomicznej i społecznej. Wroga działalność wymierzona w podstawy ekonomiczne innego podmiotu bezpieczeństwa wymaga czasu i przede wszystkim informacji, zarówno zdobytej (wykradzionej), zmodyfikowanej, jak i celowo spreparowanej. Cyberprzestrzeń w tym wymiarze będzie odgrywała coraz większą rolę, z uwagi na:

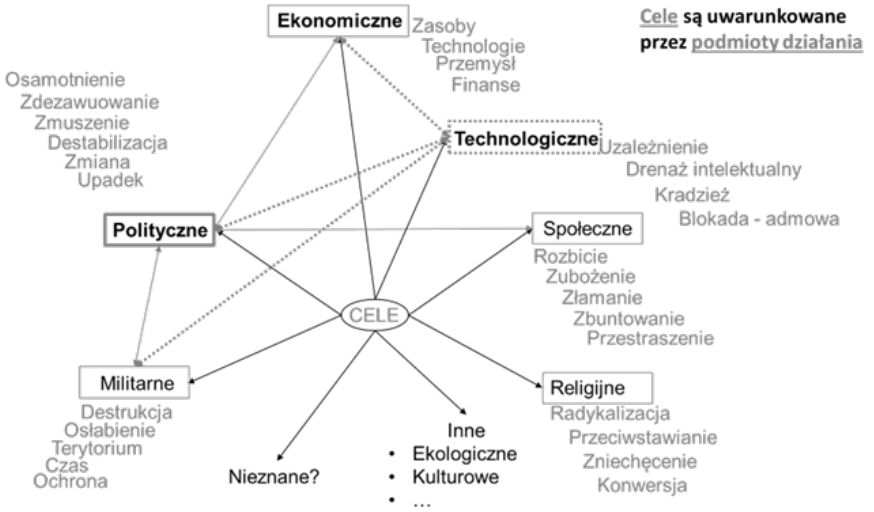
- możliwość inwigilacji systemów informacyjnych strony przeciwnej,
- możliwość prowadzenia kampanii dezinformacyjnych,
- możliwość prowadzenia kampanii propagandowych,
- uzależnienie funkcjonalności gospodarki od technologii informacyjnych.

Istotnym celem realizowanym w kooperacji negatywnej w cyberprzestrzeni jest także *cel społeczny*, realizowany najczęściej w państwa demokratycznych, w których to społeczeństwo jest elementem kształtującym kierunki rozwoju, ustrój państwa i wybiera przedstawicieli odpowiadających za prowadzenie polityki wewnętrznej i zagranicznej [3]. Najogólniej rzecz ujmując, to społeczeństwo decyduje, w którą stronę podąża państwo. Jeżeli istnieje potencjalna możliwość wyznaczenia tego kierunku na drodze negatywnego oddziaływania informacyjnego, umożliwiającego zaspokojenie własnych interesów agresora, bez potrzeby eskalacji jawnych konfliktów, to działania takie będą podejmowane coraz częściej. Cele społeczne mogą być powiązane z celami politycznymi, jak chociażby podczas wpływania na wyniki wyborów i referendów. Oddziaływanie na społeczeństwo może być ukierunkowane między innymi na takie realizację takich celów cząstkowych, jak chociażby: rozbicie, zubożenie, załamanie, zbuntowanie, przestraszenie. Zgodnie z zasadą dziel i rządź, działanie na rozbicie, zubożenie, załamanie, zbuntowanie

i przestraszenie społeczeństwa jest podyktowane osłabieniem jego woli przeciwstawienia się wszelkim przeciwnościom i zagrożeniom. Łatwiej jest rywalizować z państwem, którego społeczeństwo nie stanowi jedności, władza nie ma poparcia w całości społeczeństwa i nie może liczyć na jego poświęcenie i oddanie, zwłaszcza w sytuacjach kryzysowych. Pogłębianie i generowanie podziałów mogą mieć podłoże zarówno światopoglądowe, kulturowe, ideologiczne, jak również ekonomiczne. Różne są drogi i sposoby takiego oddziaływania, lecz wspólny cel, zniszczenie jedności narodowej. Cyberprzestrzeń, poprzez swoje właściwości, umożliwia oddziaływanie informacyjne w oderwaniu od uwarunkowań geograficznych, administracyjnych, czasowych i jest tym bardziej skuteczna, im bardziej złożone jest społeczeństwo atakowanego podmiotu (państwa). W przypadku podmiotów złożonych, takich jak Unia Europejska, kampanie propagandowe będą coraz skuteczniejszym narzędziem generowania konfliktów pomiędzy nie tylko społecznościami danych państwa, ale całymi narodami.

Kolejnym celem, realizowanym w walce w cyberprzestrzeni, jest *cel religijny,* bezpośrednio związany z atakiem na systemy wartości dominujące w danym społeczeństwie [3]. Z jednej strony dąży się do radykalizacji poglądów, z drugiej do ich złagodzenia. To także przeciwstawienie wyznawców jednej religii przeciwko wyznawcom innej, ukierunkowane na zwiększenia zasięgu własnej wiary poprzez zastraszenie lub konwersję innowierców. Wojny religijne zawsze były nieodzownym elementem ludzkości. Ich charakter był podyktowany nie tylko celem ideologicznym, lecz najczęściej czystą pragmatyką zdobycia władzy, zajęcia terenu, przejęcia zasobów, wzbogacenia się. Ich przebieg i zasięg były zawsze związany z poziomem rozwoju ludzkości. I chociaż można się zgodzić z poglądem, że ich współczesny wymiar może być równie krwawy jak wieki temu, to coraz większą aktywność ugrupowań religijnych możemy obserwować w cyberprzestrzeni. Jest to doskonałe środowisko do szerzenia idei, znajdowania i pozyskiwania wyznawców, radykalizacji poglądów, szerzenia zamętu, strachu i terroru. Cyberprzestrzeń w wymiarze religijnym stała się doskonałym środowiskiem komunikacyjnym,

pozwalającym na tworzenie organizacji rozproszonych, umożliwiającym koordynowanie działań umotywowanych ideologicznie, wymierzonych zarówno w przeciwników religijnych, jak i w społeczeństwa bazujące na innych systemach wartości. W tę działalność wpisują się fundamentaliści religijny, stosujący jako sposób oddziaływania zamachy terrorystyczne, o których informują za pomocą portali społecznościowych.



Źródło: Opracowanie własne.
Rys. 1. Cele wyznaczane w walce w cyberprzestrzeni. własne

Istotnym celem realizowanym w kooperacji negatywnej w cyberprzestrzeni jest również *cel militarny*, związany bezpośrednio z działaniami sił zbrojnych w tym piątym wymiarze [3]. Można dostrzec, że walka w cyberprzestrzeni może mieć charakter zarówno walki zbrojnej, jak i niezbrojnej, może być walką wspieraną lub też walką wspierającą inne rodzaje walk. Cele wyznaczone w cyberprzestrzeni wynikają z przyjętych celów operacyjnych i strategicznych, miejsca walki w cyberprzestrzeni w systemie obronnym państwa. Mogą być one ukierunkowane zarówno na destrukcję przeciwnika, osłabienie jego potencjału, przejęcie lub utrzymanie trenu, zyskanie czasu, ochronę własnych zasobów militarnych i cywilnych. Obywać się to będzie za

pomocą kampanii informacyjnych, oddziaływania informatycznego i kinetycznego, przy uwzględnieniu efektu synergii z działaniami prowadzonymi w pozostałych czterech wymiarach.

Sposoby oddziaływania

W konflikcie hybrydowym wykorzystanie cyberprzestrzeni związane jest bezpośrednio z celami, które zostały wyznaczone i czasem, który jest niezbędny, aby je zrealizować. Mają one najczęściej charakter wielowektorowego oddziaływania, z różną intensywnością rozłożoną w czasie. Najogólniej, walka w cyberprzestrzeni zawiera w sobie całokształt działań, zarówno ofensywnych, jak i defensywnych, koniecznych do uzyskania przewagi nad przeciwnikiem i osiągnięcia zamierzonych celów. Czynnikami krytycznymi są czas i informacja, która warunkuje wszystkie działania w cyberprzestrzeni, umożliwiając rażenie i wyzwalając ruch. Nie chodzi tylko o ochronę i niszczenie zasobów cyberprzestrzeni, ale przede wszystkim o budowanie narracji, mieszanie w umysłach, kreowanie rzeczywistości, wpływanie na postawy i poglądy. Walka w cyberprzestrzeni stała się obecnie niejako zamiennikiem lub preludium walki zbrojnej w ujęciu klasycznym, nową formą walki, prowadzoną w warunkach pokoju, kryzysu i wojny. Z tego względu, zanim dojdzie do klasycznego starcia zbrojnego, polem bitwy będzie, lub nawet już jest, cyberprzestrzeń, obejmująca swym zasięgiem nie tylko terytorium stron konfliktu, ale także cyberprzestrzeń społeczności międzynarodowej. Przebieg takiej walki może mieć charakter pełzający lub gwałtowny. W pierwszym przypadku oddziaływanie na stronę przeciwną będzie się rozwijało stopniowo, bez widocznego początku ataku i może zostać niedostrzeżone lub traktowane jako zjawisko występujące na co dzień w sieci Internet. Możemy obserwować doniesienia o coraz większej liczbie ataków w cyberprzestrzeni, próbach wpływu na demokratyczne wybory, eskalację napięć i niepokojów, wywoływanie zamieszek i nawoływanie do buntu. To wszystko stało się częścią codziennego życia. Oczywiście należy rozróżnić zagrożenia, które nie

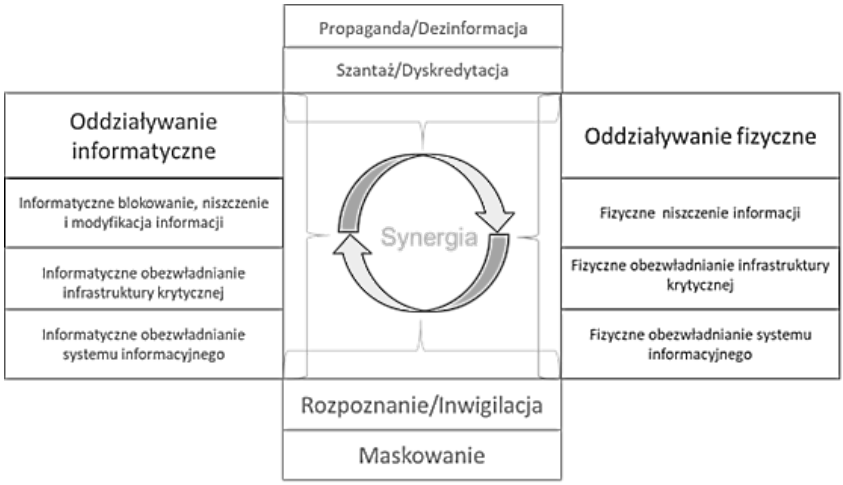
noszą znamion zorganizowanego oddziaływania ze strony podmiotu państwowego, lecz wynikają ze zwykłej przestępczości, przypadkowości, niewiedzy lub naiwności użytkowników cyberprzestrzeni. Sposoby oddziaływania w tego typu zagrożeniach są podobne do tych w walce w cyberprzestrzeni, lecz inne są cele i skala takiego działania. Z kolei atak gwałtowny będzie związany z dużą intensywnością oddziaływania w cyberprzestrzeni, a jego skutki będą dotkliwie odczuwalne. W przeszłości mieliśmy już do czynienia z kilkoma tego typu zdarzeniami, lecz nadal niełatwe jest określenie, jakie podmioty za nimi stały i jakie cele były realizowane. Nie znamy, czy realizowały je podmioty państwowe, grupy pracujące dla podmiotów państwowych czy też może niezależne grupy hakerów lub pojedynczy hakerzy, określani mianem samotnych wilków. Cyberprzestrzeń charakteryzuje się dużą anonimowością i zaprzeczalnością, co utrudnia złapanie agresora na gorącym uczynku. Pewną cześć ataków można uznać za próby testowania przyjętych rozwiązań, narzędzi ataku, zabezpieczeń i procedur postępowania. Cyberprzestrzeń jest bowiem także swoistym poligonem, na którym są testowane sposoby i narzędzia oddziaływania.

Walka w cyberprzestrzeni odbywa się na dwóch głównych płaszczyznach [3]. Pierwsza to ochrona i obrona własnych zasobów informacyjnych, własnych zamiarów, stworzenie fałszywego obrazu rzeczywistości, kreowanie fałszywego obrazu sytuacji przy jednoczesnym dążeniu do uzyskania informacji o stronie przeciwnej. Druga sprowadza się do zapewnienia żywotności własnego systemu informacyjnego i elementów infrastruktury krytycznej oraz sparaliżowania systemu informacyjnego i infrastruktury krytycznej strony przeciwnej. W cyberprzestrzeni w pierwszej kolejności zostaną wykorzystane sposoby oddziaływania niewymagające dużych nakładów finansowych, warunkujące przewagę informacyjną, kreujące postawy i poglądy, będące dotkliwe dla strony przeciwnej i jednocześnie akceptowalne przez własne społeczeństwo i społeczność międzynarodową. Do tych sposobów możemy zaliczyć:

- inwigilację, rozpoznanie i maskowanie;
- dezinformację, propagandę, szantaż i dyskredytację;

- informatyczne blokowanie, niszczenie i modyfikację informacji;
- informatyczne obezwładnianie infrastruktury krytycznej;
- informatyczne obezwładnianie systemu informacyjnego;
- fizyczne niszczenie informacji;
- fizyczne zniszczenie infrastruktury krytycznej;
- fizyczne zniszczenie systemu informacyjnego z ukierunkowaniem na decydentów.

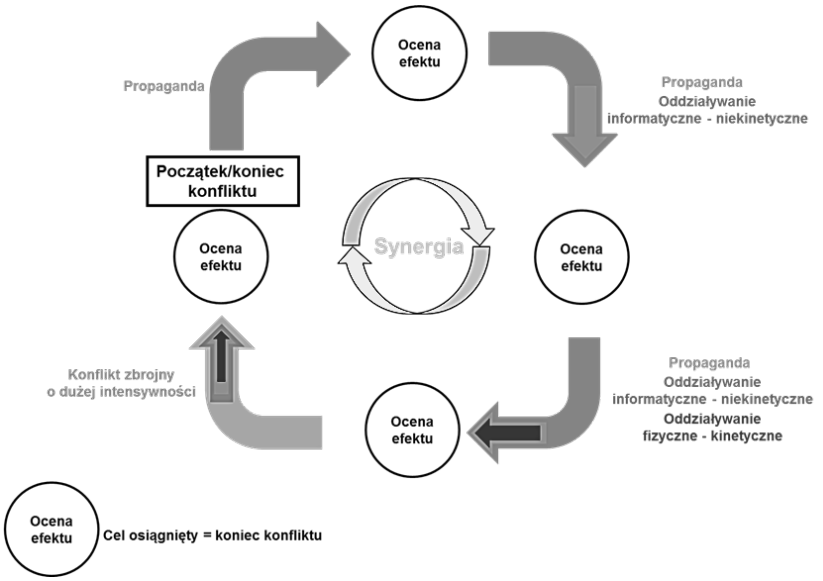
Wszystkie powyższe sposoby oddziaływania w cyberprzestrzeni muszą uwzględniać uwarunkowania: środowiskowe, organizacyjne, techniczne, technologiczne, społeczno-historyczne, kulturowe, psychofizyczne. Inne bowiem będzie oddziaływanie na wysoko rozwinięte społeczeństwa zachodnie, inne na społeczeństwa rozwijające się, inne na własne społeczeństwo i jeszcze inne na społeczeństwo państwa atakowanego. Dodatkowo powinien być uwzględniony efekt synergii, co oznacza, że wszystkie przedsięwzięcia państwa należy podporządkować osiągnięciu przyjętych celów, rozłożonych w czasie zgodnie z obowiązującą strategią i doktrynami.



Źródło: Opracowanie własne.

Rys. 2. Sposoby oddziaływania w cyberprzestrzeni

Oddziaływanie informatyczne [3] jest ukierunkowane na te elementy infrastruktury krytycznej, których sprawność i niezawodność są kluczowe w wymiarze ekonomicznymi i społecznym dla atakowanego państwa. Infrastruktura ta jest uzależniona od informatycznych systemów sterujących, których wadliwe funkcjonowanie może skutkować awariami i w konsekwencji katastrofami technicznymi i społecznymi. Narzędzia oddziaływania informatycznego są najczęściej powszechnie dostępne i tanie, a przewidywanie celu ataku, czasu i potencjalnego sprawcy jest trudne. Na potrzeby walki w cyberprzestrzeni zostaną wykorzystane także narzędzia informatyczne, które zostały do tego specjalnie stworzone, a tym samym są nieznane dla strony przeciwnej i jeszcze bardziej niebezpieczne.



Źródło: P. Dela, *Założenia działań w cyberprzestrzeni*, Wydawnictwo Naukowe PWN, Warszawa 2022.

Rys. 3. Model eskalacji konfliktu w cyberprzestrzeni

Oddziaływanie fizyczne [3] to nic innego jak kinetyczne niszczenie tych wszystkich elementów, które mają kluczowe znaczenie dla sprawności

funkcjonowania państwa, a których zniszczenie poprzez oddziaływanie informatyczne jest utrudnione lub niemożliwe. Są nimi zasoby informacyjne, elementy infrastruktury krytycznej, składowe systemu informacyjnego z decydentami włącznie. Ten rodzaj oddziaływania jest integralnym elementem walki w cyberprzestrzeni co wymusza uwzględnienia aspektów ochrony fizycznej wszystkich zasobów i obiektów krytycznych. Tym bardziej że oddziaływanie kinetyczne w czasie pokoju i kryzysu będzie nosiło znamiona awarii technicznych, skrytobójstwa, dywersji i sabotażu.

Celem poszczególnych etapów walki z wykorzystaniem cyberprzestrzeni jest zdobycie przewagi informacyjnej i przejście do działań zbrojnych z pozycji dodatniej lub zmuszenie przeciwnika do uległości na drodze samego oddziaływania w cyberprzestrzeni. Na rysunku 3. przedstawiono model eskalacji konfliktu. Kluczowym elementem modelu eskalacji konfliktu jest stopień realizacji przyjętego celu działania. Jeżeli jest on niesatysfakcjonujący dla agresora, to konflikt będzie eskalował do nowych sposobów oddziaływania, uwarunkowanych kosztami ekonomicznymi i społecznymi.

Zakończenie

Wykorzystanie cyberprzestrzeni w konflikcie hybrydowym jej kluczowym elementem, decydującym najczęściej o osiągnięciu zamierzonego celu działania. Wynika to przed wszystkim z cech cyberprzestrzeni. Jest to środowisko zapewniające ukrycie własnego potencjału, zamaskowanie realizowanego celu oddziaływania, maksymalizujące zasięg oddziaływania, umożliwiające szerokie spektrum oddziaływania, skracające czas niezbędny do przeprowadzenia ataku, umożliwiające rozpoznanie i inwigilację, pozwalające na szerzenie propagandy i dezinformacji. Kluczowe cechy cyberprzestrzeni zapewniają anonimowość działania, pozwalają na łatwe zaprzeczenia, gwarantują atakującemu bezpieczeństwo i ekonomię walki.

Nie sposób wymienić wszystkich cech cyberprzestrzeni, które przemawiają za jej wykorzystaniem w każdego rodzaju konflikcie. Można tylko przypuszczać, że wraz z rozwojem nowych technologii, w tym komputera

kwantowego i sztucznej inteligencji, wojna w cyberprzestrzeni nabierze nowego wymiaru, co zapewne zostanie odzwierciedlone w doktrynach obronnych państwa rozwiniętych. Zachowanie funkcjonalności cyberprzestrzeni w tym infrastruktury krytycznej, ochrona posiadanych zasobów informacyjnych i ograniczenie oddziaływania informacyjnego na społeczeństwa stanie się jeszcze większym wyzwaniem niż te z którymi zmaga się świat.

Bibliografia

1. Bojarski W., *Podstawy analizy i inżynierii systemów*, Państwowe Wydawnictwo Naukowe, Warszawa 1984.
2. Uchwała nr 125 Rady Ministrów z 22.10.2019 roku.
3. Dela P., *Założenia działań w cyberprzestrzeni,* Wydawnictwo Naukowe PWN, Warszawa 2022.
4. *Dictionary of Military and Associated terms*, Joint Publication 1-02, DoD November 2010.
5. Gruszczak A., *Hybrydowość współczesnych konfliktów zbrojnych – analiza krytyczna*, www.bbn.gov.pl/ download/1/8755 /Hybrydowo-swspolczesnychwojenanalizakrytyczna.pdf, [11.09.2019].
6. *https://archiwum.mswia.gov.pl/pl/aktualnosci/6966,Zalozenia-do-Rzadowego-programu-ochrony-cyberprzestrzeni-RP-na-lata-2009-2011.html*, [2.12.2020].
7. https://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf, [2.12.2020]
8. https://pl.glosbe.com/pl/pl/urz%C4%85dzenie%20elektroniczne, [11.09.2019].
9. https://scienceinpoland.pap.pl/aktualnosci/news%2C79223%2Cpol-wieku-temu-zainstalowano-pierwsze-wezly-sieci-arpanet-przodka-internetu, [2.12.2020].
10. https://www.dziennikustaw.gov.pl/D2018000156001.pdf, [2.12.2020]
11. *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf* [2.12.2020].

12. https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022, [2.12.2020].
13. Kotarbiński T., *Traktat o dobrej robocie*, Zakład Narodowy im. Ossolińskich, Wydawnictwo Polskiej Akademii Nauk, Wrocław-Warszawa-Kraków 1965.
14. Koziej S., *Teoria sztuki wojennej*, Bellona, Warszawa 1993.
15. Ottis R., Lorents P., *Cyberspace: definition and Implications*, Cooperative Cyber Defense Center of Excellence, Tallin 2010.
16. *Słownik języka polskiego*, t. I, Wydawnictwo Naukowe PWN, Warszawa 1993.
17. Sułek M., *Trzy działy prakseologii,* Rocznik Naukowy Wydziału Zarządzania w Ciechanowie Wyższej Szkoły Menadżerskiej w Warszawie", z. 1-2, t. II, Ciechanów 2008.
18. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press 2017.
19. *Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne*, DzU 2014 poz. 243, t.j.
20. *Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*, DzU 2005 nr 64 poz. 565, z późn. zm.
21. *Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw,* DzU 2011 nr 222 poz. 1323.
22. Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, [w:] Przegląd Bezpieczeństwa Wewnętrznego nr 9/2013.

Abstract

THE USE OF CYBERSPACE IN A HYBRID CONFLICT

Summary: The chapter presents the most important elements of the use of cyberspace in a hybrid conflict. The attention was focused on the essence of cyberspace and hybrid conflict, goals implemented in this type of conflict, objects and methods of interaction.

Keywords: cyberspace, cyber conflict, combat theory, cyberspace security.

Rozdział 2

Wzmocnienie bezpieczeństwa klienta bankowości elektronicznej w świetle przeprowadzonych badań

dr Paweł CISZEK[1], Paweł WAWRZYNIAK[2]

STRESZCZENIE: W rozdziale przedstawiono wyniki prac w ramach projektu pt. „Środowisko bezpieczeństwa klienta bankowości elektronicznej". Przedstawiono wykorzystane metody i narzędzia badawcze, które pozwoliły na realizację celów projektu – identyfikację stosowanych rozwiązań i towarzyszących im zagrożeń, charakterystykę klientów oraz określenie kierunku rozwoju w sferze bankowości elektronicznej. Zaprezentowano najważniejsze wyniki badań empirycznych – badań ankietowych oraz poszerzonych wywiadów eksperckich. Przedstawiono zalecenia w zakresie architektury rozwiązań oraz bezpieczeństwa środowiska bankowości elektronicznej.

SŁOWA KLUCZOWE: bezpieczeństwo, cyberbezpieczeństwo, bankowość elektroniczna, klient bankowości elektronicznej, przestępstwa na szkodę banków i ich klientów, ewolucja bankowości, vishing, phishing, transformacja cyfrowa.

[1] starszy specjalista w Narodowym Centrum Bezpieczeństwa Cyberprzestrzeni, p.ciszek71@outlook.com

[2] wykładowca, Zakład Analiz Zagrożeń Bezpieczeństwa Wewnętrznego, Wyższa Szkoła Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni, p.wawrzyniak@kadra.wsaib.pl, ORCID: 0000-0002-4689-5909.

Wstęp

Rewolucja Informacyjna, której obecnie jesteśmy świadkami, rozpoczęła się w roku 1946, kiedy na uniwersytecie stanowym w Pensylwanii zbudowano pierwszą na świecie maszynę liczącą – ENIAC[3]. Ta zajmująca 170 m^2 powierzchni i ważąca 30 ton maszyna zdeterminowała kierunek rozwoju społeczeństw, prowadząc je systematycznie do zmian, określanych obecnie mianem Rewolucji Informacyjnej. Rozwój cywilizacyjny doprowadził nas do punktu, gdy posiadanie dostępu do Internetu jest czymś tak powszechnym, że jego brak w domu dziwi bardziej, niż brak bieżącej wody. Prawie 1 milion dolarów na minutę wydaje się dzisiaj na zakupy w Internecie, a do roku 2030 planuje się, że 90% ludności w wieku powyżej sześciu lat będzie dostępnych online. Co 39 sekund w Internecie pojawia się nowy atak, codziennie tworzone jest ponad 1,3 mln fragmentów malware, którego jedynym celem jest kradzież danych i w efekcie środków finansowych – rzeczą podstawowej wagi jest diagnoza środowiska, w jakim przyszło funkcjonować klientowi bankowości, który był, jest i będzie zasadniczym ogniwem bezpieczeństwa w bankowości, jaką znamy i tej, jaka nadejdzie wraz z nieuchronnym rozwojem technologicznym.

W 2021 roku zespół badawczy pod kierunkiem dr hab. inż. Jerzego Kosińskiego w ramach Morskiego Centrum Cyberbezpieczeństwa Akademii Marynarki Wojennej w Gdyni na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości przeprowadził badania środowiska bezpieczeństwa klientów bankowości elektronicznej. Prace skoncentrowały się wokół problemów badawczych dotyczących 3 obszarów i zawarte w następujących 5 pytaniach:

I. Część diagnostyczna – strona bankowa:

[3] Electronic Numerical Integrator And Computer.

1. Jakie rozwiązania techniczne i proceduralne są stosowane w bankowości elektronicznej?
2. Jakie są zdiagnozowane zagrożenia dla obecnego klienta bankowości elektronicznej?

II. Część diagnostyczna – klient bankowości:

3. Jaka jest dojrzałość technologiczna klientów bankowości elektronicznej?
4. Jaka jest świadomość zagrożeń dla klientów bankowości elektronicznej?

III. Część prognostyczna:

5. Jakie są kierunki rozwoju usług bankowych dla klienta bankowości elektronicznej?

W efekcie prac zespołu przygotowany i wydany został szczegółowy Raport pt. „Środowisko bezpieczeństwa klientów bankowości elektronicznej opracowany na zlecenie". W niniejszym opracowaniu skupiono się na kwestiach najistotniejszych, których szczegółowe rozwinięcie znalazło się w przygotowanym raporcie. W ocenie zespołu badawczego badania pozwoliły na wstępne zdiagnozowanie wielu obszarów, które obecnie, ale i w najbliższym czasie zaczną nabierać na znaczeniu wśród praktyków i środowiska naukowego. Badania swoim zakresem objęły szerokie spektrum, stanowią przyczynek do rozwinięcia niektórych podjętych zagadnień do samodzielnych badań. Badania empiryczne wskazały na konieczność systematycznego badania środowiska klienta bankowości elektronicznej które okazało się być bardzo dynamiczne. Poruszone kwestie bezpieczeństwa, w tym zagrożeń ze strony przestępczości, tej pospolitej, ale w szczególności zorganizowanej, pozwalają na postawienie tezy, że „przestępczość jako zjawisko przystosowuje się do zmian szybciej i w sposób o wiele bardziej elastyczny aniżeli klient bankowości elektronicznej" – koniecznym zatem jest podjęcie wszelkich możliwych prac, aby będąc wyposażonym w aktualną i rzetelną wiedzę uchronić wszystkie podmioty bankowości elektronicznej przed tym zagrożeniem.

W artykule przedstawiono metody i narzędzia badawcze, wybrane wyniki obszernych badań wraz z syntetycznym omówieniem oraz zaprezentowano główne wnioski wypływające z badań.

Metody i narzędzia

W celu szczegółowej charakterystyki środowiska klienta bankowości elektronicznej wykorzystano szereg metod i narzędzi badawczych.

Jako podstawę i przygotowanie do dalszych prac nad zagadnieniem wykorzystano analizę krytyczną[4] artykułów naukowych i literatury specjalistycznej która pozwoliła na przygotowanie się uczestników badania do poszerzonej analizy zagadnienia i badań terenowych.

Zastosowano także metodę analizy indywidulanych przypadków – wykorzystaną głównie jako analiza przestępstw na szkodę klienta bankowości elektronicznej, która stanowiła podstawę do pogłębionych wywiadów eksperckich.

Z racji, iż metoda ankietowa i metoda wywiadu stanowią trzon metodologiczny nauk społecznych[5], które stanowiły podstawę prowadzonych prac, uczestnicy badania uznali, że niezbędnym krokiem w trakcie szczegółowej analizy postawionych problemów badawczych będzie ich wykorzystanie. Badania ankietowe zostały przeprowadzone z wykorzystaniem ankiety w formie elektronicznej – CAWI (Computer Assisted Web Interview) – z wykorzystaniem popularnego i uznanego narzędzia, które pozwoliło na dotarcie szerokiej grupy respondentów i wykonanie jej na dowolnej platformie[6]. Kwestionariusz

---

[4] J. Apanowicz, *Metodologia nauk*, Wyd. Dom Organizatora, Toruń 2003.

[5] L.A. Gruszczyński, *Kwestionariusze w socjologii*, Katowice 2003; L.A. Gruszczyński, *Elementy metod i technik badań socjologicznych*, Tychy 2002.

[6] Ankieta w wersji online została przeprowadzona za pomocą narzędzia Google Forms.

ankiety umożliwiał pozostawienie informacji zwrotnej lub komentarzy odnoszących się do wybranych pytań. Wypełnienie kwestionariusza zajmowało respondentom nie więcej niż 15 minut. Wywiady eksperckie były częściowo skategoryzowane, prowadzone były w formie bezpośredniej z wykorzystaniem elektronicznych środków komunikacji. Przygotowana lista pytań w większości przypadków stanowiła tylko punkt bazowy wywiadu, zaś rozległa wiedza i doświadczenie ekspertów często pozwalały na znaczące rozwinięcie podejmowanych kwestii ponad to, co wstępnie było założone w kwestionariuszu.

Zebrany materiał został poddany opracowaniu ilościowemu i jakościowemu a także szczegółowej analizie w kontekście podmiotu, przedmiotu badań oraz postawionych problemów badawczych. Do opracowania ilościowego wykorzystano program MS Excel zaś opracowanie jakościowe oparto o arkusze zebranych odpowiedzi z przeprowadzonych wywiadów.

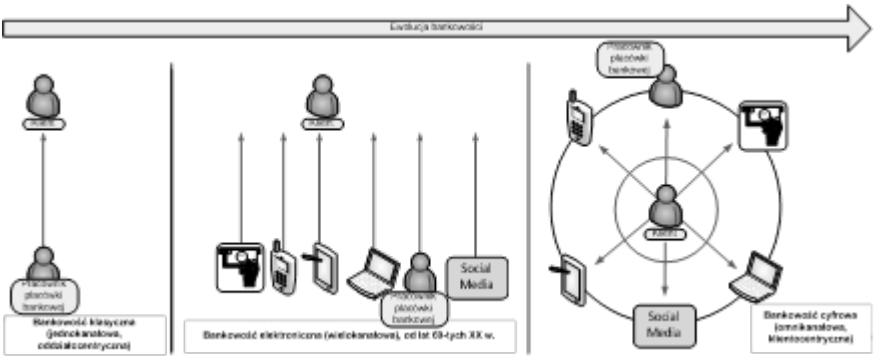
Weryfikacja postawionych hipotez możliwa była między innymi dzięki wykorzystaniu wspomnianych metod i narzędzi, jednak ich podsumowanie i prezentacja wyników w założonej formule o objętości nie miała by miejsca bez wykorzystania syntezy i uogólniania.

Wyniki

W toku prac badawczych analizie poddano stosowane rozwiązania stosowane przez podmioty sektora bankowego dla klienta bankowości elektronicznej.

Scharakteryzowano między innymi kanały komunikacji z klientem (kanały dystrybucji) za pośrednictwem których świadczone są usługi bankowe. Przeanalizowano proces ewolucji usług – od bankowości klasycznej (jednokanałowej, oddziałocentrycznej), przez bankowość elektroniczną (wielokanałową), po bankowość cyfrową (omnikanałową, klientocentryczną) i ich wpływ na wymagania, jakie klient bankowości elektronicznej stawia przed

obecnie funkcjonującymi rozwiązaniami oraz dokonano na tej podstawie wstępnej predykcji co do kierunków zmian w świadczonych usługach.



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.

Schemat 1. Kierunek ewolucji od bankowości klasycznej (jednokanałowej, oddziałocentrycznej), przez bankowość elektroniczną (wielokanałową), po bankowość cyfrową (omnikanałową, klientocentryczną)

Na Schemacie 1 przedstawiono kierunek ewolucji od bankowości klasycznej (jednokanałowej, oddziałocentrycznej), przez bankowość elektroniczną (wielokanałową), po bankowość cyfrową (omnikanałową, klientocentryczną). Ukazano podstawowe kanały komunikacji między klientem a bankiem[7].

Wyróżniono i scharakteryzowano w ramach badanego otoczenia klienta bankowości elektronicznej, proces *transformacji cyfrowej banków,*

[7] Na podst.: 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.

który można zdefiniować jako działania polegające na zmianie modelu biznesowego banku poprzez dostosowanie aktualnych, a także powołanie nowych procesów, narzędzi i rozwiązań (zarówno w ramach oferowanych produktów i usług bankowych – *transformacja zewnętrzna*, ale i ich obsługi oraz rozwoju kanałów dystrybucji – *transformacja wewnętrzna*). Ustalono, iż podstawowymi założeniami bankowości cyfrowej stały się *omnikanałowość* i *klientocentryczność*, gdzie *omnikanałowość* oznacza możliwość zmiany kanału dystrybucji w ramach jednego procesu zakupowego, np. klient realizuje pierwszą część kupna kredytu przez Internet (złożenie wniosku), a następnie może kontynuować realizację w innym kanale – bankowości mobilnej, telefonicznej lub w oddziale. Omnikanałowość różni się od wielokanałowości tym, że ta druga daje możliwość wykonania usługi w wielu kanałach, przy czym realizacja następuje od początku do końca w tym samym kanale. Istotą omnikanałowości nie jest więc równoległe, niezależne funkcjonowanie różnych kanałów komunikacji z bankiem, ale takie ich sprzężenie, by się wzajemnie przenikały i uzupełniały. Dzięki temu klient ma uzyskać swobodę wyboru i gwarancję jednakowego standardu obsługi oraz tej samej ceny produktu w każdym z dostępnych kanałów[8]. Z kolei *klientocentryczność* (koncentracja na kliencie) polega, przede wszystkim, na skupieniu się na doświadczeniach klienta połączonych z dogłębnym zbadaniem aktualnej roli oddziałów banków, co oznacza w istocie konieczność odejścia od tradycyjnej roli oddziału jako głównego kanału sprzedaży (bankowość klasyczna) na rzecz miejsca, w którym klient zasięgnie wysokiej jakości porady od prawdziwego eksperta.

---

[8] Z. Jagiełło, *Bankowość detaliczna w obecnych warunkach rynkowych. Kierunki rozwoju*, [w:] *Wyzwania bankowości detalicznej*, pod red. Z. Jagiełło, Instytut Badań nad Gospodarką Rynkową – Gdańska Akademia Bankowa, Gdańsk 2015, s. 10.

Zdefiniowano na potrzeby badań pojęcie *bankowości elektronicznej* (ang. *electronic banking* lub *e-banking*), które utożsamiono z określeniem „zdalna bankowość" jako korzystaniem z usług bez kontaktu klientów z pracownikami banków, jedynie za pomocą łączy telekomunikacyjnych oraz urządzeń elektronicznych. Tak przyjęta definicja usług niesie ze sobą szereg następstw, między innymi w rezultacie tak przyjętej organizacji to właśnie klient, a nie pracownik banku jest inicjatorem operacji z dala od fizycznej siedziby banku[9]. W następstwie umożliwia to istnienie wielu, równolegle dostępnych, elektronicznych kanałów komunikacji (dystrybucji), które pozwalają na świadczenie usług w sposób bezkontaktowy. Nie oznacza to co prawda zaprzestania świadczenia usług bankowych w modelu klasycznym – bezpośredni kontakt w placówce banku wciąż pozostaje jedną z dostępnych metod komunikacji klienta z bankiem (dystrybucji usług bankowych). Co prawda bankowość elektroniczna pozawala na dostęp zarówno do tradycyjnych usług, które świadczone są w wielu kanałach, to dodatkowo w wyniku jej zastosowania powstała możliwość oferowania usług nowych, które są wprost następstwem wykorzystania przez banki pojawiających się i możliwych do implementacji nowoczesnych technologii.

W ramach badań przeanalizowano wykorzystywany współcześnie sprzęt, taki jak najpowszechniejsze urządzenia klienta bankowości elektronicznej – komputery, laptopy, tablety, smartfony, smartwatche (i inne urządzenia typu „smart"), sprzętowe portfele kryptowalutowe itp. a także bankomaty (ang. *Automated Teller Machine*, ATM), terminale płatnicze (ang. *Point of Sale*, POS), karty płatnicze i urządzenia służące do obrotu walutami wirtualnymi (tzw. *bitomaty* – nazwa pochodzi od ang. *bitcoin*, czyli najpopularniejszej kryptowaluty i *bankomatu*). Analiza poszerzona o wyniki badań

[9] P. Niczyporuk, A. Talecka, *Bankowość. Podstawowe zagadnienia*, Temida 2, Białystok 2011.

empirycznych (wywiadów z ekspertami) pozwoliła na wyróżnienie słabych i silnych stron tych rozwiązań.

W odniesieniu do najpowszechniej formy wykorzystania bankowości elektronicznej, a mianowicie transakcji opierającymi się na wykorzystaniu kart płatniczych, wskazano zestaw niezbędnych wymagań zgodnych ze standardem PCI DSS (ang. *Payment Card Industry Data Security Standard*), który stanowi podstawę zapewnienia spójnego poziomu bezpieczeństwa w instytucjach związanych z przetwarzaniem danych kart płatniczych:

I. Zbuduj i utrzymuj bezpieczną sieć:
   1. Zainstaluj i utrzymuj odpowiednią konfigurację zapory sieciowej, aby chronić dane posiadaczy kart.
   2. Nie używaj domyślnych haseł ani innych parametrów bezpieczeństwa ustawionych przez producentów.

II. Chroń dane posiadaczy kart:
   3. Chroń dane posiadaczy kart w trakcie ich przechowywania.
   4. Szyfruj transmisję danych posiadaczy kart w otwartych, publicznych sieciach.

III. Prowadź program zarządzania podatnościami:
   5. Używaj i regularnie aktualizuj oprogramowanie antywirusowe.
   6. Twórz i utrzymuj bezpieczne systemy i aplikacje.

IV. Zaimplementuj silne mechanizmy kontroli dostępu:
   7. Ogranicz dostęp do danych posiadaczy kart płatniczych tylko dla osób, które mają taką potrzebę biznesową.
   8. Przydziel użytkownikom systemu komputerowego unikalne identyfikatory.
   9. Ogranicz fizyczny dostęp do danych posiadaczy kart.

V. Regularnie monitoruj i testuj sieci:
   10. Kontroluj i monitoruj cały dostęp do zasobów sieciowych i danych posiadaczy kart.

11. Regularnie testuj systemy i procesy bezpieczeństwa.

VI. Utrzymuj politykę bezpieczeństwa informacji:

12. Utrzymuj politykę, która obejmuje bezpieczeństwo informacji.

Zauważono przy tym, iż w odniesieniu do klienta bankowości elektronicznej nie istnieje żaden zdefiniowany standard dotyczący wymagań bezpieczeństwa. Klienci muszą tutaj polegać na informacjach przekazywanych głównie przez banki, przy czym, należy zauważyć, że w niektórych przypadkach można odnieść wrażenie nadmiaru wymagań regulacyjno-informacyjnych, co ma negatywny skutek – istotne informacje znikają bowiem w szumie wskazówek, dobrych praktyk, wymagań i ostrzeżeń.

Poddano także identyfikacji i opisowi występujące podatności analizowanych rozwiązań. Podkreślono wagę podatności wynikających ze słabości ludzkiej natury wynikającej z naszej psychiki i wpływających na nią emocji.

W odniesieniu do płatności z wykorzystaniem kart płatniczych wskazano, iż mimo powszechnej w Europie tendencji do stosowania kart mikroprocesorowych (standard EMV), to na poziomie globalnym sytuacja jest jednak inna, zwłaszcza w przypadku krajów, które jeszcze nie dostosowały się do wymagań standardu EMV. W rezultacie wypłata środków z użyciem podrobionej karty wyposażonej w pasek magnetyczny możliwa jest na terenie takich właśnie państw, co ostatecznie stanowi poważny problem także dla europejskich wydawców kart płatniczych[10]. Stwierdzono na tym tle, że w przypadku smartfonów sytuacja nie jest jednorodna i np.: dla smartfonów z systemem Android w zależności od producenta możliwość regularnej aktualizacji nie jest oczywista, co wynika ograniczonego wsparcia technicznego.

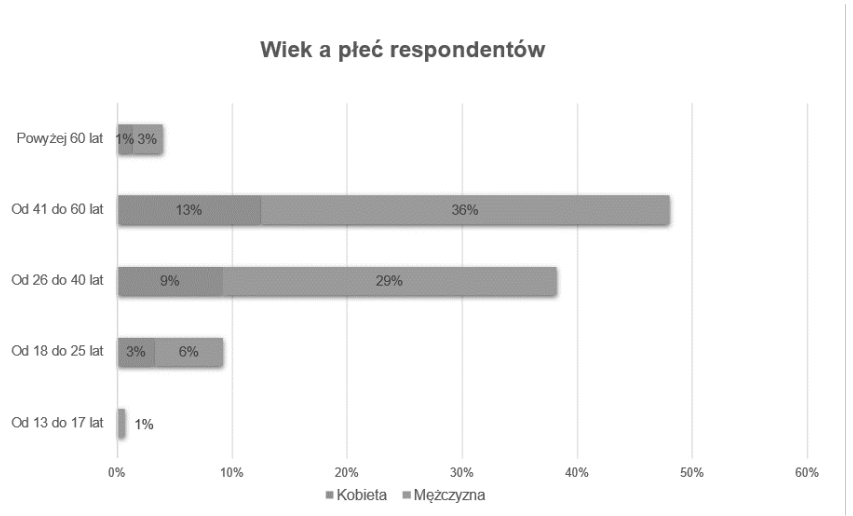
[10] Internet Organised Crime Threat Assessment (IOCTA) 2019, https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf, s. 38, stan z dn. 27 lipca 2021.

Zdiagnozowano, że niektórzy producenci, np. Samsung, oferują dużo dłuższy okres wsparcia technicznego i aktualizacji systemu.

W odniesieniu do dedykowanych aplikacji bankowych zdiagnozowano podatność, związaną z samym użytkownikiem, który mimo możliwości automatycznej aktualizacji z takiej możliwości, czasami świadomie, nie korzysta. Dodatkowo analiza pozwoliła na identyfikację słabości wynikającej z luzowania reguł bezpieczeństwa, np. rezygnację z SCA (ang. *Strong Customer Authentication* – silne uwierzytelnianie klienta), co w przypadku mniej świadomych użytkowników stwarza wysokie ryzyko oraz możliwość dokonywania zakupu bez potwierdzania kodem np.: BLIK w tzw. zaufanych sklepach.

W odniesieniu do prawidłowości i bezpieczeństwa przebiegu transakcji, zespół zidentyfikował szereg podatności. Do głównych zaliczyć należy: vishing" (od ang. *voice* i *phishing* – co oznacza odmianę ataku socjotechnicznego typu *phishing*, ale realizowaną za pomocą połączenia głosowego, np. telefonicznego), podatności systemów VoIP (ang. *Voice over IP* – systemy połączeń głosowych, które do transmisji wykorzystują sieci IP), które mogą być atakowane przez przestępców w celu przekierowania połączeń, manipulacje za pomocą wiadomości SMS (klienci bankowości z łatwością poddają się manipulacji, a przede wszystkim nie czytają dokładnie treści komunikatów SMS. W związku z tym zdarza się, że rozumieniu dyrektywy PSD2 silnie uwierzytelniają transakcję, która później jest przez nich kwestionowana.).

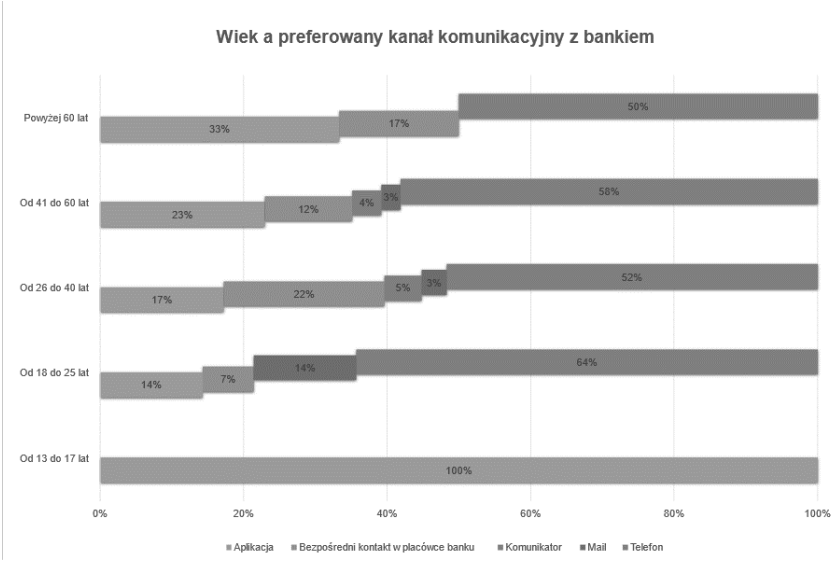
Przeprowadzone badania ankietowe, cenne źródło wiedzy na temat zarówno klienta bankowości elektronicznej jak i jego środowiska, pozwoliły zespołowi na diagnozę i analizę istotnych, założonych w badaniu kwestii. Nadmienić należy, iż dominującą grupą respondentów okazali się mężczyźni w wieku od 41 do 60 lat, w drugiej kolejności mężczyźni w wieku 26 do 40 lat. Również pośród kobiet przewagę uzyskała grupa wiekowa od 41 do 60 lat, a na drugim miejscu uplasowała się grupa wiekowa od 26 do 40 lat.



Wykres 1. Wiek a płeć respondentów.

W badanej grupie respondentów stwierdzono także zależność pomiędzy miejscem zamieszkania i wykształceniem. We wszystkich branych pod uwagę miejscach zamieszkania przeważającą grupą okazały się osoby z wykształceniem wyższym. W przypadku miast powyżej 100 tyś. mieszkańców to przewaga ponad 5-cio krotna.

Wyniki badań pozwalają dostrzec związek między preferowanym kanałem komunikacyjnym a wiekiem. Pomimo, że bezpośredni kontakt w placówce banku cieszy się najmniejszą popularnością wśród klientów w grupie wiekowej od 18 do 25 lat, to w całościowym ujęciu odpowiedzi przeczą obiegowemu stereotypowi, który głosi, że im starszy klient, tym większe preferencje, co do bezpośredniego kontaktu w placówce banku. Można tutaj postawić hipotezę, że rozkład odpowiedzi pomiędzy grupami wiekowymi wynika z faktu, iż grupa wiekowa od 26 do 40 lat podejmuje istotne decyzje związane np. z zaciąganiem kredytów hipotecznych w tym właśnie okresie życia, co przekłada się na preferencje w stosunku do wybieranej wówczas formy komunikacji z bankiem.



Wykres 2. Wiek a preferowany kanał komunikacyjny z bankiem

Poziom dojrzałości technologicznej klientów bankowości elektronicznej diagnozowano poprzez ustalenie preferencji nt. wagi wymagań bezpieczeństwa związanych z wykorzystaniem bankowości elektronicznej. Wskazane w pytaniu podstawowe zasady bezpieczeństwa znajdują silne zrozumienie wśród respondentów. Martwić jednak może, iż zarówno poprawki systemowe, jak i aktualność oprogramowania antywirusowego nie uzyskały zrozumienia i wskazane zostały jako „ważne". Eksperci, w toku prowadzonych wywiadów, wskazywali, że dojrzałość bankowości elektronicznej – w powszechnym odbiorze – jest wysoka, czego nie można jednak powiedzieć o dojrzałości jej użytkowników (klientów), jeżeli dojrzałość rozumieć tutaj nie jako świadomość zagrożeń, a realną odporność na nie. Niemniej dynamiczny rozwój technologii sprawia, że z punktu widzenia banków dojrzałość zdaje się rosnąć.

Wykres 3. Waga zagrożeń wg. respondentów (górna ćwiartka)

Respondenci w ramach badania wskazali ponadto, iż posiadają wiedzę jak szybko kontaktować się z bankiem, co świadczy o dobrym przygotowaniu i możliwości reakcji na różnego rodzaju zdarzenia, jakie mogą wpłynąć na bezpieczne funkcjonowanie w środowisku bankowości elektronicznej. Jak wynika z badania, niezależnie od płci, ponad 90% badanych zadeklarowało pełną wiedzę odnośnie szybkiego kontaktu z bankiem. Aż 83% respondentów z grupy wiekowej powyżej 60 lat potwierdziło, że zna adres mailowy lub numer telefoniczny używany do kontaktu z bankiem, w kolejnych grupach było to odpowiednio: 68% odpowiedzi w grupie wiekowej od 41 do 60 lat; 45% w grupie wiekowej od 26 do 40 lat; 36% w grupie wiekowej od 18 do 25 lat. W odniesieniu do kontaktu z przedstawicielem banku na pytanie „czy zostałeś poinformowany przez bank, jak będzie przebiegał kontakt z przedstawicielem banku?" zaobserwowano dużą liczbę odpowiedzi „nie" i „nie pamiętam".

W przypadku urządzeń mobilnych większość respondentów wskazała iż nie zna procedury postępowania w razie wymiany/utraty urządzenia mobilnego.

W odniesieniu do bezpieczeństwa danych sensytywnych, respondenci, niezależnie od płci, znali podstawowe zasady bezpieczeństwa i reguły komunikacji.

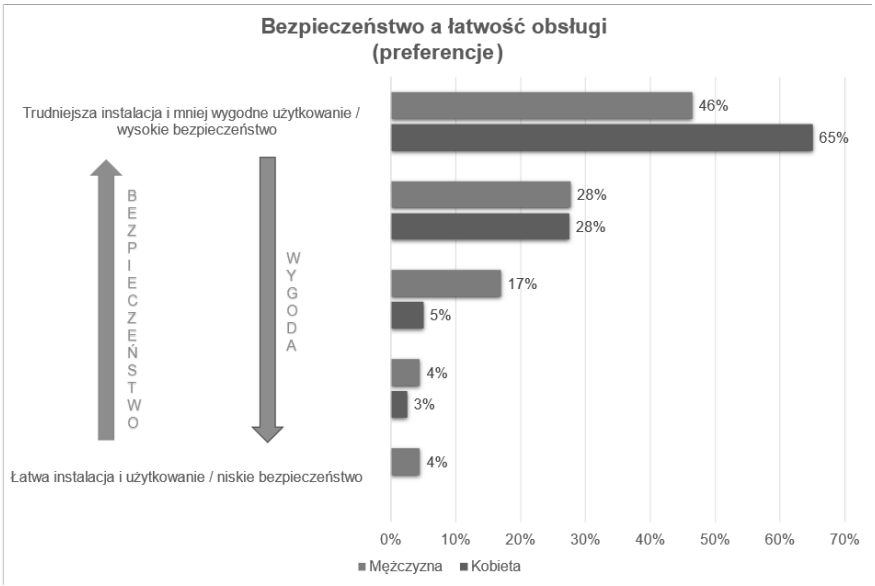
Eksperci zwracali jednak uwagę, że w powszechnym odczuciu raczej niewielu klientów bankowości w ogóle zapoznaje się z procedurami i niewielu czyta komunikację od banków informującą np. o tym, iż mamy do czynienia z jakimś nowym rodzajem ataków. Wszelkie tego typu informacje są często ignorowane jako element zakłócający dostęp w trybie pilnym do naszych środków płatniczych. Problem potęgują tutaj nieprofesjonalne biura obsługi klienta (BOK), których pracownicy często są niedostatecznie przeszkoleni, brak im wiedzy, doświadczenia, a w rezultacie często korzystają ze wsparcia II linii. Dostrzega się także wady w skryptach używanych podczas kontaktu z klientem, fakt pojawiania się sztampowych odpowiedzi nie popartych głębszą analizą zgłoszonego problemu. Odnośnie do procedur bezpieczeństwa jeden z ekspertów podkreślił, że jakakolwiek zgoda dotycząca bezpieczeństwa bankowości elektronicznej, którą wyraża klient, powinna być połączona ze świadomością dotyczącą zagrożeń. Przykładowym nieprawidłowym działaniem po stronie banków była sytuacja, w której przesyłano klientom karty zbliżeniowe, nie informując ich, czy są zainteresowani ich użyciem i nie przekazując kompletu informacji o zagrożeniach.

Wykres 4. Odpowiedź na pytanie: „jakich informacji nie może żądać od Ciebie przedstawiciel banku?" w zależności od płci

W efekcie nie każdy klient miał świadomość, że kradzież karty zbliżeniowej pozwala przestępcom na kradzież części środków pieniężnych (kiedyś do wysokości 50 PLN, obecnie do wysokości 100 PLN) – w przypadku typowej karty płatniczej dostatecznym zabezpieczeniem na okoliczność kradzieży jest kod PIN. W rzeczywistości kwota transakcji zbliżeniowych może przekroczyć limit 50 EUR – co oznacza, że do 50 EUR odpowiadać będzie klient, o ile nie zdążył zastrzec karty, a powyżej limitu 50 EUR odpowiadać będzie dostawca usługi płatniczej.

Istotną kwestią w czasie badania było ustalenie preferencji respondentów między bezpieczeństwem aplikacji bankowych, a łatwością ich użytkowania. Badani eksperci wskazują na systematyczny rozwój rozwiązań z

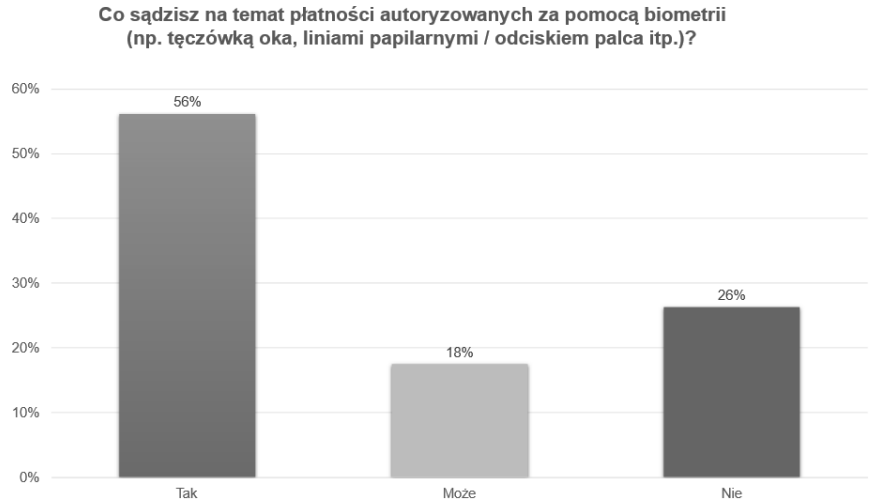
zachowaniem kompromisu pomiędzy ergonomią i bezpieczeństwem, przy czym sukcesu upatrują w ogólnych trendach środowiska i przyjętych kierunkach rozwoju. Na przestrzeni lat nowe rozwiązania stają się coraz łatwiejsze do wykorzystania, zaś w zakresie bezpieczeństwa korzystają z dopracowanych i wszechstronnie przetestowanych modułów odpornych na przełamanie zabezpieczeń. Większość użytkowników skłania się ku bezpieczeństwu aplikacji, co oznacza trudniejszą instalację i mniej wygodne użytkowanie w miarę, jak wzrasta poziom bezpieczeństwa. Innymi słowy dla bezpieczeństwa aplikacji użytkownicy są w stanie w bardzo dużym stopniu zrezygnować z wygody, czyli łatwości instalacji i użytkowania, które niosłyby za sobą niskie bezpieczeństwo.



Wykres 5. Rozkład preferencji odnośnie do bezpieczeństwa a wygody obsługi aplikacji bankowych z uwzględnieniem płci

W odniesieniu do narzędzi do płatności elektronicznych większość respondentów uznaje obecnie stosowane rozwiązania za łatwe w obsłudze, przy czym poziom zaufania rośnie wraz z powszechnością i ogólną znajomością rozwiązania (np. breloczki i naklejki w 85% mają niski poziom zaufania a smartfony cieszą się 93 % poziomem zaufania – odpowiednio 63% wysoki i 30% średni). Wśród produktów największą popularnością cieszą się szybkie przelewy przez serwis płatności (np. Przelewy24, PayU, Dotpay, tPay, eCard itd.) tzw. „Pay-by-Link", które wskazało 82% respondentów oraz płatności kartą (kredytową lub debetową) przy składaniu zamówienia, które wskazało 80% respondentów. Mniejszą popularnością cieszą się płatności BLIK, które wybrało 68% respondentów oraz przelewy tradycyjne (z wpisaniem numeru rachunku), które wybrało 64% respondentów. Na dalszych miejscach są odpowiednio płatności Google Pay (27% respondentów), płatności Apple Pay (21% respondentów), a najmniej rozpowszechnione wśród klientów są płatności aplikacją bankową realizowane z wykorzystaniem kodu QR (5% respondentów) i płatności SMS-em premium (3% respondentów). Największym zaufaniem respondentów cieszą się: przelew tradycyjny (74% odpowiedzi „zaufanie wysokie", 23% odpowiedzi „zaufanie średnie" i tylko 3% odpowiedzi „zaufanie niskie"); szybki przelew przez serwis płatności (68% odpowiedzi „zaufanie wysokie", 27% odpowiedzi „zaufanie średnie" i tylko 5% odpowiedzi „zaufanie niskie"); a wreszcie płatność BLIK, chociaż pojawia się już tutaj znaczący element braku zaufania (71% odpowiedzi „zaufanie wysokie", 15% odpowiedzi „zaufanie średnie" i aż 14% odpowiedzi „zaufanie niskie). Płatność kartą (kredytową lub debetową) obdarzona jest wysokim zaufaniem przez 58% respondentów, średnim zaufaniem przez 30% respondentów i niskim zaufaniem przez 12% respondentów. Ciekawym jest porównanie zaufania do płatności elektronicznych realizowanych za pomocą Apple Pay (37% odpowiedzi „zaufanie wysokie", 25% odpowiedzi „zaufanie średnie" i 38% odpowiedzi „zaufanie niskie") i Google Pay (35% odpowiedzi „zaufanie wysokie", 31% odpowiedzi „zaufanie średnie" i 33% odpowiedzi

„zaufanie niskie"). Obydwa produkty darzone są przez klientów podobnym poziomem zaufania z lekką przewagą Google Pay. Zdaniem respondentów najmniej godnymi zaufania produktami płatności elektronicznych są płatność SMS-em premium (14% odpowiedzi „zaufanie wysokie", 22% odpowiedzi „zaufanie średnie" i aż 64% odpowiedzi „zaufanie niskie") oraz płatność aplikacją bankową z wykorzystaniem kodu QR (18% odpowiedzi „zaufanie wysokie", 29% odpowiedzi „zaufanie średnie" i aż 52% odpowiedzi „zaufanie niskie"). W odniesieniu do możliwych nowych rozwiązań, które mogą być wprowadzone do środowiska klienta bankowości elektronicznej postawiono pytanie: „co sądzisz na temat płatności autoryzowanych za pomocą biometrii (np. tęczówką oka, liniami papilarnymi – odciskiem palca itp.?". Respondentów poproszono o udzielenie odpowiedzi w postaci krótkiej wypowiedzi pisemnej (komentarza). W oparciu o analizę treści wypowiedzi ustalono, że większość, bo aż 56% respondentów, wyraziła poparcie dla tego typu rozwiązań (wypowiedź sklasyfikowana jako odpowiedź „tak"), a 18% gotowa jest tego typu rozwiązania rozważyć (wypowiedź sklasyfikowana jako odpowiedź „może"). Nieprzychylnie wypowiedziało się 26% respondentów – nie są oni zainteresowani rozwiązaniami w zakresie bezpieczeństwa bankowości elektronicznej, które bazowałyby na biometrii (wypowiedź sklasyfikowana jako „nie").



Wykres 6. Zainteresowanie respondentów płatnościami autoryzowanymi za pomocą biometrii

W dalszej części pracy autorzy podjęli próbę wskazania kierunków rozwoju bankowości elektronicznej.

Jako główną przesłankę wskazano, iż kolejne etapy ewolucji bankowości wiążą się z przejściem od – charakterystycznej dla bankowości elektronicznej – dystrybucji wielokanałowej do dystrybucji omnikanałowej i realizacja koncepcji klientocentryczności, co stanowi fundament transformacji cyfrowej banków i ma prowadzić do powstania bankowości cyfrowej. Obok smartfonów, które wpłynęły na rozwój bankowości elektronicznej w odmianie mobilnej, należy podkreślić potencjał urządzeń ubieralnych i typu smart, które są jedną z sił napędowych transformacji cyfrowej. Tego typu rozwiązania są bowiem w stanie nie tylko tworzyć nowe kanały komunikacji z klientami, lecz także dostarczają dużej ilości danych na temat klientów, co w połączeniu z technologiami z obszaru Big Data (związanymi z przetwarzaniem wielkich zbiorów danych) wychodzi naprzeciw postulatowi klientocentryczności bankowości cyfrowej. Banki, które posiadają wiedzę i możliwości,

aby wykorzystać wielkie zbiory danych, wliczając w to dane transakcyjne, informacje z mediów społecznościowych, najróżniejsze formy korespondencji z klientami, będą uzyskiwać dużo większą wiedzę na temat działań i preferencji klientów i budować na tej wiedzy przewagę konkurencyjną[11].

W rozważaniach na temat przyszłości rozwiązań uwzględniono kryptowaluty, z których największą popularność uzyskał bitcoin (BTC), chociaż warto zwrócić uwagę także na ether, litheon, ripple i inne. Kryptowaluty stanowią instrument bardzo szeroko wykorzystywany przez uczestników rynków finansowych i indywidualnych inwestorów. Jednocześnie postrzegane są jako pieniądz przyszłości z uwagi na takie ich zalety, jak (rzekomy) brak presji inflacyjnej (typowej dla fiducjarnych jednostek pieniężnych, emitowanych przez współczesne banki centralne), wygoda i szybkość obsługi czy przejrzystość oraz bezpieczeństwo transakcji tymi jednostkami[12].

Jako kierunek rozwoju zdiagnozowano większe niż obecnie budowanie powiązań pomiędzy usługami płatniczymi, dzięki którym możliwe będzie płynne i automatyczne przekierowanie klienta za pośrednictwem zaufanego kanału z jednego serwisu do drugiego. Podstawowym założeniem jest, aby tego typu operacja nie wymagała dodatkowego logowania przy przekierowaniu, np. w momencie, kiedy klient zamierza dokonać przelewu. Osiągnięcie takiego stanu rzeczy możliwe będzie przy wykorzystaniu federalizacji usług i federalizacji zarządzania tożsamością, dzięki którym klient uzyska możliwość wykonania różnych działań – nie tylko działań w swojej usłudze bankowej, lecz także w innych, potrzebnych mu usługach. Taki kierunek rozwoju

[11] Raport Big Data w bankowości, https://www.zbp.pl/getmedia/eb647392-2e7f-48fd-8bbd-4803d0d84dec/Raport_BD_1411_final, ZBP, stan z dn. 8 sierpnia 2021, s. 4.

[12] P. Marszałek, Kryptowaluty – pojęcie, cechy, kontrowersje, Studia BAS, nr 1(57)/2019, s. 107.

wydaje się doskonale spełniać postulat klientocentryczności w zakresie dostępności usług „tu i teraz". W tym kontekście należy jednak przywołać koncepcję *Zero Trust* („zero zaufania" lub „brak zaufania" – tł. własne). Oznacza ona, że nie należy ufać niczemu wewnątrz, bądź na zewnątrz naszego otoczenia, a dodatkowo ograniczać sloty czasowe trwania transakcji, które nie powinny być otwarte zbyt długo. Wskazano na potrzebę ograniczeń z jednoczesnym monitorowaniem sesji. Ustalono, że rozwiązania oparte o biometrię (np. żądanie użycia odcisku palca lub wskazanie twarzy) nie stanowią dla klienta dużego obciążenia, a jednoczenie wychodzi naprzeciw oczekiwaniom związanym z komfortem wykorzystania bankowości elektronicznej. Należy w tym miejscu zaznaczyć, iż dyrektywa PSD2 (ang. *Payment Services Directive*)[13], która weszła w życie w dniu 13 stycznia 2016 r. zmieniła dotychczasową działalność dostawców usług płatniczych, w szczególności banków, w kierunku modelu tzw. otwartej bankowości (ang. *Open Banking*) co implikuje nowy rodzaj dostępu do rachunków płatniczych, ponieważ uprawnione *podmioty trzecie* (ang. *Third Party Provider, TTP*) mogą w imieniu i za zgodą klienta uzyskać dostęp do informacji o rachunku lub zlecać realizację płatności[14]. Dzięki temu TPP są w stanie świadczyć usługi dodatkowe w kooperacji z bankiem. Ustalono, że Integracja banków z TTP – w myśl idei otwartej bankowości i dyrektywy PSD2 – możliwa jest dzięki udostępnianiu API (ang. *Application Programming Interface* – interfejs programistyczny aplikacji). Istotnym kryterium jest tutaj standaryzacja tego typu interfejsów, warto więc

[13] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32015L2366&from=PL, stan z dn. 8 sierpnia 2021.

[14] K. Leżoń, *Otwarta bankowość w świetle wymogów dyrektywy PSD2 - wyzwania i perspektywy rozwoju dla polskiego sektora FinTech*, KNF, Warszawa 2019, s. 16.

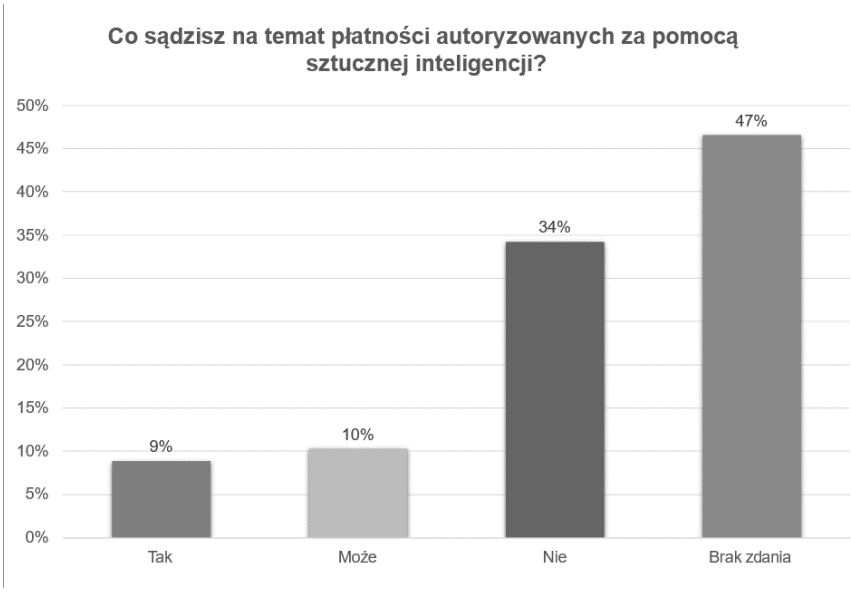
wyróżnić projekt *PolishAPI* – polski standard, który definiuje interfejs na potrzeby usług świadczonych przez strony trzecie w oparciu o dostęp do rachunków płatniczych. Twórcy standardu zakładają jego stały rozwój w odpowiedzi na zmiany regulacyjne, technologiczne i biznesowe na rynku polskim oraz europejskim. Zmiany będą publikowane jako kolejne wersje specyfikacji standardu PolishAPI. Uczestnikami projektu są Związek Banków Polskich wraz ze stowarzyszonymi bankami komercyjnymi i spółdzielczymi, Spółdzielcze Kasy Oszczędnościowo-Kredytowe, Polska Organizacja Niebankowych Instytucji Płatności wraz ze stowarzyszonymi firmami, Polska Izba Informatyki i Telekomunikacji, Polska Izba Ubezpieczeń, Krajowa Izba Rozliczeniowa, Biuro Informacji Kredytowej i Polski Standard Płatności[15].

Innym, wspomnianym już kierunkiem jest nieuchronne wykorzystanie Big Data wraz z zaawansowanymi algorytmami przetwarzania, które nie tylko ograniczy się tylko do profilowania klienta w celu dopasowania optymalnej oferty a rozszerzy swoje zastosowanie do działań pozwalających na wykrywać anomalie w zachowaniu płatnika będącego jednocześnie użytkownikiem platformy społecznościowej (np. Facebook) w celu ochrony jego środków finansowych (analiza behawioralna). Rozwiązanie takie, w przypadku wykrycia anomalii, może zablokować wykonanie podejrzanych działań np. transakcji. Jest też w stanie „uczyć się" zachowań typowych dla chronionego użytkownika. Należy jednak podkreślić, że w żadnym wypadku sztuczna inteligencja nie powinna być wykorzystywana w taki sposób, aby odbierać człowiekowi autonomii decyzji – ma wspierać ludzi, ale nie ich zastępować. W czasie badania postawiono pytanie: „Co sądzisz na temat płatności autoryzowanych za pomocą sztucznej inteligencji?". Respondenci ankiety odpowiadali na pytanie w postaci krótkiej wypowiedzi – komentarza. Z analizy

[15] *O PolishAPI*, https://polishapi.org/, stan z dn. 8 sierpnia 2021.

udzielonych odpowiedzi wynika, że większość respondentów (47%) przychyla się do odpowiedzi „brak zdania". W drugiej kolejności pojawiły się odpowiedzi kategorycznie odrzucające tego typu pomysł.

Obserwacja stanu faktycznego, jeżeli chodzi o częstotliwość i rodzaj incydentów związanych z środowiskiem bezpieczeństwa klientów bankowości elektronicznej, skłaniała ekspertów do postawienia wniosku, iż wysoki poziom świadomości zagrożeń nie niesie za sobą realnej odporności. W czasie analizy zwrócono uwagę, że zagrożenia związane z fałszywym kontaktem są w rzeczywistości wariacją uniwersalnego scenariusza, w którym przestępca podszywa się pod dowolną osobę, działającą w określonym kontekście sprzyjającym uwiarygodnieniu podejmowanych czynności, celem zmuszenia ofiary do przekazania swoich środków finansowych. Przestępcy dostosowują bowiem uniwersalny scenariusz do potrzeb chwili i określonej kategorii ofiar. Istotny wydaje się fakt, że chociaż aż 91% respondentów jest świadoma zagrożenia związanego z fałszywym kontaktem od pracownika banku, to – zdaniem ekspertów – właśnie przestępstwa oparte na podszywaniu się pod pracowników banku biją dziś rekordy popularności i okazują się skuteczne.



Wykres 7. Zainteresowanie respondentów płatnościami autoryzowanymi za pomocą sztucznej inteligencji

Obecnie jest to jeden z najpopularniejszych wektorów ataków, można więc przyjąć, że istnieje duża podatność po stronie klientów w tym zakresie. Dodatkową kwestią, którą warto poruszyć w kontekście otrzymanych wyników, jest zagadnienie faktycznego poziom zaawansowania socjotechniki przestępczej.

Dyskusja

Część diagnostyczna badania potwierdziła, że bankowość elektroniczna jest otwarta na innowacje, co pociąga za sobą projektowanie i dostarczanie nowych produktów i usług. Możliwości technologiczne stają się

głównym wyróżnikiem dla banków, jeśli chodzi o poprawę satysfakcji klientów. Konsekwencją szybkiego włączania nowych technologii i zaspokajania potrzeb klientów jest ogromne wyzwanie w obszarach architektury rozwiązań teleinformatycznych i cyberbezpieczeństwa.

Fundamentalną kwestią w zapewnieniu bezpieczeństwa bankowości elektronicznej jest przestrzeganie przyjętych standardów bezpieczeństwa. Zdiagnozowanym w badaniu, głównym zagrożeniem bankowości elektronicznej jest socjotechnika. Warto w tym kontekście zwrócić większą uwagę na uwierzytelnianie z wykorzystaniem tokenów wspierających standard U2F, aplikacji uwierzytelniających, ale także, po stronie banków, na monitoring behawioralny zachowania klienta.

Z badania klientów bankowości elektronicznej i wywiadów eksperckich wynika, że dojrzałość bankowości elektronicznej – w powszechnym odbiorze – jest wysoka. Dojrzałość użytkowników (klientów), rozumiana jako świadomość zagrożeń, deklaratywnie jest również wysoka, niestety realna odporność na nie już taka nie jest. Oznacza to, że banki muszą upewnić się, że nie tylko przekazują stosowną informację o zagrożeniach i właściwej reakcji na nie swoim klientom, lecz także powinny zweryfikować, czy informacja taka zostanie zapamiętana. Warto również zwrócić uwagę, że deklaratywnie klienci preferują bezpieczeństwo kosztem łatwości użytkowania, co kontrastuje z opiniami ekspertów.

Należy przyjąć, że na bezpieczeństwo klienta bankowości elektronicznej wpływają przede wszystkim: ewolucyjne zmiany technologiczne, większa transparentność, większa łatwość użytkowania (ergonomia), jak najmniej elementów wymagających uczenia się od klienta-użytkownika i odpowiednia komunikacja dotycząca zasadności oraz celowości wprowadzania zmian.

Sugerowany kierunek rozwoju, który wychodziłby naprzeciw postulatom klientocentryczności i omnikanałowości, wiąże się z powstaniem zintegrowanych platform typu „elektroniczne okienko bankowe". Powinno ono

pokrywać w kanałach elektronicznej komunikacji ofertę banków w sposób całościowy. Co jednak kluczowe, musi pozwalać na taki poziom silnego uwierzytelniania i autoryzacji, który nie pozwoli na późniejsze podważenie faktu dokonania jakiejś operacji.

Klienci, jak i eksperci wskazywali, że właściwym kierunkiem podnoszenia bezpieczeństwa bankowości elektronicznej jest szersze wykorzystanie biometrii. Znacznie mniej akceptacji, głównie z uwagi na wnoszenie nowych zagrożeń, znajduje stosowanie sztucznej inteligencji.

Jednocześnie należy mieć świadomość, że transformacji cyfrowej ulega obszar przestępczości bankowej. Nowoczesne technologie, które znajdują się w obszarze zainteresowania banków, pozostają także do dyspozycji przestępców – niosą więc nie tylko korzyści, ale także ryzyko, które należy uwzględniać podczas podejmowania decyzji strategicznych dotyczących włączenia danego rozwiązania do bankowego portfolio techniczno-technologicznego.

Wnioski

Na wstępie warto przywołać komentarz jednego z ekspertów: *choć sektor bankowy generalnie oceniany jest jako wiodący w obszarze cyberbezpieczeństwa, to jest jednak niejednorodny. Są banki bardzo zaawansowane we wdrażaniu najlepszych standardów i dobrych praktyk, posiadają odpowiednie możliwości finansowe, pozwalające na wdrażanie odpowiednich zasobów IT, kadr i procesów, ale są też banki, które dokładnie z tych samych względów finansowych nie mogą sobie na to pozwolić. Jeśli do tego dodamy dużą konkurencję na rynku międzybankowym oraz konkurowanie banków z innymi podmiotami wchodzącymi na rynek usług płatniczych, a także niską świadomość klientów w zakresie bezpiecznego korzystania z usług płatniczych, to wówczas nasze pierwsze wrażenie może okazać się zbyt optymistyczne*.

Szczegółowa analiza zebranego materiału pozwala na sformułowanie szeregu rekomendacji, które w ocenie autorów przyczynią się do wzmocnienia bezpieczeństwa, podniesienia ergonomii i zwiększenia funkcjonalności jakie pozostają do dyspozycji klienta bankowości elektronicznej i jednocześnie pozwolą na zbudowanie odpowiedniego środowiska przez szeroko rozumianą stronę bankową.

W odniesieniu do warstwy pojęciowej:

- Podjęcie prac nad ujednoliceniem warstwy pojęciowej poprzez przyjęcie obowiązującego (w tym tłumaczenia) zwrotów i terminów z zakresu bezpieczeństwa i organizacji środowiska bankowości elektronicznej.

W odniesieniu do architektury rozwiązań:

- Sugerowany kierunek rozwoju to spełnienie postulatu klientocentryczności i omnikanałowości, wiąże się z powstaniem zintegrowanych platform typu „elektroniczne okienko bankowe". Powinno ono pokrywać w kanałach elektronicznej komunikacji ofertę banków w sposób całościowy. Co jednak kluczowe, musi pozwalać na taki poziom silnego uwierzytelniania i autoryzacji, który nie pozwoli na późniejsze podważenie faktu dokonania jakiejś operacji.
- Budowa ekosystemu sprzyjającego bezpieczeństwu finansów elektronicznych – postulat budowy systemu składającego się z banków, instytucji finansowych, organów kontrolnych i nadzorujących, takich jak np. Komisja Nadzoru Finansowego (KNF) w Polsce, które wspólnie będą kooperować na rzecz bezpieczeństwa finansów elektronicznych.
- Kultura bankowości elektronicznej nie powinna być budowana przez każdy bank osobno, aby klienci nie zaczęli się gubić w rozmaitości pojęć, zasad i standardów. Wydaje się, że rolę lidera

mógłby pełnić tutaj Związek Banków Polskich – ma to być bowiem kultura bankowości elektronicznej, a nie kulturze bankowości elektronicznej określonego banku.

W odniesieniu do szeroko rozumianego bezpieczeństwa:

- Wdrożenie rozwiązania typu „KLIENT MÓWI: STOP!" – pozwalającego klientowi na natychmiastowe zablokowanie niechcianej transakcji w dowolnym momencie.
- Podniesienie poziomu i zakresu współpraca oraz usprawnienie komunikacji pomiędzy Policją a bankami.
- Odejście od transakcji realizowanych z użyciem połączeń telefonicznych.
- Wymuszenie instalacji na urządzeniach klientów oprogramowania zabezpieczającego, które będzie prowadziło monitoring behawioralny.
- Wykrywanie podatności na urządzeniach końcowych – wdrażanie i dalszy rozwój rozwiązań, które służą do wykrywania podatności na urządzeniach końcowych (komputer PC, laptop, tablet lub smartfon) – np. wykrywanie obecności na urządzeniu klienta oprogramowania typu AnyDesk lub TeamViewer, które przekazuje kontrolę nad pulpitem ofiary do osoby trzeciej (przestępcy).
- Lepsza kontrola nad płatnościami zbliżeniowymi realizowanymi z użyciem aplikacji mobilnych – Banki nie powinny zezwalać na dokonywanie płatności zbliżeniowych za pomocą aplikacji mobilnych, jeżeli nie zostanie zdjęta blokada ekranu urządzenia (np. za pomocą kodu PIN lub odcisku palca). Z kolei w przypadku, kiedy blokada ekranu na urządzeniu nie jest aktywna, aplikacja mobilna nie powinna w ogóle działać.

- Szersze użycie rozwiązań opartych o tokeny – wykorzystanie generatorów tokenów, takich jak np. Google Authenticator i Microsoft Authenticator, co pozwoli odejść od stałego atrybutu bezpieczeństwa (np. stałe, niezmieniane hasło).
- Udostępnienie dzienników operacji wykonywanych na koncie dla klientów – użytkownik powinien mieć możliwość sprawdzenia historii (dziennika) operacji wykonywanych na jego koncie, np. aby sprawdzić fakt logowania się z innych urządzeń niż zwykle przez niego używane, sprawdzić dane dotyczące uwierzytelniania i autoryzowania transakcji itd.
- Wprowadzenie okresów przejściowych dla nowych rozwiązań – okres przejściowy ma klientom dać szansę, aby przystosowali się do zmiany.

W odniesieniu do klienta bankowości elektronicznej:

- Prowadzenie spójnej i jednolitej polityki informacyjnej na poziomie rodzajów usług.
- Wprowadzenie aktywnych form przekazu, pozwalających na wdrożenie efektywnych kanałów komunikacji o zagrożeniach i sposobach przeciwdziałania im.

Przedstawione rekomendacje, potwierdzone w zgromadzonym materiale badawczym, stanowić winny podstawę pogłębionej analizy tych wszystkich, którzy mają realny wpływ na kształt środowiska klienta bankowości elektronicznej. Autorzy pokładają nadzieję, że wskazówki te znajdą zastosowanie w już istniejących a także nowych, projektowanych usługach.

Bibliografia

1. Apanowicz J., *Metodologia nauk*, Wyd. Dom Organizatora, Toruń 2003.

2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE.
3. Gruszczyński L.A., *Elementy metod i technik badań socjologicznych*, Tychy 2002.
4. Gruszczyński L.A., *Kwestionariusze w socjologii*, Katowice 2003.
5. Internet Organised Crime Threat Assessment (IOCTA) 2019, https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf, s. 38, stan z dn. 27 lipca 2021.
6. Jagiełło Z., *Bankowość detaliczna w obecnych warunkach rynkowych. Kierunki rozwoju*, [w:] *Wyzwania bankowości detalicznej*, pod red. Z. Jagiełło, Instytut Badań nad Gospodarką Rynkową – Gdańska Akademia Bankowa, Gdańsk 2015.
7. Leżoń K., *Otwarta bankowość w świetle wymogów dyrektywy PSD2 - wyzwania i perspektywy rozwoju dla polskiego sektora FinTech*, KNF, Warszawa 2019.
8. Marszałek P., *Kryptowaluty – pojęcie, cechy, kontrowersje*, Studia BAS, nr 1(57)/2019.
9. Niczyporuk P., Talecka A., *Bankowość. Podstawowe zagadnienia*, Temida 2, Białystok 2011.
10. O PolishAPI, https://polishapi.org/, stan z dn. 8 sierpnia 2021.
11. Raport Big Data w bankowości, https://www.zbp.pl/getmedia/eb647392-2e7f-48fd-8bbd-4803d0d84dec/Raport_BD_1411_final, ZBP, stan z dn. 8 sierpnia 2021.
12. Rehfisch M., 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.

13. Rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32015L2366&from=PL, stan z dn. 8 sierpnia 2021.

Abstract

STRENGTHENING SECURITY OF ELECTRONIC BANKING CLIENTS IN THE LIGHT OF RESEARCH CONDUCTED

Summary: The chapter presents the results of the project "Security environment for e-banking customers". It presents the methods and research tools used to achieve the objectives of the project - to identify the solutions used and associated risks, the characteristics of customers and to determine the direction of development in the field of e-banking. The most important results of empirical research - surveys and extended expert interviews - are presented. Recommendations are presented in the field of solution architecture and security of e-banking environment.

Keywords: security, cybersecurity, e-banking, e-banking customer, crimes against banks and their customers, evolution of banking, vishing, phishing, digital transformation

.

Rozdział 3

Zwalczanie nielegalnych działań w zakresie pośredniczenia w transakcjach finansowych przez zorganizowane grupy przestępcze wykorzystujące mechanizm zdalnego pulpitu. Modus operandi działania sprawców

Marta STECIAK[1], Piotr SZYMAŃSKI[2],
Kamil BOROSZKO[3]

STRESZCZENIE: Rozdział został poświęcony charakterystyce i skali zjawiska przestępstw związanych z nielegalnym działaniem podmiotów oferujących usługi w zakresie pośredniczenia w transakcjach finansowych, a także przedstawieniu procedury, która powinna być w tym zakresie przeprowadzona w ramach czynności procesowych realizowanych z udziałem osób pokrzywdzonych oraz w fazie in rem postępowania przygotowawczego. Opracowanie posłużyć ma zarówno celom poznawczym, jak i zaproponowaniu schematu postępowania w trakcie podejmowanych czynności procesowych, celem stworzenia skutecznego systemu zapobiegania tego typu nadużyciom, a tym samym zwalczania nieuczciwych praktyk w tym zakresie. Celem niniejszego opracowania nie jest zatem

[1] Prokurator delegowany do Podkarpackiego Wydziału Zamiejscowego Departamentu Do Spraw Przestępczości Zorganizowanej i Korupcji Prokuratury Krajowej w Rzeszowie.

[2] Naczelnik Wydziału Do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Rzeszowie.

[3] Koordynator Zespołu Dochodzeniowo–Śledczego Wydziału Do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Rzeszowie, kamil.boroszko@rz.policja.gov.pl.

analiza wszystkich czynów zabronionych określanych mianem cyberprzestępczości, lecz przedstawienie sposobów i środków działania cyberprzestępców w zakresie oszustw związanych z inwestowaniem na „platformach inwestycyjnych",
a także wskazanie na pewne rozwiązania w obrębie gromadzenia informacji i dowodów winy sprawców owych czynów, w tym szczegółowego opisu ich struktury przestępczej
i utworzonej na ten cel infrastruktury.

SŁOWA KLUCZOWE: zorganizowana grupa przestępcza, cyberprzestępczość, cyberbezpieczeństwo, inwestycje finansowe, platformy inwestycyjne.

Wstęp

Aktualna sytuacja związana z trwającą pandemią COVID-19, na wiele sposobów oddziałuje niemal na wszystkie sektory gospodarki. W znacznym stopniu uderza także w rynki finansowe, a tym samym ma wpływ m.in. na decyzje obywateli w zakresie lokowania swoich środków pieniężnych. Z jednej strony, w warunkach niepewności, naturalnym wydaje się, że inwestorzy chętniej podejmują działania mniej ryzykowne, choć przez to jednocześnie mniej zyskowne. Z drugiej zaś strony, ratowanie gospodarki i decyzje w zakresie obniżki stóp procentowych (spadek oprocentowania lokat bankowych czy też bezpiecznych aktywów państwowych) powoduje, iż inwestorzy zaczynają rozglądać się za bardziej intratnymi rozwiązaniami lokowania swoich środków. Rozwijający się rynek usług i produktów finansowych daje w tym zakresie coraz to większe możliwości. Jednocześnie jego uczestnicy są coraz bardziej narażeni na złożone ryzyko inwestowania, a także ryzyko wyłudzeń i oszustw. Jak wynika z raportu EY i Związku Przedsiębiorstw Finansowych, w dobie pandemii - pracy zdalnej, ograniczonego funkcjonowania placówek stacjonarnych oraz przeniesienia większości aktywności do świata

wirtualnego, klienci instytucji finansowych są bardziej skłonni do podejmowania ryzykownych zachowań konsumenckich[4]. Brak wystarczającej ochrony danych, nieintencjonalne udostępnianie loginów lub haseł i inne nieostrożne decyzje konsumenckie, stanowią z kolei doskonałą okazję dla oszustów, którzy często manipulując swoimi ofiarami, sięgają po coraz to skuteczniejsze metody i sposoby, aby wyłudzić ich oszczędności.

Mechanizmów oszustw finansowych jest bardzo wiele. Jednym z nich są oszustwa z użyciem funkcji zdalnego pulpitu. Charakter oraz sposób działania sprawców w zakresie pośredniczenia w transakcjach finansowych wykorzystujących mechanizm zdalnego pulpitu, dowodzi utworzeniu i istnieniu w tym celu wewnętrznych struktur organizacyjnych malwersantów. Działalność zorganizowanych grup przestępczych zajmujących się przedmiotowym procederem, doskonale wpisuje się w orzecznictwo sądowe w tym zakresie, bowiem wskazuje na trwałość oraz istniejące więzy organizacyjne w ramach wspólnego porozumienia, planowanie przestępstwa przez jej członków, akceptacji celów, trwałość zaspokojenia potrzeb grupy oraz skoordynowanego sposobu działania.[5]

Rozmiar i obserwowane tendencje nielegalnych działań zorganizowanych grup przestępczych w zakresie oszustw związanych z inwestowaniem, stanowią realny sprawdzian dla formacji powołanych do walki z cyberprzestępczością oraz struktur Prokuratury Krajowej zajmującej się przestępczością

[4] Raport z badania EY i Związku Przedsiębiorstw Finansowych, Nadużycia w sektorze finansowym, edycja 2020, [z:] https://assets.ey.com/content/dam/ey-sites/ey-com/pl_pl/news/2020/10/ey-raport-naduzycia-2020.pdf, z dnia 12.11.2021.

[5] Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 11 grudnia 2019 r., sygn. II AKa 271/19.

zorganizowaną, ale także dla obowiązującego prawa karnego, które, aby skutecznie przeciwdziałać temu niekorzystnemu zjawisku, wymaga zmian. Niezbędnym jest tworzenie nowych rozwiązań, dostosowywanie prawa do pojawiających się potrzeb będących naturalnym efektem rozwoju nowych technologii, czy też przyjęcia jednolitych rozwiązań prawnych w ustawodawstwie jak największej liczby państw. Brakuje bowiem jednolitych reguł postępowania oraz unormowania podstawowych kwestii, takich jak jurysdykcja czy sposób zarządzania cyberprzestrzenią.[6] Działania te zdecydowanie ułatwiłoby walkę z cyberprzestępcami. Sprawy bowiem związane z przestępczością w Internecie często wykraczają poza jurysdykcję prawa krajowego. Dodatkowo, konieczne jest zaangażowanie i wyposażenie w odpowiednią wiedzę oraz narzędzia służby i instytucje działające na rzecz walki z cyberprzestępczością, tak aby zwiększyć skuteczność rozpoznawania i wykrywania sprawców, a także gromadzenia informacji i dowodów winy owych zabronionych czynów.

Niniejsze opracowanie ma na celu zaproponowanie schematu postępowania w trakcie podejmowanych czynności procesowych, celem stworzenia skutecznego systemu zapobiegania nadużyciom, a tym samym zwalczania nieuczciwych praktyk w zakresie pośredniczenia w transakcjach finansowych przez zorganizowane grupy przestępcze. Celem opracowania jest także zaprezentowanie sposobów i środków działania cyberprzestępców w zakresie oszustw związanych z inwestowaniem na „platformach inwestycyjnych", a także wskazanie na pewne rozwiązania w obrębie gromadzenia informacji i dowodów winy sprawców owych czynów, w tym szczegółowego opisu ich struktury przestępczej i utworzonej na ten cel infrastruktury. Wskazanie na

[6] Worona, J., Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy, Wolters Kluwer, Warszawa 2020, s. 20.

możliwe rozwiązania w zakresie omawianej w niniejszym rozdziale problematyki, wymagało zdobycia praktyki i doświadczenia w tym zakresie, a także analizy opracowań teoretycznych - studiów literatury krajowej i zagranicznej, analizy aktów prawnych oraz dokumentów tworzonych przez podmioty zajmujące się zagadnieniami występującymi w cyberprzestrzeni. Punktem wyjścia dla omawianej problematyki jest charakterystyka zjawiska przestępczości zorganizowanej wykorzystującej mechanizm zdalnego pulpitu, szczególnie w zakresie przestępstw ukierunkowanych na inwestycje na rynku finansowym - forex, kryptowalut, a przy tym rola i zadania organów ścigania z chwilą podjęcia walki z tym procederem, czemu poświęcona została pierwsza część opracowania. Rozważania nad ww. kwestiami stanowią wprowadzenie do analizy zagadnień mających znaczenie praktyczne: poznanie sposobów działania przestępców i środków, jakie stosują w zakresie oszustw, a także omówienia struktury przestępczej, jej hierarchii, organizacji i podziału zadań poszczególnych jej struktur. W opracowaniu zaproponowano procedurę postępowania w ramach czynności procesowych - w zakresie przesłuchania osób pokrzywdzonych oraz poszczególnych czynności śledztwa, czemu poświęcono kolejne części rozdziału. Wskazane w opracowaniu rozwiązania, mogą przyczynić się do zwiększenia efektywności działań w zakresie skutecznego przeciwdziałania cyberprzestępczości w omawianym zakresie.

Modus operandi przestępczości zorganizowanej wykorzystującej mechanizmu zdalnego pulpitu

Proceder wykorzystania mechanizmu zdalnego pulpitu w przestępczości zorganizowanej, najczęściej polega na przekonaniu ofiary przestępstwa do zainstalowania programu, który pozwala oszustom na zdalne przejęcie kontroli nad komputerem. Dzieje się to np. pod pozorem organizowanego

„szkolenia" z platformy inwestycyjnej, za pośrednictwem której można uzyskać pokaźne zyski albo np. pod pozorem kontaktu przedstawiciela banku czy biura maklerskiego, w którym klient ma rachunek. Wykorzystując zaufanie klientów, oszuści przejmują kontrolę nad ich komputerem i dokonują korzystnych dla siebie transakcji. Przestępcy do czynu zabronionego, wykorzystują najczęściej tzw. środowiska "platform inwestycyjnych" o różnych nazwach marketingowych, które w większości przypadków zostają zbieżne z ich adresami https://, poprzez które są identyfikowane w sieci Internet. Pokrzywdzeni będąc przekonani, że otwierają na wskazanych stronach internetowych autentyczne konta umożliwiające samodzielne inwestowanie, w rzeczywistości otwierają fikcyjne konta inwestycyjne, zarządzane w rzeczywistości przez oszustów. Nabór osób zainteresowanych inwestycjami na fałszywych platformach odbywa się najczęściej wedle powtarzającego się schematu.

W pierwszej kolejności, następuje kontakt oszusta z potencjalną ofiarą, która mogła, ale nie musiała wykazywać zainteresowania tematem inwestycji w sieci. Sprawcy korzystają przy tym często z dostępnych baz kontaktowych udostępnionych w Internecie (tzw. *„wycieki danych").* Gdy mamy do czynienia z osobą zainteresowaną tematem inwestycji, która korzysta z forów inwestycyjnych, w tym grup społecznościowych utworzonych na portalach społecznościowych, kontakt może nastąpić poprzez tzw. „lidera" zajmującego się np. rynkiem Forex czy kryptowalutami, który oferuje swoją pomoc przy inwestowaniu pieniędzy, zapewniając jednocześnie o możliwości szybkiego i łatwego zysku. Na tym etapie, pokrzywdzonemu często przedstawiane są materiały (artykuły, opracowania itp.), których treść niesie za sobą możliwości uzyskania wysokich zysków w krótkim horyzoncie czasowym. Niejednokrotnie sprawcy posiadają wiedzę na temat aktualnie zaistniałego wydarzenia mającego wpływ na opinię publiczną. Potrafią powoływać się na instytucje publiczne lub znane osoby, w celu uwiarygodnienia swoich zamiarów bądź odwrotnie – w celu wywarcia wpływu na psychikę inwestora, co ma na celu wzbudzenie w nim obawy przed zablokowaniem intratnej inwestycji,

w której właśnie uczestniczy przez instytucje państwa zajmujące się nadzorem rynku finansowego.

Udostępnienie danych osobowym pokrzywdzonego, takich jak imię i nazwisko, adres e-mail czy numer kontaktowy, umożliwia kontakt przestępcy z pokrzywdzonym i następuje z chwilą wypełnienia formularza kontaktowego na jednej ze stron internetowych, która powiązana jest z „platformą inwestycyjną". Po nawiązaniu kontaktu z pokrzywdzonym, sprawca często identyfikuje się nazwą platformy, którą reprezentuje w celu uwiarygodnienia i spoufalenia się z poszkodowanym. Na tym etapie, oszuści intensyfikują działania i kontakt z klientem. Stają się oni bardziej zaangażowani, często wywierają presję na klientów, strasząc ich stratami lub krótkimi terminami na podjęcie decyzji inwestycyjnej. Z chwilą połączenia sprawcy prowadzą często długie rozmowy z pokrzywdzonymi, jednocześnie mając wiedzę na temat aktualnej sytuacji rynkowej, namawiają pokrzywdzonego do konkretnej inwestycji na rynku forex, w metale szlachetne, akcje spółek giełdowych czy kryptowaluty. Relacja sprawca-pokrzywdzony przyjmuje również często charakter koleżeńskiej znajomości i niestety jednostronnego zaufania, którym pokrzywdzony obdarza swojego menagera, w rzeczywistości będącego w strukturach zorganizowanej grupy przestępczej człowieka, mającego wyłącznie na celu doprowadzenie do niekorzystnego rozporządzenia mieniem pokrzywdzonego.

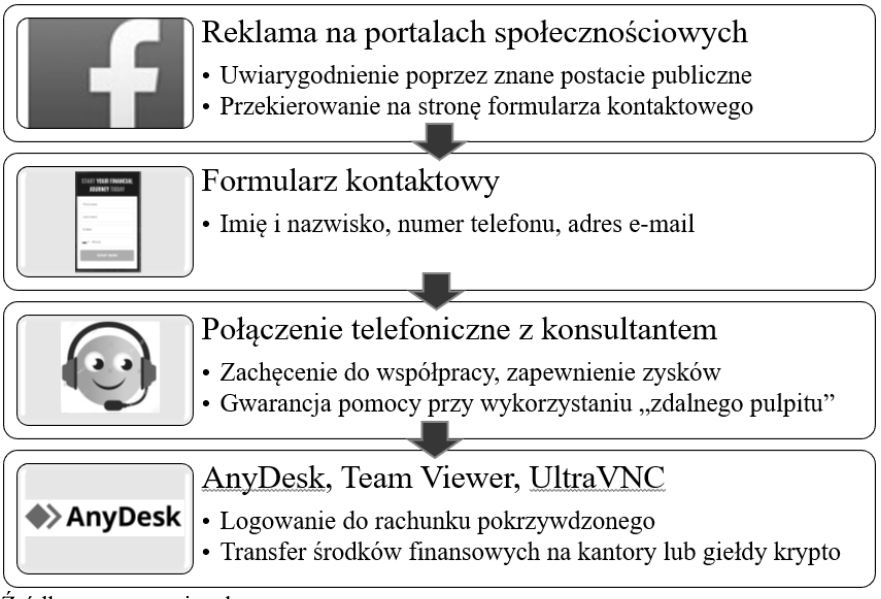
Następnie zakładane jest indywidualne „konto inwestycyjne" pokrzywdzonego, który podejmuje tym samym współpracę w daną „platformą inwestycyjną". Następuje wpłata określonej sumy tzw. „opłaty wpisowej" (np. w wysokości 250 USD). W kolejnym etapie, sprawcy dokonują licznych połączeń telefonicznych oraz stosując różne metody socjotechniczne doprowadzają do zainstalowania przez pokrzywdzonego oprogramowania umożliwiającego zdalną obsługę jego komputera. Najczęściej odbywa się to poprzez polecenie ustne bądź też za pośrednictwem przesłanego linku prowadzącego

do pliku instalacyjnego. Przestępcy, oprogramowanie to określają mianem robota inwestycyjnego bądź wsparciem technicznym do realizacji zysków oraz nauki obsługi silników inwestycyjnych. Często też wprost wskazują na sposób działania oprogramowania poprzez udostępnienie środowiska urządzenia pokrzywdzonego, co ma na celu ułatwić obsługę rachunku bankowego czy nowoutworzonego konta giełdowego w celu skutecznego osiągnięcia zysków i zminimalizowania błędów, które początkujący inwestor (tu: pokrzywdzony) wg zapewnień sprawców, może popełnić. Socjotechniczne aspekty i możliwości przestępców, na tym etapie procederu, pełnią kluczową rolę. Jednocześnie, pokrzywdzony przez cały okres werbunku, zapewniany jest przez przypisanego mu indywidualnego menagera o wysokim zysku inwestycyjnym w krótkim horyzoncie czasowym.

W konsekwencji pokrzywdzony, posiadając zainstalowane oprogramowanie umożliwiające zdalna obsługę jego komputera, które na dostępnym rynku pozostaje zupełnie legalne, loguje się do bankowości internetowej udostępniając sprawcy w całości swoje środki finansowe, dane autoryzacyjne, saldo konta, ale też i zdolność kredytową, którą sprawcy w przypadku niskich wartości środków pieniężnych zgromadzonych na rachunku wykorzystują, zaciągając on-line kredyty na konto swojej ofiary. Środki pieniężne wytransferowane z rachunków pokrzywdzonych, często przekazywane są przelewami natychmiastowymi na rachunki innych osób fizycznych (np. innych pokrzywdzonych zwerbowanych w zbieżnym czasie przez drugiego z przedstawicieli danej „platformy inwestycyjnej") bądź bezpośrednio tzw. przelewami internetowymi na rzecz giełd lub kantorów umożliwiających wymianę waluty rynkowej na kryptowalutę. Na tym etapie, wykorzystywane są dane kart bankowych wydanych do rachunku przez samych pokrzywdzonych, takich jak numer karty, data ważności czy kod CVV/CVC. Z chwilą wytransferowania środków z rachunku pokrzywdzonego, która w konsekwencji przewalutowana pozostaje z waluty rynkowej (FIAT) na walutę cyfrową (BTC, ETH, LSK, itp.), sprawcy w celu jej dalszego transferu podstawiają będące w ich

władaniu publiczne portfele kryptowalutowe i dokonują wytransferowania środków poza konto użytkownika. Transakcje w zależności od ilości środków finansowych na rachunku pokrzywdzonego, są często wielokrotne i mają na celu całkowite wytransferowanie jego środków finansowych. Bezpośrednio po wymianie tzw. waluty FIAT (waluty rynkowej wychodzącej z rachunku pokrzywdzonego), następuje jej przekazanie na portfele kryptowalutowe, wygenerowane i podstawione przez sprawców w celu dalszego transferu środków w ramach *Blockchain*. Sprawcy, nieustannie utrzymują przy tym kontakt telefoniczny oraz połączenie *on-line* pomiędzy wykorzystywanym przez nich urządzeniem, a urządzeniem pokrzywdzonego. W konsekwencji opisanych powyżej działań, oszukani klienci stają się ofiarami przestępstw internetowych. Nie odzyskują swoich środków, a w najgorszym scenariuszu, pozostają nie tylko ze stratami w postaci utraconych oszczędności, ale także zaciągniętymi przez siebie lub przez „analityków" platform, zobowiązaniami kredytowymi.

Na rysunku 1 przedstawiono proces realizacji zagrożenia w początkowym etapie werbunku pokrzywdzonego.



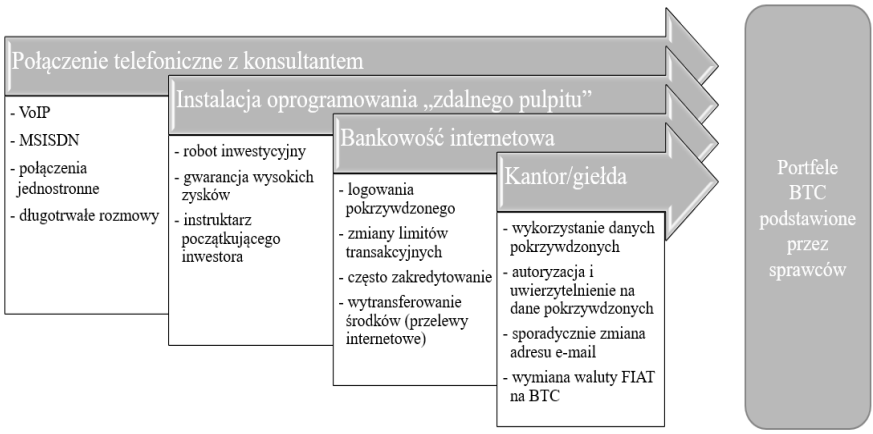
Źródło: opracowanie własne.

Rys. 1. Proces realizacji zagrożenia w początkowym etapie werbunku pokrzywdzonego

Zarówno domeny wykorzystywane do przestępstwa, rachunki bankowe zależne od sprawców czy wykorzystane numery telefonów, najczęściej rejestrowane i administrowane pozostają przez podmioty zewnętrzne, które działają poza jurysdykcją prawną Rzeczypospolitej Polskiej. Stąd też, na początkowym etapie podejmowanych czynności, sprawa często przyjmuje charakter międzynarodowy, a tym samym skomplikowany pod względem faktycznym i prawnym. Przestępcy w kontakcie z pokrzywdzonym wykorzystują numery identyfikacyjne o konstrukcji wskazującej na polski stacjonarny numer telefonu, najczęściej o kierunkowym 12 (Kraków), 22 (Warszawa) lub 71 (Wrocław), w rzeczywistości jednak są to numery wykorzystywane w technologii VoIP *(Voice over Internet Protocol)*, bez możliwości realizacji połączenia zwrotnego inicjowanego przez pokrzywdzonego. Z uwagi na wysokie

wyspecjalizowanie struktur grupy, bowiem w ich skład wchodzą rekrutrzy, informatycy, menagerowie, dyrektorowie oraz osoby z pierwszego kontaktu, tzw. c*all center*, sprawcy wykorzystując dostępną nielegalną infrastrukturę sieciową, inicjują połączenia także z dostępnych i istniejących numerów MSISDN zupełnie postronnych osób lub podmiotów, nie mających związku z procederem.

Na rysunku 2 przedstawiono schemat działania sprawców względem pokrzywdzonych i poszczególne powiązane ze sobą etapy ich aktywności:



Źródło: opracowanie własne.

Rys. 2. Schemat działania sprawców względem pokrzywdzonych i poszczególne etapy ich aktywności

Mimo dostępnych narzędzi autoryzacyjnych jak dwuetapowa weryfikacja, kody zdrapki, ale też i połączenia weryfikacyjne pracowników banków zaniepokojonych koniecznością realizacji wysokiego przelewu na rzecz zagranicznego podmiotu, powiązanego z wymianą waluty rynkowej na walutę cyfrową, pokrzywdzeni, żyjący w przekonaniu, że realizują swoją życiową

inwestycję, autoryzują zlecone przez sprawców przelewy ze swoich rachunków bankowych. Dla przykładu, aby możliwe było przewalutowanie wypłacanych środków pieniężnych, sprawcy podczas telefonicznych rozmów, uzyskują uprzednio dokumenty pokrzywdzonych służące do utworzenia profilu na nieistniejącym koncie inwestycyjnym, powiązanym z platformą inwestycyjną. Sprawcy tym samym dokonują jednoczesnego utworzenia, bez wiedzy pokrzywdzonych, profili na kantorach lub giełdach kryptowalutowych na dane pokrzywdzonych, które pokrzywdzeni ponownie pod naciskiem socjotechnicznych wpływów swoich doradców autoryzują poprzez własnoręcznie wykonane *selfie* oraz odręcznie naniesione treści wymagane przez poszczególne giełdy czy kantory, co służy uwierzytelnieniu i legalnemu procesowi autoryzacji danych osobowych.

Częstokroć pokrzywdzeni, włączają w opisany powyżej proceder zupełnie nieświadomie także swoich bliskich, którzy pod wpływem namowy i możliwości osiągnięcia szybkich zysków inwestycyjnych, w krótkim horyzoncie czasowym, podobnie zawierzają swoje prywatne środki finansowe w ręce oszustów.

Struktura zorganizowanej grupy przestępczej wykorzystującej mechanizm zdalnego pulpitu

Karalność i udział w zorganizowanej grupie przestępczej lub związku przestępczym reguluje art. 258 Kodeksu karnego.[7] Zorganizowana grupa przestępcza musi liczyć co najmniej trzech członków, wśród których musi występować podział ról. Struktura musi posiadać przywódcę oraz osoby mu w hierarchii podległe. Dla bytu zorganizowanej grupy przestępczej nie jest

[7] Art. 258 Kodeksu karnego (Dz.U.2020.1444 t.j.)

konieczna rozwinięta jej sieć czy wielość uczestników i ich wzajemnych powiązań. Stopień jej zorganizowania może być podstawowy i nie musi być bliżej sprecyzowany. Ponadto nie jest konieczne, aby wszyscy członkowie zorganizowanej grupy przestępczej wspólnie uzgadniali sposób popełnienia przestępstwa, a nadto byli połączeni więzami wzajemnej zależności, wystarczające jest, aby każdy z uczestników grupy posiadał świadomość działania w jej strukturze organizacyjnej. Wymagany jest element trwałości, polegający nie tylko na popełnieniu przestępstw w sposób ciągły, ale także na zapewnieniu sobie stałych źródeł dochodu trwających jakiś czas.[8] Istotą grupy przestępczej jest także stałe dążenie do zaspokajania nielegalnych potrzeb.[9]

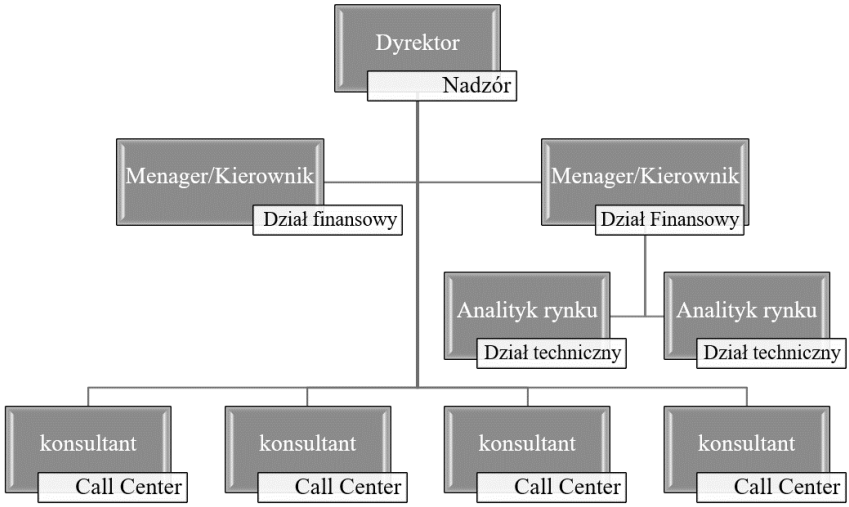
Aby możliwe było przypisanie przestępstwa danej osobie w ramach działalności w zorganizowanej grupie przestępczej, konieczne jest, aby taka grupa zorganizowała się jeszcze przed popełnieniem tego przestępstwa. Organizacja grupy wymaga bowiem pewnego rodzaju wcześniejszego przygotowania i opracowania, a to odróżnia ją od zwykłej formy popełnienia przestępstwa w formie współsprawstwa, które w przeciwieństwie do zorganizowanej grupy przestępczej, może ukształtować się dopiero w momencie popełnienia dane przestępstwa.[10]

Struktura zorganizowanej przestępczości wykorzystującej mechanizm zdalnego pulpitu opiera się na profesjonalnie postawionej infrastrukturze sieciowej, począwszy od zanonimizowanych rejestratorów domen, po ich administrowanie przez podmioty mające siedzibę w Stanach Zjednoczonych

[8] Wyrok Sądu Apelacyjnego w Łodzi z dnia 3 lipca 2019 r., sygn. akt II AKa 95/18
[9] Wyrok Sądu Apelacyjnego w Poznaniu z dnia 14 marca 2018 r., sygn. akt II AKa 157/17
[10] https://ifor.pl/prawo/prawo-karne/przestepstwa/5240322,Udzial-w-zorganizowanej-grupie-przestepczej.html, z dnia 12.11.2021.

Ameryki. Wiąże się to z utrudnioną możliwością zidentyfikowania ich docelowych właścicieli. Witryny internetowe mające wskazywać na rzetelnie działający podmiot rynku inwestycyjnego są utworzone w doskonałej szacie graficznej. To za ich pośrednictwem pokrzywdzeni dokonują zapoznania się z ofertą danej platformy inwestycyjnej oraz zakładają indywidualne konto inwestycyjne. Stoją za tym ludzie mocno związani z działem informatycznym, posiadający wiedzę oraz zaplecze do utworzenia, zarejestrowania i administracji takiego serwisu na potrzeby przestępstwa.

Rysunek 3 przedstawia strukturę zorganizowanej grupy przestępczej wykorzystującej mechanizm zdalnego pulpitu:



Źródło: opracowanie własne.

Rys. 3 Struktura zorganizowanej grupy przestępczej wykorzystującej mechanizm zdalnego pulpitu

W strukturze zorganizowanej grupy przestępczej wykorzystującej mechanizm zdalnego pulpitu, wyróżnić należy działalność struktur tzw. *call*

center, gdzie na potrzeby werbunku pokrzywdzonych działa kilka bądź kilkanaście osób odpowiedzialnych za kontakt z potencjalną ofiarą. To właśnie te osoby z chwilą uzyskania danych kontaktowych pokrzywdzonego telefonują do niego i namawiają do intratnej inwestycji. Wskazują za szybką konieczność podjęcia decyzji, zapewniając o wysokim zwrocie inwestycyjnym, jak również opisują procedurę inwestycyjną oraz wskazują na przekazanie inwestora pod skrzydła profesjonalnego doradcy – menagera bądź kierownika działu finansowego. Na tym etapie werbunku konsultant *call center* sugeruje możliwość instalacji robota inwestycyjnego bądź programu mającego ułatwić naukę na rynku inwestycyjnym, którym najczęściej docelowo pozostaje popularne i legalne oprogramowanie o nazwie AnyDesk lub TeawViewer, o czym początkujący „inwestor" nie ma pojęcia.

Pokrzywdzonym zachęcony szybką możliwością zysku inwestycyjnego często zgadza się na współpracę, a wówczas następuje kontakt z indywidualnym menagerem/kierownikiem od spraw inwestycji, którego celem pozostaje wytransferowanie jak największej ilości środków finansowych z rachunku/-ów swojej ofiary przy wykorzystaniu narzędzia zdalnego pulpitu. W przypadku pojawienia się wątpliwości pokrzywdzonego, co do wiarygodności inwestycji i rzetelności „opiekuna" inwestycyjnego, w strukturze przestępczej oszuści wyodrębnili tzw. dział techniczny, gdzie osoby pełniące rolę analityków rynku, telefonują do pokrzywdzonych zapewniając o w pełni legalnym procesie inwestycyjnym, nad to wielokrotnie wykorzystując sytuację rynkową, która może w danej chwili pozwolić osiągnąć wysoki zysk. Istotnym jest, że w znakomitej większości konsultanci posługują się doskonałą polszczyzną i bogatym zasobem słownictwa języka polskiego, lecz z wyraźnie słyszalnym wschodnim akcentem językowym.

Rola jaką odgrywa menager/kierownik, którego zadaniem pozostaje wyłącznie wytransferowanie pieniędzy pokrzywdzonego, jest kluczowa dla procederu. Częstokroć, po upływie określonego czasu na zwrot wypłaconych

środków pokrzywdzonemu lub wypłaty ustalonych zysków, z pokrzywdzonym kontaktuje się dyrektor, pełniący rolę nadzoru, który przekonuje już wówczas zaniepokojonego pokrzywdzonego o legalności działania jego firmy i podjęcia niezwłocznych starań do wypłaty powierzonych środków pieniężnych, rzecz jasna wraz z wypracowanym zyskiem. Pod wpływem namowy, pokrzywdzony bardzo często decyduje się na ponowne zainwestowanie pieniędzy, nie czekając na wcześniej obiecany zwrot funduszy, po czym inicjatywę „inwestycyjną" przejmuje ponownie menager bądź kierownik, działający pod dyktando wcześniej wspomnianego dyrektora.

Procedura przesłuchania pokrzywdzonych przez Policję – sporządzenie protokołu przyjęcia ustnego zawiadomienia o przestępstwie i przesłuchania świadka

W przypadku ujawienia przestępstwa związanego z działalnością nielegalnej platformy inwestycyjnej, a tym samym wykorzystaniem mechanizmu zdalnego pulpitu, koniecznym jest przeprowadzenia czynności procesowych z udziałem osoby pokrzywdzonej celem zebrania istotnych dla sprawy informacji i dowodów. Pomocne w tym zakresie jest zadanie kluczowych pytań pokrzywdzonemu w zakresie:

1. Sposobu nawiązania kontaktu/współpracy pokrzywdzonego z oszustami oraz udostępnionych przez świadka danych i dokumentów przy nawiązaniu owego kontaktu, a także okoliczności, w jakich dochodziło do późniejszych kontaktów z przedstawicielami spółki/podmiotu już po nawiązaniu współpracy. Niezbędne dla sprawy jest ustalenie wszystkich numerów telefonów, z jakich telefonowali sprawcy, jak również adresów e-mail, z których nadawali korespondencję. Istotnym jest także uzyskanie od świadka szczegółowego opisu charakteru rozmów telefonicznych z oszustami pod kątem realizacji znamion przestępstwa z art. 286 § 1 k.k., jak również wskazanie języka, jakim posługiwali się rozmówcy, dialektu, dźwięków

słyszalnych w tle, czy też charakterystycznych słów i zwrotów, które zapadły świadkowi w pamięć.

2. Powodów podjęcia kontaktu/współpracy oraz ewentualnej weryfikacji (np. w sieci Internet) „platformy inwestycyjnej" czy spółki/podmiotu oraz osób je reprezentujących m.in. w kwestii wiarygodności, legalności działania, opinii, itp.
3. Poniesionych przez świadka opłat wstępnych oraz ustalenia, gdzie przelane zostały środki z opłaty wpisowej, a także ustalenie dat transakcji, danych rachunku, na który przelano środki, pełnej nazwy podmiotu odbiorcy środków etc. (niezbędne jest dołączenie do protokołu potwierdzenia tych transakcji).
4. Zawartych umów w związku z powierzeniem środków finansowych na rzecz danego podmiotu oraz sposobów przekazania dokumentacji.
5. Motywów podjęcia decyzji nt. zainwestowania środków finansowych oraz uzasadnienia ew. przekonań co do osiągniętych zysków, a także znajomości sposobów na ich osiągnięcie (rodzaj inwestycji). Czy świadek był o tym informowany, czy samodzielnie uzyskiwał informacje na ten temat.
6. Procedury przekazywanych środków finansowych (samodzielnie, przez przedstawicieli platform inwestycyjnych bądź inne osoby trzecie).
7. Wiedzy pokrzywdzonego dotyczącego inwestowania i ryzyka z tym związanego, a tym samym możliwości utraty wszystkich lub części środków pieniężnych.
8. Kwoty jaką świadek miał uzyskać na skutek dokonanej inwestycji oraz okresu czasu, w jakim zysk miał zostać wypłacony,

a także czy świadek był informowany, ile środków finansowych powinien zainwestować, zanim dokonał pierwszej płatności.

9. Ewentualnych podejmowanych przez świadka prób kontaktu z oszustami mających na celu zwrócenie zainwestowanych środków.
10. Instalowanych na komputerze oprogramowania umożliwiającego zdalną obsługę komputera. Tego, w jaki sposób nastąpiło udostępnienie oprogramowania i jego instalacja, a także czy pokrzywdzony działał w tym zakresie z własnej woli, czy też na polecenie oszustów oraz ustalenie czy w dalszym ciągu posiada zainstalowane oprogramowanie na swoim komputerze.
11. Ewentualnego dostępu pokrzywdzonego do „platformy inwestycyjnej", celem identyfikacji nazwy użytkownika oraz ustalenia usługodawcy internetowego, z którego usługi świadek logował się do swojej bankowości internetowej oraz innych usług.
12. Zapoznania się z regulaminem spółki/podmiotu oferującego współpracę w zakresie inwestycji. Posiadania wiedzy na temat istnienia ewentualnego regulaminu dostępnego na stronie internetowej spółki/podmiotu?
13. Podpisania tzw. „Deklaracji Klienta" z chwilą podjęcia współpracy np. z „platformą inwestycyjną".
14. Doświadczenia pokrzywdzonego nt. inwestycji w kryptowaluty?
15. Wiedzy nt. kantorów czy giełdy kryptowalut, na które przekazywano środki pieniężne oraz czy świadek prowadził z nimi korespondencję. (zasadne jest wymienienie świadkowi nazwy wykorzystanych kantorów lub giełd, zadając pytanie czy je rozpoznaje).
16. Wiedzy świadka nt. ewentualnego wykorzystania jego danych osobowych do utworzenia konta na ww. giełdach/kantorach oraz sposobu założenie ew. konta (samodzielnie, przez przedstawicieli platform inwestycyjnych bądź inne osoby trzecie).

17. Prób kontaktu świadka z odpowiednim bankiem, celem zwrotu zainwestowanych środków oraz wyniku tych prób.
18. Ustalenia wysokości przelewanych środków pieniężnych z rachunków pokrzywdzonego oraz „miejsca", do których trafiały. (zasadnym jest uzyskanie potwierdzeń dokonywanych przelewów dla każdej z transakcji oraz pełnej historii wszystkich rachunków bankowych w czasookresie, gdy do nich dochodziło.
19. Posiadanej przez świadka wiedzy nt. portfeli kryptowalutowych, na które zostały przekazane środki w postaci waluty wirtualnej.

Celem sformułowanych w toku przesłuchania pytań, jest uzyskanie jak największej ilości informacji, danych oraz dowodów w sprawie, które mogą przyczynić się do identyfikacji sprawców i tym samym przyczynić się do efektywniej walki z nielegalnymi działaniami w zakresie pośredniczenia w transakcjach finansowych przez zorganizowane grupy przestępcze.

Czynności prokuratora po ujawnieniu przestępstwa z wykorzystaniem zdalnego pulpitu

W sprawach oszustw o znacznych skutkach finansowych, należy przyjąć zasadę minimalizacji strat, uznając, iż priorytetem jest uchronienie potencjalnych inwestorów przed utratą mienia. W przestępczości, charakteryzującej się ofensywnym działaniem sprawców z wykorzystaniem socjotechnicznych środków oddziaływania na ofiary (obietnice szybkich, znacznych zysków, ale także działania nękające pokrzywdzonych, szantaż i groźby), tzw. cisza procesowa i „niepłoszenie" sprawców muszą zejść na dalszy plan.

Nawet przy uwzględnieniu ryzyka uzyskania przez sprawców wiedzy, iż organy ścigania podjęły działania procesowe, należy dotrzeć do jak naj-

większej liczby osób i sprawić by wiedza o mechanizmie nowego typu oszustwa dotarła do potencjalnych inwestorów i uchroniła ich przed ryzykownym działaniem.

W fazie *in rem,* pominięcie rutynowych działań pozyskiwania dowodów bezwpływowych jest naturalne także z uwagi na fakt, iż podmiot, którym posługują się sprawcy jest wirtualny co nie pozwala na gromadzenie danych z Krajowego Rejestru Sądowego, danych dotyczących struktury kapitałowo-organizacyjnej czy dokumentacji podatkowej.

W pierwszej kolejności należy sięgnąć po:

- komunikat prasowy wzywający pokrzywdzonych do zgłoszenia oszustwa. Komunikat zawierający opis mechanizmów przestępczych jest też formą ostrzeżenia o procederze,
- analizę wszystkich zgłoszonych przestępstw z wykorzystaniem tego samego mechanizmu działania i identycznej platformy inwestycyjnej.

Analiza jednostkowego zgłoszenia może bowiem wpłynąć na błędną ocenę znamion czynu zabronionego i prowadzić do podjęcia decyzji o braku podstaw do wszczęcia lub dalszego prowadzenia postępowania przygotowawczego. Na tę ocenę może mieć wpływ okoliczność, iż dyspozycje dotyczące przelewów środków finansowych podejmowane są za zgodą i akceptacją pokrzywdzonego przy braku widocznego elementu wprowadzenia w błąd. Wymóg zaakceptowania regulaminu uczestnictwa w inwestycji ma potwierdzać dobrowolność przystąpienia do procesu inwestycyjnego i zgodę na przekazywanie środków finansowych, a nawet na ryzyko ich utraty. Dopiero kompleksowa ocena zdarzeń pozwala na pełne ujawnienie mechanizmów działania sprawców, tj. wytransferowanie środków z rachunków pokrzywdzonych na zakup kryptowaluty i utratę ich władzy nad nimi. Należy uwzględnić również

sprawy zakończone prawomocnymi decyzjami o umorzeniu postępowania (głównie na podst. art. 17 § 1 pkt 2 k.p.k.[11]) i zlecić podjęcie tych postępowań.

- zawiadomienie Komisji Nadzoru Finansowego powołując się na uprawnienia w zakresie podejmowania działań służących prawidłowemu funkcjonowaniu rynku finansowego. Interwencja winna polegać na zwróceniu się o weryfikację podmiotu i ujawnienie na Liście Ostrzeżeń. W takim wypadku należy podjąć ustalenia czy nie zachodzi uzasadnione podejrzenie popełnienia przestępstwa nieuprawnionego obrotu instrumentami finansowymi, które daje podstawy do umieszczenia podmiotu na liście ostrzeżeń,[12]
- zawiadomienie Rzecznika Finansowego, także Urzędu Ochrony Konkurencji i Konsumentów.

Wymiana informacji z wyżej wymienionymi podmiotami pozwala na pozyskanie nowych danych. Pokrzywdzeni, z reguły pierwsze swoje kroki kierują do tych właśnie organów informując o nieuczciwych praktykach. Organy te bywają jedynymi dysponentami informacji o utracie środków, które pozyskują bezpośrednio od pokrzywdzonych. Wynika to z faktu, iż Rzecznik Finansowy ma uprawnienie do wytoczenia powództwa na rzecz klientów podmiotów rynku finansowego w sprawach dotyczących nieuczciwych praktyk rynkowych, jak również za zgodą powoda wziąć udział w toczącym się już postępowaniu. Biuro Rzecznika Finansowego tworzyło istotne raporty, które były podstawą wielu późniejszych inicjatyw ustawodawczych. Rzecznik ana-

[11] Art. 17 § 1 pkt 2 Kodeksu postępowania karnego (Dz.U.2021.534 t.j.)
[12] Art. 178 Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U.2021.328 t.j.)

lizował np. umowy dotyczące zaciągania pożyczek min. w bitcoinach oferowanych przez jeden z podmiotów, uznając, iż umowy zawierają szereg budzących wątpliwości postanowień dotyczących czynności poprzedzających udzielenia pożyczki. Zwrócił uwagę także na przewidziany mechanizm przekazania środków klientowi.[13]

- rozesłanie do innych jednostek prokuratury schematu przesłuchania pokrzywdzonego i zabezpieczania dowodów (głównie sprzętu komputerowego) celem zgromadzenia w śledztwie pełnego materiału co do danych możliwych do pozyskania od pokrzywdzonego,
- stosownie do art. 20 § 3 Prawa o prokuraturze.[14] Sprawy dotyczące działania grup przestępczych cechujących się wysokim stopniem zorganizowania, a zwłaszcza dopuszczających się przestępstw o charakterze transgranicznym, mają być prowadzone w Wydziałach Zamiejscowych Departamentu do Spraw Przestępczości Zorganizowanej i Korupcji Prokuratury Krajowej. Postulowanie przekazania tego rodzaju postępowań na wyższy szczebel struktury organizacyjnej prokuratury jest w pełni zasadny. Dotyczy to także zasadności powołania zespołu prokuratorów, o którym mowa w §126 Regulaminu wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury, który należy rozważyć w przypadku najbardziej skomplikowanych spraw, o charakterze wielowątkowym, wielopodmiotowym lub transgranicznym.[15]

---

[13] https://fr.gov.pl/2021/03/19/rzecznik-finansowy-ostrzega-uwaga-na-kryptowalutowe-pożyczki, z dnia 12.11.2021.

[14] Art. 20 § 3 Ustawa z dnia 28 stycznia 2016 r. - Prawo o prokuraturze (Dz.U.2021.66 t.j.).

[15] § 126. 1. Rozporządzenia Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. - Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury (Dz.U.2017.1206 t.j.)

Czynności w celu ustalenia lokowania środków finansowych

Idealnym dla celów dowodowych byłoby pozyskanie analizy przepływów środków finansowych od ich pierwszego lokowania przez pokrzywdzonego, po przepływ do ostatniego ustalonego rachunku bankowego. W przypadku lokowania środków na rachunkach bankowych istotnym dowodem jest pozyskanie informacji od Generalnego Inspektora Informacji Finansowej, co służy dwóm celom:

- ustaleniu i zabezpieczeniu utraconego przez pokrzywdzonych mienia,
- uzyskaniu danych o dalszym lokowaniu środków.

Niejednokrotnie, środki finansowe uzyskiwane przez grupy przestępcze są dalej transferowane, wyczerpując znamiona czynu zabronionego z art. 299 k.k.[16], a także wyprowadzane poza polski system bankowy, co z kolei stanowi istotne zagrożenie dla bezpieczeństwa ekonomicznego państwa. W takim wypadku niezbędne będzie pozyskanie informacji od Generalnego Inspektora Informacji Finansowej (GIIF). Prokurator może skierować pisemny wniosek na podstawie art. 103 ust. 1 i art. 104 ust. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[17] o udostępnienie przez GIIF na potrzeby postępowania karnego informacji zgromadzonych w trybie i zakresie przewidzianym przepisami ustawy.[18]

---

[16] art. 299 Kodeksu karnego (Dz. U. 2020.1444 t.j.)
[17] art. 103 ust. 1 i art. 104 ust. 1 Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu
[18] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U.2021.1132 t.j.)

Poznanie schematu i metody działania sprawców warunkuje właściwe zaplanowanie dalszych czynności procesowych i ich prawidłowe wykonanie. W przypadku ustaleń, iż pokrzywdzeni padli ofiarą procederu związanego z zakupem kryptowalut, nie ma możliwości uzyskania istotny danych, które byłyby gromadzone przez GIIF. W takim wypadku jedyne transakcje na rachunkach bankowych, dotyczą:

- dokonania opłaty wstępnej,
- przekazania środków finansowych na konta/giełdy i kantory bitcoinowe.

Znacznym uproszczeniem procedury pozyskania danych objętych tajemnicą bankową, a tym samym uniknięcia wydłużonej czasowo i proceduralnie drogi jest konieczność odebrania od pokrzywdzonego, na podstawie art. 104 ust. 3 Ustawy Prawo bankowe z dnia29 sierpnia 1997 roku z późn. zm.[19], upoważnienia Banku do udzielnie organom ścigania danych bankowych dotyczących wszystkich rachunków bankowych pokrzywdzonego, z których wypłaty środków nastąpiły. Pozwoli to na uniknięcie konieczności kierowania wniosku do sądu i jego przekazania do wykonania bankom, z możliwością także zaskarżenia takiego orzeczenia.

Zgodnie z artykułem 104 ust. 3 zd. 2 w/wymienionej ustawy klient jest wyłącznym dysponentem tajemnicy bankowej i to on udziela bankowi zgody na ujawnienie innym podmiotom informacji uzyskanych przez bank w związku z czynnością bankową z tym klientem, nawet gdy dotyczą innych osób. Zgoda przyjmuje formę upoważnienia. Bank nie może odmówić przyjęcia upoważnienia o ile zawiera ono wskazanie konkretnego podmiotu, który ma być odbiorcą informacji przekazanych przez bank. Upoważnienie może być złożone bezpośrednio przez klienta banku lub osoby działającej na jego

[19] Art. 104 ust. 3 Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U.2020.1896 t.j.)

rzecz np. pełnomocnika lub prokurenta. Pozyskanie upoważnienia pozwala na uzyskanie informacji bezpośrednio od banku z pominięciem procedury sądowej, co znacznie przyspiesza czas pozyskiwania dowodów.

Wstrzymanie transakcji lub blokada środków na rachunku – decyzje i czynności prokuratora

Złożenie formalnego zawiadomienia przez pokrzywdzonego o możliwości popełnienia przestępstwa może być poprzedzona działaniem banku, który kieruje zawiadomienie do organów ścigania. Zawiadomienie dot. jedynie przypadku zaistnienia uzasadnionego podejrzenia, że działalność banku jest wykorzystywana w celu ukrycia działań przestępczych lub dla celów mających związek z przestępstwem skarbowym lub innym przestępstwem niż przestępstwo, o którym mowa w art. 165a k.k. (finansowanie przestępstwa o charakterze terrorystycznym) lub art. 299 k.k. (tzw. pranie brudnych pieniędzy). Jest to obowiązek denuncjacyjny banku wynikający z treści w art. 106a ustawy Prawo bankowe. W praktyce zawiadomienie w tym trybie dotyczyć będzie podejrzenia popełnienia przestępstwa np. oszustwa stypizowanego w art. 286 § 1 k.k.

Bank jest uprawniony do dokonania blokady środków na rachunku bankowym w przypadku powzięcia uzasadnionego podejrzenia, że zgromadzone na rachunku bankowym środki pochodzą z przestępstwa lub mają związek z przestępstwem, innym niż przestępstwo określone w art. 165a i 299 k.k. Blokada dokonywana jest wówczas w trybie w art. 106a ust. 3 Prawa bankowego i wiąże się z jednoczesnym zawiadomieniem prokuratora. W praktyce najczęściej dotyczy to powzięcia informacji przez bank od klienta banku o nieuprawnionych transakcjach na rachunku bankowym lub pochodzącego od zagranicznego banku z systemu SWIFT. Blokada w takim trybie nie może objąć innych środków finansowych poza kwotę co do której zachodzi podejrzanie, iż pochodzi z przestępstwa.

Zgodnie z art. 106a ust. 4 Prawa bankowego, blokada w tym trybie nie może trwać dłużej niż 72 godziny. Jest to czas niezbędny prokuratorowi na analizę zawiadomienia i podjęcie niezwłocznych decyzji o wszczęciu śledztwa i o wstrzymaniu transakcji lub dokonaniu blokady środków.

Prokurator wydaje postanowienie o wstrzymaniu transakcji lub dokonaniu blokady środków, którego istotnym elementem jest określenie czasu trwania nie dłuższego niż 3 miesiące od otrzymania zawiadomienia. Ustawa nie przewiduje możliwości kolejnego przedłużenia czasu trwania blokady. Zatem termin ten jest niezbędny na uzupełnienie materiału dowodowego. W praktyce, w przypadku przestępstw o charakterze transgranicznym, jest on niewystarczający, niemniej po tym okresie blokada „upada" jeżeli nie zostanie wydane postanowienie o zabezpieczeniu majątkowym (w przypadku przejścia postępowania w fazę *in personam*) lub postanowienie w przedmiocie dowodów rzeczowych. Fakt zawiadomienia oraz blokady, nie wiąże prokuratora obowiązkiem wszczęcia śledztwa. Jeżeli według jego oceny brak jest podstaw do wydania takiej decyzji, odmawia jego wszczęcia. W każdym wypadku ma obowiązek zawiadomić o podjętej decyzji bank. Niemniej czas na podjęcie decyzji procesowej jest krótki w porównaniu do terminu procesowego określonego w art. 307 § 1 k.p.k.[20]

Postanowienie prokuratora w przedmiocie blokady podlega kontroli sądowej. Właściwym rzeczowo i miejscowo jest sąd właściwy do rozpoznania sprawy. Zażalenie przysługuje zarówno właścicielowi rachunku bankowego, jak i osobie dokonującej przelewu. W praktyce często ta druga strona korzysta z uprawnienia do wniesienia środka odwoławczego, uznając blokadę za ingerencję w swoje dobra.

[20] Art. 307 § 1 Kodeks postępowania karnego (Dz.U.2021.534 t.j.)

Podsumowanie

Ujawniony mechanizm przestępstw związanych z nielegalnym działaniem w zakresie pośredniczenia w transakcjach finansowych przez zorganizowane grupy przestępcze wykorzystujące mechanizm zdalnego pulpitu, różni się od dotychczasowych, znanych organom ścigania schematom postępowania zorganizowanych grup społecznych. Jest też procederem dalece skomplikowanym. Sprawcy, wykorzystując wysoki poziom wiedzy w zakresie sposobów maskowania zarówno danych teleinformatycznych, jak i w Internecie, wprowadzając w błąd co do danych i kierunkując postępowanie na osoby nie mające nic wspólnego z procederem, stanowią dla organów ścigania nie lada wyzwanie. Co więcej, inwestowanie środków pochodzących od pokrzywdzonych poprzez lokowanie w krypto walutę, a następnie przetransferowanie jej przez kilkadziesiąt portfeli, uniemożliwia prześledzenie drogi przepływu do momentu i ich ostatecznego ulokowania i wypłaty środków.

Skomplikowaną materię utrudnia fakt, iż większość czynności w śledztwie wykonywana jest w drodze międzynarodowych pomocy prawnych. Jakość tych realizacji jest coraz lepsza, jednakże zasadniczo wydłuża czas trwania postępowania. Prace w tym zakresie, wymagają także działań koordynacyjnych w związku z aktywnością szeregu platform inwestycyjnych i znaczną ilością spraw o podobnym sposobie działania prowadzonych przez inne jednostki. Priorytetem jest rozpracowanie zorganizowanej grupy przestępczej oraz ustalenie operacji finansowych sprawców, miejsc lokowania środków płatniczych pochodzących z korzyści majątkowych związanych z popełnieniem czynu zabronionego. Można przyjąć, iż w tego rodzaju przestępczości mamy do czynienia ze zorganizowaną strukturą o znacznie rozbudowanym schemacie, gdzie za każdą z czynności stoją inne osoby: werbujący, doradcy, lokujący środki, przenoszący na dalsze portfele, zarządzający strukturą. Wynika, m.in. z faktu działającego schematu wręcz „prowadzenia" tzw.

inwestora od pierwszego kontaktu telefonicznego, po opróżnienie konta bankowego ze środków tam zgromadzonych.

W dobie ciągłego rozwoju technologii informacyjno-komunikacyjnych, technologii mobilnych czy systemów urządzeń elektronicznych oraz wyjątkowego i trudnego czasu, w którym się znajdujemy - czasach pandemii COVID-19, skala zagrożeń i ryzyka związanego z przestępczością w sieci Internet rośnie i będzie rosła. To bowiem okres otwarcia wielu kanałów online dla codziennych transakcji. Niniejsze opracowanie mające na celu zaprezentowanie sposobów i środków działania przestępców oraz metod zwalczania cyberprzestępczości w zakresie oszustw związanych z inwestowaniem na „platformach inwestycyjnych", wskazuje jednocześnie na obszary newralgiczne, które wymagają zmian, i z których powinniśmy wyciągać właściwe wnioski. Opisane w niniejszym opracowaniu metody wykorzystywane przez oszustów, pokazują, że przestępcy szybko adaptują się do zmieniającej się rzeczywistości. Konieczne zatem staje się bardziej wnikliwe podejście do identyfikacji tożsamości klienta, oceny jego wiarygodności, jak również poszukiwanie nowych, skutecznych metod walki z tego typu przestępstwami.

Bibliografia

1. Raport z badania EY i Związku Przedsiębiorstw Finansowych, Nadużycia w sektorze finansowym, edycja 2020, [z:] https://assets.ey.com/content/dam/ey-sites/ey-com/pl_pl/news/2020/10/ey-raport-naduzycia-2020.pdf, z dnia 12.11.2021.
2. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U.2020.1444 t.j.)
3. Ustawa z dnia 28 stycznia 2016 r. Prawo o prokuraturze (Dz.U.2021.0.66 t.j.)
4. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz.U.2021.534 t.j.)
5. Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U.2014.94 t.j.)

6. Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 11 grudnia 2019 r., sygn. II AKa 271/19
7. Wyrok Sądu Apelacyjnego w Łodzi z dnia 3 lipca 2019 r., sygn. akt II AKa 95/18
8. Wyrok Sądu Apelacyjnego w Poznaniu z dnia 14 marca 2018 r., sygn. akt II AKa 157/17
9. Rozporządzenia Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury (Dz.U.2017.1206 t.j.)
10. Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U.2020.1896 t.j.)
11. Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U.2021.1132 t.j.)
12. Worona, J., Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy, Wolters Kluwer, Warszawa 2020.

Strony internetowe

13. https://anydesk.com
14. https://teamviewer.com
15. https://fr.gov.pl/2021/03/19/rzecznik-finansowy-ostrzega-uwaga-na-kryptowalutowe-pożyczki
16. https://ifor.pl/prawo/prawo-karne/przestepstwa/5240322,Udzial-w-zorganizowanej-grupie-przestepczej.html

Abstract

FIGHTING ILLEGAL ACTIVITIES IN THE AREA OF MEDIATION IN FINANCIAL TRANSACTIONS BY ORGANIZED CRIME GROUPS USING THE REMOTE DESKTOP MECHANISM. MODUS OPERANDI ACTIONS OF PERPETRATORS

Summary: This chapter has been devoted to the characteristics and scale of the phenomenon of crimes related to the illegal operation of entities offering services in the field of financial transaction mediation, as well as to the presentation of the procedure that should be carried out in this regard within the framework of procedural actions performed with the participation of victims and at the initial stage of pre-trial proceedings. The paper is intended to serve both cognitive purposes, as well as to develop a scheme of conduct during the undertaken procedural actions, in order to create an effective system to prevent this type of abuse, and thus combat unfair practices in this area. The goal of this study is not, then, to analyze all criminal acts referred to as cybercrime, but to attempt to understand the ways and means of cybercriminals in the area of fraudulent activities related to investment on "investment platforms", as well as to point to certain solutions in the collection of information and evidence of guilt of the perpetrators of these acts, including a detailed description of their criminal structure and the infrastructure created for this purpose.

Keywords: organized crime, cybercrime, cybersecurity, financial investment, investment platforms.

ROZDZIAŁ 4

Możliwości i ograniczenia w śledzeniu kryptowalut pochodzących z przestępstw

Jan KLIMA[1]

STRESZCZENIE: w rozdziale przedstawiono podstawy technologii blockchain i obrotu kryptowalutami oraz problemy występujące podczas śledzenia transakcji Bitcoin, Ether i Monero. W części drugiej zaprezentowano analizę przepływu środków w kampanii ransomware Wannacry.

SŁOWA KLUCZOWE: blockchain, kryptowaluty, transakcje, portfele i adresy, Bitcoin, Ether, Monero, giełdy kryptowalutowe, analiza transferów.

Wstęp

Ostatnie kilkadziesiąt lat to dynamiczny rozwój nowoczesnych technologii, które całkowicie zmieniają nasz sposób postrzegania otaczającego świata. Internet sprawił, że jeszcze nigdy dostęp do informacji czy komunikacja międzyludzka nie była tak prosta i szybka, niezależnie od dzielących odległości. Zalety ogólnoświatowej sieci doceniły państwa, organizacje międzynarodowe, biznes i użytkownicy prywatni. Komputer stał się narzędziem pracy, nauki, komunikacji i rozrywki. Technologie informacyjne idą jednak dalej – do sieci podłączanych jest coraz więcej urządzeń i wszystko wskazuje na to, że za sprawą „Internetu rzeczy" będzie następował dalszy,

[1] Naczelnik, Wydział do walki z Cyberprzestępczością, Komenda Wojewódzka Policji w Krakowie, Jan.Klima@malopolska.policja.gov.pl.

dynamiczny rozwój infrastruktury sieciowej. Nowoczesne technologie umożliwiły powstanie wielu innowacyjnych koncepcji, które zastosowane w praktyce doprowadziły do swoistej rewolucji w wielu obszarach naszego życia. Z uwagi na dynamiczny rozwój sieci i usług internetowych, również cyberprzestępczość podlega systematycznym zmianom. Niektóre przestępstwa powoli odchodzą do historii, inne ewoluują, jeszcze inne na stałe wpisały się w działalność grup przestępczych. Dalszy rozwój technologii przyniesie zapewne nowe, dziś jeszcze nieznane rodzaje przestępstw i postawi nowe wyzwania przed organami ścigania. Już teraz Policja zwalczając cyberprzestępczość na co dzień spotyka się z ukrywaniem przez przestępców adresów IP z wykorzystaniem sieci botnet, TOR lub usługi VPN, co sprawia, że szczególnie trudno jest ustalić miejsce działania sprawcy. Zyski z cyberprzestępstw najczęściej są wykorzystywane do zakupu kryptowalut, gdyż ze względu na anonimowość ich właścicieli i możliwość szybkiego przesyłania w dowolne miejsce globu stanowią doskonały instrument do prania brudnych pieniędzy i utrudniania organom ścigania śledzenia przepływów finansowych.

Podstawy technologii blockchain

Technologia łańcucha bloków (blockchain), w oparciu o którą powstały kryptowaluty, zupełnie zmieniła nasze poglądy na gromadzenie, przesyłanie i przetwarzanie informacji o transakcjach finansowych realizowanych w Internecie. Jej historia sięga 1991 roku, gdy Stuart Haber i Scott Stornetta opracowali i przedstawili sposób oznaczania dokumentów znacznikami czasowymi[2]. Technologia wykorzystywała zabezpieczone kryptograficznie ciągi bloków, co uniemożliwiało manipulację dokumentami poprzez ich zmianę lub

[2] S. Haber, W. Scott Stornetta, How to time-stamp a digital document, „Journal of Cryptology", 1991, https://link.springer.com/article/10.1007%2FBF00196791 dostęp 06.12.2021 r.

oznaczenie datą wsteczną. Pomimo tych zalet, nigdy nie została zastosowana w praktyce, a patent wygasł ostatecznie w 2004 roku[3]. W tym samym roku Hal Finney opracował system tzw. „wielokrotnego dowodu pracy (RPoW – reusable proof of work), polegający na otrzymywaniu – w wyniku skomplikowanych obliczeń – cyfrowych tokenów podpisanych kluczami RSA. Istniała możliwość przekazywania tokenów pomiędzy użytkownikami sieci, a zastosowana technologia uniemożliwiała podwójne ich wydatkowanie, gdyż bazowała na ogólnodostępnym rejestrze własności tokenów, w którym każdy mógł dokonać weryfikacji i integralności danych w czasie rzeczywistym. RPoW uznaje się za pierwowzór późniejszego „dowodu pracy" i ważny krok w historii kryptowalut[4].

W 2008 roku wspomniane technologie stanowiły istotny element w opracowaniu teoretycznych podstaw kryptowaluty Bitcoin opartej na łańcuchu bloków. Blockchain to zdecentralizowana i rozproszona baza danych w sieci Internet, o architekturze peer-to-peer (P2P), bez centralnego miejsca przechowywania danych, służąca do księgowania poszczególnych transakcji, płatności lub zapisów księgowych, zakodowana za pomocą algorytmów kryptograficznych. Nie wchodząc w szczegóły techniczne, technologia ta opiera się na kryptografii klucza publicznego, zwanej też kryptografią asymetryczną, z wykorzystaniem algorytmu opartego na krzywych eliptycznych. Algorytmy służące do szyfrowania asymetrycznego generują pary kluczy (publiczny i prywatny), które są ze sobą matematycznie powiązane, ale ich długość i sposób generowania sprawia, że niezwykle trudno jest wyliczyć klucz prywatny z jego publicznego odpowiednika. W technologii blockchain do potwierdzania transakcji wykorzystywane jest uwierzytelnianie danych za pomocą tzw.

[3] https://academy.binance.com/en/articles/history-of-blockchain dostęp 06.12.2021 r.
[4] Tamże,

podpisów cyfrowych. Generalnie rzecz ujmując podpis cyfrowy to skrót stworzony za pomocą tzw. funkcji skrótu na podstawie danych zawartych w samej wiadomości. Po wysłaniu takiej wiadomości, jej podpis może zostać sprawdzony przez odbiorcę przy użyciu klucza publicznego nadawcy - który jest publicznie znany - co pozwala odbiorcy na zweryfikowanie źródła wiadomości i upewnienie się, że jej treść nie została w jakikolwiek sposób naruszona[5]. Sam łańcuch bloków jest strukturą przechowywania danych uporządkowanych w postaci listy kolejnych bloków, w których znajdują się transakcje. Każdy blok transakcji jest identyfikowany za pomocą skrótu generowanego na podstawie nagłówka danego bloku. Każdy kolejny blok zawiera odwołanie do bloku poprzedniego, a cały system tworzy powiązany ze sobą „łańcuch bloków"[6]. Bloki dokumentują czas i kolejność transakcji, a przy tym są powiązane w sposób uniemożliwiający zmianę danych lub wstawienie nowego bloku między istniejące. Jakakolwiek próba ingerencji w strukturę danego bloku zmieni jego skrót (hash) i w konsekwencji nastąpi brak zgodności z hashem tego bloku znajdującym się w nagłówku bloku następnego. Ten brak zgodności jest natychmiast wykrywany przez sieć, a dzięki replikacji pełnej bazy bloków we wszystkich węzłach sieci jest możliwe przywrócenie stanu sprzed ingerencji. W ten właśnie sposób łańcuchy bloków uzyskują pewność i niezmienność[7]. Każdy dodatkowy blok wzmacnia wiarygodność poprzedniego bloku i tym samym całego łańcucha[8].

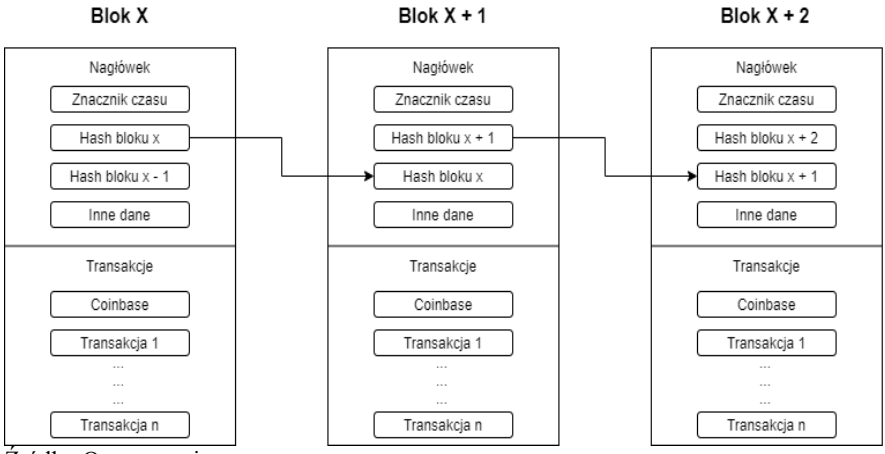
---

[5] https://academy.binance.com/pl/articles/what-is-public-key-cryptography, dostęp 25.11.2021 r.

[6] P. Rodwald, Kryptowaluty z perspektywy informatyki śledczej, Wydawnictwo Akademickie AMW, Gdynia 2020 r.

[7] https://aspolska.pl/blockchain-5-faktow-o-jakich-powinienes-wiedziec-a-boisz-sie-zapytac/ dostęp 3.01.2022 r.

[8] https://www.ibm.com/pl-pl/topics/what-is-blockchain, dostęp 25.11.2021 r.



Źródło: Opracowanie

Rys. 1. Schemat powiązań między poszczególnymi blokami

Aby blok mógł być dodany do łańcucha już istniejących bloków, musi być poddany weryfikacji w procesie zwanym wydobywaniem nowego bloku, polegającym na sprawdzeniu – w drodze skomplikowanych obliczeń matematycznych – poprawności wszystkich transakcji zawartych w bloku. Kompletny rejestr bloków jest przechowywany w tzw. węzłach (nodach) sieci, tworząc rozproszony i zdecentralizowany rejestr. Dzięki takiemu rozwiązaniu niemożliwa jest modyfikacja danych, usuwanie czy dodawanie fałszywych informacji[9]. Rejestr jest jawny i każdy użytkownik może sprawdzić każdą transakcję od początku istnienia rejestru. Taka organizacja bazy danych transakcji sprawia, że system jest odporny na ataki i awarie systemów informatycznych –

[9] https://businessinsider.com.pl/poradnik-finansowy/blockchain-na-czym-polega/fdctpsb, dostęp 25.11.2021 r.

kompletna, identyczna baza danych jest przechowywana niezależnie na tysiącach węzłów sieci[10]. Sieć blockchain może być siecią publiczną (jak w przypadku kryptowalut), prywatną, dostępną dla uprawnionych użytkowników lub stworzoną przez konsorcjum firm, organizacji itp. Podsumowując – blockchain to sieć oparta na zaawansowanej kryptografii (krzywych eliptycznych), odporna na ataki i awarie systemów informatycznych, bezpieczna, jawna, szybka, zdecentralizowana, bez instytucji pośredniczących, nie podlegająca żadnej kontroli, o niskich kosztach działania.

Kryptowaluty

Kryptowaluta to rozproszony system księgowy bazujący na kryptografii i technologii blockchain, przechowujący informację o stanie posiadania umownych, wirtualnych jednostek. Stan posiadania jest związany z równie wirtualnymi „portfelami" w ten sposób, aby kontrolę nad danym portfelem miał wyłącznie posiadacz odpowiadającego mu klucza prywatnego i niemożliwe było dwukrotne wydanie tej samej jednostki[11]. Tak w 2008 roku zdefiniował pojęcie Satoshi Nakamoto, twórca pierwszej na świecie kryptowaluty o nazwie Bitcoin. Do dziś prawdziwa tożsamość twórcy kryptowaluty Bitcoin nie została potwierdzona – nie wiadomo nawet, czy „Satoshi Nakamoto" to jedna osoba, czy też grupa osób, która opracowała kompletną dokumentację opublikowaną jako „white paper"[12]. Zaznaczyć należy, że nazwa „Bitcoin" odnosi się również do otwartoźródłowego oprogramowania węzłów tworzących sieć typu peer-to-peer.

---

[10] w przypadku sieci Bitcoin na dzień 25.11.2021 roku było to 11.336 węzłów - https://bitnodes.io/, dostęp 25.11.2021 r.

[11] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, dostęp 01.12.2021 r.

[12] Tamże,

Aby w pełni zrozumieć obrót kryptowalutami (zwanymi również bitmonetami), trzeba zdefiniować specyficzne w tym obszarze pojęcia: portfeli, adresów i transakcji oraz ich rodzajów i wskazać podstawowe reguły, na których opiera się ten obrót. Mówiąc o „portfelach" kryptowalut należy na wstępie zaznaczyć, że żadne jednostki kryptowaluty nie są fizycznie przesyłane pomiędzy portfelami czy też na nich przechowywane. Do kryptowalut przypisane są jednak klucze prywatne, które pozwalają uzyskać do nich dostęp i np. przenieść je na inny adres w sieci. Oznacza to, że każdy, kto zna dany klucz prywatny, może korzystać z przypisanych do niego aktywów. Portfel kryptowalut jest miejscem przechowywania nie tyle aktywów cyfrowych, co powiązanych z nimi kluczy prywatnych[13]. Klucz publiczny nie musi być przechowywany, gdyż można go wyznaczyć na podstawie klucza prywatnego. Wymieniona para kluczy jest generowana automatycznie przy zakładaniu portfela kryptowalutowego. Portfele mogą występować w następujących postaciach:

- internetowy (sieciowy),
- desktopowy,
- mobilny,
- sprzętowy,
- papierowy.

Portfel internetowy (sieciowy) – zakładany na giełdach i w kantorach kryptowalutowych, najmniej bezpieczny (klucze prywatne są przechowywane w zasobach on-line firm udostępniających takie usługi – występuje ryzyko włamania i przejęcia klucza prywatnego, umożliwiającego dysponowanie posiadanymi środkami). Ten typ portfeli należy do najliczniejszych z uwagi na

[13] https://www.najlepszekonto.pl/portfel-kryptowalut-jak-dziala-i-ktory-wybrac, dostęp 02.12.2021 r.

darmowość, dostępność z każdego miejsca na Ziemi, anonimowość (weryfikacja tożsamości następuje powyżej tzw. progu transakcyjnego, określonego przez międzynarodowe przepisy dotyczące przeciwdziałania praniu brudnych pieniędzy).

Portfel desktopowy – program instalowany na komputerze i tu jest przechowywany klucz prywatny. Wyróżniamy portfele „lekkie", korzystające z łańcucha bloków przechowywanego na zewnętrznych serwerach oraz „pełne", zawierające kompletny rejestr bloków (pełny blockchain), przechowywany na lokalnym komputerze.

Portfel mobilny – ma postać aplikacji na telefon lub smartfon, pozwala na dokonywanie transakcji poprzez zeskanowanie kodu QR, zawierającego klucz prywatny (jest on przechowywany na urządzeniu mobilnym).

Portfele: desktopowy i mobilny – podobnie jak internetowy – należą do mniej bezpiecznych portfeli, z uwagi na możliwość przejęcia dostępu do urządzenia i utraty kluczy prywatnych. Dlatego też wymienione typy portfeli nie są rekomendowane do przechowywania większej ilości kryptowalut.

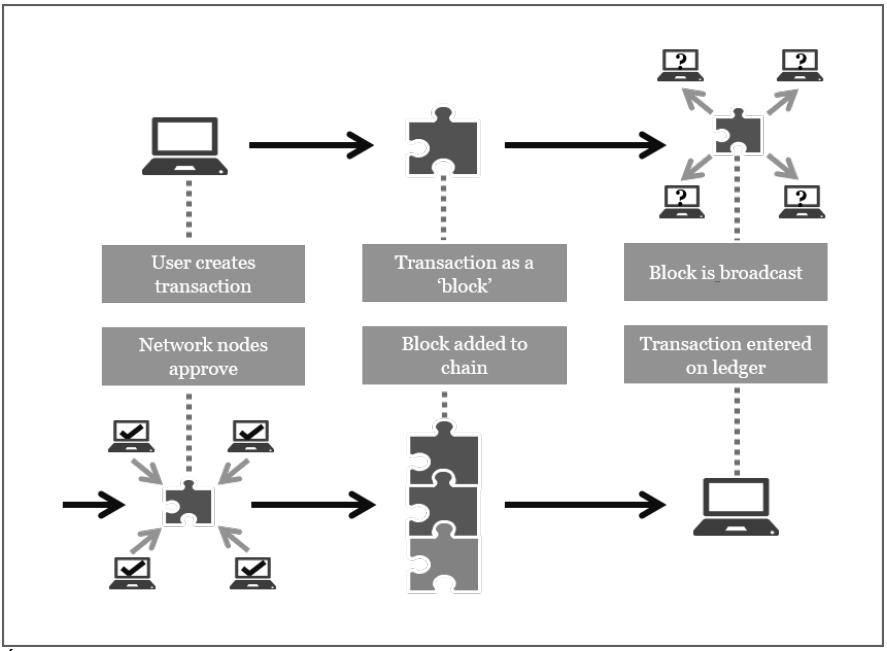
Portfel sprzętowy – urządzenie USB z zainstalowanym specjalizowanym oprogramowaniem do obrotu kryptowalutami, a wszelkie operacje odbywają się w odizolowanym od środowiska zewnętrznego wnętrzu portfela, który przechowuje również klucz prywatny. Z uwagi na fakt, że klucz prywatny jest przechowywany wyłącznie na urządzeniu USB (nie trafia nawet do pamięci komputera, do którego podłączone jest urządzenie), portfel uważany jest – obok papierowego – za najbardziej bezpieczny, dedykowany do przechowywania większej ilości kryptowalut.

Portfel papierowy – wydruk zawierający parę kluczy (publiczny i prywatny), często również w postaci kodu QR. Bezpieczny, ale znacznie mniej wygodny w użytkowaniu – każda transakcja wymaga zaimportowania klucza prywatnego do jej autoryzacji. Ponadto na tego typu portfelu możemy przechowywać tylko jeden rodzaj waluty.

Generalnie rekomendowane jest posiadanie portfela off-line (sprzętowego lub papierowego) do przechowywania większej ilości kryptowalut i jednego z portfeli on-line do realizacji bieżących płatności, na których przechowujemy mniejsze sumy. Dodatkowo, aby była możliwość odzyskania dostępu do środków (w przypadku np. zapomnienia hasła, utraty portfela sprzętowego lub zniszczenia papierowego), istnieje możliwość wygenerowania tzw. ziarna (seed) portfela, które najczęściej ma postać 12 lub 24 słów, o ściśle ustalonej kolejności, zwanego czasem „frazą mnemoniczną". Na podstawie tych słów oprogramowanie jest w stanie wygenerować nasz klucz prywatny, dlatego ziarno musi być równie ściśle chronione, jak sam klucz.

Do portfela może być przypisane wiele **adresów**, pozwalających na wysyłanie i otrzymywanie kryptowalut. Można to porównać do posiadanego konta w banku, do którego przypisane jest kilka rachunków. Adres to unikalny ciąg alfanumeryczny, charakterystyczny dla danego rodzaju kryptowaluty, który może mieć również postać kodu QR. Nie wchodząc w szczegóły techniczne, adresy są tworzone na podstawie klucza publicznego za pomocą kilkustopniowego algorytmu, wykorzystującego kryptograficzne funkcje skrótu. Tworzenie adresu zostanie omówione w dalszej części rozdziału.

Transakcja kryptowalutowa to przekazanie pewnej „kwoty" z jednego lub więcej adresów na inny adres lub adresy. Aby dokonać transakcji należy być dysponentem środków należących do danego adresu (tzn. posiadać przypisany mu klucz prywatny) oraz znać adres odbiorcy. W świecie kryptowalut występuje kilka różnych metod transakcji, przy czym szczególnie wyróżnia się sieć Bitcoin, bazująca na schemacie tzw. niewydanego wyjścia transakcji (unspend transaction output, UTXO), omówiony w dalszej części rozdziału. Zdecydowana większość pozostałych kryptowalut używa zwykłego schematu opartego na aktualnym saldzie konta.



Źródło: PwC Digital Services.

Rys. 2. Ogólny schemat przebiegu transakcji kryptowalutowej. Źródło: PwC Digital Services

Użytkownik sieci tworzy transakcję wskazując adres docelowy i autoryzuje ją swoim kluczem prywatnym. Transakcja jest dołączana do aktualnego bloku zawierającego inne transakcje i taki blok jest rozgłaszany w danej sieci kryptowalutowej. Pełne węzły sieci (tzw. górnicy) weryfikują poprawność wszystkich transakcji w bloku rozwiązując skomplikowane problemy matematyczne. Górnik, który pierwszy rozwiąże problem (tzw. „wykopanie bloku"), otrzymuje nagrodę w postaci określonej ilości nowych jednostek kryptowaluty oraz sumę opłat transakcyjnych z wszystkich transakcji w bloku. Jest to pierwsze potwierdzenie prawidłowości całego bloku. Kolejne węzły sieci potwierdzają prawidłowość bloku, przy czym nie muszą już roz-

wiązywać całego problemu matematycznego, a sprawdzają jedynie poprawność pierwszej weryfikacji. Całą operację potwierdzania prawidłowości bloku można porównać do popularnej łamigłówki Sudoku o bardzo wielu polach – prawidłowe rozwiązanie jest czasochłonne i skomplikowane, natomiast sprawdzenie poprawności rozwiązania nie stanowi problemu. Po otrzymaniu odpowiedniej ilości potwierdzeń z sieci blok jest dołączany do łańcucha bloków, a transakcje w nim zawarte zostają zapisane w porządku chronologicznym w „elektronicznej księdze rachunkowej" wszystkich transakcji danej sieci.

Bazując na technologii blockchain powstały kryptowaluty. Pierwszą w historii kryptowalutą był – jak już wspomniano – Bitcoin, którego pierwsze 50 jednostek powstało 3 stycznia 2009 roku w wyniku wygenerowania (wykopania) bloku zero (tzw. genessis block) przez Satoshi Nakamoto. Środki trafiły na adres:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

w tzw. transakcji coinbase i nie zostały nigdy wydane. Coinbase to jedyny rodzaj transakcji, która nie posiada adresu wejściowego, gdyż są to nowe jednostki kryptowaluty, stanowiące wynagrodzenie górnika, który „wykopie" jako pierwszy dany blok. Tak więc każda pierwsza transakcja w bloku będzie transakcją coinbase. Ciekawostką jest fakt, że adres 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa ciągle otrzymuje środki[14], i przez ponad 12 lat w 3185 transakcjach otrzymał łącznie 18.52833043 BTC (jednostek bitcoin). Adres nie posiada żadnych transakcji wychodzących, to znaczy, że posiadacz klucza prywatnego tego adresu jest dysponentem kwoty ponad 68 BTC, co na dzień 3 stycznia 2022 roku daje równowartość około 13 milionów złotych (3,17 mln dolarów USA). Drugą ciekawostką jest ukrycie

[14] https://www.blockchain.com/btc/address/1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa dostęp 03.01.2022 r.

wewnątrz bloku dodatkowych danych – tytułu artykułu pochodzącego z pierwszej strony dziennika „The Times" z dnia 3 stycznia 2009 roku o treści „The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"[15]. Artykuł dotyczył dyskusji prowadzonej w brytyjskim rządzie na temat drugiego dofinansowania banków, a było to w szczytowym okresie światowego kryzysu gospodarczego na rynkach finansowych. Dziś interpretuje się ten wpis jako pochwałę przez Satoshi Nakamoto znaczenia niezależnego systemu płatności kryptowalutą Bitcoin.

Kolejne bitmonety uzyskane w wyniku wykopania nowych bloków od 1 do 8 również trafiają na pojedyncze adresy i do dziś nie zostały wydane.

Blok 0	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Blok 1	12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX
Blok 2	1HLoD9E4SDFFPDiYfNYnkBLQ85Y51J3Zb1
Blok 3	1FvzCLoTPGANNjWoUo6jUGuAG3wg1w4YjR
Blok 4	15ubicBBWFnvoZLT7GiU2qxjRaKJPdkDMG
Blok 5	1JfbZRwdDHKZmuiZgYArJZhcuuzuw2HuMu
Blok 6	1GkQmKAmHtNfnD3LHhTkewJxKHVSta4m2a
Blok 7	16LoW7y83wtawMg5XmT4M3Q7EdjjUmenjM
Blok 8	1J6PYEzr4CUoGbnXrELyHszoTSz3wCsCaj

Tabela 1. Adresy, na które trafiły nowe bitcoiny wykopane w blokach 0-8

Dopiero bitcoiny uzyskane z 9 bloku są przekazywane na inne adresy portfeli. Co ciekawe, pierwszą w historii transakcją kryptowalutą Bitcoin jest przekazanie 10 BTC z portfela należącego do Satoshi Nakamoto (12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S) na portfel Hala Finneya,

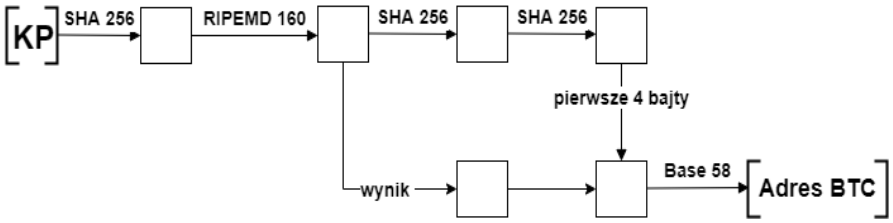
[15] https://comparic.pl/11-rocznica-genesis-pierwszego-bloku-bitcoina-jak-od-tego-czasu-zmienil-sie-btc/ dostęp 04.01.2022 r.

(1Q2TWHE3GMdB6BZKafqwxXtWAWgFt5Jvm3), twórcy wspomnianego już systemu „wielokrotnego dowodu pracy" (RPoW – reusable proof of work). Swoje kontakty z Satoshim oraz „przygodę" z kryptowalutą Bitcoin Hal Finney opisał na blogu[16].

Nowe bloki powstają średnio co 10 minut, a za „wykopanie" każdego bloku tzw. górnicy otrzymują nagrodę w postaci nowych bitmonet. Wraz ze wzrostem mocy obliczeniowej komputerów wzrasta również stopień skomplikowania obliczeń, a nagroda co cztery lata maleje o połowę – od 50 BTC w początkowej fazie do 6,25 BTC w roku 2021. Jeden bitcoin dzieli się na 100.000.000 mniejszych jednostek zwanych Satoshi. Zastosowana technologia ogranicza maksymalną ilość bitcoinów na rynku do 21 milionów, a ostatnia jednostka zostanie wydobyta około roku 2040.

Zanim zostaną przedstawione inne rodzaje transakcji w sieci Bitcoin, niezbędne jest poznanie typów adresów BTC oraz ich cech charakterystycznych. Historycznie pierwszym typem były adresy zaczynające się od cyfry 1 (Pay to PubkeyHash), do których przyporządkowany był jeden klucz prywatny wystarczający do autoryzowania transakcji. Adres składa się z 34 cyfr i liter, ale aby ograniczyć możliwości występowania pomyłek nie może zawierać dużych liter: O i I, małej litery l oraz cyfry 0. Adres jest tworzony na podstawie klucza publicznego za pomocą kilkustopniowego algorytmu przedstawionego na rysunku 3.

[16] https://bitcointalk.org/index.php?topic=155054.0 dostęp 04.01.2022 r.



Opracowanie własne.
Rys. 3. Algorytm tworzenia adres BTC z klucza publicznego

Dla klucza publicznego [KP] wylicza się wartość kryptograficznej funkcji skrótu SHA-256, a wynik stanowi argument kolejnej funkcji skrótu – RIPEMD-160. Uzyskaną wartość poddaje się dwukrotnie ponownemu działaniu kryptograficznej funkcji skrótu SHA-256, a wynik (pierwsze cztery bajty) dodaje się do prawej strony wyniku działania funkcji RIPEMD-160. Tak utworzoną wartość poddaje się przekształceniu za pomocą funkcji kodującej Base58 a otrzymany ciąg znaków jest adresem BTC. Przykładem adresu typu pierwszego jest przedstawiony już 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. Przyczynami dość skomplikowanego uzyskiwania adresu BTC są:

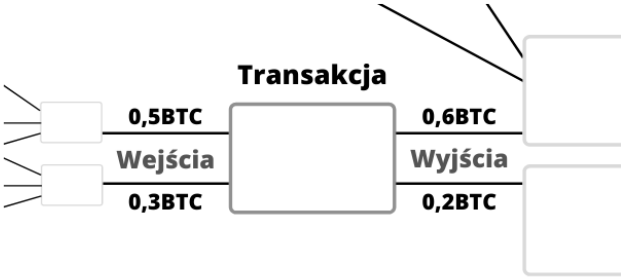
- bezpieczeństwo – zastosowanie dwóch różnych funkcji skrótu powoduje, że nawet złamanie algorytmu jednej z nich nie powoduje kompromitacji całego procesu obliczania adresu,
- redukcja długości adresu – łatwiejsze zarządzanie adresem długości 35 znaków niż kilkakrotnie dłuższym kluczem publicznym,
- uniknięcie możliwych pomyłek przez zastosowanie kodowania Base58 (wynik nie zawiera znaków 0, O, I, l)[17].

[17] P. Rodwald, Kryptowaluty z perspektywy informatyki śledczej, Wydawnictwo Akademickie AMW, Gdynia 2020 r.

Drugim typem są adresy zaczynające się od cyfry 3 (Pay to ScriptHash), do których przyporządkowana jest większa ilość kluczy prywatnych, umożliwia zarządzanie środkami przez więcej niż jedną osobę i do autoryzacji transakcji wymagana jest znajomość n kluczy z ogólnej puli m. Należy to rozumieć również w ten sposób, że do portfela przypisane są dwa klucze prywatne, a do wydania środków wystarczy użycie jednego z nich. Podobnie jak w adresach typu pierwszego, nie mogą zawierać dużych liter: O i I, małej litery l oraz cyfry 0. Przykładem adresu 2 typu jest 33Nzsv2jtUPkzoqXTvU1qZZhHyYR5TJnJN.

Typ trzeci, adresy zaczynające się od bc1, to najnowszy rodzaj wprowadzony w 2017 roku w wyniku jednej z najważniejszych zmian w pierwotnym protokole Bitcoin (Segregated Witness – SegWit). Adresy tego typu mogą zawierać tylko cyfry i małe litery (bez wyłączenia małej litery l), a dopuszczalna długość adresu to 62 znaki. Transakcje wychodzące z tych adresów charakteryzują się najmniejszą objętością w bloku, co powoduje niższe opłaty transakcyjne dla użytkowników. Aktualnie jeszcze niewiele giełd obsługuje ten typ adresów. Przykładem adresu typu 3 jest bc1qfuwvcfk42nnyv8rjgr9ml3ru49cl8drlc8km5r.

Zmierzając do przedstawienia możliwości śledzenia transakcji kryptowalutą Bitcoin niezbędne jest zrozumienie reguł, na których się opierają oraz poznanie ich rodzajów. Cechą charakterystyczną wszystkich transakcji w sieci Bitcoin jest oparcie ich na schemacie tzw. niewydanego wyjścia transakcji (unspend transaction output – UTXO). Transakcje kryptowalutowe składają się z co najmniej jednego wejścia i wyjścia. Za każdym razem, gdy dokonywana jest transakcja, użytkownik przyjmuje środki z jednego lub więcej adresów, aby służyły jako dane wejściowe. Następnie użytkownik dostarcza swój podpis cyfrowy, aby potwierdzić własność środków wejściowych i uzyskuje prawo do ich wydania. Środki te stają się nowymi niewydanymi wyjściami transakcji (UTXO), które później stają się danymi wejściowymi w nowej transakcji.



Źródło: https://blokpres.pl/jak-dzialaja-transakcje-bitcoin-wyjasnienie-modelu-utxo.
Rys. 4. Model transakcji Bitcoin

Wyjaśnijmy to na przykładzie. Alicja ma w portfelu 0,8 BTC. To raczej zbiór niewydanych wyjść, które otrzymała wcześniej. W szczególności posiada dwa UTXO o wartości 0,5 BTC i 0,3 BTC – dane wyjściowe z poprzednich dwóch transakcji. Teraz wyobraźmy sobie, że Alicja musi zapłacić Stefanowi 0,6 BTC. Jej jedyną opcją jest skumulowanie środków z wejścia, wysłanie 0,6 BTC do Stefana i 0,2 BTC z powrotem do siebie. Normalnie odzyskałaby mniej niż 0,2 BTC z powodu opłat za transakcję, ale dla uproszczenia pominiemy tą należność. Alicja tworzy transakcję, którą sieć rozumie jako: weź moje 0,8 BTC jako dane wejściowe, podziel je, wyślij 0,6 BTC na adres Stefana i zwróć 0,2 BTC na mój adres. Wysłane 0,6 BTC to teraz zużyte UTXO i Alicja nie można go ponownie wykorzystać. W międzyczasie powstały dwa nowe UTXO: 0,6 BTC u Stefana i 0,2 BTC u Alicji[18].

Mając powyższe na uwadze, można sformułować podstawowe zasady, na których opierają się transakcje w sieci Bitcoin:

[18] https://academy.binance.com/en/glossary/unspent-transaction-output-utxo dostęp 07.12.2021 r.

- każda transakcja składa się ze strony wejściowej (co najmniej jeden adres BTC) oraz strony wyjściowej (co najmniej jednego adresu, na który zostaną wysłane bitcoiny),
- wejściowe adresy muszą posiadać co najmniej taką wielkość sumy niewykorzystanych wyjść, jak wartość transakcji (z uwzględnieniem opłaty transakcyjnej),
- cała suma z adresów wejściowych musi zostać wydana w pojedynczej transakcji, przy czym po stronie wyjściowej może znajdować się jeden z adresów ze strony wejściowej,
- przesłanie środków na inny adres nie musi oznaczać przekazania ich innej osobie – istnieją transakcje, w których właściciel przekazuje środki z jednego adresu na drugi w ramach tego samego portfela lub też różnych portfeli. Jednym z przykładów może być tzw. transakcja konsolidująca omówiona w dalszej części rozdziału,
- każdy użytkownik może posiadać wiele portfeli, a każdy portfel zawierać wiele adresów,
- jeżeli po stronie wejściowej w jednej transakcji występuje dwa lub więcej portfeli, tzn., że są one podpisane tym samym kluczem prywatnym, czyli ich dysponentem jest jedna osoba (podmiot). O takiej sytuacji mówi się, że adresy należą do wspólnego klastra.

W sieci Bitcoin możemy wyróżnić następujące rodzaje transakcji:

- „zero do jeden" – opisana już tzw. coinbase, nie posiadająca adresu wejściowego, a tylko adres wyjściowy,
- „jeden do jeden" – posiada jeden adres wejściowy i jeden wyjściowy, gdzie całość środków z adresu A jest przekazana na adres B. Tego rodzaju transakcje stosunkowo rzadko występują w łańcuchu bloków (mniej niż 10 % ogólnej liczby),

- „jeden do dwóch" – środki z jednego trafiają na dwa adresy, przy czym jeden z adresów wyjściowych może być tożsamy z wejściowym, na który trafia reszta z transakcji. Niektóre portfele każdorazowo generują nowy adres dla resztowej kwoty. Takie transakcje stanowią większość w łańcuchu bloków,
- „wiele do wielu" – ten rodzaj można podzielić na typy, różniące się między sobą:
  - „wiele do jeden" – środki z kilku (wielu) adresów trafiają na jeden. Jest to przykład transakcji konsolidacyjnej, gdzie środki z wielu adresów należących do tego samego dysponenta trafiają na adres zbiorczy, również do niego należący. Mniej prawdopodobna (ale nie niemożliwa) jest sytuacja, kiedy dysponent dokonuje płatności innej osobie kumulując dokładnie taką kwotę z wielu swoich adresów,
  - „wiele do dwóch" – występuje w sytuacji, gdy dysponent dokonuje płatności z kilku swoich adresów ma adres odbiorcy, a reszta trafia na adres resztowy dysponenta. Ten typ transakcji stanowi drugi najczęściej występujący w łańcuchu bloków z udziałem ponad 20%,
  - „wiele do wielu" – z wielu adresów wejściowych środki są przekazywane na wiele adresów wyjściowych. Transakcje tego typu są wykonywane przez podmioty lub serwisy obsługujące znaczną liczbę transakcji, a ich celem jest oszczędność na opłatach transakcyjnych lub zwiększenie anonimowości

użytkowników (w przypadku mikserów). Tego typu transakcje nie przekraczają 5 % udziału w ogólnej liczbie[19].

Wyjaśnienia wymaga pojęcie miksera. Jest tu usługa udostępniona przez dedykowane serwisy internetowe, której zadaniem jest dalsze zwiększenie anonimowości właścicieli portfeli poprzez zmieszanie środków pochodzących od wielu użytkowników i tym samym przerwanie możliwości śledzenia konkretnego ciągu transakcji. Po rejestracji na takiej platformie generowany jest indywidualny adres dla każdego użytkownika, na który przesyła on bitmonety, mieszane następnie ze środkami innych użytkowników, a często są one dodatkowo przesyłane pomiędzy wieloma portfelami należącymi do tego miksera. Po zakończeniu procesu i odliczeniu prowizji środki mogą być zwrócone nadawcy bądź przesłane – zgodnie z dyspozycją – do nowego właściciela[20].

Podsumowując, pomimo ograniczeń technologicznych w maksymalnym dopuszczalnym wolumenie Bitcoina i specyficznym, stosunkowo skomplikowanym przesyłaniu środków opartym na schemacie niewydanego wyjścia transakcji, BTC nadal dominuje na rynku kryptowalut oraz zachowuje najwyższą kapitalizację[21]. Jak każda kryptowaluta, Bitcoin jest walorem szczególnie spekulacyjnym, zaliczającym nagłe wzrosty i spektakularne

[19] Udział procentowy określonych rodzajów transakcji zawarty w: P. Rodwald, Kryptowaluty z perspektywy informatyki śledczej, Wydawnictwo Akademickie AMW, Gdynia 2020 r.

[20] P. Opitek, K. Góral, Analiza kryminalna transferów kryptowalutowych w pracy prokuratora, cz. II, (w) Prokuratura i Prawo, 6/2020

[21] Na dzień 7 grudnia 2021 roku na rynku było 18.894.075 BTC, a jego kapitalizacja wynosiła 950.244.244.218 USD, https://bitinfocharts.com/index_v.html dostęp 07.12.2021 r.

spadki, często bez wyraźnych powodów, co nie przeszkadza w systematycznym, znacznym wzroście jego wartości[22].

Ethereum jest zdecentralizowaną platformą opartą o oprogramowanie open source, bazujące na technologii blockchain. Pomysłodawcą był zespół skupiony wokół Vitalika Buterina, który w latach 2013-2014 opracował podstawy platformy, a środki na dalszy rozwój (ponad 18 milionów dolarów) pozyskano dzięki emisji własnych tokenów, które miały być wymienione na przyszłą kryptowalutę.

Ether, często błędnie nazywany „Ethereum", jest kryptowalutą protokołu Ethereum i – podobnie jak w przypadku Bitcoina – bazuje na systemie dowodu pracy (Proof Of Work) oraz generuje nowe jednostki Ether jako nagrodę dla węzłów (górników), które dodały nowy blok do łańcucha bloków (dzieje się to co 12 sekund). Zastosowana technologia nie ogranicza ilości jednostek Ether na rynku, a model transakcji bazuje na aktualnym saldzie konta, co jest znacznie prostsze niż model UTXO. Adresy portfeli mają długość 40 znaków i zawierają tylko znaki wykorzystywane w notacji heksadecymalnej, to jest cyfry od 0 do 9 oraz litery a,b,c,d,e,f. Przykładem adresu kryptowaluty Ether jest:

0x0681d8Db095565FE8A346fA0277bFfdE9C0eDBBF.

Transakcje są realizowane pomiędzy pojedynczymi portfelami, co znacznie upraszcza analizę drogi przesyłanych środków w Ether. Platforma Ethereum, oprócz środowiska emisji i płatności Ether, obsługuje zdecentralizowane aplikacje oraz tzw. inteligentne kontrakty (smart contract) w ramach sieci peer-to-peer. Warto wspomnieć, że platforma Ethereum jest wykorzystywana w środowisku Initial Coin Offering (ICO) jako metoda pozyskiwania

---

[22] sierpień 2016: 1 BTC=2315 zł., marzec 2017: 3880 zł., marzec 2018: 31756 zł, marzec 2019: 15.800 zł, marzec 2020: 33.930 zł., grudzień 2020: 69.632 zł., styczeń 2021: 119.028 zł., wrzesień 2021: 176.900 zł., grudzień 2021: 208.000 zł., https://www.blockchain.com/explorer dostęp 07.12.2021 r.

kapitału w postaci kryptowalut lub tokenów w celu finansowania przedsięwzięcia, najczęściej typu startup. Ether jest drugą po Bitcoinie najpopularniejszą kryptowalutą na rynku[23].

Kryptowaluta Monero, powstała w 2014 roku, również jest oparta na technologii blockchain oraz oprogramowaniu open source, ale z wbudowanymi mechanizmami zwiększającymi prywatność. Pomimo wykorzystywania publicznej księgi transakcji, adresy i kwoty transakcji nie są ujawniane. Adresy użytkowników są zabezpieczone przez tzw. sygnatury pierścieniowe, które grupują adres nadawcy z innymi adresami, a odbiorcy są chronieni za pomocą „ukrytych adresów", generowanych tylko do przyjęcia środków z pojedynczej transakcji. Te funkcje są wbudowane w protokół, chociaż użytkownicy mogą opcjonalnie udostępniać adresy i kwoty transakcji. Sieć Monero również jest oparta na systemie dowodu pracy, nowe jednostki są generowane jako nagroda dla górników, a zastosowany algorytm umożliwia dość wydajne wydobywanie bitmonet na pojedynczych komputerach dobrej klasy. Nowe bloki są generowane średnio co dwie minuty, brak jest ograniczeń maksymalnego wolumenu Monero na rynku, a przykładowy adres ma postać: 42jFnXU5ic82n8JhJEdnEw7PxZDS1qcu7Emzj1wSmZSn-HEn7CpJbKPLdg8eM8pi7l[24]. Funkcje ochrony prywatności sprawiły, że Monero stało się bardzo popularne wśród przestępców chcących skutecznie ukryć transfery pieniężne.

[23] Na dzień 8 grudnia 2021 roku na rynku było 118.655.928 ETH, a jego kapitalizacja wynosiła 522.398.022.396 USD, https://bitinfocharts.com/index_v.html dostęp 08.12.2021 r.

[24] Na dzień 8 grudnia 2021 roku na rynku było 18.042.711 XMR, a jego kapitalizacja wynosiła 3.753.675.481 USD, https://bitinfocharts.com/index_v.html dostęp 08.12.2021 r.

Jan KLIMA

Analiza przepływów kryptowalutowych

Znając podstawy technologii blockchain, rodzaje transakcji, portfeli i adresów a także charakterystykę trzech rodzajów bitmonet najczęściej wykorzystywanych w przestępczym procederze można przystąpić do przedstawienia możliwości i ograniczeń w śledzeniu transferów kryptowalut pochodzących z przestępstw. Ze względu na swoją specyfikę, zwłaszcza w zakresie ochrony prywatności właścicieli portfeli, dostępności dla każdego, ale również szybkości transferów, braku ograniczeń geograficznych oraz niskich kosztów transakcyjnych kryptowaluty stały się bardzo popularne w środowiskach przestępczych. Zjawisko to jest widoczne na całym świecie, a ograny ścigania zostały postawione przed kolejnym wyzwaniem postawionym przez zaawansowane technologie, zaadoptowane przez świat przestępczy do własnych, nielegalnych celów. Ostatni raport Europolu „Internet Organised Crime Threat Assessment 2020" w jednym z kluczowych wniosków wskazał na kryptowaluty jako istotny element działalności przestępczej i legalizacji zysków na świecie[25]. „Cryptocurrency Crime and Anti-Money Laundering Report", wydawany co kwartał przez firmę Ciphertrace, znaną na świecie z produkcji oprogramowania do śledzenia transferów bitmonet, kolejny raz wskazuje na ciągły, systematyczny wzrost kradzieży i oszustw na rynku kryptowalut, a także prania pieniędzy z ich wykorzystaniem[26]. Przedstawienie poszczególnych rodzajów przestępstw, ukierunkowanych na kradzież kryptowalut czy też sposób ich wykorzystania w procederze prania pieniędzy wykracza jednak poza ramy tego rozdziału. Organy ścigania każdego roku prowadzą tysiące postępowań przygotowawczych z zakresu

[25] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_ iocta_2020.pdf dostęp 08.12.2021 r.

[26] https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/ dostęp 08.12.2021 r.

oszustw komputerowych, hackingu, wykorzystania ransomware do żądania okupu, cryptojackingu[27] czy też prania pieniędzy przy pomocy kryptowalut. Jednym z narzędzi skutecznego przeciwdziałania i ścigania takich przestępstw jest analiza historii adresów kryptowalutowych i aplikacji do ich przechowywania, a przede wszystkim transferu środków w celu identyfikacji innych portfeli i adresów należących tej samej osoby, portfeli innych osób uczestniczących w procederze, adresów pośrednich oraz ustalenie giełd i innych podmiotów, które umożliwiają wymianę kryptowalut na dowolną walutę fiducjarną[28]. Metoda „follow the money" (podążaj za pieniędzmi) stanowi od lat jedną z najbardziej skutecznych metod rozpoznania grup przestępczych i rozmiaru ich działalności.

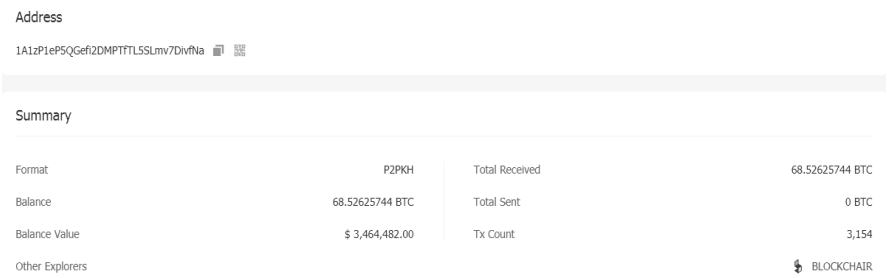
Większość postępowań przygotowawczych, w których występuje potrzeba śledzenia transferów kryptowalutowych rozpoczyna się od identyfikacji adresu, należącego do sprawcy. Aby zachować przejrzystość rozdziału, w tej części zostaną przedstawione możliwości i trudności w analizie transakcji Bitcoin. Pierwszym krokiem jest sprawdzenie adresu w serwisach bazujących na kompletnym łańcuchu bloków (blockchain explorer). W sieci istnieje wiele takich serwisów[29]. Podsumowanie historii danego adresu znajduje się w górnej części strony i zawiera kilka istotnych informacji: sumę otrzymanych i wysłanych środków, ilość transakcji, aktualne saldo w BTC i USD (w przeliczeniu po aktualnym kursie).

---

[27] Cryptojacking – przestępstwo polegające na zainfekowaniu komputera złośliwym oprogramowaniem, które uruchamia na urządzeniu skrypt do wydobywania kryptowalut bez wiedzy użytkownika, co w efekcie prowadzi do kradzieży energii elektrycznej.

[28] Waluty fiducjarne, zwane też walutami FIAT, to legalne środki płatnicze, emitowane przez poszczególne państwa (związki państw) i przez nie gwarantowane np. dolar USA, polski złoty, EURO.

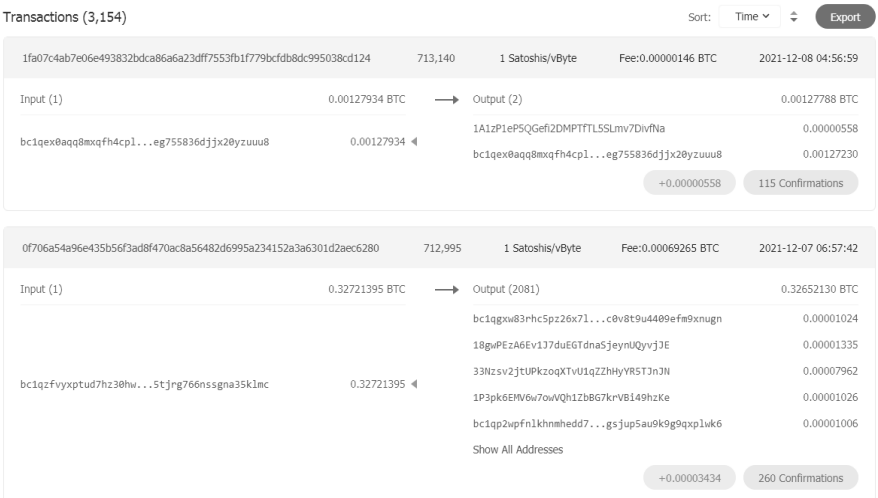
[29] Np. www.blockchain.com/explorer, www.btc.com.



Źródło: opracowanie własne na podstawie www.btc.com.

Rys. 5. Podsumowanie adresu BTC

Poniżej znajduje się historia wszystkich transakcji, w jakich uczestniczył adres BTC. Każda transakcja zawiera następujące dane: jej identyfikator, numer bloku, w którym jest zawarta, datę i godzinę, adresy wejściowe i wyjściowe, kwotę, wartość opłaty transakcyjnej (fee) oraz liczbę potwierdzeń sieci.



Źródło: opracowanie własne na podstawie www.btc.com.

Rys. 6. Fragment historii transakcji

Zanim rozpoczniemy śledzenie poszczególnych transakcji, warto dokonać jeszcze kilku sprawdzeń danego adresu. Serwis wwww.walletexplorer.com umożliwia identyfikację części adresów należących do giełd, niestety – nie wszystkich. Ponadto umożliwia sprawdzenie, czy i ile adresów występuje w tzw. klastrze, to znaczy jest podpisanych tym samym kluczem prywatnym, co świadczy, że ich dysponentem jest jedna osoba lub podmiot. Taka informacja jest niezmiernie istotna w ustaleniu innych, nieznanych wcześniej adresów będących w dyspozycji sprawcy. Przykładem niech będzie:

18x222Km8Pj2ZbMUQbqyYAJA1nw6fBtv6m,

jeden z adresów pośrednich, poprzez który były prane środki pochodzące z kampanii ransomware Petya.

Wallet [00d5f506df] (show transactions)

Page 1 / 1 (total addresses: 5)

address	balance	incoming txs	last used in block
13Bi8RCWsrKzHUGfFozRbeHrx84TUxTLAQ	0.	1	506280
18hwy8F5coHAdWzKe56u2Sf7wGjb2phmH3	0.	1	506280
18x222Km8Pj2ZbMUQbqyYAJA1nw6fBtv6m	0.	1	506280
1Hj2b6mcqKWTQi7hSW8WwCemZKw4mXdteM	0.	1	506280
1QHWLhtKAMg4bQQgUg8kfuWXDa1Qdb3yVH	0.	1	506280

Page 1 / 1 (total addresses: 5)

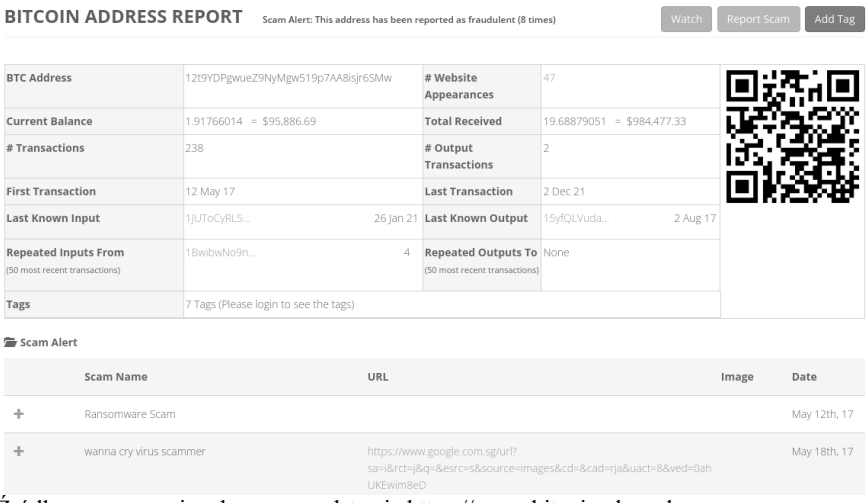
Źródło: opracowanie własne na podstawie www.walletexplorer.com.

Rys. 7. Identyfikacja innych adresów w klastrze

Jak przedstawiono na rysunku 7, adres 18x222Km8Pj2ZbMUQbqyYAJA1nw6fBtv6m został zidentyfikowany w klastrze z czterema innymi portfelami. Niestety, sprawcy często wykorzystują jeden klucz prywatny przypisany tylko do jednego adresu.

Innym serwisem, na którym warto dokonać sprawdzeń, jest www.bitcoinwhoswho.com, który oferuje kilka ciekawych opcji oprócz podstawowych danych

dotyczących podsumowania historii adresu. Można tu znaleźć informacje dotyczące występowania adresu w oszukańczych kampaniach (np. scam[30], ransomware), dane o powtarzających się adresach wejściowych i wyjściowych z ostatnich 50 transakcji oraz linki do artykułów w sieci, w których wystąpił dany adres.



BITCOIN ADDRESS REPORT Scam Alert: This address has been reported as fraudulent (8 times) — Watch | Report Scam | Add Tag

BTC Address	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	**# Website Appearances**	47
Current Balance	1.91766014 = $95,886.69	**Total Received**	19.68879051 = $984,477.33
# Transactions	238	**# Output Transactions**	2
First Transaction	12 May 17	**Last Transaction**	2 Dec 21
Last Known Input	1JUToCyRL5... 26 Jan 21	**Last Known Output**	15yfQLVuda... 2 Aug 17
Repeated Inputs From (50 most recent transactions)	1BwibwNo9n... 4	**Repeated Outputs To** (50 most recent transactions)	None
Tags	7 Tags (Please login to see the tags)		

Scam Alert

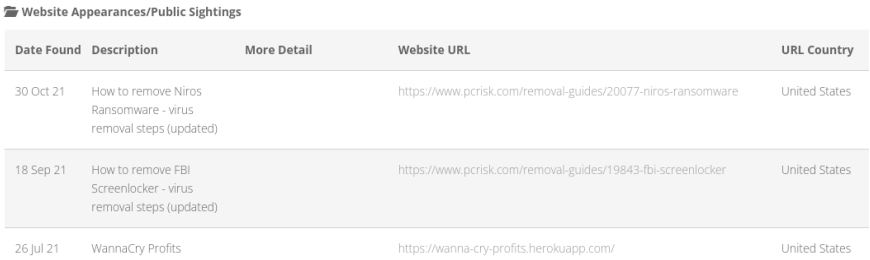
	Scam Name	URL	Image	Date
+	Ransomware Scam			May 12th, 17
+	wanna cry virus scammer	https://www.google.com.sg/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwim8eD		May 18th, 17

Źródło: opracowanie własne na podstawie https://www.bitcoinwhoswho.com.

Rys. 8. Identyfikacja alertów

[30] Scam – metoda oszustwa polegająca na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy lub innych składników majątkowych.

Zwłaszcza w powiązanych artykułach można znaleźć sporo interesujących i potrzebnych informacji, często identyfikujących kolejne adresy uczestniczące w przestępczym procederze, a nawet całościową analizę kampanii wraz z wykorzystywanymi adresami IP, domenami, serwerami C&C itp[31].



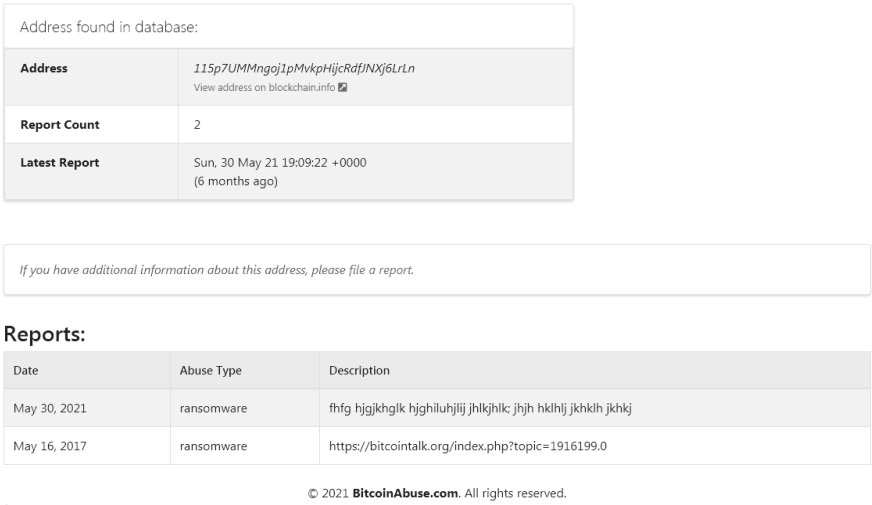
Website Appearances/Public Sightings

Date Found	Description	More Detail	Website URL	URL Country
30 Oct 21	How to remove Niros Ransomware - virus removal steps (updated)		https://www.pcrisk.com/removal-guides/20077-niros-ransomware	United States
18 Sep 21	How to remove FBI Screenlocker - virus removal steps (updated)		https://www.pcrisk.com/removal-guides/19843-fbi-screenlocker	United States
26 Jul 21	WannaCry Profits		https://wanna-cry-profits.herokuapp.com/	United States

Źródło: opracowanie własne na podstawie https://www.bitcoinwhoswho.com.
Rys. 9. Linki do artykułów powiązanych z adresem

Równie wartościowy serwis identyfikujący oszukańcze kampanie, w których występował adres, to www.bitcoinabuse.com. Strona zawiera publiczną bazę adresów bitcoin wykorzystywanych przez hakerów i przestępców. Poprzez dedykowany formularz można dokonać zgłoszenia adresu zidentyfikowanego jako wykorzystywany do popełniania przestępstw, jak również uzyskać dodatkowe informacje dotyczące adresów aktualnie uczestniczących w oszukańczych kampaniach.

[31] np. https://malware.news/t/an-analysis-of-the-wannacry-ransomware-outbreak/11908



Address found in database:

Address	*115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn* View address on blockchain.info
Report Count	2
Latest Report	Sun, 30 May 21 19:09:22 +0000 (6 months ago)

If you have additional information about this address, please file a report.

Reports:

Date	Abuse Type	Description
May 30, 2021	ransomware	fhfg hjgjkhglk hjghiluhjlij jhlkjhlk; jhjh hklhlj jkhklh jkhkj
May 16, 2017	ransomware	https://bitcointalk.org/index.php?topic=1916199.0

Źródło: opracowanie własne na podstawie https://www.bitcoinabuse.com.

Rys. 10. Identyfikacja alertów

Warto również wykorzystać możliwości wyszukiwawcze ogólnodostępnych wyszukiwarek internetowych. W zasobach sieci znajduje się mnóstwo informacji często mogących pomóc poszerzyć wiedzę na temat danego adresu BTC, przy czym warto stosować operatory wyszukiwawcze pozwalające na ograniczenie ilości wyników. Poszukując informacji o kolejnym adresie występującym w kampanii Wannacry –

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

bez problemu trafimy na informację o jego powiązaniach z innymi adresami uczestniczącymi w tej kampanii.

Źródło: opracowanie własne na podstawie bitcointalk.org/index.php?topic=1916199.0.
Rys. 11. Identyfikacja innych adresów powiązanych z daną kampanią

Przystępując do analizy transferów pomiędzy adresami BTC należy zaznaczyć, że ze względu na specyfikę sieci Bitcoin oraz rodzaje transakcji, każda analiza będzie oparta na metodach opartych o heurystykę[32], czyli nie

[32] Heurystyka - umiejętność wykrywania nowych faktów i związków między faktami, zwłaszcza czynność formułowania hipotez (przeciwstawiana czynności uzasadniania) prowadząca do poznania nowych prawd naukowych. https://encyklopedia.pwn.pl/haslo/heurystyka;4008452.html dostęp 08.12.2021 r.

gwarantująca kategorycznych wniosków. Wskazując możliwości śledzenia transferów kryptowalutowych będziemy bazować na rozwiązaniach ogólnodostępnych, przy czym należy zauważyć, że oferowane na rynku programy komercyjne również nie gwarantują 100 % poprawności dokonywanych analiz, gdyż nie istnieje metoda pozwalająca na jednoznaczną, niepodważalną identyfikację ścieżki przepływu środków, a tym bardziej personalizacji właściciela. Przedstawiony już został sposób ustalania innych adresów będących we wspólnym klastrze z analizowanym adresem. Natomiast jeżeli po prawej stronie występują dwa adresy wyjściowe, to z dużą dozą prawdopodobieństwa jeden z nich jest adresem, na który trafia reszta z transakcji. Identyfikacja adresu resztowego do 2013 roku była bardzo prosta, gdyż wskutek błędu w protokole sieci Bitcoin adres resztowy występował zawsze jako pierwszy z portfeli wyjściowych. W roku 2013 błąd został naprawiony i obecnie identyfikacja adresu resztowego nie jest tak oczywista. Niemniej jednak umiejętność jego prawidłowego wskazania jest bardzo istotna z punktu widzenia dalszej analizy przepływu środków. Ważne jest, by ustrzec się od błędnego stwierdzenia, że adres resztowy jest faktycznym odbiorcą środków, zwłaszcza jeśli trafia na niego większa kwota niż na drugi z adresów wyjściowych występujący w transakcji. Wracając do istoty problemu, należy wziąć pod uwagę kilka elementów:

- jeżeli portfel generuje nowe adresy dla każdej reszty z transakcji, to adresy te muszą być podpisane tym samym kluczem prywatnym, czyli należeć do wspólnego klastra, który można zidentyfikować,
- sprawdzenie historii adresów wyjściowych w eksploratorze bloków (np. na btc.com) – jeżeli jeden z adresów nigdy wcześniej nie był używany, a drugi (i ewentualnie kolejne) posiada już historię, to z dużym prawdopodobieństwem pierwszy z nich jest adresem resztowym,
- jeżeli obydwa adresy wyjściowe posiadają już historię (a żaden nie jest tożsamy z adresem wejściowym), to mamy do czynienia albo ze

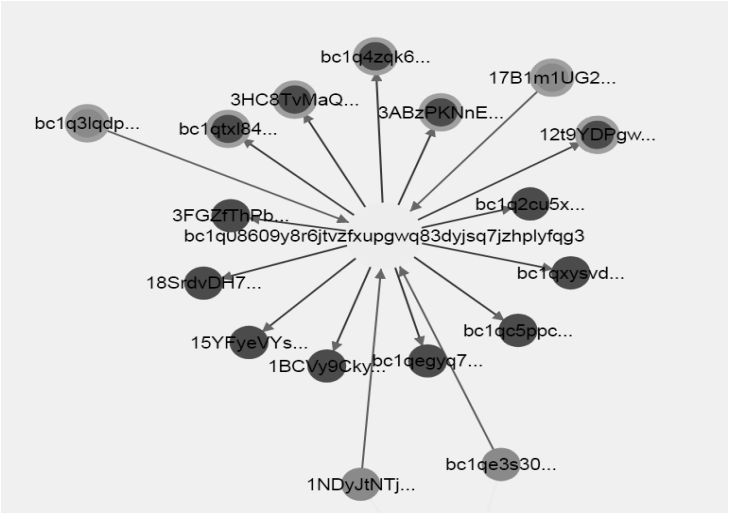
stosunkowo rzadko występującą transakcją 1 do 2, gdzie wyjściowe adresy należą do różnych portfeli, albo też z sytuacją, gdy portfel jest założony na platformie podmiotu (giełdy), która wszystkie transakcje wychodzące kieruje najpierw na własne adresy, a dopiero w kolejnym kroku środki trafiają na adresy docelowe. W takim przypadku ustalenie docelowego adresu jest możliwe jedynie na podstawie informacji posiadanych przez ten podmiot,

– istnieje możliwość, że na adres portfela założonego w podmiocie zajmującym się obrotem kryptowalutami użytkownik wpłaca większą, często „okrągłą" kwotę, a w późniejszym okresie następują systematyczne transfery mniejszych kwot w jednej transakcji na różne adresy, a reszta (dalej stosunkowo duża kwota) zostaje przesłana na nowy adres użytkownika.

Jak wynika z powyższych rozważań, prawidłowa interpretacja zapisów transakcji w sieci blockchain i właściwa identyfikacja adresów resztowych jest kluczowa dla dalszej analizy. Niestety, czasem się zdarza, że nie ma pewności co do prawidłowego zidentyfikowania danego adresu jako resztowego, dlatego zawsze trzeba mieć na uwadze ryzyko popełnienia błędu.

Analiza adresów, które uczestniczą w kilkudziesięciu lub kilkuset transakcjach byłaby bardzo utrudniona, a często wręcz niemożliwa bez stosowania specjalistycznego oprogramowania bądź wykorzystania serwisów internetowych oferujących taką możliwość. Jak wspomniano, zostaną przedstawione rozwiązania ogólnodostępne pozwalające na analizą przepływów kryptowalutowych. Na każdym etapie konieczne jest korzystanie z dowolnego eksploratora łańcucha bloków, np. z www.blockchain.com/explorer lub wspomnianego już btc.com. Równie niezbędne jest używanie serwisów wizualizujących transfery, zwłaszcza tych, które umożliwiają oznaczanie różnymi kolorami transakcji wychodzących i przychodzących, ukrycie niektórych transakcji, wyszukiwanie powiązań pomiędzy dwoma adresami czy też

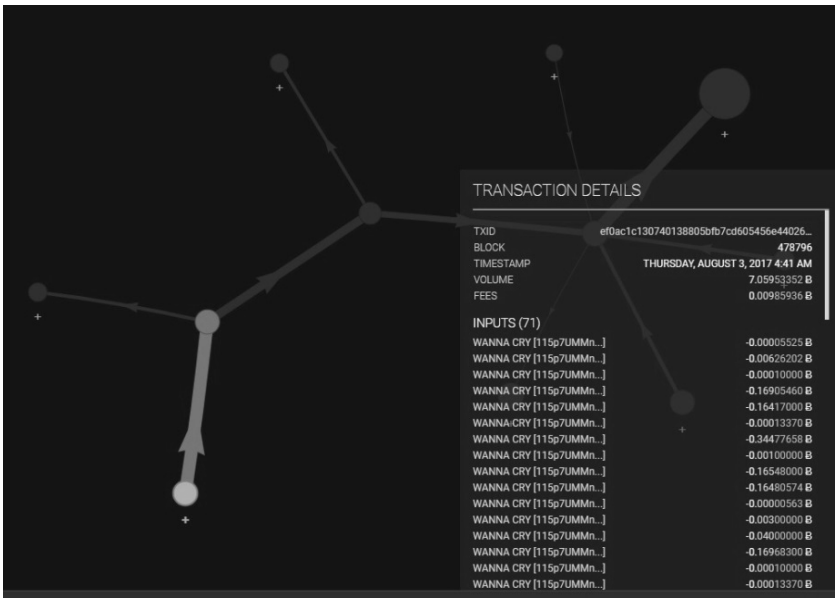
eksport danych do formatu csv lub xls. Przykładem takiego serwisu jest blockpatch.com.



Źródło: opracowanie własne na podstawie https://blockpath.com.

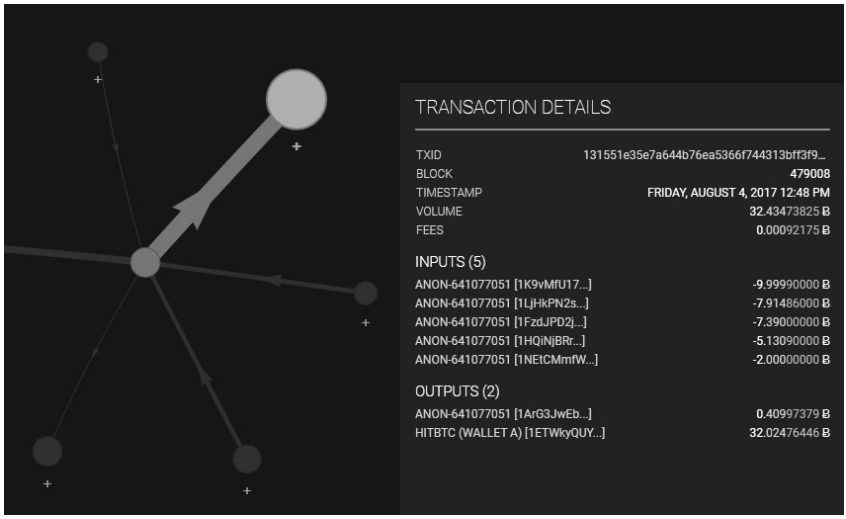
Rys. 12. Kolorowanie transakcji

Warto wspomnieć o jeszcze jednym serwisie, który integruje szereg opcji ciekawych z punktu widzenia analityka. Strona oxt.me do wykorzystania pełnych jej możliwości żąda założenia darmowego konta, wymagającego podania adresu e-mail i hasła. Po zalogowaniu się otrzymujemy dostęp do narzędzia, które umożliwia zarówno przeglądanie historii adresów, szczegółów transakcji, sprawdzenie ilości portfeli w klastrze, jak też wizualizuje transfery, identyfikuje giełdy kryptowalutowe na podstawie przypisanych do nich adresów a nawet potrafi wskazać, czy któryś z adresów był wykorzystywany w oszukańczych kampaniach. Niestety, nie ma możliwości ustawienia różnych kolorów dla transakcji przychodzących i wychodzących.



Źródło: opracowanie własne na podstawie otx.me.

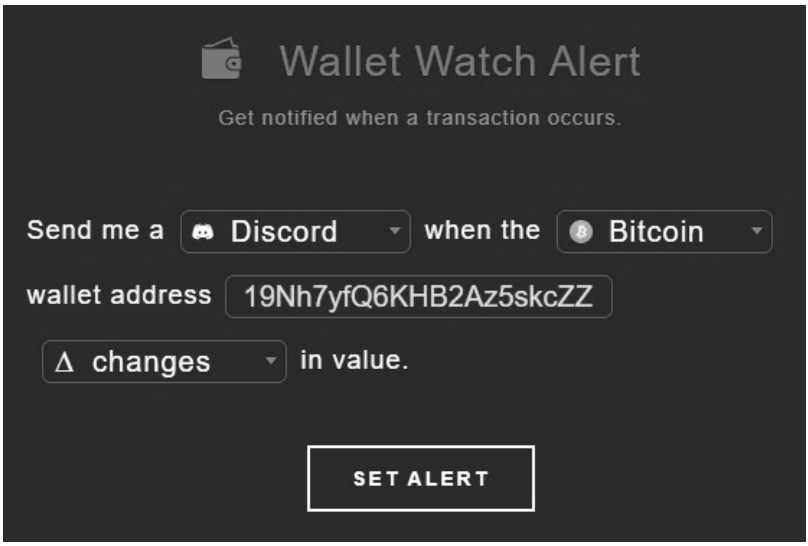
Rys. 13. Identyfikacja adresów z oszukańczych kampanii



Źródło: opracowanie własne na podstawie otx.me.

Rys. 14. Identyfikacja giełd kryptowalutowych

W analizie przepływów kryptowalutowych czasem może zaistnieć konieczność monitorowania adresów w oczekiwaniu na uruchomienie zawartych na nich środków. Z pomocą znów przychodzą nam serwisy internetowe. Jednym z nich jest https://cryptocurrencyalerting.com/wallet-watch.html, który w wersji bezpłatnej umożliwia nam ustawienie alertu w przypadku zmiany salda. Powiadomienie może być wysłane na adres e-mail, SMS, na komunikator Telegram, Slack, Discord i kilka jeszcze innych sposobów.



Źródło: opracowanie własne na podstawie https://cryptocurrencyalerting.com/wallet-watch.html.

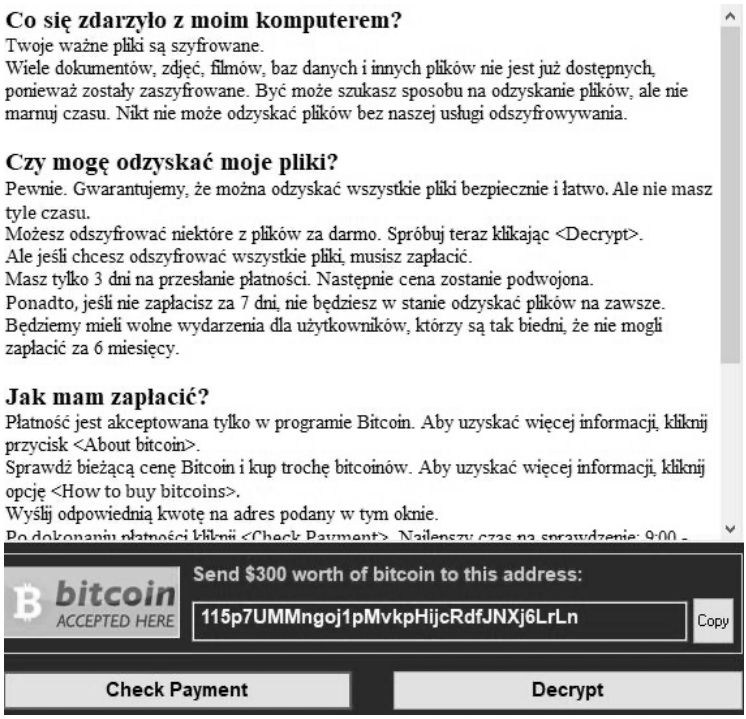
Rys. 15. Monitorowanie adresów Bitcoin. Ustawienie alertu

Analiza przepływu BTC w kampanii WannaCry.

Wykorzystując wymienione w artykule możliwości autor podjął próbę prześledzenia środków wpływających na adres:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn,

wykorzystywany w kampanii ransomware WannaCry. Zaczęło się od otrzymania takiego komunikatu:



Źródło: Materiały własne.

Rys. 16. Żądanie okupu za odszyfrowanie plików

Celem analizy była identyfikacja innych adresów powiązanych z adresem źródłowym, portfeli pośrednich oraz giełd kryptowalutowych, na których środki z kampanii zostały spieniężone. Analizą objęto czasokres od 3 do 10 sierpnia 2017 roku z uwagi na największe nasilenie ataków na terenie Polski. Ze względu na obszerność analizy, w artykule zostaną przedstawione tylko jej najważniejsze elementy.

Środki z portfela 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn (pojedynczy adres w klastrze) trafiają na 3 inne:

– 14Y8rfeRAcZkGqG451UGk1epq5zw3dVQif (pojedynczy w klastrze),
– 18gsrbQsTY7HzYVZEbvtVBfhywpQk6No2Q (w klastrze z 2 innymi),
– 1Q8maVpVNAZbPiavySQz9JaiwsfhbT9vBz (pojedynczy w klastrze).

W związku z faktem, że środki z pierwotnego adresu:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
trafiły na adres 18gsrbQsTY7HzYVZEbvtVBfhywpQk6No2Q, będący w klastrze z dwoma innymi:

– 1ARirZgU4q61sSjVK2iB8BEYC5w2B8ZnE9
– 1JC41YHmjKEcW1rLH6pmMWEFHkoNwSmhnC

przyjęto założenie, że mogą być to również pierwsze adresy pośrednie z innych adresów pierwotnych biorących udział w kampanii.

Wallet [12713bf467] (show transactions)

Page 1 / 1 (total addresses: 3)

address	balance	incoming txs	last used in block
18gsrbQsTY7HzYVZEbvtVBfhywpQk6No2Q	0.	1	478814
1ARirZgU4q61sSjVK2iB8BEYC5w2B8ZnE9	0.	1	478814
1JC41YHmjKEcW1rLH6pmMWEFHkoNwSmhnC	0.	1	478814

Page 1 / 1 (total addresses: 3)

Źródło: Opracowanie własne na podstawie www.walletexplorer.com.

Rys. 17. Identyfikacja innych portfeli w klastrze z 18gsrbQsTY7HzYVZEbvtVBfhywpQk6No2Q

Analizując wpływy w badanym okresie na te adresy fatycznie zidentyfikowano kolejne dwa adresy pierwotne:

– 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw,

– 3AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94.

Wyniki wyszukiwarki Google potwierdziły wykorzystanie tych adresów w kampanii Wannacry[33]. Na tym etapie mamy zidentyfikowane 3 adresy kryptowalutowe, na które trafiały środki od pokrzywdzonych w przedmiotowej kampanii.

Wracamy do początku analizy, tzn. poddajemy analizie część środków z adresu pierwotnego (115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn), które trafiły na adres:

14Y8rfeRAcZkGqG451UGk1epq5zw3dVQif.

Z tego adresu trafiają na dwa kolejne:

– 1Gb74viaTcmRpEf5E8znnHsj34yjRkCx83 (pojedynczy w klastrze)

– 19JCSFRPyXnVn7ptXyqmhLKNBAmPcksZS6 (w klastrze z 5 innymi adresami – Rys. 16).

Wallet [18045961a0] (show transactions)

Page 1 / 1 (total addresses: 6)

address	balance	incoming txs	last used in block
1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx	0.	2	479006
164Cg2p4QQ16VJGoBgiST5v2yDZtrvPgan	0.	1	479009
1A6ezvhzGmCqNmGTTzxphLkByuJfjbuwxr	0.	1	479009
1CZH527GEeR5WDyGac5WHrD6tnW5qJkFGR	0.	1	479009
1Em7vKSqAnFMpejf3fSPSQdxrx99ma856h	0.	1	479009
19JCSFRPyXnVn7ptXyqmhLKNBAmPcksZS6	0.	1	479006

Page 1 / 1 (total addresses: 6)

Źródło: Opracowanie własne na podstawie www.walletexplorer.com.

Rys. 18. Identyfikacja innych portfeli w klastrze z 19JCSFRPyXnVn7ptXyqmhLKNBAmPcksZS6

[33] https://cert.pl/posts/2017/05/wannacry-ransomware/ dostęp 10.12.2021 r.

W tej sytuacji można postawić hipotezę, że pozostałe adresy w klastrze również będą stanowić portfele pośrednie. Natomiast idąc śladem środków z adresu:
19JCSFRPyXnVn7ptXyqmhLKNBAmPcksZS6
okazuje się, że są one przesłane na dwa kolejne adresy:

- 1J8gPWbDb7cVdfaAvioaLhgYPPGA127UQL (pojedynczy adres). Bitcoiny z tego adresu trafiają na: 19Nh7yfQ6KHB2Az5skcZZMAbB4uiz4fWUy, zidentyfikowany jako giełda MercadoBitcoin.com.br (w klastrze 391.714 adresów - rys. 17).
-

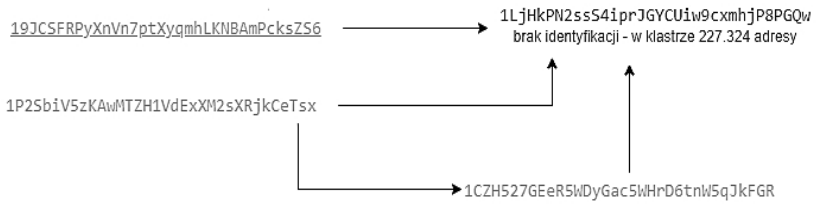
Źródło: Opracowanie własne na podstawie www.walletexplorer.com.

Rys. 19. Identyfikacja adresu 19Nh7yfQ6KHB2Az5skcZZMAbB4uiz4fWUy należącego do giełdy

oraz:

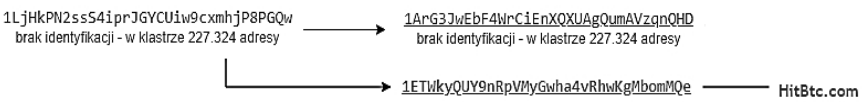
- 1LjHkPN2ssS4iprJGYCUiw9cxmhjP8PGQw (w klastrze 227.324 adresy – prawdopodobnie giełda, ale brak identyfikacji podmiotu).

Na adres 1LjHkPN2ssS4iprJGYCUiw9cxmhjP8PGQw trafiają również środki z dwóch innych adresów będących we wspólnym klastrze (patrz Rys. 16), jak pokazano na rys. 20.



Materiały własne.
Rys. 20. Fragment wykresu analizy środków z kampanii Wannacry

Z adresu 1LjHkPN2ssS4iprJGYCUiw9cxmhjP8PGQw część środków trafia na adres 1ArG3JwEbF4WrCiEnXQXUAgQumAVzqnQHD (będący z nim we wspólnym klastrze liczącym – jak już wskazano – 227.324 adresów, ale brak identyfikacji podmiotu) natomiast część na adres 1ETWkyQUY9nRpVMyGwha4vRhwKgMbomMQe, jednoznacznie zidentyfikowany jako należący do giełdy HitBtc.com[34].



Materiały własne.
Rys. 21. Fragment wykresu analizy środków z kampanii Wannacry

Jak wcześniej wspomniano, z adresu 14Y8rfeRAcZkGqG451UGk1epq5zw3dVQif środki trafiają na dwa kolejne:

– 1Gb74viaTcmRpEf5E8znnHsj34yjRkCx83 (pojedynczy w klastrze)

[34] https://www.walletexplorer.com/wallet/HitBtc.com?from_address=1ETWkyQUY9nRpVMy Gwha4vRhwKgMbomMQe

– 19JCSFRPyXnVn7ptXyqmhLKNBAmPcksZS6 (w klastrze z 5 innymi).

Analiza drugiego z wymienionych została przedstawiona wyżej. Teraz zajmiemy się przepływem z adresu 1Gb74viaTcmRpEf5E8znnHsj34yjRkCx83, z którego środki przez dwa kolejne adresy pojedyncze w klastrze trafiają docelowo na adresy będące w klastrze z dziesiątkami tysięcy innych:

– 3MsLXgc452gNMmS7uhXm9sEYmaCecPSDsP z 1.223.261 adresów,
– KwA4fS4uVuCNjCtMivE7m5ATbv93UZg8V - z 73.725 adresów,
– 13B9CuS24yyy9q3KV6PtSkbrG74BBVRDYm oraz
– 13KFUKV1XAy3uGcdjWk5bkVx5oxjL4QraP z 40.090 adresami (rys. 22).

Z uwagi na ilość adresów w klastrze można przypuszczać, że są to adresy giełd lub kantorów zajmujących się obrotem kryptowalutami, ale niestety we wszystkich czterech przypadkach bezpłatne narzędzia nie identyfikują podmiotu. W tej sytuacji należałoby przesłać zapytanie o przedmiotowe adresy do zidentyfikowanych w tej analizie giełd (istnieje szansa, że sprawcy korzystają tylko z kilku sprawdzonych przez siebie podmiotów), a w przypadku negatywnej odpowiedzi przesłać zapytanie do największych światowych giełd. Z posiadanego doświadczenia wynika, że prawdopodobieństwo identyfikacji podmiotu w ten sposób jest dość duże.

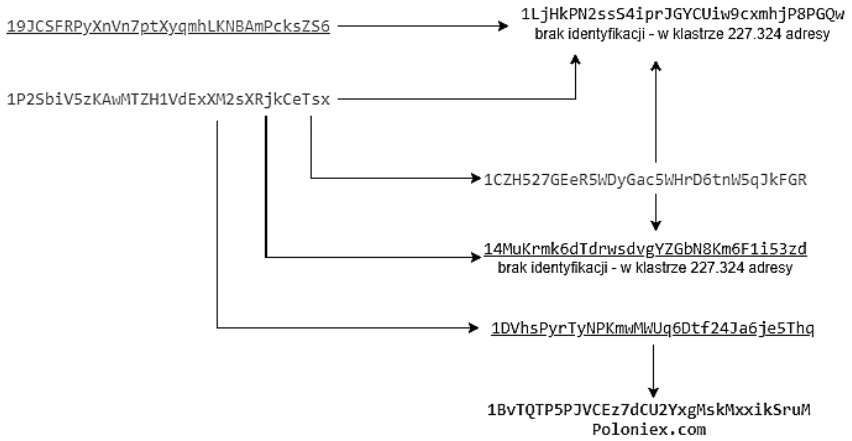
Materiały własne.

Rys. 22. Przepływ środków z adresu 1Gb74viaTcmRpEf5E8znnHsj34yjRkCx83

W dalszej części analizy należałoby prześledzić środki z pozostałych 5 adresów będące w klastrze z 19JCSFRPyXnVn7ptXyqmhLKNBAmP-cksZS6:

- 1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx,
- 1CZH527GEeR5WDyGac5WHrD6tnW5qJkFGR,
- 164Cg2p4QQ16VJGoBgiST5v2yDZtrvPgan,
- 1A6ezvhzGmCqNmGTTzxphLkByuJfjbuwxr,
- 1Em7vKSqAnFMpejf3fSPSQdxrx99ma856h.

Poddamy analizie adres 1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx:



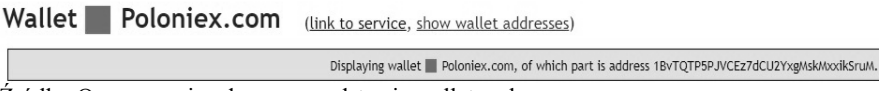
Materiały własne.

Rys. 23. Przepływ środków z adresu 1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx

Jak wynika z Rys. 23, część środków jest przesyłana na adres 1LjHkPN2ssS4iprJGYCUiw9cxmhjP8PGQw (na który też trafiają środki z analizowanego już adresu 19JCSFRPyXnVn7ptXyqmhLKNBAmPcksZS6), część trafia na trzeci adres w klastrze 1CZH527GEeR5WDyGac5WHrD6tnW5qJkFGR, (patrz też Rys. 18) a część poprzez adres 1DVhsPyrTyNPKmwMWUq6Dtf24Ja6je5Thq jest kierowana na 1BvTQTP5PJVCEz7dCU2YxgMskMxxikSruM, zidentyfikowany jako należący do giełdy Poloniex.com[35] (Rys. 24). Pozostałe środki trafiają na adres 14MuKrmk6dTdrwsdvgYZGbN8Km6F1i53zd, będący w klastrze z 227.324 innymi adresami, w tym ze wspomnianym wyżej 1LjHkPN2ssS4iprJGYCUiw9cxmhjP8PGQw (prawdopodobnie podmiot

[35] https://www.walletexplorer.com/wallet/Poloniex.com?from_address=1BvTQTP5PJVCEz7dCU2 Yxg MskMxxikSruM

handlujący kryptowalutami, ale brak jego konkretnej identyfikacji). Analizowana gałąź przepływu kryptowalut pozwoliła nam ustalić trzecią giełdę kryptowalut – Poloniex.com oraz powiązania z już znanymi adresami.



Źródło: Opracowanie własne na podstawie walletexplorer.com.

Rys. 24. Identyfikacja adresu 1BvTQTP5PJVCEz7dCU2YxgMskMxxikSruM

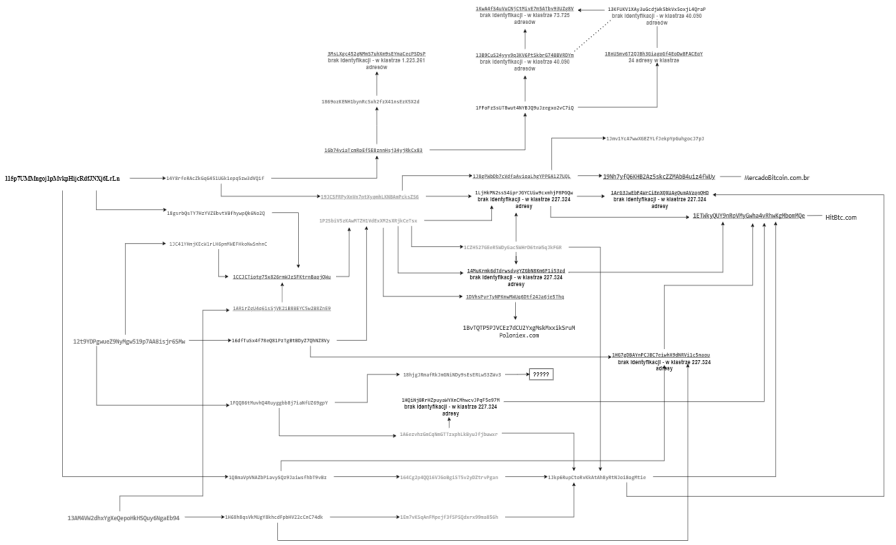
W kolejnym etapie należy sprawdzić źródło pochodzenia środków trafiających na analizowany adres, tj. 1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx. Z Rys. 25 wprost wynika, że kryptowaluty – poprzez adresy pośrednie – pochodzą z wcześniej zidentyfikowanych wszystkich trzech adresów pierwotnych z kampanii Wannacry:

- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn,
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw,
- 3AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94.

Materiały własne.

Rys. 25. Pochodzenie środków na adresie 1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx

Identyfikacja trzech giełd i ustalenie trzech ścieżek przepływu środków wymaga potwierdzenia, czy w przypadku pozostałych adresów pośrednich również powtarza się podobny schemat. Końcowy wynik analizy potwierdził poprawność rozumowania i umożliwił wykonanie grafu przypływu środków oraz wzajemnych powiązań między adresami.



Materiały własne.

Rys. 26. Wykres przepływu środków w kryptowalucie Bitcoin w kampanii ransomware Wannacry

Analiza przepływu kryptowaluty Bitcoin w kampanii Wannacry rozpoczęła się od jednego adresu 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn, podanego pokrzywdzonym do wpłat. Wykorzystując ogólnodostępne źródła danych i znajomość zasad obrotu kryptowalutami możliwe było wykonanie kompleksowej analizy przepływu środków, która pozwoliła na identyfikację dwóch innych adresów pierwotnych, szeregu adresów pośrednich

i ostatecznie trzy giełdy kryptowalutowe, na które trafiły bitcoiny. Końcowy wykres przepływu wyraźnie wskazuje na zorganizowany, powiązany poszczególnymi adresami charakter transferu środków. Na podstawie wyników analizy można postawić wniosek, że za organizację tej części kampanii Wannacry odpowiadają te same osoby, a do ich identyfikacji niezbędne jest uzyskanie odpowiedzi od podmiotów zajmujących się obrotem kryptowalut wskazanych w analizie, to jest giełd: mercadobitcoin.com.br, hitbtc.com i poloniex.com.

Podsumowanie

Powyżej przedstawiono szereg ogólnodostępnych, darmowych możliwości, które mogą być wykorzystane w śledzeniu większości popularnych kryptowalut (w tym wspomnianego już Ether) pochodzących z przestępstw. Oczywiście na rynku istnieją komercyjne programy wspomagające analizę transferów kryptowalutowych. Do bardziej znanych i wykorzystywanych w Europie należą Chainanalysis oraz Ciphertrace, jednakże bardzo wysoka cena skutecznie ogranicza ich szersze wykorzystanie. Natomiast z uwagi na anonimizację adresów Monero i kwot transakcji oczywiste jest, że wszelkie wymienione metody zawodzą, dlatego Monero jest coraz bardziej popularne w środowiskach przestępczych. Organy ścigania wielu państwo dostrzegają ten problem, a amerykański Urząd Skarbowy (IRS - Internal Revenue Service) w 2020 roku ogłosił przetarg na stworzenie oprogramowania do analizy przepływu Monero. Pod koniec września ogłoszono, że przetarg wygrało konsorcjum firm Chainanalysis i Intergra FEC LLC[36]. Gotowe rozwiązanie do analizy transferów Monero oferuje też firma CipherTrace[37]. Niestety, na

[36] https://beincrypto.pl/chainalysis-wygral-kontrakt-irs-na-sledzenie-monero-xmr/ dostęp 09.12.2021 r.
[37] https://ciphertrace.com/enhanced-monero-tracing/ dostęp 09.12.2021 r.

obecną chwilę brak jest możliwości jednoznacznego stwierdzenia czy narzędzia te faktycznie umożliwiają śledzenie transakcji w Monero.

Analizując transfery kryptowalutowe należy dążyć do zidentyfikowania podmiotu, do którego trafiają środki celem ich wymiany na waluty fiducjarne. Ustalenie takiego podmiotu umożliwi zwrócenie się do niego przez uprawnione organy (prokuraturę i policję) o dane użytkownika portfela, poczynając od danych osobowych (o ile podmiot ich żąda), poprzez adresy e-mail, dane dotyczące wypłat (numer rachunku bankowego, numer telefonu w przypadku wypłat w bankomacie) aż po dane logowania do portfela. Istnieje również możliwość wystąpienia do tego podmiotu o blokadę środków na portfelu oraz ich zabezpieczenia na poczet przyszłych kar i środków karnych. Dopiero personalizacja właścicieli portfeli wykorzystywanych w przestępczym procederze, zebranie dowodów winy pozwalające na ich zatrzymanie i przedstawienie zarzutów oraz konfiskata środków gwarantuje pełny sukces organów ścigania. Jak przedstawiono w artykule, nie jest to zadanie łatwe, wymaga bowiem specjalistycznej wiedzy, profesjonalizmu, analitycznego myślenia i żmudnej, systematycznej pracy. Kryptowaluty coraz częściej są wykorzystywane przez środowiska przestępcze w celu ukrycia pierwotnego źródła pieniędzy pochodzących z czynów zabronionych przez prawo. Stawia to przed organami ścigania konieczność wykształcenia specjalistycznych kadr zajmujących się zarówno rozpoznaniem i ściganiem przestępstw z wykorzystaniem walut cyfrowych, jak również analityków rozumiejących możliwości i ograniczenia w śledzeniu transferów kryptowalutowych.

Bibliografia

1. academy.binance.com/pl/articles/what-is-public-key-cryptography, dostęp 25.11.2021 r.
2. academy.binance.com/en/articles/history-of-blockchain, dostęp 06.12.2021 r.

3. academy.binance.com/en/glossary/unspent-transaction-output-utxo, dostęp 07.12.2021r.
4. Antonopoulos A.M., Bitcoin dla zaawansowanych. Programowanie z użyciem otwartego łańcucha bloków, Helion, Gliwice 2018.
5. aspolska.pl/blockchain-5-faktow-o-jakich-powinienes-wiedziec-a-boisz-sie-zapytac/, dostęp 3.01.2022 r.
6. beincrypto.pl/chainalysis-wygral-kontrakt-irs-na-sledzenie-monero-xmr/, dostęp 09.12.2021 r.
7. bitcointalk.org/index.php?topic=155054.0, dostęp 04.01.2022 r.
8. bitinfocharts.com/index_v.html, dostęp 07.12.2021 r.
9. bitnodes.io/, dostęp 25.11.2021 r.
10. businessinsider.com.pl/poradnik-finansowy/blockchain-na-czym-polega/fdctpsb, dostęp 25.11.2021 r.
11. cert.pl/posts/2017/05/wannacry-ransomware/, dostęp 10.12.2021 r.
12. ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/, dostęp 08.12.2021 r.
13. ciphertrace.com/enhanced-monero-tracing/, dostęp 09.12.2021 r.
14. comparic.pl/11-rocznica-genesis-pierwszego-bloku-bitcoina-jak-od-tego-czasu-zmienil-sie-btc/, dostęp 04.01.2022 r.
15. Cryptocurrency Crime andAnti-Money Laundering Report, https://ciphertrace.com/ August 2021.
16. Furneaux N., Investigating Cryptocurrencies. Understanding, Extracting, and Analyzing Blockchain Evidence, Indianapolis 2018.
17. Grzyb J., Kosiński J., Podstawy metodyki pracy organów ścigania w zakresie technologii blockchain, (w) Przestępczość teleinformatyczna 2018, Wydawnictwo Akademickie AMW, Gdynia 2019 r.
18. Haber S., Scott Stornetta W., How to time-stamp a digital document, „Journal of Cryptology", 1991, https://link.springer.com/article/10.1007%2FBF00196791, dostęp 06.12.2021 r.
19. Internet Organised Crime Threat Assessment 2020, Europol, Haga 2020.

20. Opitek P., Góral K., Analiza kryminalna transferów kryptowalutowych w pracy prokuratora, cz. II, (w) Prokuratura i Prawo, 6/2020.
21. Rodwald P., Kryptowaluty z perspektywy informatyki śledczej, Wydawnictwo Akademickie AMW, Gdynia 2020 r.
22. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, dostęp 01.12.2021 r.
23. The 2021 Crypto Crime Report, www.chainalysis.com, February 2021
24. www.blockchain.com/btc/address/1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa, dostęp 03.01.2022 r.
25. www.blockchain.com/explorer, dostęp 07.12.2021 r.
26. www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_ iocta_2020.pdf, dostęp 08.12.2021 r.
27. www.ibm.com/pl-pl/topics/what-is-blockchain, dostęp 25.11.2021 r.
28. www.najlepszekonto.pl/portfel-kryptowalut-jak-dziala-i-ktory-wybrac, dostęp 02.12.2021 r.

Abstract

OPPORTUNITIES AND LIMITATIONS IN TRACKING CRIMINAL CRYPTOCURRENCIES

Summary: The chapter presents the basics of blockchain technology and trading in cryptocurrencies, as well as the problems that occur when tracking Bitcoin, Ether, and Monero transactions. The second part presents an analysis of the flow of funds in the Wannacry ransomware campaign.

Keywords: blockchain, cryptocurrencies, transactions, wallets and addresses, Bitcoin, Ether, Monero, cryptocurrency exchanges, transfer analysis.

Rozdział 5

Szacowanie historycznego zużycia energii podczas nielegalnego wydobywania kryptowaluty ETH

Przemysław RODWALD[1]

STRESZCZENIE: Dynamicznie zwiększająca się liczba przestępstw popełnianych przy użyciu kryptowalut wymusza rosnące zapotrzebowanie na narzędzia wspomagające analizy śledcze wśród organów ścigania. Większość dostępnych rozwiązań koncentruje się na śledzeniu przepływów kryptowalut i próbie deanonimizacji właścicieli poszczególnych adresów. Jednak zarówno rosnąca popularność kryptowalut jak i wyceny poszczególnych krypto aktywów prowadzą do zwiększenia się statystyk czynów związanych z nielegalnym ich wydobywaniem. Nielegalność rozumiana jest tutaj jako bezprawne wykorzystanie zasobów zarówno sprzętowych jak i energetycznych. Istnieje więc coraz częściej realna potrzeba szacowania ilości energii zużywanej podczas takich procederów. W niniejszym rozdziale przedstawiono zarówno metodykę tego szacowania opartą na publicznie dostępnych danych dla kryptowaluty Ethereum, jak i wdrożony ogólnodostępny system realizujący jej założenia.

SŁOWA KLUCZOWE: wydobywanie kryptowalut, mining, PoW, zużycie energii.

Wprowadzenie

Kryptowaluty stają się coraz popularniejszym instrumentem finansowym. Oprócz wielu zalet walut opartych na publicznym łańcuch bloków (*ang.*

[1] Katedra Informatyki, Akademia Marynarki Wojennej, p.rodwald@amw.gdynia.pl, ORCID: 0000-0003-4261-8688.

blockchain), takich jak decentralizacja, prywatność, szybkość transakcji, jeden kluczowy czynnik wskazywany jest przez ich przeciwników – wysokie zużycie energii. W przypadku kryptoaktywów opartych na modelu osiągania konsensusu zwanego dowodem pracy (*ang. Proof-of-Work, PoW*) bezpieczeństwo wynika z zastosowanego systemu motywacyjnego. Uczestnicy, zwani górnikami, w zamian za skuteczne rozwiązanie „zagadki kryptograficznej[2]" otrzymują nagrodę w postaci nowych jednostek danej kryptowaluty. Proces ten, zwany wydobywaniem lub miningiem[3] (*ang. mining*), charakteryzuje się systematycznie zwiększającym się zużyciem energii elektrycznej. Szacunki dotyczące zużycia energii elektrycznej wykorzystywanej do wydobywania kryptowalut są zatrważające, przykładowo na początku 2020 roku wskazywano zapotrzebowanie energetyczne na poziomie 4,29 GW dla sieci Bitcoin; czy 0,72 GW dla sieci Ethereum [**Błąd! Nie można odnaleźć źródła odwołania.**].

Mimo, że wydobywanie kryptowalut nie jest działalnością nielegalną, przestępcy znajdują nowe sposoby wykorzystania miningu do popełniania przestępstw. Kradzież energii elektrycznej lub nielegalne użycie zasobów sprzętowych należą do najczęściej wykorzystywanych technik. W szczególności pierwsza z wymienionych aktywności może być kusząca dla przestępców, gdyż przy zerowych kosztach energii zysk z wydobycia jest osiągany

---

[2] Rozwiązanie „zagadki kryptograficznej" dla danego bloku polega na znalezieniu takiej wartości losowej, która w połączeniu ze skrótem wszystkich transakcji wchodzących w skład danego bloku da skrót (wynik działania kryptograficznej funkcji skrótu) zaczynający się pewną liczbą zer, np. 000000000…. Liczba zer dostosowywana jest do aktualnych możliwości obliczeniowych sieci danej kryptowaluty w taki sposób, aby średni czas potwierdzenia bloku wynosił zadana dla danej sieci kryptowaluty wartość (około 12 sekund w sieci Ethereum).

[3] Mimo, że słowo „mining" nie występuje jeszcze w słownikach (np. Słownik języka polskiego PWN) to ze względu na swoją powszechność i ogólne zrozumienie znaczeniowe będzie używany w artykule.

bez względu na aktualną moc obliczeniową (*ang. hashrate*) sieci danej kryptowaluty [**Błąd! Nie można odnaleźć źródła odwołania.**]. Ostatnie lata pokazują wzmożone zainteresowanie omawianym procederem. Przykłady można znaleźć zarówno w kraju, jak i poza jego granicami. W lutym 2019 roku w Klingenthalu (Niemcy) zatrzymano grupę sześciu podejrzanych w związku z odkryciem górniczej farmy kryptowalutowej, działającej na skradzionej energii elektrycznej, której wartość oszacowano na około 220 tys. EUR [**Błąd! Nie można odnaleźć źródła odwołania.**]. We wrześniu tego samego roku firma z Armenii została oskarżona o uruchomienie operacji wydobywania kryptowalut w elektrowni wodnej i nielegalne wykorzystywanie wytwarzanej energii elektrycznej przez ponad rok – straty oszacowano na kwotę 150 tys. USD [**Błąd! Nie można odnaleźć źródła odwołania.**]. W lipcu 2021 roku w Ukrainie została zidentyfikowana kopalnia kryptowalut podłączona nielegalnie do sieci energetycznej – wstępne straty oszacowano na kwotę do 256 tys. USD [**Błąd! Nie można odnaleźć źródła odwołania.**]. Do ciekawszych przykładów na rynku krajowym zaliczyć można incydenty związane z nielegalnym miningiem w instytucjach organów ścigania. W 2021 roku zarówno w Centrum Szkolenia Policji w Legionowie [**Błąd! Nie można odnaleźć źródła odwołania.**], jak i w Komendzie Głównej Policji [**Błąd! Nie można odnaleźć źródła odwołania.**] zidentyfikowane zostały przypadki wykorzystania służbowego sprzętu do procederu miningu z nielegalnym wykorzystaniem energii elektrycznej.

Zauważyć należy dodatkowo, że mining może być także wykorzystywany jako jedna z technik legalizujących dochody pochodzące z czynów zabronionych. Zakup sprzętu do miningu i wydobywanie nowych kryptowalut

należy do współczesnych technik „prania" pieniędzy[4] [**Błąd! Nie można odnaleźć źródła odwołania.**].

Wydobywanie kryptowalut w modelu PoW

Wydobywanie jest kluczowym elementem zapewnienia konsensu w sieciach opartych na dowodzie pracy PoW. Choć głównym motywatorem do kopania (jak potocznie określa się wydobywanie) dla większości górników jest nagroda w postaci nowo wykopanych jednostek danej kryptowaluty, to właśnie mining jest tym mechanizmem, dzięki któremu bezpieczeństwo sieci jest zdecentralizowane [**Błąd! Nie można odnaleźć źródła odwołania.**]. Koncepcja dowodu pracy wywodzi się z pomysłu zaprezentowanego w 1997 roku przez anonimowego użytkownika, a opisanego później przez Backa [**Błąd! Nie można odnaleźć źródła odwołania.**] zapobiegającemu problemowi spamowania poczty elektronicznej. W koncepcji tej wykorzystywana była rozszerzona postać adresu e-mail, polegająca na dodaniu do niego specjalnej pieczęci, której wygenerowanie wymagało pewnego nakładu pracy po stronie nadawcy. Koncepcja ta została wykorzystana została w sieci Bitcoin jak i rozpatrywanej w niniejszej pracy sieci Ethereum. Tym co skłania górników do zużywania swojej mocy obliczeniowej jest nagroda w postaci nowo wykopanych jednostek danej kryptowaluty. Tylko górnik, który najszybciej wydobędzie nowy blok otrzymuje nagrodę. Dodanie nowego bloku do łańcucha jest możliwe tylko wówczas, gdy skrót wygenerowany z konkatenacji kliku elementów składowych, między innymi: skrótu za poprzedni blok, korzenia drzewa Merklego transakcji wchodzących w skład wykopywanego

[4] 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.

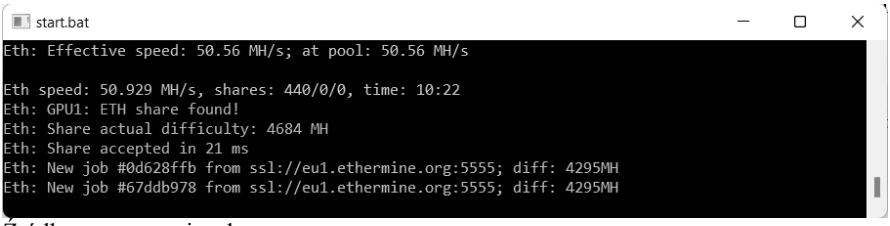
bloku, wartości *nonce*, będzie się rozpoczynał pewną liczbą zer. Jedynym zmiennym elementem składowym jest właśnie wartość *nonce* i to właśnie jej znalezienie jest dowodem wykonanej pracy w celu potwierdzenia nowego bloku [**Błąd! Nie można odnaleźć źródła odwołania.**]. Trudność wykonywania tej pracy dostosowywana jest dynamicznie do całkowitej mocy obliczeniowej udostępnianej przez górników w sieci na potrzeby wydobywania danej kryptowaluty.

Współcześnie górnicy najczęściej nie decydują się na samodzielne wydobywanie, lecz łączą się w spółdzielnie wydobywcze zwane kopalniami (*ang. minig pools*). Ma to na celu zwiększenie prawdopodobieństwa wykopania nowego bloku. Przy aktualnej mocy obliczeniowej najpopularniejszych kryptowalut pojedynczy górnik (*ang. solo miner*) praktycznie nie ma szans na wykopanie nowego bloku (choć statystycznie jest to możliwe [**Błąd! Nie można odnaleźć źródła odwołania.**]). Dodając swoją moc obliczeniową do wybranej kopalni górnik znacznie zwiększa prawdopodobieństwo wydobycia nowego bloku na rzecz kopalni. Gdy kopalnia wydobędzie blok, górnicy otrzymują w zamian procentowy udział w nagrodzie, zależny od mocy jaką udostępnili. Sam proces dołączenia do kopalni jest bardzo prosty dla użytkownika. W najpopularniejszych programach do kopania wystarczy po prostu podać nazwę kopalni i adres na jaki ma być przekazywana nagroda. Przykładowe polecenie (*) uruchamiające program do wydobywania kryptowaluty ETH o nazwie *PhoenixMiner*[5] za pośrednictwem spółdzielni *nanopool* wygląda następująco:

```
PhoenixMiner.exe -pool ssl://eu1.ethermine.org:5555 -nvidia -log 0 -wal 0xdba4c80e8a1298228d31d822dae069fd624d7b16.nazwa
```
(*)

[5] https://phoenixminer.org/

Ekran przedstawiający realizację procesu wydobycia pokazany został na rysunku 1.



Źródło: opracowanie własne.

Rys. 1. Ekran ukazujący realizację miningu kryptowaluty ETH za pomocą programu PhoenixMiner

Górnik przystępując do udostępniania swojej mocy obliczeniowej może oszacować oczekiwany zysk na podstawie aktualnego stanu sieci Ethereum (aktualna moc obliczeniowa sieci, średnia nagroda za wydobycie bloku, średni czas wydobycia bloku). W sieci Internet znajduje się wiele kalkulatorów[6] dzięki którym można łatwo oszacować potencjalne przyszłe zyski. Moc obliczeniowa dostarczana przez górników zmienia się w czasie, więc takie kalkulatory bazują w swoich szacowaniach na aktualnych wartościach panujących w sieci kryptowaluty ETH.

W niniejszy artykule uwaga nie jest jednak skupiona na potencjalnych zyskach możliwych do osiągnięcia w przyszłości i istotnych z inwestycyjnego punktu widzenia, lecz na analizie zdarzeń historycznych dla których kalkulacje powinny być oparte na danych archiwalnych. Ze względu na fakt, iż liczba jednostek wydobywanej kryptowaluty w danym momencie zależy od wielu czynników zmiennych w czasie, do szacowania historycznych zysków konieczne jest w pierwszym kroku pozyskanie danych archiwalnych dla sieci

[6] Przykładowe kalkulatory wydobycia: https://whattomine.com, https://coinwarz.com

Ethereum, a następnie dla zadanych parametrów karty graficznej wyliczenie historycznego przychodu z wydobycia (*ang. miningreword*):

$$miningreward = \frac{hashpower}{hashrate} \times \frac{(blockreward + transfee)}{blockcount} \times \frac{T}{blocktim} \quad (**)$$

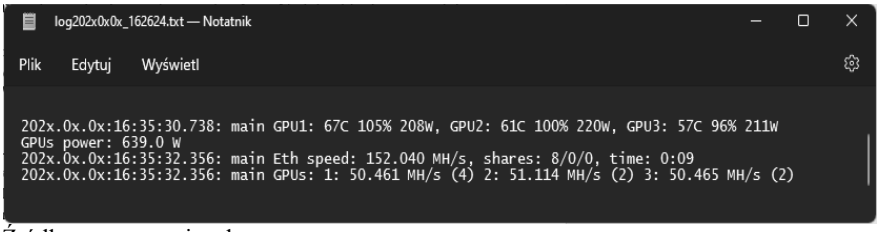
gdzie: *hashrate* - historyczna moc obliczeniowa całej sieci Ethereum, *blocktime* - historyczny średni czas potrzebny na uwzględnienie nowego bloku w łańcuchu bloków sieci Ethereum, *blockcount* - historyczna liczba bloków umieszczanych dziennie w łańcuchu bloków sieci Ethereum, *blockreward* - całkowita historyczna dzienna liczba nowych ETH powstających w sieci Ethereum, *transfee* - całkowita historyczna dzienna liczba ETH zapłacona jako opłata transakcyjna w sieci Ethereum, *hashpower* - średnia moc obliczeniowa (efektywność) górnika, *T* - czas trwania wydobycia.

Scenariusze śledcze

Opierając się na doświadczeniu autora jako biegłego sądowego w rzeczywistych sprawach karnych dotyczących tematyki kryptowalut, można wysnuć wniosek iż rośnie liczba górników korzystających w sposób nieuprawniony zarówno z zasobów sprzętowych jak i energetycznych w instytucjach publicznych: agencjach rządowych, uczelniach wyższych czy instytutach badawczych. Po wykryciu na sprzęcie oprogramowania do miningu, śledczy mogą napotkać dwa najpowszechniejsze scenariusze: z włączonym lub wyłączonym dziennikiem logów programu do miningu.

W pierwszym scenariuszu, gdy wydobycie było realizowane z włączonym dziennikiem logów (przykładowo jest to domyślny parametr -log 1 w popularnych programach do miningu), na zabezpieczonych dyskach znajdować się może cała historia miningu. Szacowanie zużytej energii może być wówczas wykonane bezpośrednio z analizy zawartości dzienników logów.

W wielu przypadkach pliki dziennika dostarczają informacje nie tylko o czasie realizacji procesu wydobycia, ale także o energii zużywanej przez poszczególne karty graficzne (*ang. graphics processing unit, GPU*). Przykładowa zawartość pliku logów programu zaprezentowana została na rysunku 2. Analityk śledczy w takim scenariuszu powinien dokonać analizy plików logów i na ich podstawie dokonać kalkulacji zużytej energii [7]. W przypadku gdy oprogramowanie do miningu nie zapisuje danych o rzeczywistym zużyciu energii przez karty graficzne, wówczas szacowania takiego można dokonać na podstawie powszechnie dostępnych danych dla zidentyfikowanego modelu karty [8]. Śledczy powinni pamiętać, że nawet jeśli jedne pliki dzienników logów zostały znalezione, to inne pliki mogły być celowo i skutecznie usunięte.



Źródło: opracowanie własne.

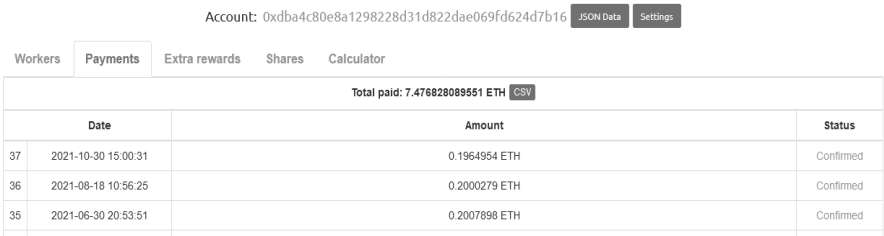
Rys. 2. Przykładowa zawartość fragmentu zanonimizowanego pliku logów programu PhoenixMiner

W drugim scenariuszu, gdy wydobywanie było realizowane przez bardziej świadomych górników przy wyłączonym dzienniku logów (parametr

[7] Przykładowy skrypt napisany w języku PHP analizujący pliki logów pochodzące z dwóch programów Claymore oraz PhoenixMiner, zaprojektowany przez autora, został udostępniony pod adresem https://rodwald.pl/cmepce/PL/LOG/.

[8] Przykładowo: https://whattomine.com/gpus, https://minermonitoring.com/benchmark/

-log 0) lub pliki logów zostały bezpowrotnie usunięte z dysku, na zabezpieczonych dyskach znajduje się najczęściej tylko oprogramowanie do miningu z plikiem uruchomieniowym (najczęściej jest to plik .bat) w którym znajduje się adres ETH oraz nazwa spółdzielni wydobywczej na poczet której realizowany był mining. W przedstawionej wcześniej (*) przykładowej zawartości pliku bat są to wartości -wal 0xdba4c80e8a1298228d31d822dae069fd624d7b16 oraz -pool ssl://eu1.ethermine.org:5555. Po zidentyfikowaniu adresu ETH i spółdzielni wydobywczej śledczy może pozyskać informacje o historycznych wypłatach na dany adres. Strony internetowe pool-i dostarczają te dane w ustrukturyzowanych plikach .csv, które mogą być punktem wyjścia do dalszej analizy. Przykładowe dane historyczne wypłat realizowanych przez spółdzielnię nanopool na poczet przykładowego adresu przedstawiono na rysunku 3.



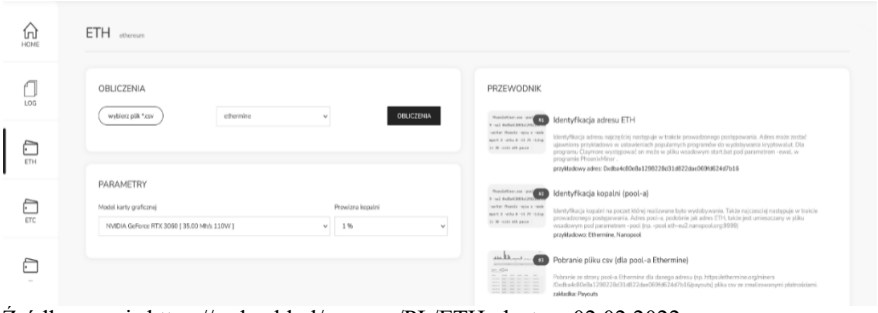
Źródło:
https://eth.nanopool.org/account/0xdba4c80e8a1298228d31d822dae069fd624d7b16, dostęp: 02.02.2022.

Rys.1. Ekran przedstawiający historię wypłat dla przykładowego adresu w spółdzielni nanopool

System do szacowania historycznego zużycia energii podczas miningu

W odpowiedzi na rosnącą liczbę spraw związanych z omawianą tematyką został zaprojektowany i wdrożony system do szacowania historycznego zużycia energii elektrycznej podczas miningu. System ma budowę

modułową, podzieloną funkcjonalnie na trzy główne komponenty. W pierwszym z nich następuje przetwarzanie dynamicznie pobieranych danych historycznych dla sieci Ethereum, a jako źródło danych został wybrany serwis etherscan.io[9]. Dodatkowo w etapie tym pobierane są parametry dotyczące wydobycia i energochłonności dla różnych kart graficznych[10]. Drugi komponent odpowiada za przetwarzanie pliku csv pochodzącego ze stron spółdzielni wydobywczych i uploadowanego do systemu przez użytkownika. Ekran przedstawiający okno początkowe działania systemu dla analizy ether-a pokazany został na rysunku 4.



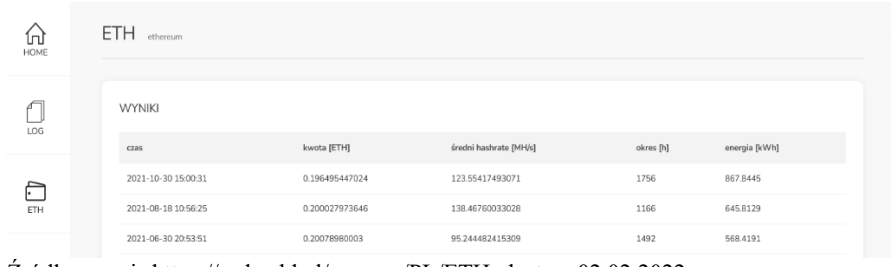
Źródło: serwis https://rodwald.pl/cmepce/PL/ETH, dostęp: 02.02.2022.

Rys. 4. Ekran systemu do szacowania historycznego zużycia energii dla miningu - ekran początkowy dla kryptowaluty ETH

[9] Dane pobierane są w postaci plików csv z lokalizacji: https://etherscan.io/chart/hashrate?output=csv, https://etherscan.io/chart/blocktime?output=csv, https://etherscan.io/chart/blocks?output=csv, https://etherscan.io/chart/blockreward?output=csv, https://etherscan.io/chart/transactionfee?output=csv

[10] Dane pobierane są ze strony https://whattomine.com/gpus

Po wczytaniu i poprawnym przetworzeniu danych wejściowych, ostatni komponent agreguje pozyskane dane i dokonuje odpowiednich obliczeń według przekształconego wzoru (**) w interwałach dziennych. Finalnie użytkownikowi prezentowana jest tabela z szacunkowymi danymi dotyczącymi zużytej energii zaprezentowana na rysunku 5.



Źródło: serwis https://rodwald.pl/cmepce/PL/ETH, dostęp: 02.02.2022.

Rys. 2. Ekran systemu do szacowania historycznego zużycia energii dla miningu - ekran prezentujący wyniki szacowanego zużycia dla kryptowaluty ETH

Utworzony system został udoskonalony w porównaniu ze swoją poprzednią wersją [**Błąd! Nie można odnaleźć źródła odwołania.**]. W szacowaniu można zarówno wybrać rodzaj karty graficznej i związane z nią efektywność wydobycia oraz zapotrzebowanie energetyczne, jak również procentową wysokość prowizji pobieranej przez spółdzielnię wydobywczą (od 1% do 5%)

Podsumowanie

Rosnąca popularność kryptowalut, ich wysokie wyceny i łatwość rozpoczęcia miningu powodują zauważalny wzrost nielegalnych działań polegających na kradzieży prądu i użyciu zasobów sprzętowych pracodawcy niezgodnie z ich przeznaczeniem. Zaproponowany system wspomaga organy procesowe w szacowaniu energii zużytej do miningu w procederze zaboru - podłączenie się do jej źródła i czerpanie tej energii bez zgody osoby uprawnionej do dysponowania nią. Na tej podstawie w kolejnym kroku, korzystając z cennika energii elektrycznej, można szacować poniesione przez poszkodowanego szkody.

Zaprojektowany system ze względu na swoją modułową budowę jest przygotowany do rozszerzania o analizę dla innych kryptowalut opartych na

modelu PoW. Autor, w miarę wzrostu popularności wydobycia innych kryptowalut, szczególnie prawdopodobnym przy przejściu sieci Ethereum na model osiągania konsensusu opartym na dowodzie posiadania (ang. *Proof-of-Stake*), w ramach swoich badań oraz czynności wykonywanych jako biegły sądowy planuje dalszy rozwój systemu, w szczególności dodawanie modułów analitycznych dla nowych kryptowalut.

Bibliografia

1. Gallersdörfer, U., Klaaßen, L., Stoll, C.: *Energy consumption of cryptocurrencies beyond bitcoin*. Joule 4(9), 1843–1846 (2020).
2. Furneaux, N.: *Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence.* John Wiley & Sons (2018).
3. Rodwald, P.: *Kryptowaluty z perspektywy informatyki śledczej,* Akademia Marynarki Wojennej, Gdynia (2021), ISBN 978-83-959756-7-7.
4. Alexandre, A.: *Germany: Suspects arrested for stealing electricity in crypto mining operation* (2019-02-07). https://cointelegraph.com/news/germany-suspects-arrested-for-stealing-electricity-in-crypto-mining-operation (dostęp: 02.02.2022).
5. Cant J.: *Armenian IT Company Accused of Illegal Electricity Use to Mine Crypto* (22.09.2019), https://cointelegraph.com/news/armenian-it-company-accused-of-illegal-electricity-use-to-mine-crypto (dostęp: 02.02.2022).
6. Tassev L.: *Ukraine Uncovers Country's Largest Illegal Mining Farm to Date* (10.07.2021), https://news.bitcoin.com/ukraine-uncovers-countrys-largest-illegal-mining-farm-to-date/ (dostęp: 02.02.2022).
7. Zieliński R.: *Kopalnia kryptowalut w Komendzie Głównej Policji?* (29.07.2021), https://tvn24.pl/polska/kopalnia-kryptowalut-w-komendzie-glownej-policji-zawiadomienie-do-prokuratury-5160978 (dostęp: 02.02.2022).

8. Żak K.: *Nielegalna "kopalnia kryptowalut" w szkole policyjnej w Legionowie. Prokuratura bada sprawę* (2021-09-30), https://www.rmf24.pl/fakty/polska/news-,nId,5545873 (dostęp: 02.02.2022).
9. Back A.: *Hashcash - a denial of service counter-measure*, 2002, http://www.hashcash.org/papers/hashcash.pdf
10. La Rosa F., *Yet another solo Bitcoin miner solved a valid block, earning a reward worth over $220,000* (25.01.2022), https://cointelegraph.com/news/yet-another-solo-bitcoin-miner-solved-a-valid-block-earning-a-reward-worth-over-220-000 (dostęp: 02.02.2022).
11. Rodwald P.: Estimation of Ethereum mining past energy consumption for particular addresses, Theory and Engineering of Dependable Computer Systems and Networks, DepCoS-RELCOMEX 2022. Advances in Intelligent Systems and Computing (przyjęty do druku 04.03.2022).

Abstract

ESTIMATING HISTORICAL ENERGY CONSUMPTION DURING ILLEGAL MINING OF ETH CRYPTOCURRENCY

Summary: The rapidly increasing number of crimes committed using cryptocurrencies is forcing a growing demand for tools to support investigative analysis among law enforcement agencies. Most available solutions focus on tracking cryptocurrency flows and attempting to de-anonymize the owners of individual addresses. However, both the growing popularity of cryptocurrencies and the valuations of individual crypto assets are leading to an increase in the statistics of acts related to illegal mining. Illegality is understood here as the unlawful use of both hardware and energy resources. Thus, there is an increasingly real need to estimate the amount of energy consumed during such procedures. This paper presents both the methodology of this estimation based

on publicly available data for the Ethereum cryptocurrency, as well as the implemented publicly available system realizing its assumptions.

Keywords: digital evedence, cryptocurrency mining, PoW, power consumption.

Rozdział 6

II zasada termodynamiki - każdy zna, niewielu stosuje

Paweł BARANIECKI[1]

STRESZCZENIE: W rozdziale przedstawiono trudności, tak w realizacji, jak i towarzyszące przechwytowi i utrwaleniu danych przekazywanych poprzez sieć Internet dla podmiotów zobowiązanych, jak i uprawnionych (art. 179 prawa telekomunikacyjnego). Zaproponowano też rozwiązanie pozwalające na znaczne zredukowanie zapotrzebowania na przechwyt i utrwalenie „danych internetowych".

SŁOWA KLUCZOWE: przechwyt i utrwalenie danych pakietowych, optymalizacja procesu.

Wstęp

Przywołana w tytule II zasada termodynamiki określa, kiedy zachodzą procesy samorzutne, naturalne. Optymalizacja drogi do zamierzonego celu, tak by go osiągnąć możliwie niskim nakładem pracy jest „kontrolowanym lenistwem". A lenistwo jest zjawiskiem naturalnym.

Od około 10 lat ilość (wolumen) danych przekazywanych poprzez Internet bardzo szybko rośnie. Realizując obowiązek przechwytu i utrwalenia treści komunikatów (art. 179 prawa telekomunikacyjnego) podmioty zobowiązane (dalej: operator) przekazują podmiotom uprawnionym (dalej PU) coraz to większe ilości danych. Ci pierwsi muszą to wysłać, a ci drudzy przyjąć

[1] LL. M., Członek Zarządu Stowarzyszenia Sygnał, Kierownik Działu Ochrony Własności Intelektualnej Cyfrowego Polsatu, lsternowski@cyfrowypolsat.pl.

i poddać analizie. Wszystko w warunkach ochrony informacji niejawnej. Wydaje się, że drogą stosunkowo prostego zabiegu można to ułatwić.

Obecne warunki realizacji obowiązku przechwytu i utrwalenia treści.

Zgodnie z prawem przechwyt i utrwalenie treści są objęte tajemnicą państwową w rozumieniu ustawy o ochronie informacji niejawnej. Narzuca to operatorom i PU dodatkowe wymagania dla systemów wspomagających jego realizację. Co przekłada się na koszty urządzeń technicznych i zasobów ludzkich.

Treści są przekazywane PU poprzez:

- interfejs LiHi;
- na nośnikach fizycznych.

Od 2012 roku obserwowane jest zjawisko „przenoszenia" połączeń głosowych i SMS do domeny PS, czyli „do Internetu". De facto jest to przenoszenie komunikacji z domeny usług telekomunikacyjnych do domeny usług świadczonych drogą elektroniczną. Największymi dostawcami tych usług są podmioty spoza obszaru EU.

Rośnie wykładniczo wolumen danych transmitowanych poprzez sieć Internet.

Rynek komunikacji w Polsce pokazują poniższe dwa rysunki (rys. 1, rys 2):

Źródło: https://ircenter.com/wp-content/uploads/2018/04/komunikatory__PR3.jpg.

Rys. 1. Rynek komunikacji; korzystanie z komunikatorów

Dane dotyczą 2018 roku. Ale już wtedy niemal każdy użytkownik Internetu korzystał z jakiegoś komunikatora. Brak nowszych danych, uwzględniających takie komunikatory jak Signal, czy Telegram.

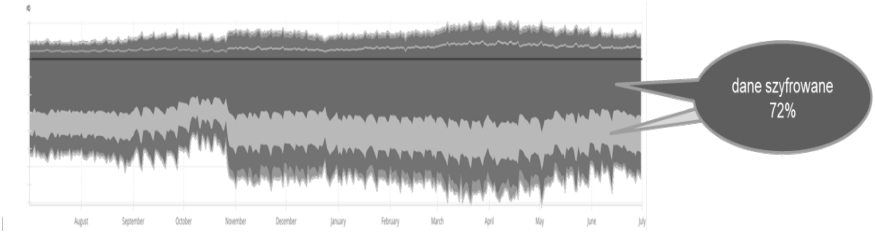
Źródło: https://ircenter.com/wp-content/uploads/2018/04/spicy__PR3.jpg.

Rys. 2. Rynek komunikacji; Miesięczne wykorzystanie komunikatorów Polsce w styczniu lat 2016 do 2018

Drugi rysunek pokazuje estymowaną ilość rozmów w kolejnych 3 styczniach. W styczniu 2018 łączna ilość takich połączeń przekracza 120

milionów. Tego nie sposób zauważyć. Zwłaszcza, że takie połączenia są realizowane z wykorzystaniem transmisji szyfrowanej, a w niektórych przypadkach jest stosowane szyfrowanie „end2end".

Udział transmisji szyfrowanej rośnie. Na kolejnym rysunku (rys. 3) przedstawiono udział szyfrowanej transmisji danych w sieci Plus[2] od lipca 2020 do lipca 2021.



Rys. 3 Struktura danych transmitowanych w sieci „Plus" od lipca 2020 do lipca 2021

72% danych jest przekazywanych w transmisji szyfrowanej. To oznacza, że treść 72% danych jest niedostępna dla PU. Szyfrowane są transmisje danych korzystające w sieci z usług:

- komunikatorów głos, video, pliki;
- finansowych;
- medycznych;
- publicznych;
- kupna-sprzedaży;
- platform społecznościowych;
- innych, gdzie przetwarzane są dane osobowe.

[2] Właścicielem marki „Plus" jest Polkomtel Sp. z o.o.

Wydaje się, że te usługi są dominującą dziedziną, w której zdarzają się czyny będące w obszarze zainteresowania PU.

Kolejnym czynnikiem utrudniającym kontrolę treści jest wolumen przekazywanych danych. W tabelach 1 i 2 przedstawiono średnie wyniki prędkości transmisji danych zmierzonych przy pomocy speedtest.pl w sierpniu 2021 roku.

Najlepsi dostawcy	Prędkość pobierania [Mb/s]	Prędkość wysyłania [Mb/s]	PING [ms]	Liczba testów
T-Mobile	**44,0**	**9,8**	**31**	**50 tys.**
Orange Mobile	38,6	9,7	30	65 tys.
Play	35,3	9,4	35	76 tys.
Plus	33,7	9,3	40	61 tys.

Tabela 1. Dla „Internetu mobilnego". Źródło: https://www.speedtest.pl/ranking/internet-mobilny udostępnienie wrzesień 2021

Najlepsi dostawcy	Prędkość pobierania [Mb/s]	Prędkość wysyłania [Mb/s]	PING [ms]	Liczba testów
Orange	**209,6**	**73,2**	**12**	**185 tys.**
Netia	195,4	82,5	15	27 tys.

Tabela 2. Dla „Internetu stacjonarnego" w technologii światłowodowej. Źródło: https://www.speedtest.pl/ranking/internet-domowy-swiatlowod-ftth-operatorzy-ogolnopolscy udostępnienie wrzesień 2021

Należy pamiętać o powodach wykonania testu. Najczęściej jest to niezadowolenie z aktualnej szybkości transmisji danych. Czyli dane przedstawiają dolne wartości szybkości transmisji.

Wolumen przekazywanych danych jest bodaj najistotniejszym kryterium trudności realizacji obowiązku przechwytu i utrwalenia treści. Do zobrazowania tej istotności weźmy najniższy z zaprezentowanych wyników: 33,7

Mb/s. To znaczy, że dla każdego zakończenia sieci, np. karty SIM, w każdej godzinie PU otrzyma jakieś 14 GB (lub więcej) danych[3]. Z czego:

- ok. 72% nie da się odczytać, bo są szyfrowane;
- trzeba „wyłowić" MMS;
- być może przejrzeć ok. 4 GB danych nieszyfrowanych.

14 GB danych odpowiada 3 pełnometrażowym filmom w dobrej jakości.

Propozycja optymalizacji.

Wobec dominującego udziału transmisji szyfrowanej i w większości przypadków nieprzydatnych dla postępowania danych nieszyfrowanych, dobrym rozwiązaniem będzie działanie operatora polegające na wydzieleniu z transmisji pakietowej treści MMS i udostępnianie jej PU wraz z innymi danymi.

Przy takim rozwiązaniu PU otrzyma treści komunikatów:

- MMS (wyodrębnionych przez operatora z danych pakietowych);
- SMS i połączenia głosowe;
- połączenia głosowe i SMS z platformy IMS (VoLTE);
- dane stowarzyszone (pliki *.iri),

bez balastu danych szyfrowanych.

Takie rozwiązanie zapewni PU treści wszystkich komunikatów jakie może dostarczyć operator bez przesyłania danych niosących nie dającą się odczytać treść, tym samym zbędny balast.

---

[3] Intencjonalnie - na użytek w tej dyskusji - pomijam przepustowość urządzeń sieciowych takich jak szyfratory.

Korzyści wspólne (operatorów i PU) to brak kosztów skalowania systemów, a dodatkowo PU w większości przypadków nie będą musiały wykonywać przetwarzania bardzo dużych wolumenów danych.

Należy też podkreślić opłacalność ekonomiczną proponowanego rozwiązania dla obu stron.

Abstract

THE RESPONSIBILITY OF ONLINE INTERMEDIARIES IN THE LIGHT OF EUROPEAN UNION LAW

Summary: The paper presents difficulties with performing, as well as occurring during, interception and retention of data transmitted through Internet network, both for obliged entities and authorized entities (179th article of the Polish Telecommunications Act). The author proposes a solution that allows considerable reduction of the need for interception and retention of "Internet data".

Keywords: interception and retention of packet data, process optimization.

Rozdział 7

Analysis of Mobile Forensics Tools

Adam ZIELIŃSKI[1], dr inż. Przemysław RODWALD[2]

SUMMARY: Mobile forensics (MF) is facing new challenges and experiencing rapid development each year. The growing number of smartphones, systematic updates of operating systems, a wide variety of system applications become an obstacle for a forensic investigator. That is why a proper knowledge of forensic tools, their features as well as limitations are required to provide a reliable investigation. The research was conducted to perform a forensic analysis of seven mobile devices using the logical acquisition of five forensic tools: MicroSystemation XRY, Cellebrite UFED, Magnet AXIOM, MOBILedit Forensic Express, and Oxygen Forensic Detective. We are pleased to present the results of quantitative analysis whose aim was to measure and compare the quality of the mentioned forensics tools.

KEYWORDS: mobile forensics, tools.

Introduction

At present, smartphones are used less for calling and more for socializing; The process has had its effects on smartphones that started to gather a lot of sensitive data about their users [3]. Mobile devices store the users' contacts, history of phone calls, text messages, and e-mails. There are also browser logs and cached geolocation information; pictures and videos that

[1] Katedra Informatyki, Akademia Marynarki Wojennej, adam.zielinski.bf@gmail.com.
[2] Katedra Informatyki, Akademia Marynarki Wojennej, p.rodwald@amw.gdynia.pl, ORCID: 0000-0003-4261-8688.

were recorded with the phone's camera; credentials to cloud services, forums, social networks, online portals, and shopping websites; stored payment data; and a lot of other information that can be essential for forensic investigations.

The National Institute of Standards and Technology defines mobile phone forensics as "the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods". This process must be a sequence of actions, consisting of the four following steps: acquisition, examination, analysis, and reporting of retrieved data [6]. A comprehensive review of mobile forensic investigation process models is presented in a paper [4]. Forensics investigator faces choosing the proper tool that automates his work and provides the most reliable evidence for the examined device. The growing volume and variety of mobile devices, operating system updates, hardware and software updates has resulted in the growth in the number of mobile device forensics tools as well as challenges they face [7][8]. There are diverse tools available for examining and analysing mobile devices: commercial and open-source, forensic and non-forensic, designed for investigations, management, testing, or diagnosing. These tools are rarely verified and validated by independent organizations. The vendors' evaluation results, which are rather not unbiased, are the only ones available to the investigator for selecting the right tool in a particular case. National Institute of Standards and Technology (NIST) identified a need in the law enforcement community to ensure computer forensic tools' reliability. As a result, a Computer Forensic Tool Testing (CFTT) project was run to establish a methodology for testing computer forensic software tools. One of its products is the document "Mobile Device Forensic Tool Specification, Test Assertions and Test Cases" [2], which defines mobile forensic data acquisition tools requirements. Additionally, examiners from NIST are testing the most popular MF products and (they are) presents results on separate reports [1]. Their analyses are limited to a few mobile devices per report, and the lists of the mobile devices used for testing

are different in each document what makes the comparison of tools quite difficult.

Beginning in February 2016, the quality of the reports degrades notably, and it is unclear in many cases whether data was extracted from Android and not displayed properly by the forensic software, or simply not extracted at all. Some reports showed inconsistencies between the notes of analysts on forensic performance and the summary tables in the final report [9].

Our research is expected to provide recommendations for mobile forensic tools and help investigators to understand its limitation. We try to compare five of the most popular MF tools and present our results in a clean and transparent form. Our long-term goal is to provide a periodically updated comparison of the selected MF tools based on mobile devices examined in the mobile forensics laboratory currently being built at the Polish Naval Academy.

Aquisition Techniques

The types of software available for mobile forensic could be categorised as commercial and open-source, forensics and non-forensic tools intended for device testing or diagnostics. In this article, only commercial forensic solutions are considered. To better understand types of mobile acquisition tools and the data they are capable of recovering,

a classification system titled "Cell Phone Tool Classification Pyramid" presented in 2008 by Sam Brothers [5] is used. The main objective of this pyramid is to classify and compare the extraction method of different tools. Moving in the pyramid from the bottom (Level 1 - Manual Extraction), to the top (Level 5 - Micro Read), the acquisition becomes more detailed, technical, invasive, time and money consuming. The three remaining levels of the pyramid are as follows: 2 - Logical Extraction, 3 - Hex Dumping / JTAG (called in this article Physical Extraction), 4 - Chip-Off. A Manual Extraction is viewing the data stored on a mobile device. With the manual manipulation

of the keyboard or touchscreen, the content is displayed on the mobile device screen. The examiner uses an external digital camera to save discovered print screens. To initialize the Logical Extraction, firstly the connection between a mobile device and the workstation must be established. It could be achieved by either a wired (USB, RS-232) or wireless (IrDA, WiFi, Bluetooth) connection, depending on the mobile device model and used software. Then the software is sending a series of commands over the established interface to the mobile device. And finally, the device responds by sending the requested data based upon the command request. The response (mobile device data) is sent back to the workstation and presented to the forensics examiner for reporting purposes. Taking a step up on the Brothers' pyramid, Physical Extraction deals with the raw information stored in the flash memory of the mobile device. Direct access to the flash enables the forensic investigator to find the information. The process creates a binary bit-for-bit copy of an entire file system, similar to the approach known in computer forensic investigations. This method can acquire all of the data present on the flash memory, including the deleted data and access to unallocated space on most devices. The most promising part of this method is the ability of the forensic tool to parse and decode the captured image and make this information available to the examiner. There are a lot of techniques responsible for extracting an image from the mobile device: a. uploading a modified boot loader (or another software) into the RAM, capturing the flash memory and finally sending it to the workstation; b. Joint Test Action Group (JTAG), where the microprocessor of the mobile device is accessed to produce an image. The next level, Chip-off, requires physical removal of the flash memory. Then examiner creates a binary image of the removed chip and net with the power of the forensic tool parsing and decoding the captured image. The last level, Micro Read, requires the usage of an electron microscope to record the physical observation of the gates (NAND or NOR) on the chip.

This research was limited to logical acquisitions by adjusting to the

conditions of the smartphone devices used in the experiment.

Research Procedure

Our experiment was carried out on the up-to-date versions in the period of data acquisition (December 2020) MF tools: Cellebrite UFED 4PC 7.38.0.12 [UFED], Magnet AXIOM Complete 4.7.0.22371 [AXIOM], MicroSystemation XRY 9.2.1 [XRY], MOBILedit Forensic Express 7.3.0.19270 [MOBILedit] and Oxygen Forensic Detective 13.1.0.43 [OXYGEN].

In this research, we decided to investigate the following seven mobile devices: iPhone 5 (A1429) with iOS 10.3.4 [iPhone 5], iPhone SE (A1723) with iOS 14.2 [iPhone SE], Alcatel Rise 31 (4034) with Android 7.1.2 [Alcatel R31], One Plus 3T (A3010) with Android 9.0 [OnePlus 3T], Huawei Mate 10 Lite (RNE-L21) with Android 8.0.0.346 [Huawei M10L], Samsung Galaxy S7 (SM-GF930F) with Android 8.0.0 [Samsung S7], Samsung Galaxy S10 (SM-G973F) with Android 10.0.0 [Samsung S10]. Our choice was forced by accessibility to this devices, diversity and popularity of embedded operating systems (Android is the most popular smartphone platform in the world, with 74,6% of global market share as of May 2020 [9], iOS maintains approximately a 48% share of the smartphone market in the United States, with similar percentages in many western nations [9]) and finally by time constraints caused by the limitation of trial versions of analysed tools. This research was limited to logical acquisitions by adjusting to the conditions of the smartphone devices used in the experiment. The physical acquisition was not used because the smartphone devices used in the research were not rooted or jailbroken.

To make our comparison fully verifiable, the same procedure was applied for each mobile device. Firstly, the device was wiped out, then was properly configured. Android **devices** were set up by synchronization with the Google account. On the other hand, iOS devices were set up via the iCloud service. In the next step a SIM card was inserted into the device to connect to

the operator's network, then the device was restarted. After restarting the device, the SIM card was removed. Call histories as well as SMS and MMS messages have been restored through the dedicated application. Half of data that was saved locally to the device as a result of synchronization has been deleted. In order to be able to proceed with the main part of the research, it was necessary to enable USB debugging mode, disable the application verification via USB and remove the screen lock in Android devices. On the other hand, in devices with iOS, the automatic screen lock and screensaver had to be turned off. In the last step, flight mode had to be turned on in all devices. This activity is to protect the devices against any exchange of data during extraction. The device prepared in this way could be tested.

Results

AXIOM, MOBILedit, OXYGEN, UFED, XRY have been tested for their ability to acquire data from the internal memory of mobile devices using logical extraction. The results of the tests are presented in the table~\ref{tab:caption}. The table is presented in such a way as to present separate results for each tool. The Test Cases column contains two sub-columns that define the categories and the relevant subcategories of the data types that are extracted during the test for each case. Each tool was tested on seven phones. The results are as follows: Green color: the mobile forensic application returned full information about the phone or acquired both existing and deleted data - the tool acquired and reported data from mobile device successfully. Yellow color: the mobile forensic application returned some of information about phone and apps or acquired only existing data. Red color: the mobile forensic application did not acquire supported data or does not provide support for the acquisition for a particular data element. Grey color: application is not supported for this mobile device. With selected extraction method, none of the tools had access to all types of data. The exceptions for each tool are listed below.

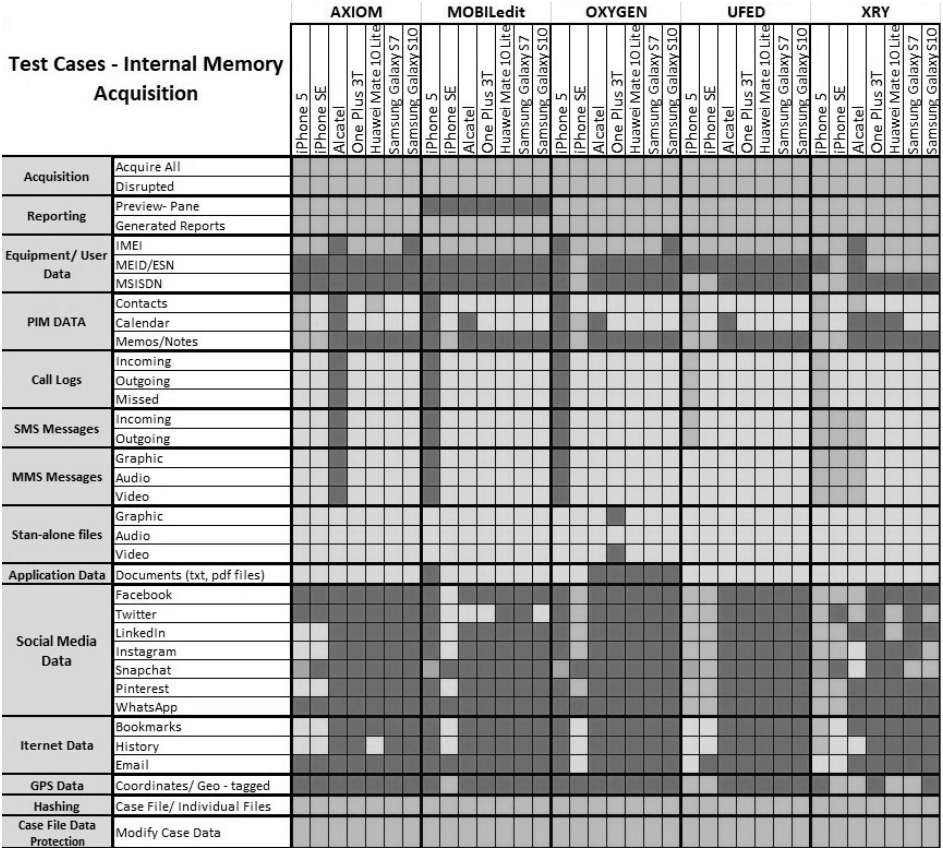


Table 1. Research findings

AXIOM

– MEID/ESN numbers are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.

- MSISDN numbers are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- IMEI numbers are not reported for: Alcatel R31, Samsung S10.
- Calendar events and contacts are not reported for Alcatel R31.
- Notes are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Call logs (incoming, outgoing, missed) are not reported for Alcatel R31.
- SMS and MMS messages are not reported for Alcatel R31.
- Social media related data (i.e., Facebook, Twitter) are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., LinkedIn, Instagram) are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., LinkedIn, Instagram) are partially reported for: iPhone 5, iPhone SE.
- Social media related data (i.e., Snapchat) are not reported for: iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10)
- Social media related data (i.e., Pinterest) are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., WhatsApp) are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.

- Bookmarks are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Browser history is not reported for: Alcatel R31, OnePlus 3T, Samsung S7, Samsung S10.
- Email related data are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- GPS related data (i.e., longitude, latitude coordinates) are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.

MOBILedit

- MEID/ESN numbers are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- MSISDN numbers are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- IMEI numbers are not reported for: Alcatel R31, Samsung S10.
- Calendar events and contacts are not reported for Alcatel R31.
- Notes are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Call logs (incoming, outgoing, missed) are not reported for Alcatel R31.
- SMS and MMS messages are not reported for Alcatel R31.

- Social media related data (i.e., Facebook, Twitter) are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., LinkedIn, Instagram) are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., LinkedIn, Instagram) are partially reported for: iPhone 5, iPhone SE.
- Social media related data (i.e., Snapchat) are not reported for: iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10)
- Social media related data (i.e., Pinterest) are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., WhatsApp) are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Bookmarks are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Browser history is not reported for: Alcatel R31, OnePlus 3T, Samsung S7, Samsung S10.
- Email related data are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- GPS related data (i.e., longitude, latitude coordinates) are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.

OXYGEN

- MEID/ESN numbers are not reported for: iPhone 5, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- MSISDN numbers are not reported for: iPhone 5, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- IMEI numbers are not reported for: iPhone 5, Samsung S10.
- Calendar events are not reported for iPhone 5, Alcatel R31.
- Contacts are not reported for iPhone 5.
- Notes are not reported for: iPhone 5, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Call logs (incoming, outgoing, missed) are not reported for iPhone 5.
- SMS and MMS messages are not reported for iPhone 5.
- Graphic and video files are not reported for OnePlus 3T.
- Document files (i.e., .txt, .pdf) are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., Facebook, Twitter, LinkedIn, Instagram, Pinterest) are not reported for: iPhone 5, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., Snapchat) are not reported for: iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., WhatsApp) are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.

- Bookmarks, browser history and email related data are not reported for: iPhone 5, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- GPS related data (i.e., longitude, latitude coordinates) are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.

UFED

- MEID/ESN numbers are not reported for: iPhone 5, iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- MSISDN numbers are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Calendar events are not reported for Alcatel R31.
- Notes are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., Facebook, Twitter, LinkedIn, Instagram, Snapchat, Pinterest, WhatsApp) are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Bookmarks and browser history are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Email related data are not reported for: iPhone SE, Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- GPS related data (i.e., longitude, latitude coordinates) are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.

XRY

- MEID/ESN numbers are not reported for: iPhone 5, Alcatel R31.
- MSISDN numbers are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- IMEI number is not reported for Alcatel R31.
- Calendar events are not reported for Alcatel R31, OnePlus 3T, Huawei M10L.
- Notes are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., Facebook) are not reported for: OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Social media related data (i.e., Twitter) are not reported for: iPhone SE, OnePlus 3T, Samsung S7.
- Social media related data (i.e., LinkedIn) are not reported for: Alcatel R31, OnePlus 3T, Samsung S7, Samsung S10.
- Social media related data (i.e., Instagram) are not reported for: OnePlus 3T, Huawei M10L, Samsung S7.
- Social media related data (i.e., Snapchat) are not reported for: iPhone SE, OnePlus 3T, Huawei M10L.
- Social media related data (i.e., Pinterest, WhatsApp) are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Bookmarks and email related data are not reported for: Alcatel R31, OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- Browser history is not reported for: OnePlus 3T, Huawei M10L, Samsung S7, Samsung S10.
- GPS related data (i.e., longitude, latitude coordinates) are not reported for: iPhone 5, OnePlus 3T, Samsung S10.

Conclusions

In this paper we have tested five mobile forensic tools on seven different mobile devices according to the NIST methodology [2].

Our tests have shown that there are significant differences in results between individual data types across the tested tools. There is no single tool that demonstrates strong predominance in all testing categories, but in our experiment XRY and UFED provided the most accurate results. One of the conclusions proves that there is a significant increase in the success rate when performing a cross-reference tool analysis, which is extremely important in the real world where each piece of evidence matters and whose findings could become of vital importance in the courtroom where people's cases are judged.

Acknowledgments

We would like to express our sincere thanks to Mediarecovery company for providing 30-day trial versions of all mobile forensic tools that were mentioned in the article.

References

1. NIST: Mobile device acquisition tool,https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/mobile. (last access 2021.01.10).
2. NIST: Mobile device forensic tool test spec v 3.0, https://www.nist.gov/document/mobile_device_forensic_tool_test_spec_v_3.0.pdf. (last access 2021.01.10).
3. Afonin, O., Katalov, V.: Mobile Forensics–Advanced Investigative Strategies. Packt Publishing Ltd (2016).
4. Al-Dhaqm, A., Abd Razak, S., Ikuesan, R.A., Kebande, V.R., Siddique, K.: A review of mobile forensic investigation process models. IEEE Access 8, 173359–173375 (2020).

5. Brothers, S.: How cell phone “forensic” tools actually work–cell phone tool levelling system. Mobile Forensic World, Chicago, IL (2008).
6. Jansen, W., Ayers, R.: Guidelines on cell phone forensics. NIST Special Publication 800(101), 800–101 (2007).
7. Lutes, K.D., Mislan, R.P.: Challenges in mobile phone forensics. Proceeding of the 5th International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA) (2008).
8. Sai, D.M., Prasad, N., Dekka, S.: The forensic process analysis of mobile device. Int. J. Comput. Sci. Inf. Technol6(5), 4847–4850 (2015).
9. Zinkus, M., Jois, T., Green, M.: Data security on mobile devices: Current state of the art, open problems, and proposed solutions, https://securephones.io/main.pdf. (last access 2021.01.10).

Abstrakt

ANALIZY NARZĘDZI DO KRYMINALISTYCZNEGO BADANIA URZĄDZEŃ MOBILNYCH

Streszczenie: Kryminalistyczne badanie urządzeń mobilnych jawi się jako nowe wyzwanie doświadczające gwałtownych zmian każdego roku. Wzrastająca liczba smartfonów, systematyczne uaktualnianie ich systemów operacyjnych, duża różnorodność aplikacji systemowych utrudniają pracę analityka kryminalistycznego. Niezbędna dlatego jest właściwa wiedza cech i ograniczeń używanych narzedzi kryminalistycznych, aby analiza była przeprowadzona rzetelnie. Badanie było przeprowadzone z wykorzystaniem siedmiu urządzeń mobilnych, z których wykonano akwizycję logiczną za pomocą pięciu narzedzi: MicroSystemation XRY, Cellebrite UFED, Magnet AXIOM, MOBILedit Forensic Express, and Oxygen Forensic Detective. W rozdziale przedstawiono rezultaty analizy ilościowej, która została wykorzystana do zmierzenia i porównania jakości wskazanych narzedzi.

Słowa kulczowe: smartfon, badanie kryminalistyczne, narzędzia.

Rozdział 8

Przestępstwa przeciwko integralności danych informatycznych – wybrane aspekty karnomaterialne i techniczne

dr Filip RADONIEWICZ[1]

STRESZCZENIE: Celem niniejszego rozdziału jest przedstawienie aspektów technicznych cyberprzestępstw skierowanych przeciwko integralności danych informatycznych oraz aspektów karnomaterialnych tej problematyki. Jego pierwsza część poświęcona jest sposobom naruszania integralności danych („technikom hackerskim" oraz „programom hackerskim"), druga – ich kwalifikacji prawnej. Autor, dokonując krytycznej analizy przepisów kodeksu karnego, przedstawia jednocześnie swoje propozycje zmian.

SŁOWA KLUCZOWE: wirus komputerowy, sieć teleinformatyczna, internet, malware, złośliwe oprogramowanie, hacker.

Działania sprawców nazywanych potocznie hackerami[2] albo trochę

---

[1] Adiunkt, Wydział Bezpieczeństwa Narodowego Akademii Sztuki Wojennej, f.radoniewicz@akademia.mil.pl, ORCID: 0000-0002-7917-4059.

[2] Początkowo termin „hacker" miał trochę inne znaczenie niż obecnie – oznaczał po prostu zdolnego programistę. Później, po zlaniu się w latach 70. subkultury hackerów z phreakerami (od ang. *phone freak* – „telefoniczny maniak") – osoby włamujące się do sieci telekomunikacyjnych, by móc nawiązywać darmowe połączenia), zaczął nabierać innego (bliskiego dzisiejszemu) znaczenia – kogoś działającego w podziemiu, włamującego się do komputerów i sieci, często ze szlachetnych pobudek, a czasami po prostu dla zabawy i zdobycia sławy. Taki obraz w kulturze

trafniej – cyberprzestępcami - mają często czysto destrukcyjny charakter. Polegają na elektronicznym (logicznym) niszczeniu danych np. poprzez ich kasowanie czy formatowanie dysków. Korzystają oni w tym celu z programów komputerowych, wśród których w pierwszej kolejności należy wskazać wirusy.

Wirusy są to programy instalujące się zazwyczaj bez wiedzy i zgody 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). Pojęcia „wirus", na określenie takiego samoreplikującego się programu, użył po raz pierwszy amerykański informatyk F. Cohen (twórca pierwszych systemów antywirusowych). Jednym z pierwszych takich wirusów był Michał Anioł, który uaktywniał się i próbował kasować dane 6 marca – w dniu urodzin artysty. 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

utrwaliły filmy (zwłaszcza *Gry wojenne* J. Badhama z 1983 r. czy *Hakerzy* I. Softleya z 1995 r.). Obecnie pod pojęciem „hacker" często rozumie się osobę, która „sieje zamęt" w Internecie, czyli zarówno włamuje się do sieci komputerowych i komputerów, jak i działa w celu zakłócenia ich pracy. W języku potocznym często określenie to używane jest dla generalnego określenia przestępców działających w Internecie, w tym internetowych oszustów. Zob. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 31-32.

mutacji; nie jest to jednak proces zamierzony, ma raczej charakter losowy, a ponadto nie wiąże się ze zmianą funkcji poszczególnych instrukcji – zob. dalsze uwagi) – hackerzy w oparciu o stary kod często tworzą ich ulepszone wersje. Zmniejszają tym samym możliwość wykrycia ich przez programy antywirusowe. Miesięcznie pojawia się co najmniej kilkaset wirusów[3].

Przyjmując różne kryteria, można wskazać następujące typy wirusów[4]:

1) z uwagi na umiejscowienie wirusa zwykle wyróżnia się:
   a) wirusy sektora startowego (ang. *Boot Sector Virus*) – zapisywane są w głównym rekordzie rozruchowym dysku twardego (ang. *master boot record*), skąd ładowane są do pamięci jeszcze przed uruchomieniem systemu operacyjnego;
   b) wirusy plikowe (ang. *File-infecting Viruses*), infekujące pliki (niegdyś jedynie pliki wykonywalne). Jest to najczęściej spotykany rodzaj wirusów. Kod wirusa umieszcza się na początku (w najstarszych wirusach), na końcu lub w losowo wybranej części pliku (w nowszych odmianach). W momencie załadowania pliku do pamięci w pierwszej kolejności wykonywany jest kod wirusa. Po jego wykonaniu plik, który jest jego nosicielem, zaczyna często działać w sposób poprawny, w związku z czym sam fakt uaktywnienia wirusa może pozostać niezauważony;

---

[3] S.W. Brenner, *Cybercrime and the Law. Cheallenges. Issues, and Outcomes*, Boston 2012, s. 36–37; B. Fischer, *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000, s. 40–50.

[4] R. Russell (red.), *Hack Proofing Your Network.* Edycja Polska, Gliwice 2002, s. 567–575; D.L. Shinder, E. Tittel, *Cyberprzestępczość.Jak walczyć z łamaniem prawa w sieci,* Gliwice 2004*,* s. 319–322, 326–327; A. Warhole, *Atak z Internetu*, Warszawa 1999, s. 119–121.

c) wirusy wieloczęściowe (ang. *Multipartite Viruses*) nazywane często hybrydowymi – są to wirusy, które łączą w sobie cechy wirusa rezydującego w boot sektorze dysku twardego (MBR) i wirusa plikowego. Jest w związku z tym trudniejszy do usunięcia – jeżeli w trakcie jego usuwania pominie się część rezydującą w MBR, wkrótce odrodzi się on w oparciu o kod tam zawarty i zainfekuje system ponownie;

d) wirusy makra (makrowirusy, ang. *macro viruses*) – uruchamiają się tak, jak zwykłe makro (makra są to niewielkie aplikacje zawarte w dokumentach), a więc w środowisku innego programu (programu biurowego, zwykle edytora tekstu, ale może być to również np. arkusz kalkulacyjny). Atakują nie pliki wykonywalne, lecz pliki zawierające definicje makr;

2) miejsce położenia w pamięci jest podstawą podziału wirusów na:

a) wirusy rezydentne (ang. *Resident Viruses*), których „instalacja" odbywa się w pamięci zainfekowanego hosta, a jego uruchomienie następuje, gdy zostaną spełnione określone warunki (np. uruchomienie programu). Większość wirusów to wirusy z tej grupy;

b) wirusy nierezydentne (ang. *Non-resident Viruses*; inaczej: *Direct-action Viruses*, czyli wirusy atakujące bezpośrednio pliki) – wirus z tej grupy może zostać uaktywniony tylko w wyniku uruchomienia zainfekowanego programu. W przeważającej liczbie wypadków zostanie uaktywniony tylko raz (chyba że nastąpi kolejne uruchomienie zainfekowanego programu), w tym czasie aktywnie szuka sposobów rozprzestrzenienia się (za pomocą lokalnych napędów lub za pośrednictwem sieci), czyli zainfekowania innych plików;

3) ze względu na cechy charakterystyczne można przykładowo wskazać następujące typy wirusów:

a) wirusy ukryte (ang. *stealth viruses*) – są w stanie ukryć się przed programami antywirusowymi poprzez np. usunięcie się z zainfekowanego pliku i umieszczenie w innej lokalizacji czy wykonanie kopii zainfekowanego wcześniej pliku niezawierającej jego kodu w celu niejako „podsunięcia jej" skanerowi antywirusowemu podczas skanowania dysku twardego;
b) wirusy polimorficzne (ang. *polymorphic viruses*) – potrafią się replikować, ale tworzone przez nie kopie nie są identyczne (np. w wyniku szyfrowania swojego kodu za każdym razem przy pomocy innego klucza), przez co są trudniejsze do wykrycia przez programy antywirusowe, które mogą nie zawierać w swych bazach danych wszystkich ich odmian;
c) wirusy metamorficzne (ang. *methamorphic viruses*) – podobnie jak wirusy polimorficzne zmieniają swój kod, ale nie poprzez szyfrowanie, a przez usuwanie bądź dodawanie instrukcji lub zmianę sposobu zakodowania tychże instrukcji (bez zmiany ich funkcji);
d) wirusy opancerzone (ang. *armored viruses*) – stosują różne techniki mające na celu utrudnienie ich wykrycia przez programy antywirusowe (np. poprzez wprowadzanie w błąd co do lokalizacji na dysku);
e) wirusy szczelinowe, wypełniające (ang. *cavity viruses*) – nadpisują zawartość plików, nie zmieniając jednocześnie ich długości (nie dopisują się do pliku, ale wykorzystują – wypełniają – znajdujące się w nim puste przestrzenie), przez co utrudniają wykrycie faktu ich zainfekowania;
f) wirusy zakamuflowane (ang. *camouflage viruses*) – wirusy udające nieszkodliwe programy. Obecnie – z uwagi na rozwój oprogramowania antywirusowego i stosowanie

zaawansowanych metod wykrywania wirusów – łatwe do wykrycia, a w związku z tym rzadko spotykane;

g) wirusy towarzyszące (ang. *companion viruses*) – wirusy tworzące osobny plik wykonywalny z własnym kodem i zastępujące nim plik z oryginalnym programem (który przechowywany jest pod zmienioną nazwą lub usuwany na stałe z systemu). Jest to bardzo prymitywny rodzaj wirusa tworzony zazwyczaj przez początkujących programistów w językach wysokiego poziomu;

h) wspomniane już wcześniej bomby czasowe i logiczne[5].

Innymi używanymi przez sprawców programami są tzw. konie trojańskie, zwane potocznie trojanami. Są to nieszkodliwe na pierwszy rzut oka programy, w których zapisano dodatkowe instrukcje. Wykonują one działania, o których użytkownik nie wie. Służą one hackerom do obejścia zabezpieczeń systemu. Po zainstalowaniu trojana hacker może uzyskiwać dostęp do danych. Ponadto sam trojan może wykonywać pewne czynności, takie jak usuwanie danych lub ich modyfikacja czy przesyłanie plików do napastnika. Trojany często zamaskowane są jako nieszkodliwe programy (np. wygaszacze ekranu) czy jako skrypty wykonywalne na witrynach internetowych, które następnie instalują się w komputerze użytkownika w momencie wejścia na zainfekowaną stronę. Za przykład trojana może posłużyć Pokemon Trojan (który zaklasyfikowano jako *W32.Pokemon.Worm*). Po uruchomieniu pliku pokemon.exe na ekranie zostaje wyświetlona animacja Pikachu (postać z japońskiej serii anime pt. *Pokemon*), a jednocześnie wysyła się on pocztą elektroniczną do każdego adresata znajdującego się w książce adresowej programu pocztowego i przystępuje do usunięcia wszystkich plików z katalogu Windows. Bardzo

[5] F. Radoniewicz, *Odpowiedzialność karna…,* s. 82-85.

popularnym trojanem jest napisany w 1998 r. przez szwedzkiego programistę C.F. Neiktera Netbus. Po umieszczeniu w komputerze ofiary pozwala on sprawcy – poza wykonywaniem „klasycznych czynności" (tj. np. zarządzaniem plikami czy przechwytywaniem znaków wpisywanych za pomocą klawiatury) – na dokonywanie bardzo wielu operacji, takich jak np. wysuwanie i wsuwanie tacki napędu optycznego (CD-ROM/DVD-ROM), zamianę klawiszy myszy (lewy przycisk staje się prawym i odwrotnie), wyświetlanie plików graficznych na ekranie, wyłączenie systemu, uruchamianie dowolnego programu czy zamykanie systemu operacyjnego[6].

Kolejnym przykładem programu zagrażającego danym jest robak. Obecnie różnica między robakami a wirusami jest mniej czytelna niż kiedyś – program ten przemieszcza się za pomocą sieci i infekuje wiele komputerów, co niegdyś wyraźnie odróżniało go od wirusów, które początkowo nie były do tego zdolne (replikowały się na pojedynczych komputerach). Ponadto robaki, w przeciwieństwie do wirusów, są samodzielne – nie są powiązane z innymi programami. 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. Z założenia miał być niegroźny. Ponadto zawierał mechanizm mający ograniczyć jego powielanie się. Ponieważ mechanizm ów nie

[6] Zob. R. Russell (red.), *Hack Proofing …*, s. 570–571; D.L. Shinder, E. Tittel, *Cyberprzestępczość*..., s. 286. Zob szerzej A. Warhole, *Atak z Internetu*…, s. 96–101.

zadziałał, robak replikował się w oszałamiającym tempie, unieruchamiając w ciągu kilku godzin 6000 komputerów podłączonych do Internetu (wówczas stanowiło to ok. 10% ogółu). Morris próbował przeciwdziałać skutkom swojego działania, umieszczając w sieci rozwiązanie problemu. Równolegle naukowcy z uniwersytetu w Berkeley oraz Massachusetts Institute of Technology znaleźli sposób na poradzenie sobie z robakiem. Po wszystkim Morris przyznał się do spowodowania całego zamętu i został pierwszym skazanym na podstawie *Computer Fraud and Abuse Act* z 1986 r. (na 3 lata dozoru sądowego, 400 godzin prac społecznych oraz grzywnę wysokości 10.000 dolarów)[7].

Trojany – razem z omówionymi wyżej wirusami i robakami– należą do grupy tzw. *malware* (jest to skrót od ang. *malicious software* – oprogramowanie złośliwe). Ponadto do tej kategorii zalicza się przede wszystkim oprogramowanie szpiegujące (ang. *spyware*). Programy należące do tej grupy zbierają 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. Wśród innych metod instalacji należy wskazać przesłanie takiego programu pocztą elektroniczną jako załącznik do e-maila (po otwarciu którego program instaluje się w systemie),.

W polskim kodeksie karnym[8] zamachy na integralność danych informatycznych kryminalizują aż trzy przepisy – art. 268 § 2 i 3, art. 268a oraz art. 269.

Przepis art. 268 § 2 kk kryminalizuje bezprawne zachowania polegające na niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu zapisu

---

[7] Zob. szerzej S.W. Brenner, *Cybercrime and the Law…,* s. 57 i n.; F Radoniewicz, *Odpowiedzialność karna…,* s. 85-86.

[8] Dz. U. 2021 r., poz. 2345 ze zm.

istotnej informacji na informatycznym nośniku danych[9] albo udaremnianiu lub znacznym utrudnianiu w inny sposób osobie uprawnionej zapoznania się z informacją utrwaloną na takim nośniku. Ze względu na wyższy stopień szkodliwości społecznej tego czynu stanowi on typ kwalifikowany przestępstwa z art. 268 § 1 kk.

W doktrynie w zasadzie nie budzi wątpliwości, iż przedmiotem ochrony jest integralność zapisu informacji, czyli danych informatycznych (mowa jest o całkowitym unicestwieniu zapisu – wskazują na to zwroty „niszczy", „usuwa", oraz o modyfikacji bez unicestwienia, ale w stopniu znacznym – „uszkadza", „zmienia") oraz jej dostępność (czyli możliwość korzystania) dla osoby uprawnionej (mowa jest bowiem o udaremnieniu lub znacznym utrudnieniu zapoznania się z informacją[10])[11]. Ustawodawca jednocześnie wymaga, aby była to informacja „istotna" – przede wszystkim w sensie obiektywnym (ze względu na jej treść, wagę i znaczenie[12]) – ale z uwzględnieniem interesów osoby uprawnionej do zapoznania się z nią[13],

---

[9] Pojęcie „informatyczny nośnik danych" zostało wprowadzone ustawą z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej, zastępując budzące w doktrynie wątpliwości sformułowaniem „komputerowy nośnik informacji" (Dz.U. 2008, nr 171, poz. 1056).

[10] Sąd Najwyższy w postanowieniu z dnia 29 września 2009 r. wskazał, że znacznym utrudnieniem będzie sytuacja, w której odczytanie informacji wymaga znacznego nakładu czasu lub wysiłku bądź też w której informacja ma charakter niekompletny lub zniekształcony (WK 15/09, „Orzeczenia Sądu Najwyższego w Sprawach Karnych" 2009, nr 1, poz. 1903).

[11] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 64–65.

[12] P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego,* CzPKiNP 2000, nr 1, s. 88.

[13] Ibidem, s. 88; P. Kozłowska-Kalisz, *Komentarz do art. 268 kk,* [w:] M Mozgawa (red.), *Kodeks karny. Praktyczny komentarz,* Warszawa 2015; W. Wróbel, D. Zając, *Komentarz do art. 268 kk*, [w:] W. Wróbel (red.), A. Zoll (red.), *Kodeks karny.*

w tym także celu, jakiemu jej służyła lub miała służyć[14].

Przedmiotem czynności wykonawczej – zgodnie z literalnym brzmieniem – jest informacja zapisana na informatycznym nośniku danych. W związku z tym uważam, że przepis art. 268 § 2 kk nie znajdzie zastosowania w sytuacji, gdy utrudnienie w zapoznaniu się z informacją będzie rezultatem zachowań polegających na zakłócaniu pracy sieci. Wtedy zastosowanie znajdzie przepis art. 268a lub 269a kk.

Działania wymienione w tym przepisie mogą być zarówno celem sprawcy, jak i środkiem zatarcia przez hakera śladów jego obecności w systemie. Zwykle będzie to modyfikacja logów, które nie zawsze można uznać za „istotny zapis informacji". Jednak czasami mogą to być poważniejsze zniszczenia.

Pierwszą grupę czynności wykonawczych – jak wskazano wyżej – stanowią czyny godzące w integralność danych. Będą to przede wszystkim działania o charakterze logicznym, polegające np. na ich kasowaniu, usuwaniu, często za pomocą specjalnych programów, takich jak wirusy, robaki, trojany. Oczywiście, dane na informatycznym nośniku danych można unicestwić również poprzez działania fizyczne, np. niszcząc nośnik czy uszkadzając go (np. przez umieszczenie w polu elektromagnetycznym).

Druga grupa czynności wykonawczych – udaremnianie lub znaczne utrudnianie osobie uprawnionej zapoznanie się z informacją – ma charakter dopełniający. Użyte przez ustawodawcę sformułowanie jest bardzo pojemne[15]. Zachowanie sprawcy może polegać np. na zamontowaniu hasła uniemożliwiającego dostęp lub zniszczeniu programu umożliwiającego

---

Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d, Warszawa 2017.

[14] O. Górniok, [w:] O. Górniok i in., *Kodeks karny. Komentarz,* t. 2, Gdańsk 2005, s. 363–364.

[15] Ibidem, s. 90.

zapoznanie się z informacją[16].

Zniszczenie jednej z wielu kopii zapisanej informacji nie wypełnia znamion omawianego przestępstwa. Podobnie, według A. Adamskiego, znamion tego przestępstwa nie wyczerpuje zachowanie sprawcy, który niszczy nośnik w sytuacji, gdy dysponent posiada kopię zapasową[17]. Wydaje się, że w takim przypadku można mówić o usiłowaniu.

Podkreślić należy, ze ustawodawca traktuje komputer jako zaawansowaną maszynę do pisania, ograniczając ochronę zapewnianą przez przepis art. 268 § 2 k.k. jedynie do informacji zrozumiałych dla człowieka, podczas gdy procesy składające się na funkcjonowanie systemu komputerowego polegają na wymianie danych między jego elementami (programowymi i sprzętowymi) i wykonywaniu instrukcji, odbywającymi się w pełni automatycznie, bez udziału i kontroli człowieka, w języku binarnym, bezpośrednio niezrozumiałym dla niego[18].

Przepis art. 268 § 3 kk jest typem kwalifikowanym przestępstwa naruszenia integralności zapisu informacji. Znamieniem kwalifikującym jest wyrządzenie przez sprawcę znacznej szkody majątkowej[19]. Niewątpliwie chodzi tu nie o wartość informatycznego nośnika danych (która może być

---

[16] W. Wróbel, D. Zając, *Komentarz do art. 268 kk*, [w:] *Kodeks karny*…, red. W. Wróbel, A. Zoll.

[17] A. Adamski, *Prawo karne...*, s. 72; podobnie: W. Wróbel, D. Zając, *Komentarz do art. 269 kk*, [w:] W. Wróbel, D. Zając, *Komentarz do art. 269 kk*, [w:] W. Wróbel (red.), A. Zoll (red.), *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d*, Warszawa 2017. N. Kłączyńska, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J.W. Giezek, Warszawa 2014, s. 993; B. Kunicka-Michalska, [w:] L. Gardocki (red.) *System Prawa karnego. T. 8 Przestępstwa przeciwko państwu i dobrom zbiorowym,* Warszawa 2018*,* s. 947.

[18] A. Adamski, *Prawo karne...*, s. 76.

[19] Przez znaczną szkodę majątkową rozumie się (zgodnie z przepisami art. 115 § 7 w związku z art. 115 § 5 kk) szkodę, której wartość w czasie popełnienia czynu zabronionego przekracza 200 000 zł.

symboliczna), ale o szkodę, jaką faktycznie ponosi dysponent informacji w następstwie czynu, np. mogą to być koszty związane z odtworzeniem zapisów księgowości czy utracony przez autora dzieła zysk związany z jego sprzedażą[20]. Jak wskazują W. Wróbel i D. Zając, szkoda majątkowa może być następstwem czynu zabronionego określonego w omawianym przepisie, gdy pokrzywdzony wskutek niemożności zapoznania się z określoną informacją podejmuje decyzje majątkowe, które przynoszą mu straty[21]. Obejmuje ona zarówno uszczerbek w majątku pokrzywdzonego (*damnum emergens*), jak i utracone korzyści (*lucrum cessans*)[22]. W związku z faktem, że Internet jest w coraz większym stopniu wykorzystywany do wszelkiego rodzaju działalności gospodarczej, problem z tego typu przestępstwami będzie narastał.

W zasadzie panuje zgoda w doktrynie, że czynu tego można się dopuścić tylko umyślnie, zarówno w zamiarze bezpośrednim, jak i ewentualnym[23] – sprawca musi co najmniej godzić się na to, że jego zachowanie może skutkować zniszczeniem, uszkodzeniem, usunięciem lub zmianą zapisu istotnej informacji bądź z uniemożliwieniem lub znacznym utrudnieniem zapoznania się z nią przez uprawnioną osobę (a w przypadku czynu z art. 268 § 3 kk musi ponadto co najmniej godzić się na spowodowanie znacznej szkody majątkowej). Nie jest możliwe popełnienie tego występku nieumyślnie. Przykładowo nie wypełnia znamion niezachowanie ostrożności

---

[20] A. Marek, *Kodeks karny. Komentarz*, Warszaawa 2010, s. 573; B Kunicka-Michalska, [w:] *Kodeks karny. Część szczególna. Komentarz do artykułów 222–316*, t. II, red. A. Wąsek, R. Zawłocki, Warszawa 2010, s. 715–716.

[21] W. Wróbel, D. Zając, *Komentarz do art. 268 kk*, [w:] *Kodeks karny*…, red. W. Wróbel, A. Zoll.

[22] P. Kardas, *Prawnokarna ochrona...*, s. 92.

[23] Odmiennie A. Marek, według którego „usuwanie", „zmienianie", „udaremnianie" lub „utrudnianie" wymagają zamiaru bezpośredniego (A. Marek, *Kodeks karny...*, s. 573. Podobnie B. Kunicka-Michalska, [w:] *System prawa...*, s. 1029).

przy korzystaniu z komputera podłączonego do sieci i przypadkowe zainfekowanie pozostałych pracujących w niej komputerów wirusem otrzymanym jako załącznik do poczty elektronicznej.

Uważam, że przepis ten obecnie można uznać za zbędny, gdyż jego rolę mógłby z powodzeniem odgrywać art. 268a § 1 kk.

Zgodnie z art. 268a § 1 kk karze pozbawienia wolności do lat 3 podlega ten, kto – nie będąc do tego uprawniony – niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych. Przedmiotem ochrony przytoczonego wyżej przepisu są dane informatyczne, a ściśle – ich integralność (mowa jest o niszczeniu, uszkadzaniu, usuwaniu danych) oraz ich dostępność (bezpieczne gromadzenie, przetwarzanie i przekazywanie przez osoby uprawnione). Ochronie podlegają również programy komputerowe (z uwagi na posłużenie się przez ustawodawcę pojęciem danych informatycznych, a nie informacji, jak w art. 268 kk)[24].

---

[24] Podobnie P. Kozłowska-Kalisz (zob: P. Kozłowska-Kalisz, *Komentarz do art. 268a kk*, *pkt 2*, [w:] *Kodeks karny…,* red. M. Mozgawa). M. Siwicki wskazuje jeszcze prawidłowość funkcjonowania programów komputerowych, co w zasadzie mieści się w zakresie „integralności danych". Zob. M. Siwicki, *Cyberprzestępczość,* Warszawa 2013, s. 147. W doktrynie jednak nie ma w tej kwestii zgodności. A. Adamski uważa, że przepis art. 268a kk chroni jedynie dostępność danych, co wynika z przyjętej przez niego interpretacji tego przepisu (A. Adamski, *Cyberprzestępczość – aspekty prawne i kryminologiczne,* „Studia Prawnicze" 2005, s. 58–59). W. Wróbel i D. Zając wskazują ogólnie na „bezpieczeństwo informacji przechowywanych, przesyłanych i przetwarzanych w systemach funkcjonujących w oparciu o dane informatyczne" (W. Wróbel, D. Zając, *Komentarz do art. 268a kk, pkt 1*, [w:] W. Wróbel (red.), A. Zoll (red.), *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d*, Warszawa 2017). Natomiast A. Sakowicz prezentuje stanowisko, że poza integralnością i dostępnością danych informatycznych przedmiotem ochrony art. 268a kk jest również ich poufność, co

Ustawodawca nie użył w treści omawianego przepisu pojęcia systemu komputerowego, systemu informatycznego, systemu teleinformatycznego ani sieci telekomunikacyjnej czy teleinformatycznej. Nie ulega jednak wątpliwości, że środowiskiem, w którym następuje przetwarzanie, gromadzenie lub przekazywanie danych, są właśnie te struktury.

Przepis art. 268a § 1 kk sformułowany jest niezwykle nieprecyzyjnie. Brzmi on następująco: „kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych". Wątpliwości powstają przy próbie odpowiedzi na pytanie, co jest przedmiotem wykonawczym kryminalizowanych zachowań polegających na „niszczeniu", „uszkadzaniu", „usuwaniu", „zmienianiu"? Czy jest to – jak wynika z literalnego brzmienia – dostęp do danych informatycznych (co trudno sobie w praktyce wyobrazić), czy dane informatyczne? Skłaniam się ku tej drugiej interpretacji jako bardziej logicznej[25].

Przedmiotem ochrony omawianego przepisu są dane komputerowe przetwarzane w systemie komputerowym, informatycznym oraz sieci telekomunikacyjnej, a ponadto dane zapisane na nośnikach informatycznych niebędące istotnym zapisem informacji, gdyż te chroni przepis art. 268 § 2 kk[26], jako przepis o charakterze szczególnym, przewidujący jednak tę samą

---

według mnie jest domeną przepisów art. 267 § 1–4 kk (A. Sakowicz, [w:] *Kodeks karny. Część szczególna*, red. M. Królikowski, R. Zawłocki, t. II, *Komentarz do artykułów 222–316,* Warszawa 2013. Podobnie uważają J. Giezek i B. Kunicka-Michalska (J.W. Giezek, [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J.W. Giezek, Warszawa 2014, s. 996; B. Kunicka-Michalska, [w:] *System prawa…,* red. L. Gardocki, s. 1031.

[25] Podobnie: W. Wróbel, D. Zając, *Komentarz do art. 268a kk, pkt 8*, [w:] *Kodeks karny*…, red. W. Wróbel, A. Zoll. Przeciwnie: B. Kunicka-Michalska, [w:] *System prawa…*, s. 1031; A. Adamski, *Cyberprzestępczość – aspekty...*, s. 59.

[26] Stosownie do tego przepisu, jeżeli czyn określony w § 1 (nieuprawnione niszczenie, uszkadzanie, usuwanie lub zmienianie zapisu istotnej informacji albo w inny

sankcję (karę pozbawienia wolności do lat 3). Tym samym, w przypadku rezygnacji z przepisu art. 268 § 2 kk, art. 268a § 1 kk mógłby pełnić jego funkcję, zapewniając ochronę przed zamachami na wszelkie dane informatyczne, bez względu na stopień „istotności", zarówno przechowywane na nośnikach, jak i przetwarzane w systemach informatycznych.

Pierwsza część przepisu art. 268a § 1 kk kryminalizuje działania polegające na niszczeniu i modyfikacji danych oraz utrudnianiu dostępu do danych informatycznych.

W omawianym przepisie ustawodawca nie wprowadza wymogu istotności danych informatycznych, będących przedmiotem wykonawczym czynu jako warunku pociągnięcia sprawcy do odpowiedzialności karnej. W związku z tym możliwe jest przyjęcie, iż przepis art. 268a § 1 kk może służyć do kryminalizacji działań polegających na zainstalowaniu przez sprawcę w zaatakowanym przez niego systemie komputerowym np. trojana, programu typu spyware czy programu służącego przejęciu nad nim kontroli w celu wykorzystania go do przeprowadzenia rozproszonego ataku odmowy usługi (dDoS). Zachowanie takie niewątpliwie stanowi bowiem nieuprawnioną modyfikację danych komputerowych, a zatem zamach na ich integralność[27].

W drugiej części przepisu penalizowane są działania polegające na istotnym zakłócaniu (czyli utrudnianiu funkcjonowania systemu informatycznego) lub uniemożliwianiu przetwarzania, gromadzenia lub przekazywania danych informatycznych. Sformułowanie to odnosi się do

---

sposób udaremnianie lub znaczne utrudnia osobie uprawnionej zapoznanie się z nią) dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

[27] Zob. A. Adamski, *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę,* [w:] *Internet. Ochrona wolności, własności i bezpieczeństwa*, red. G. Szpor, Warszawa 2011, s. 349.

wszelkich czynności oddziałujących na te procesy, których skutkiem jest ich nieprawidłowy przebieg lub spowolnienie, a także zniekształcenie czy modyfikacja przetwarzanych, przekazywanych lub gromadzonych danych informatycznych[28]. Pod pojęciem przetwarzania danych komputerowych rozumie się wykonywanie na nich operacji logicznych, przekazywania – przesyłanie w ramach systemu informatycznego[29], gromadzenia – przechowywanie w systemie informatycznym. Dwa ostatnie pojęcia zawierają się w pierwszym. Czynności automatyczne to takie, które w całości lub części odbywają się bez ingerencji człowieka.

Przepis art. 268a § 2 kk przewiduje typ kwalifikowany przestępstwa z art. 268a § 1 kk. Znamieniem kwalifikującym jest spowodowanie przez sprawcę znacznej szkody majątkowej, a grożącą sankcją – kara pozbawienia wolności od trzech miesięcy do pięciu lat.

Czyn zabroniony, stypizowany w art. 269 kk, w doktrynie prawa karnego jest określany jako „sabotaż komputerowy" lub „sabotaż informatyczny". Jego istotą jest niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Zgodnie z przepisem art. 269 § 2 kk przestępstwo sabotażu

---

[28] W. Wróbel, D. Zając, *Komentarz do art. 268a, pkt 10*, [w:] *Kodeks karny...*, red. W. Wróbel, A. Zoll. Por. P. Kardas, *Prawnokarna ochrona*…, s. 96.

[29] Inaczej P. Kozłowska-Kalisz, która uważa, że za przekazywanie danych informatycznych należy uznać zarówno transmisję danych, jak i przekazanie nośnika danych (P. Kozłowska-Kalisz, *Komentarz do art. 268a, pkt 10*, [w:] *Kodeks karny...*, red. M. Mozgawa). Podobnie: A. Sakowicz, [w:] *Kodeks karny...,* s. 448; J.W. Giezek, [w:] *Kodeks karny...,* s. 998.

informatycznego polegać może również na niszczeniu albo wymianie informatycznego nośnika danych lub niszczeniu albo uszkadzaniu urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przekazywania chronionych danych informatycznych.

Zagrożone jest ono wysoką – jak na przestępstwa komputerowe – sankcją, a mianowicie karą pozbawienia wolności od sześciu miesięcy do ośmiu lat. Związane jest to oczywiście z przedmiotem ochrony przepisów art. 269 § 1 i 2 kk, którym jest integralność oraz dostępność danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, zarówno przechowywanych na informatycznych nośnikach danych, jak i przetwarzanych w systemach informatycznych i przesyłanych między nimi. Omawiane przepisy chronią zatem szczególne dane informatyczne, a ponadto – pośrednio – obronność kraju (termin ten odnosi się w tym wypadku zarówno do bezpieczeństwa zewnętrznego, jak i wewnętrznego), bezpieczeństwo w komunikacji (w ruchu lądowym, morskim i powietrznym) oraz funkcjonowanie szeroko pojętej administracji państwowej[30].

Na marginesie należy dodać, że przepis kryminalizujący podobne – jak art. 269 § 1 i § 2 kk – zachowania i jednocześnie chroniący szeroko pojęte bezpieczeństwo (a zatem dobro prawne „zawierające" w swoim zakresie np. bezpieczeństwo w komunikacji) znajdziemy w rozdziale XX kodeksu karnego (Przestępstwa przeciwko bezpieczeństwu powszechnemu). W art. 164 § 1 pkt 4 kk – bo o nim mowa – stypizowano bowiem czyn zabroniony polegający na sprowadzeniu niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla

[30] Por. P. Kardas, *Prawnokarna ochrona…*, s. 94; A. Adamski*, Prawo karne...*, s. 76–77.

mienia w wielkich rozmiarach, w wyniku zakłócenia, uniemożliwienia lub wywarcia innego negatywnego wpływu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych.

Konstruując typ przestępstwa z art. 269 § 1 kk, ustawodawca posłużył się alternatywnymi znamionami. Pierwsza ich grupa to niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. Przedmiot ochrony stanowi w tym wypadku integralność danych należących do wskazanej w nim kategorii. Przedmiotem wykonawczym są dane informatyczne o szczególnym znaczeniu dla jednej z dziedzin wymienionych w tym przepisie. Jak zauważa J.W. Giezek, ocena, czy mają one takie znaczenie, powinna być przeprowadzona z obiektywnego punktu widzenia, gdyż nie istnieje w tym przypadku możliwość jej subiektywizacji[31]. Przez niszczenie, usuwanie należy rozumieć całkowite unicestwienie danych, natomiast przez zmianę, uszkodzenie – ich modyfikację w stopniu znacznym.

Na drugą grupę znamion, wymienionych w drugiej części przepisu art. 269 § 1 kk, składa się zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania organów administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. W tym wypadku przedmiotem ochrony jest dostępność danych o szczególnym znaczeniu dla wymienionych w przepisie wartości.

Wydaje się, że ustawodawca tworząc art. 269 § 1 kk zamierzał uczynić z niego narzędzie do zwalczania ataków o charakterze logicznym.

---

[31] J.W. Giezek, [w:] *Kodeks karny*…, red. J.W. Giezek, s. 1001.

Natomiast przed atakami o charakterze fizycznymi miałby chronić dane informatyczne przepis art. 269 § 2 kk, kryminalizujący zniszczenie albo wymianę informatycznego nośnika danych (tj. zastąpienie go innym) lub zniszczenie albo uszkadzanie urządzeń służących do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych o szczególnym znaczeniu. Skutkiem wymienionych zachowań może być zarówno fizyczne unicestwienie danych (np. w wyniku zniszczenia dysków twardych w serwerze), jak i utrudnienie lub uniemożliwienie ich przetwarzania (np. w rezultacie uszkodzenia urządzeń sieciowych).

Nie stanowi przestępstwa określonego w art. 269 § 2 kk takie zachowanie, które prowadzi do zniszczenia lub wymiany nośnika danych albo do zniszczenia lub uszkodzenia urządzenia służącego do przetwarzania, gromadzenia lub przekazywania danych, jeżeli jednocześnie sprawca nie zniszczył, nie uszkodził, nie usunął lub nie zmienił zapisu danych o szczególnym znaczeniu w rozumieniu tego przepisu, bądź nie doprowadził do zakłócenia lub uniemożliwienia automatycznego przetwarzania, gromadzenia lub przekazywania takich danych[32]. Moim zdaniem jednak – jeżeli sprawca wiedział, jakie jest przeznaczenie urządzeń będących przedmiotem jego czynu – możliwe będzie zakwalifikowanie jego zachowania jako usiłowania. Analogicznie sytuacja będzie się przedstawiać w przypadku, gdy czyn sprawcy skutkować będzie jedynie uszkodzeniem nośnika danych (a nie jego zniszczeniem). Jeżeli jednak jednocześnie będzie się wiązał z modyfikacją czy zniszczeniem szczególnych danych, może stanowić przestępstwo wymienione w § 1[33]. Podobnie będzie w przypadku

[32] Por. A. Sakowicz, [w:] *Kodeks karny…*, s. 451; W. Wróbel, D. Zając, *Komentarz do art. 269 kk*, [w:] *Kodeks karny*…, red. W. Wróbel, A. Zoll.

[33] Por. W. Wróbel, D. Zając, [w:] *Kodeks karny...*, s. 677; J. Znamierowski, *Prawnokarna ochrona funkcjonowania państwa przed sabotażem komputerowym*, „Edukacja Prawnicza" 2014, nr 4, s. 24.

ataku na urządzenia informatyczne – jego uszkodzenie powodujące zakłócenie w przekazywaniu danych będzie można zakwalifikować z art. 269 § 1 kk[34].

Nie stanowi przestępstwa sabotażu informatycznego z art. 269 § 2 kk uszkodzenie przez sprawcę samych kabli czy przewodów służących do transmisji – nie można ich uznać za urządzenia. Działania takie mogą natomiast być uznane za zakłócenie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych o szczególnym znaczeniu, czyli czyn z art. 269 § 1 kk[35].

Powyższe rozważania prowadzą według mnie do wniosku, że przepis art. 269 § 2 kk można uznać za zbędny[36].

Z uwagi na zdecydowanie wyższe znaczenie informacji chronionych przez przepis art. 269 § 1 kk w porównaniu z informacją podlegającą ochronie na podstawie art. 268 § 2 kk[37] oraz identyczność pozostałych znamion czynów kryminalizowanych przez te przepisy, przy jednoczesnej różnicy w wysokości zagrożenia karą i środkami karnymi, przestępstwo z art. 269 § 1 kk uważa się za typ kwalifikowany w stosunku do przestępstw z art. 268 § 2 kk[38]. Podobna relacja występuje moim zdaniem pomiędzy przestępstwami z art. 268a § 1

---

[34] Por. W. Wróbel, D. Zając, *Komentarz do art. 269 kk*, [w:] *Kodeks karny…,* red. W. Wróbel, A. Zoll.

[35] W. Wróbel, D. Zając, *Komentarz do art. 269 kk*, [w:] *Kodeks karny…,* red. W. Wróbel, A. Zoll.

[36] Por. F. Radoniewicz, *Odpowiedzialność karna…,* s. 325; W. Wróbel, D. Zając, *Komentarz do art. 269 kk*, [w:] *Kodeks karny…,* red. W. Wróbel, A. Zoll.

[37] Przepis ten kryminalizuje zachowanie polegające na nieuprawnionym, niszczeniu, uszkadzaniu, usuwaniu lub zmienianiu zapisu istotnej informacji na informatycznym nośniku danych oraz udaremnianie lub znaczne utrudnienie osobie uprawnionej zapoznanie się z nią w inny sposób.

[38] P. Kardas, *Prawnokarna ochrona...,* s. 96. Zob. A. Adamski*, Prawo karne...*, s. 77; M. Kalitowski, *Komentarz do art. 269 kk, pkt 3*, [w:] *Kodeks karny. Komentarz,* red. M. Filar, Warszawa 2016/Lex.

kk[39] i art. 269 § 1 kk. Przepisy te kryminalizują w rzeczywistości identyczne zachowania, będące zamachami na bezpieczeństwo danych komputerowych oraz systemów informatycznych, różniąc się jednocześnie surowością sankcji, jakie można za ich popełnienie wymierzyć. W związku z tym sabotaż informatyczny z art. 269 § 1 kk stanowi typ kwalifikowany występku z art. 268a § 1 kk ze względu na rodzaj chronionych danych i systemów informatycznych, w których są przetwarzane, a także – z tego samego powodu – przestępstwa o analogicznych do niego znamionach określonego w art. 269a kk (nieuprawnione zakłócenie w istotnym stopniu pracy systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych)[40].

Przestępstwo sabotażu informatycznego ma charakter materialny[41], z uwagi na sposób ujęcia znamion czasownikowych, które determinują wystąpienie skutku[42] - dla jego bytu konieczne jest wystąpienie skutku w postaci unicestwienia lub uszkodzenia danych określonych w przepisie art. 269 § 1 kk albo zakłócenia lub uniemożliwienia automatycznego ich przetwarzania, gromadzenia lub przekazywania bez względu na to, czy jest to efekt ataku logicznego, czy działania fizycznego.

---

[39] W przepisie tym stypizowano czyn polegający na nieuprawnionym, niszczeniu, uszkadzaniu, usuwaniu, zmienianiu lub utrudnianiu dostępu do danych informatycznych oraz zakłócaniu w istotnym stopniu lub uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych.

[40] F. Radoniewicz, *Odpowiedzialność karna…,* s. 325. Por. P. Kozłowska-Kalisz, *Komentarz do art. 269,* [w:] *Kodeks karny…,* red. M. Mozgawa.

[41] Por. P. Kozłowska-Kalisz, *Komentarz do art. 269 kk,* [w:] *Kodeks karny…,* red. M. Mozgawa; R. Hałas, [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2018, s. 1281; S. Hoc, [w:] *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2017, s. 1619.

[42] J.W. Giezek, [w:] *Kodeks karny...*, red. J.W. Giezek, s. 1001.

Strona podmiotowa obejmuje obie odmiany umyślności – zarówno zamiar bezpośredni, jak i ewentualny[43]. Sprawca musi chcieć popełnienia tego czynu lub przynajmniej godzić się, że swoim zachowaniem wypełni znamiona przestępstwa. Jednocześnie musi mieć ponadto świadomość, że dane informatyczne, na które oddziaływa, mają lub mogą mieć szczególne znaczenie dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania organów administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, albo że jego zachowanie doprowadzi lub może doprowadzić do zakłócenia lub uniemożliwienia automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. W przypadku czynów z art. 269 § 2 kk sprawca musi zdawać sobie sprawę z przeznaczenia niszczonych nośników lub urządzeń (lub przynajmniej podejrzewać, do czego służą)[44].

Podsumowując, w polskim kodeksie karnym zamachy na integralność danych informatycznych kryminalizują obecnie trzy przepisy a w zasadzie cztery). Uważam, że wskazana byłaby rezygnacja z art. 268 § 2 kk – jego rolę przejąłby art. 268a § 1 kk Trzeci z tychże przepisów - art. 269 § 1 kk – można umieścić jako typ kwalifikowany czynu z art. 268a § 1 kk. Natomiast czwarty (art. 269 § 2 kk) - jak wykazano wyżej - jest zbędny gdyż jego funkcję mógłby spełniać art. 269 § 1 kk. Uczyniłoby to regulację kodeksową w zakresie przepisów typizujących przestępstwa komputerowe bardziej spójną i przejrzystą.

---

[43] Zdaniem A. Marka czynności sprawcze muszą być objęte zamiarem bezpośrednim, natomiast szczególne znaczenie danych informatycznych może być objęte również zamiarem ewentualnym. Zob. A. Marek, *Kodeks karny…*, s. 575.

[44] A. Adamski, *Prawo karne...*, s. 80.

Bibliografia

1. Adamski A., *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" 2005.
2. Adamski A., *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę,* [w:] *Internet. Ochrona wolności, własności i bezpieczeństwa*, red. G. Szpor, Warszawa 2011.
3. Adamski A., *Prawo karne komputerowe*, Warszawa 2000.
4. Brenner S.W., *Cybercrime and the Law. Challenges. Issues, and Outcomes*, Boston 2012.
5. Czarny-Drożdżejko E., Ochrona informacji i programów komputerowych w nowym kodeksie karnym, [w:] Prawo autorskie a postęp techniczny, red. J. Barta, R. Markiewicz, Kraków 1999.
6. Fischer B., *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000
7. Giezek J.W., [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J.W. Giezek, Warszawa 2014.
8. Górniok O., [w:] O. Górniok i in., *Kodeks karny. Komentarz*, t. 2, Gdańsk 2005
9. Hałas R., [w:] *Kodeks karny. Komentarz*, red. A. Grześkowiak, K. Wiak, Warszawa 2018.
10. Hoc S., [w:] *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2017.
11. Kalitowski M., *Komentarz do art. 269 kk, pkt 3,* [w:] *Kodeks karny. Komentarz,* red. M. Filar, Warszawa 2016/Lex.
12. Kardas P., *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, CzPKiNP 2000, nr 1.
13. Kłączyńska N., [w:] *Kodeks karny. Część szczególna. Komentarz*, red. J.W. Giezek, Warszawa 2014
14. Kozłowska-Kalisz P., *Komentarz do art. 268 kk*, [w:] M. Mozgawa (red.), *Kodeks karny. Praktyczny komentarz*, Warszawa 2015.

15. Kozłowska-Kalisz P., *Komentarz do art. 268a kk*, [w:] M. Mozgawa (red.), *Kodeks karny. Praktyczny komentarz*, Warszawa 2015.
16. Kozłowska-Kalisz P., *Komentarz do art. 269 kk*, [w:] M. Mozgawa (red.), *Kodeks karny. Praktyczny komentarz*, Warszawa 2015.
17. Kunicka-Michalska B., [w:] *Kodeks karny. Część szczególna. Komentarz do artykułów 222–316*, t. II, red. A. Wąsek, R. Zawłocki, Warszawa 2010
18. Kunicka-Michalska B., [w:] L. Gardocki (red.) *System Prawa karnego. T. 8 Przestępstwa przeciwko państwu i dobrom zbiorowym,* Warszawa 2018.
19. Marek A., *Kodeks karny. Komentarz*, Warszawa 2010.
20. Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
21. Russell R. (red.), *Hack Proofing Your Network*. Edycja Polska, Gliwice 2002.
22. Sakowicz A., [w:] *Kodeks karny. Część szczególna*, red. M. Królikowski, R. Zawłocki, t. II, *Komentarz do artykułów 222–316*, Warszawa 2013.
23. Shinder D.L., Tittel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Gliwice 2004.
24. Siwicki M., Cyberprzestępczość, Warszawa 2013.
25. Warhole A., *Atak z Internetu*, Warszawa 1999.
26. Wróbel W., Zając D., *Komentarz do art. 268 kk,* [w:] W. Wróbel (red.), A. Zoll (red.), *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d*, Warszawa 2017.
27. Wróbel W., Zając D., *Komentarz do art. 268a kk, pkt 1*, [w:] W. Wróbel (red.), A. Zoll (red.), *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d*, Warszawa 2017.
28. Wróbel W., Zając D., *Komentarz do art. 269 kk,* [w:] W. Wróbel (red.), A. Zoll (red.), *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d*, Warszawa 2017.

Abstract

CRIMES AGAINST COMPUTER DATA INTEGRITY - SELECTED CRIMINAL AND TECHNICAL ASPECTS

Summary: The purpose of this chapter is to present the technical aspects of cybercrimes against the integrity of computer data and the criminal aspects of this issue. Its first part is devoted to the ways of violating data integrity ("hacking techniques" and "hacking programs"), the second part - to their legal qualification. The author, while critically analyzing the provisions of the penal code, also presents his proposals for changes

Keywords: computer virus, ICT network, internet, malware, malicious software, hacker.

ROZDZIAŁ 9

Jeszcze o statusie i odpowiedzialności biegłego

dr inż. Maciej SZMIT[1]

STRESZCZENIE: Rozdział poświęcony jest zagadnieniu roli biegłego sądowego, w szczególności wybranym przepisom regulującym jego status oraz wybranym rodzajom odpowiedzialności: odpowiedzialności cywilnej za skutki wyroku wydanego w oparciu o opinię kłamliwą oraz odpowiedzialności karnej za wydanie opinii fałszywej.

SŁOWA KLUCZOWE: kryminalistyka, opinia fałszywa, biegli sądowi.

Wstęp

Pojęcia biegłego sądowego nie definiuje i nie definiowała w przeszłości żadna z polskich ustaw dopuszczających możliwość powoływania biegłych. Zazwyczaj przyjmuje się, zgodnie z wykładnią językową, że biegły jest osobą posiadającą wiedzę fachową i doświadczenie w jakiejś dziedzinie. Większość teoretyków prawa uznaje, że biegły – oprócz odpowiedniej wiedzy fachowej – powinien posiadać odpowiednią praktykę zawodową. W polskim prawie brakuje – postulowanej od co najmniej kilkunastu lat – ustawy o biegłych, co powoduje, że przepisy o nich są rozproszone w licznych aktach prawnych, zatem konieczne jest rozważanie zapisów poszczególnych przepisów i ich implikacji.

[1] Uniwersytet Łódzki, maciej.szmit@uni.lodz.pl; ORCID: 0000-0002-6115-9213.

Maciej SZMIT

Kim (nie) jest biegły – próba wyjaśnienia pojęcia

Biorąc pod uwagę wzrost złożoności systemu prawnego, styl stanowienia prawa, charakteryzujący się skłonnością do nadregulacji w połączeniu z wybitną (ilościowo) kreatywnością ustawodawcy[2], który obrazowo w tekstach popularnych[3] nazywany bywa „biegunką legislacyjną" oraz wzrost znaczenia opinii biegłych (wynikający z rosnącej złożoności zarówno rozwiązań technicznych jak i społeczno-gospodarczych) mamy do czynienia z lawinowym przyrostem liczby przepisów, często między sobą nie do końca spójnych i nie poddających się łatwiej interpretacji. W książce [1], wydanej w roku 2004, wymieniono explicite 22 pozakodeksowe akty prawne regulujące różne aspekty opiniowania sądowego, w publikacji [2], wydanej 16 lat później, omówiono przepisy dotyczące biegłych zawarte w 60 ustawach oraz 22 rozporządzeniach. Kwerenda hasła „Biegli sądowi" w bazie Legalis we wrześniu 2021 r, zwraca 72 ustawy (pomijając te, które mają w tytule „przepisy wprowadzające" albo „o zmianie ustawy"), choć w rzeczywistości liczba ta może być nieco mniejsza[4]. Jednocześnie status biegłego, który jest bardzo specyficznym uczestnikiem postępowania procesowego, określać przecież powinien szereg niezbędnych do jego funkcjonowania zasad, począwszy od zakresu możliwych do wykonania przez niego czynności, poprzez uwarunkowania formalne (np. warunki wyłączenia biegłego w tym formalne kryteria bezstronności, wysokość wynagrodzenia itd.), uwarunkowania metodologiczne (np. dostęp do materiałów postępowania,

---

[2] Według [3] w 2021 r. uchwalono w Polsce 24620 stron ustaw, rozporządzeń i umów międzynarodowych.

[3] A czasami nawet naukowych – zob. np. [4].

[4] Może budzić wątpliwości czy posiada treść normatywną np. – jak się zdaje ciągle formalnie obowiązująca – ustawa [5], zawierająca zresztą przepisy o biegłych (precyzująca m.in. kwestie kosztów wezwania biegłych przez sędziów pokoju czy właściwości sędziego śledczego do karania biegłych za niestawiennictwo).

swoboda formułowania pytań do uczestników postępowania, dopuszczalność metod i narzędzi badawczych) aż do niebagatelnej kwestii odpowiedzialności za wydaną opinię. O ile w opiniowaniu w sprawach karnych kwestie te są – przynajmniej w pewnym stopniu – klarowne, o tyle już inne przepisy takiej klarowności nie zapewniają.

Dla przykładu: ustawa – Prawo zamówień publicznych [6] mówi o biegłych:

- w art. 55 ust. 4 oraz art. 73 ust. 1 (gdzie tym słowem oznacza biegłego komisji przetargowej powołanego przez kierownika zamawiającego);
- w art. 529 ust. 2, art. 538 ust. 1, art. 539 oraz art. 569 ust. 2, w których mowa jest o biegłych Krajowej Izby Odwoławczej (KIO);
- w art. 605 ust. 2 i 3, gdzie mowa o biegłych Urzędu Zamówień Publicznych (UZP).

Każdy z tych trzech rodzajów biegłych powoływany jest przez kogo innego i działa w oparciu o inne zasady. W szczególności biegły komisji przetargowej pracuje za nieokreślone ustawowo wynagrodzenie, podczas, gdy wynagrodzenie biegłych KIO i UZP reguluje ustawa, biegły komisji — podlega wyłączeniu zgodnie z przepisami art. 56 Prawa zamówień publicznych, podczas gdy nie ma takiego uregulowania wobec biegłych KIO ani UZP, wreszcie ustawa umożliwia KIO powołanie biegłego z listy stałych biegłych sądowych albo spoza niej[5], nie precyzuje jednak jakich biegłych (z listy czy również spoza niej) może powoływać komisja czy UZP.

Inny akt prawny – Kodeks morski [7] operuje, obok pojęcia biegłego

[5] Który to zapis jest o tyle nieprecyzyjny, że odnosi się do wszystkich osób bądź organizacji na świecie, dowolna bowiem osoba fizyczna bądź prawna albo jest wpisana na jakąś listę biegłych albo na żadną nie jest wpisana.

(w art. 142) pojęciem biegłego-komisarza o kompetencjach znacznie szerszych niż kompetencje biegłego (np. art. 319 § 3 oraz § 4). Może on prowadzić korespondencję z uczestnikami postępowania, w tym wzywać ich do złożenia wyjaśnień i oświadczeń, wnioskować o przeprowadzenie przez sąd postępowania dowodowego, sąd może też powierzyć mu zarządzanie kwotami, z których ustanowiono fundusz ograniczenia odpowiedzialności.

W jeszcze innej ustawie – Karcie Nauczyciela [8] ustawodawca – poza dopuszczeniem możliwości zasięgania opinii biegłych (art. 85g) uznał za wskazane (w art. 85q) uregulowanie kwestii wynagrodzenia biegłego w postępowaniach: wyjaśniającym i dyscyplinarnym[6]. Pozostałe kwestie związane z opiniowaniem w takich postępowaniach są w tym akcie prawnym nieuregulowane.

Obok biegłych sądowych w polskich przepisach istnieje szereg ról związanych z wydawaniem opinii[7]: biegli rewidenci, biegli skarbowi, biegli w postępowaniu administracyjnym, specjaliści w postępowaniu karnym, audytorzy, rzeczoznawcy majątkowi, rzeczoznawcy budowlani, opiniodawcze zespoły sądowych specjalistów[8] czy konsultanci wojewódzcy w zakresie medycyny. Oczywiście byłoby nierozsądne postulować, żeby wszystkie te – tak bardzo różniące się role – uregulować jednym aktem prawnym, wydaje się jednak, że obecnie istniejące rozdrobnienie świadczy

---

[6] A w zasadzie brak takowego wynagrodzenia, w myśl przepisu bowiem biegłym przysługuje równowartość zarobku utraconego w związku z udziałem w rozprawie oraz zwrot kosztów przejazdu zgodnie z przepisami w sprawie należności przysługujących pracownikowi zatrudnionemu w państwowej lub samorządowej jednostce sfery budżetowej z tytułu podróży służbowej, na obszarze kraju.

[7] Pomijając nawet role związane z wydawaniem orzeczeń, czyli np. jednostki orzecznicze uprawnione do orzekania o chorobach zawodowych czy lekarzy sądowych.

[8] Zob. [9].

o braku systemowego podejścia do zagadnienia opiniowania[9] w ogóle.

Odpowiedzialność cywilna biegłego sądowego za wydanie opinii kłamliwej

Biegły sądowy za swoje czynności (bądź za odmowę ich dokonania) ponosi odpowiedzialność, a w zasadzie kilka jej rodzajów: karną, cywilną i quasi-dyscyplinarną (np. może zostać skreślony z listy biegłych). O ile w literaturze i orzecznictwie panowała zgodność odnośnie do możliwości odpowiedzialności karnej biegłego (biegły może przecież popełnić szereg czynów wyczerpujących ustawowe znamiona czynów przestępnych, np. tak sformułować opinię, żeby była ona znieważająca dla którejś ze stron postępowania czy zamieścić w niej celowo fałszywe informacje odnośnie do twierdzeń dyscypliny, którą reprezentuje), o tyle możliwość odpowiedzialności cywilnej biegłego była niejednokrotnie podawana w wątpliwość w literaturze przedmiotu. Mocnym głosem w tej sprawie stał się wyrok Sądu Apelacyjnego w Katowicach z 29 listopada 2019 r. (sygn. akt V ACa 266/18[10]), który uznał – w postępowaniu cywilnym – biegłą winną popełniania przestępstwa wydania opinii i zasądził od pozwanej biegłej na rzecz powoda dochodzoną kwotę[11]. Wyrok ten doczekał się szerokich komentarzy. W szczególności w krytycznej glosie [12] słusznie podniesiony zostały dwa argumenty (poniżej przytoczone in extenso):

---

[9] Do określenia zagadnień związanych z opiniowaniem używa się czasami terminu „ekspertologia", choć nie jest to najlepiej brzmiące określenie.

[10] Legalis.

[11] Omówienie wyroku jak również ważniejszych argumentów w dotychczasowej dyskusji dotyczącej odpowiedzialności cywilnej biegłego, zostało przedstawione w artykule [11].

- „Biegły (…) nie wchodzi w relacje prawne z osobami trzecimi; jedynym podmiotem, z którym biegły pozostaje w relacji prawnej, jest organ procesowy (…). Skutki prawne (w tym dla stron) rodzi nie sama opinia (…), ale decyzja organu procesowego (...).
- Wydanie kłamliwej opinii jest czynem penalizowanym w art. 233 § 1 k.k., pomieszczonym w rozdziale XXX (>>Przestępstwa przeciwko wymiarowi sprawiedliwości<<). Dobrem chronionym jest wiarygodność orzeczeń, a nie interesy stron procesowych i właśnie w wiarygodność orzeczeń, a nie w interesy stron/uczestników postępowania, czynami swymi uderzają kłamliwi biegli. Podobny problem rozstrzygała Izba Karna Sądu Najwyższego w odniesieniu do kwestii cywilnej odpowiedzialności kłamliwych świadków (…) Postanowieniem z 1.04.2005 r. [SN] uznał, że strony lub uczestnicy postępowania nie mogą skutecznie pozywać kłamliwego świadka a za podstawę tego stanowiska Sąd Najwyższy przyjął właśnie rezultaty tu opisywanej wykładni systemowej”[12].

W konsekwencji cały wyrok nazywa ekscesem (odchyleniem) orzeczniczym postulując, że „powinien być rychło zdezawuowany, by nie stał się precedensem początkującym linię orzeczniczą”[13]. Rzeczywiście wspomniany wyrok zdążył być już cytowany w innym wyroku[14], zanim – po kolejnej (trzeciej już w toku tej sprawy) skardze kasacyjnej pozwanej – SN go uchylił i przekazał sprawę do ponownego rozpoznania sądowi II instancji. Sąd Najwyższy podkreślił, że wprawdzie podstawa odpowiedzialności biegłego została już przesądzona w poprzednim orzeczeniu SN, ale ustalone okoliczności nie dają podstawy do przyjęcia, iż zostały wypełnione znamiona przestępstwa określonego w art. 233 § 4 KK w postaci zamiaru ewentualnego,

[12] Zob. [12].
[13] Ibidem.
[14] Wyrok Sądu Okręgowego w Białymstoku z dnia 25 września 2020 r., II Ca 1172/19, Legalis.

nie można bowiem przyjmować domniemania dotyczącego odpowiedzialności karnej, zaś ocena, że spełnione zostały znamiona przedmiotowe i podmiotowe przestępstwa, musi być oparta na materiale dowodowym. Chociaż biegła przy wydawaniu opinii popełniła szereg błędów, to w opinii zwróciła uwagę na braki w posiadanych informacjach dotyczących sprawy, co nie daje podstaw do przypisania odpowiedzialności za występki w takim zakresie, w jakim orzekł sąd II instancji.

Jako ciekawostkę można przytoczyć fakt zabrania publicznie głosu przez samą pozwaną (po wyroku SA), w która w artykule [13] tak odniosła się do wyroku SA: „(…) Aktualnie, po ponad 8 latach postępowań na wszystkich szczeblach orzekania (…), które albo orzekały o braku mojej winy albo o przedawnieniu, zostałam uznana winną celowego sporządzenia >>fałszywej<< opinii (…) Największym zaskoczeniem jest to, że Sąd cywilny po prawie 18 latach od zdarzenia i ponad 7 latach postępowania sądowego, nie widząc mnie na oczy, orzekł też o moich predyspozycjach psychicznych na przełomie 2001/2002 r. do działania z winy umyślnej z zamiarem ewentualnym czyli uznał, że świadomie popełniłam przestępstwo (…). Należy podkreślić, że stanowisko wyrażone przez Sąd Apelacyjny w Katowicach prowadzi do uznania, że (…) to opinia biegłego rozstrzyga o treści wyroku w sprawie a nawet o licytacji nieruchomości przegranej strony (w toku postępowania egzekucyjnego) w innej sprawie o której biegły nie ma wiedzy ani nie jest stroną (...) pomimo umorzenia postępowania karnego na etapie postępowania przygotowawczego (wobec braku znamion przestępstwa) możliwe jest przyjęcie w postępowaniu cywilnym, że dany czyn – mimo wszystko – stanowił przestępstwo (…)”.

Rzeczywiście sytuacja, w której w postępowaniu cywilnym sąd uznaje kogoś za winnego popełnienia czynu przestępnego wydaje się być co najmniej bardzo niepokojąca (choćby biorąc pod uwagę tak elementarne wartości jak prawo do obrony). Niezależnie jednak od niedociągnięć tego konkretnego postępowania należy również zgodzić się z tezą, że biegły nie

wchodzi w relacje prawne z osobami trzecimi, a jedynie z organem procesowym, a skutki prawne dla stron rodzi nie jego opinia, ale decyzja organu procesowego, stąd też odpowiedzialność cywilna biegłego nie powinna obejmować merytorycznej strony jego opinii[15].

Odpowiedzialność karna biegłego sądowego za wydanie opinii fałszywej

Odpowiedzialność karna biegłego za wydanie opinii fałszywej kształtowana była przez kolejne zmiany przepisów, z których ostatnią była nowelizacja art. 233 § 4a KK wprowadzająca penalizację nieumyślnego przedstawienia opinii fałszywej. Ten model rozwoju litery prawa doprowadził do powstania sytuacji mocno ekstraordynaryjnej, grożącej biegłym zaiste drakońskimi karami[16]. W szczególności kategoria nieumyślnego

---

[15] Warto jednak na marginesie zauważyć, że nie jest to do końca oczywiste w przypadku odpowiedzialności karnej. Wypowiedział się na ten temat Sąd Najwyższy w postanowieniu z dnia 23 kwietnia 2002 r. (I KZP 10/02, Lex nr 53077): „(...) dopuszczalne jest przyznanie legitymacji pokrzywdzonego podmiotowi występującemu jako strona w postępowaniu określonym w § 1 art. 233 KK, tzn. w postępowaniu sądowym lub w innym postępowaniu prowadzonym na podstawie ustawy również wtedy, gdy przedstawienie fałszywej opinii >>bezpośrednio<< dobro prawne tego podmiotu narusza lub mu zagraża, choćby nie naruszało to równocześnie innej normy karnej". Czym innym jest jednak odpowiedzialność karna za czyn przestępny (wyłączenie jej prowadziłoby do swoistego immunitetu biegłego, który mógłby bezkarnie znieslawiać strony w swojej opinii), a czym innym potencjalna odpowiedzialność cywilna biegłego za skutki wyroku wydanego przez sąd, który przecież ma obowiązek oceny dowodu, jakim jest opinia biegłego.

[16] W artykule [10] Autor przytacza następujący przykład: „(…) Biegły, który po raz kolejny, >>uporczywie podtrzymuje opinię niepełną<<, odmawiając przy tym uzupełnienia nieistniejących jego zdaniem nieścisłości czy nieuwzględniający materiału dowodowego, który w jego ocenie nie posiada wartości poznawczej, może być najpierw ukarany karą finansową (w oparciu o art. 285 § 1a w zw. z § 1), na-

przedstawienia opinii fałszywej doczekała się szeregu głosów krytycznych w literaturze przedmiotu (zob. np. [13], [14]), trudno bowiem sobie nawet wyobrazić zawinione nieumyślne przedstawienie opinii fałszywej. Formami winy nieumyślnej są: lekkomyślność (sprawca, świadomie łamiąc zasady ostrożności przewiduje możliwość popełnienia czynu zabronionego, ale przypuszcza, że popełnienia tego czynu uniknie) i niedbalstwo (sprawca popełnia czyn zabroniony na skutek niezachowania wymaganych reguł ostrożności, gdy nie przewidywał możliwości jego popełnienia, choć mógł ją przewidzieć). Można wprawdzie wyobrazić sobie sytuację, w której biegły przygotowuje opinie alternatywne i na skutek jakiegoś skrajnego roztargnienia przedstawia tylko jedną z nich, niemniej jest to sytuacja mocno teoretyczna[17]. Bardziej realna jest sytuacja, w której biegły w niestaranny sposób prowadzi badania w ramach przygotowania opinii, doprowadzając np. do zniszczenia czy kontaminacji materiału dowodowego (w szczególności odnośnie do informatyki sądowej można przywołać, niestety ciągle zdarzające się, niefachowe badania prowadzące do niezamierzonej utraty czy modyfikacji danych ulotnych, w tym metadanych), niemniej problemem jest

stępnie aresztowany na okres do 30 dni (w oparciu o art. 287 § 2 k.p.k.), jego wynagrodzenie może być zmniejszone (w oparciu o art. 618f § 4b), a następnie może być pociągnięty do odpowiedzialności karnej na podstawie art. 233 § 4a k.k. i skazany na karę pozbawienia wolności do lat 3. Niedorzeczność takiej konstrukcji zdaje się wręcz razić, co nie zmienia faktu, że jest ona, jak się zdaje, możliwa pod rządami aktualnie obowiązujących przepisów(…)".

[17] W artykule [14] przedstawiono analizę prawnoporównawczą: „W wielu państwach odpowiedzialność karna biegłego, rzeczoznawcy i tłumacza jest uregulowana w tym samym przepisie, co odpowiedzialność świadka za składanie fałszywych zeznań (…) W niektórych państwach zostało podkreślone znamię strony podmiotowej („świadomie", „wiedząc", „złośliwie") (…). Wiele państw ma typy kwalifikowane analizowanego przestępstwa. Znamieniem kwalifikującym bardzo często jest spowodowanie pewnego skutku (...) Typ nieumyślny znany jest niewielu porządkom prawnym (Bułgaria, Finlandia, Niemcy, Węgry, Szwecja)".

tu nie tyle wytworzenie opinii fałszywej, co niepotrzebna utrata możliwości powtórzenia (ang. *repeatability*) badania (co zresztą pociąga za sobą niemożliwość zweryfikowania materialnej prawdziwości wydanej opinii). Może oczywiście zdarzyć się również niezamierzona kontaminacja (zanieczyszczenie) materiału dowodowego i wyciągnięcie wniosków w oparciu o materiał tak zanieczyszczony, albo niewłaściwe określenie stanowczości wniosków przez biegłego, powstaje jednak pytanie, czy tego rodzaju błędy powinny być ścigane w reżimie odpowiedzialności karnej. W ludzkiej działalności, szczególnie intelektualnej, nie sposób ustrzec się błędów i pomyłek. Czasami trudno zresztą uznać, że np. wybór badania niszczącego w miejsce nieniszczącego (albo sposobu obarczonego większym ryzykiem w miejsce mniej ryzykownego, ale znacznie droższego czy dłużej trwającego[18]) był stricto sensu błędem czy lekkomyślnością: wybór konkretnej metody badawczej jest kwestią, która powinna być pozostawiona autonomii biegłego. Najlepszą znaną dotychczas metodą radzenia sobie z takimi sytuacjami jest stosowanie podejścia iteracyjnego: wieloinstanacyjność postępowania sądowego, wieloetapowość procesu recenzowania publikacji naukowych, możliwość walidacji wadliwych opinii w drodze ich uzupełnienia przez tego samego bądź innego biegłego, możliwość konfrontacji biegłych czy wydawania metaopinii (zob. art. 198 § 1 KPK) itd. Biegły, który będzie się kierował w badaniach minimalizacją ryzyka możliwości popełnienia niezamierzonej pomyłki, będzie miał skłonność do wykonywania nadmiarowych badań[19] czy nieuzasadnionego

[18] W informatyce śledczej np. stosowanie metod *triage* w miejsce pełnego badania całości dostępnych danych.

[19] Warto przypomnieć, że zazwyczaj w obrębie konkretnej metody badawczej, nie ma możliwości jednoczesnej minimalizacji prawdopodobieństwa popełnienia błędów pierwszego i drugiego rodzaju: albo zwiększa się czułość badania albo jego

zaniżania kategoryczności opinii.

Podsumowanie

W ostatnich latach daje się zauważyć znaczący wzrost restrykcyjności przepisów odnośnie do odpowiedzialności biegłych. Nie idzie za tym – niestety – uregulowanie ich statusu ani uporządkowanie system prawnego. Multiplikacja odpowiedzialności biegłych oraz zaostrzanie potencjalnych kar idzie w dokładnie przeciwnym kierunku. Groźby – choćby stosowanego jako narzędzi obstrukcji procesowej – nękania biegłego przy wykorzystaniu coraz szerszego wachlarza możliwości prawnych czy ponoszenia nieproporcjonalnie wysokich konsekwencji drobnych pomyłek, już powodują trudności ze znalezieniem biegłych. W chwili obecnej mniej-więcej połowa sądów okręgowych na swoich stronach ma zamieszczone informacje o poszukiwaniu biegłych (obecnie głównie lekarzy). Można obawiać się, że bez gruntownej, systemowej zmiany podejścia do instytucji biegłego sądowego negatywne zjawiska w opiniowaniu będą się jedynie nasilać.

Bibliografia

1. Balcerowicz L., *Kryzys a gospodarka polska*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny", rok LXXII, Nr 2/2010 s. 31-40.
2. Barometr Prawa Grant Thornton, https://barometrprawa.pl/.
3. Budyn-Kulik M., *Kilka uwag o przestępstwie z art. 233 k.k. (składanie fałszywych zeznań) po nowelizacji z 11 marca 2016 r.*, „Annales Universitat Mariae Curie – Skłodowska Lublin – Polonia" Vol. LXIII, 1/2016, DOI: 10.17951/g.2016.63.1.23.

swoistość, test nadmiernie czuły daje dużo błędów fałszywej klasyfikacji, test nadmiernie specyficzny daje błędy fałszywego odrzucenia.

4. Figa-Gieruszyńska K. (red.), *Biegły w postępowaniu sadowym cywilnym i karnym*. Komentarz praktyczny, orzecznictw, wzory pism, procesowych, wydanie 2, C.H. Beck Warszawa 2020.
5. Kegel A., Kegel Z., *Przepisy o biegłych sądowych, tłumaczach i specjalistach. Komentarz*, Zakamycze, Kraków 2004.
6. Kuczera I., *Biegły sądowy*, „e-czasopismo Nieruchomości", http://www.srm.com.pl/kwartalnik-art,biegly-sadowy,75 (2020-08-05)
7. Nowak M.: Wątpliwości związane z odpowiedzialnością prawną biegłego sądowego w świetle znowelizowanego art. 233 § 4a KK, „Zeszyty Prawnicze" Nr 17(2)/2017, s. 76–102.
8. Szmit M., *O pewnym nowym przepisie i jednym precedensowym wyroku*, „Rocznik Bezpieczeństwa Morskiego" (1898-3189), Przestępczość Teleinformatyczna 2020, Gdynia 2021, s. 195-208.
9. Ustawa z dnia 1 grudnia 1961 r. – Kodeks morski, t. jedn.: Dz.U. z 2018 r. poz. 2175 ze zm.
10. Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych, t. jedn.: Dz.U. z 2021 r. poz. 1129 ze zm.
11. Ustawa z dnia 25 lutego 1921 r. w przedmiocie zmian w ustawodawstwie karnem, obowiązującem w b. zaborze rosyjskim, Dz.U. Nr 30 z 1921 r., poz. 169 ze zm.
12. Ustawa z dnia 26 stycznia 1982 r. – Karta Nauczyciela, t. jedn.: Dz.U. z 2021 r. poz. 1762 ze zm.
13. Ustawa z dnia 5 sierpnia 2015 r. o opiniodawczych zespołach sądowych specjalistów, t. jedn.: Dz.U. z 2018 r. poz. 708 ze zm.
14. Widła T., *Odpowiedzialność biegłego za wydanie nieprawidłowej opinii – glosa do wyroku Sądu Apelacyjnego w Katowicach z 29.11.2019 r.*, V ACa 266/18, „Glosa" Nr 2/2020 s. 128-134.

Abstract

MORE ABOUT THE STATUS AND RESPONSIBILITY OF THE LEGAL EXPERT

Summary: The chapter is devoted to the role of a court expert, especially to selected acts regulating his status and selected types of liability: civil liability for the consequences of a judgment issued on the basis of a deceitful expertise and criminal liability for issuing a false court expert opinion.

Keywords: forensics, false opinion, legal experts.

Rozdział 10

Oddziaływanie informacyjne i dyplomatyczne Federacji rosyjskiej w czasie pandemii covid-19. Studium przypadku na przykładzie wykorzystania rosyjskiej szczepionki sputnik V jako argumentu w walce informacyjnej

Tomasz ZAWADZKI, Kornel KOWIESKI, Anna ROŻEJ[1]

STRESZCZENIE: Rozdział przedstawia i opisuje metody i techniki jakimi posługuje się Federacja Rosyjska przy prowadzeniu działań informacyjnych względem Zachodu – wraz z wykorzystaniem social mediów. Autorzy podjęli również próbę określenia i analizy celów FR w oddziaływaniu informacyjnym i realizacji własnych celów politycznych, a szczepionka Sputnik V była jednym z kluczowych elementów, jakimi FR dysponowała i który eksploatowała, aby osiągnąć własne założenia. W ostatniej części publikacji autorzy przedstawili metodologię opracowywania analiz na podstawie działań informacyjnych w social mediach na przykładzie szczepionki Sputnik V oraz podjął próbę odpowiedzi na pytania dotyczące zasadności i czasu reakcji na wrogie oddziaływanie informacyjne ze strony Rosji.

SŁOWA KLUCZOWE: walka informacyjna, Sputnik V, oddziaływanie informacyjne, Covid-19, Rosja.

[1] Inseqr sp. z o.o., t.zawadzki@inseqr.pl.

Tomasz ZAWADZKI, Kornel KOWIESKI, Anna ROŻEJ

Wstęp

Rok 2020 był rokiem niespotykanym w najnowszej historii człowieka, ponieważ to właśnie wówczas wybuchła pandemia COVID-19, dzięki czemu można było doskonale zaobserwować, jak mocno zglobalizowany jest współczesny świat. Pomimo podjęcia stosunkowo szybkich działań przez państwa nie udało się, zatrzymać rozprzestrzeniania się wirusa Sars-Cov-2, który pojawił się na wszystkich kontynentach na początku roku 2020, a potrzebował na to zaledwie kilku miesięcy, aby być obecnym w najdalszych zakątkach świata. Istniejące procedury ochronne państw, a przede wszystkim procedury organizacji międzynarodowych odpowiedzialnych za światowe zdrowie – WHO, okazały się niewystarczające. Rosnący szybko brak zaufania do organizacji międzynarodowych i współpracy międzynarodowej poskutkował tym, że wiele krajów – w tym Zachodu, które co najmniej od czasów Zimnej Wojny podejmowały decyzje w sposób sojuszniczy, a nierzadko kolegialny w sprawach kluczowej wagi, w sytuacji wystąpienia nagłego i gwałtownego zagrożenia zaczęły podejmować decyzje własne i jednostronne, a co najwyżej bilateralnie – nawet wewnątrz UE.

Pandemia doprowadziła do przełomu, który sprawił, iż państwa zaczęły zmieniać swój sposób działań, co doprowadziło do zmian w obrębie poszczególnych systemów państwowych, jak i międzynarodowych. Zarówno w polityce wewnętrznej i zewnętrznej można zauważyć, że zmieniona została tendencja zachowań elementów systemu (jednostek, społeczeństw, państw narodowych, organizacji ponadnarodowych). Kryzys wywołany pandemią COVID-19 doprowadził do sytuacji, że dotychczas współpracujące państwa zaczęły ze sobą rywalizować, m.in. na rynku materiałów medycznych, przebijając swoje oferty, prowadząc działania oparte o metody wywiadowcze, sabotażowe czy nawet nieetyczne akcje związane z rekwirowaniem materiałów strategicznych do walki z pandemią. Konieczność gwałtownych zmian w prowadzeniu polityk zdrowotnych poszczególnych państw, doprowadziła zatem

do przemian w istniejącym systemie międzynarodowym, co przełożyło się zarówno na relacje między państwami, jak i stan ich gospodarek, rynki pracy, możliwości podróżowania, dotychczasowe relacje międzyludzkie, a w konsekwencji na społeczeństwa.

Powyższe zarysowanie problemów, jakie napotkały na swojej drodze państwa, aby zminimalizować skutki zderzenia z nowym i nieznanym wirusem doskonale wykorzystała FR w swojej walce o wpływy i realizację celów politycznych. Niniejsza publikacja ma na celu dokonanie analizy wpływu szczepionki Sputnik V oraz podjętych działań informacyjne w social mediach wraz z określeniem odpowiedniej metodologii oraz wpływ dyplomacji szczepionkowej dot. Sputnik V na Zachód oraz analiza bilansu stopnia realizacji tych celów przez Rosję.

Sputnik V – pierwsza szczepionka na Covid-19 na świecie?

W sierpniu 2020 r. Prezydent Rosji – Władimir Putin, zaskoczył świat, ogłaszając, że FR ukończyła pracę, jako pierwszy kraj na świecie nad szczepionką przeciwko wirusowi Sars-Cov-2. Ogłoszenie Wladimira Putina odbyło się przed rozpoczęciem III fazy badań klinicznych nad szczepionką, czyli tej związanej z bezpieczeństwem podawania preparatu medycznego dla szerokiej populacji.[2]

Sputnik V – taką nazwę nosi szczepionka, jest szczepionką w całości wynalezioną i wyprodukowaną w Rosji, a nazwa nawiązuje bezpośrednio do wyścigu kosmicznego prowadzonego pomiędzy USA a ZSRR w latach ’50 XX w. W marcu 2020 r., gdy WHO ogłosiło, że COVID-19 jest chorobą, która

[2] M.R. Gordon, D. Volz, Russian Disinformation Campaign Aims to Undermine Confidence in Pfizer, Other Covid-19 Vaccines, U.S. Officials Say, The Wall Street Journal, 7 March 2021, www.wsj.com [dostęp: grudzień 2021].

stała się pandemią na skalę światową, Narodowe Centrum Epidemiologiczne i Mikrobiologii Gamelaya już pracowało nad prototypem szczepionki, co było finansowane bezpośrednio z „Rosyjskiego Funduszu Bogactwa”[3].

Rosyjska szczepionka jest oparta na powszechnie występującym wirusie grypy – adenowirusie i opiera się na tym, że podawane w dwóch dawkach są adenowirusy rAd26 i rAd25, które nieznacznie różnią się między sobą, dzięki czemu organizm wytwarzając odporność nie uodparnia się na drugą dawkę szczepionki i nie neutralizuje jej zaraz po podaniu. Oczywiście adenawirusy, które są budulcem szczepionki zawierają w swojej budowie białko kolca Sars-Cov-2, dzięki czemu organizm jest w stanie wytworzyć odporność na wirus powodujący chorobę COVID-19.

Bezpieczeństwo i efektywność szczepionki Sputnik V

Faza badań klinicznych nr I oraz nr II została przeprowadzona na 76 osobach jako grupie badawczej, która została poddana szczepieniu Sputnikiem V, po czym wyniki badań zostały opublikowane w czasopiśmie Lancet we wrześniu 2020 r. – według przedstawionych tam badań, wszyscy uczestnicy badania wytworzyli przeciwciała wobec wirusa Sars-Cov-2. Nie zanotowano również żadnych poważnych odczynów poszczepiennych, a większość z nich była łagodna, np. wywołująca ból ramienia w miejscu podania szczepionki. Należy również podkreślić, że przebadana wówczas grupa badawcza nie była dobrana według standardowej metodologii badań, tj. nie uwzględniono, grupy badawczej, która otrzymałaby placebo, czy nie była w żaden sposób zróżnicowana pod ściśle określonymi względami, np. ze względu na wiek, stan zdrowia itd.

[3] W. Konończuk, Najlepszy Najlepszy Sojusznik Rosji, Kondycja i Perspektywy Rosyjskiego Sektora Naftowego, OSW 2012. [dostęp: grudzień 2021].

Wyniki badań fazy klinicznej nr III zostały opublikowane w lutym 2021 r. w czasopiśmie Lancet. W tym przypadku (wg opublikowanych w Lancet danych) zastosowano standardową metodologię przeprowadzania badań medycznych, m.in. uwzględniającą grupę placebo itd. III faza badań klinicznych objęła niemal 22 tys. osób. Wyniki badań, jakie uzyskano z grupy 14 964 osób, które otrzymały szczepionkę i 4902 osób, które otrzymały placebo dały rezultat jej skuteczności na poziomie 91,6%, która została oparta na jej zdolności na zapobieżenie wystąpienia zakażeniu objawowemu.[4]

Społeczność międzynarodowa naukowców przyjęła z dużą domieszką sceptycyzmu ogłoszenie Prezydenta Wladimira Putina na temat wynalezienia i awaryjnego dopuszczenia do użycia szczepionki Sputnik V w sierpniu 2020 r., jeszcze zanim zostały opublikowane wyniki I oraz II fazy badań klinicznych i przed rozpoczęciem fazy III.

Publikacja w czasopiśmie Lancet wyników I oraz II fazy badań, a następnie odpowiedź na list otwarty sztabu stojącego za pracami nad wynalezieniem Sputnik V i publikacja go w tym samym czasopiśmie rozwiała część wątpliwości środowiska międzynarodowego naukowców, a publikacja wyników III fazy badań dodatkowo ociepliła wizerunek Rosyjskiego Instytutu Gamaleya oraz szczepionki Sputnik V, gdyż jawiła się ona jako jeden z ważniejszych graczy na rynku, który swoją skutecznością dorównywał lub przewyższał konkurencyjne szczepionki wytworzone na Zachodzie.

[4] Ministerstwo Zdrowia Publicznego Argentyny, Long-term analysis of antibodies elicited by Sputnik V: A prospective cohort study in Tucuman, Argentina, Argentyna, październik 2021, https://www.thelancet.com/ [dostęp: grudzień 202].

Sukces FR? Sputnik V i jego wykorzystanie w krajach ościennych

Rosjanie uruchomili wszelkie kanały promocji swoich szczepionek tzw. dyplomacji szczepionkowej od momentu zaistnienia wyścigu międzynarodowego po wynalezienie skutecznej szczepionki lub leku przeciwko wirusowi Sars-Cov-2. Jednym z głównych argumentów optujących za wyborem szczepionki rosyjskiej jest jej wysoka skuteczność porównywalna bądź przewyższająca tę wytwarzaną przez szczepionki zachodnie oraz cena.

W początkowym okresie dystrybucji szczepionek, jedna dawka szczepionki firmy Pfizer kosztowała 15.50 € ~ 19$, a pojedyncza dawka szczepionki firmy Moderna kosztowała ~ 22.6$, podczas gdy Rosjanie deklarowali koszt pojedynczej dawki szczepionki Sputnik V na poziomie niższym niż 10$.[5]

Rosjanie używali również innych technik, aby osiągnąć swoje dyplomatyczne cele, połączonych z działaniami w sferze informacyjnej, nastawionymi głównie na dyskredytację zachodnich szczepionek lub działania informacyjne względem zachodnich społeczeństw, co do wartości zamówienia rosyjskiej szczepionki, zwłaszcza w sytuacji początkowej, gdzie istniały poważne deficyty w zamówieniach szczepionek do Europy firm zachodnich, FR jawiła się jako „wybawiciel". Jednakże poza sferą informacyjną i dyplomatyczną Rosyjska szczepionka nie miała faktycznego pokrycia w faktach, ponieważ Rosjanie również mieli problemy z produkcją i zaspokajaniem zamówień, będących w trakcie realizacji. Niedobór elementów składowych szczepionek oraz opóźnienia w produkcji czy w przypadku FR problemy logistyczne z dostarczeniem powyższych do fabryk, spowodowały tożsame problemy z tymi, z jakimi borykały się firmy zachodnie – konieczność dokonywania wyborów, któremu odbiorcy wysłać szczepionki w pierwszej

[5] Ibidem

kolejności i na jakich zasadach. Co spowodowało perturbacje dyplomatyczne, ponieważ w pierwszej kolejności realizowane były zamówienia do Europy oraz Ameryki Łacińskiej, a kraje azjatyckie i bliskiego wschodu musiały czekać na swoją kolej.

	Sputnik V – dawki dostarczone (w mln. sztuk)	Całkowita ilość otrzymanych dawek szczepionek (w mln.)	Procent populacji, który otrzymał 1 i 2 dawkę szczepionki	Procent zaszczepionych, którzy otrzymali Sputnik V	Zarejestrowane szczepionki
Argentyna	4	5,6	10/1,6	x>60%	AstraZeneca SinoPharm SputnikV
Węgry	1,1	4,8	32/13	23	AstraZeneca Moderna Pfizer-BioNTech Sputnik V
Meksyk	0,9	11,7	7,5/1,8	x>10%	AstraZeneca Pfizer-BioNTech SinoPharm SputnikV
Serbia	0,34	2,9	25/17	12	AstraZeneca Pfizer-BioNTech SinoPharm SputnikV
Słowacja	0,2	1,1	18/6	18	AstraZeneca Moderna Pfizer-BioNTech

Tab. 1. Wykorzystanie szczepionki Sputnik V w wybranych państwach. Źródło: Opracowanie własne na podstawie www.ecdc.europa.eu – stan na kwiecień 2021 r.

Jak możemy zaobserwować na podstawie powyższych danych (Tab. 1) – szczególnie jeżeli weźmiemy pod uwagę sytuację na rynku szczepionkowym na świecie na początku 2021 r. – można powiedzieć, że FR odniosła wówczas sukces propagandowy i polityczny, ponieważ w krajach, gdzie

szczepionka rosyjska została dopuszczona do użytku, wyszczepialność społeczeństwa tą szczepionką była na wysokim poziomie.

Cele Federacji Rosyjskiej

Głównymi celami FR w działaniach dyplomacji szczepionkowej i działań informacyjnych względem zachodnich społeczeństw było przekonanie opinii publicznej i polityków UE, że szczepionka Sputnik V mogła być rozwiązaniem problemów Europy – przede wszystkim co do dostępności szczepionki, ale również co do ceny i mniejszego obciążenia ekonomicznego dla budżetów państw. Rosjanie prowadzili szereg szeroko zakrojonych działań dyplomatycznych, gdzie oferowali państwom członkowskim – dostawy szczepionek lub technologię produkcji, używając przy tym argumentów o niezależności UE względem świata i innych zachodnich dostawców. Prowadzono przy tym rozmowy dwustronne najwyższego szczebla z poszczególnymi krajami Europy. Pomimo powyższych działań Rosjanie rozpoczęli procedurę rejestracyjną w Europejskiej Agencji Leków dopiero w marcu 2021 r., pomimo iż możliwe jest rozpoczęcie procesu oceny szczepionki przeciwko Sars-Cov-2 jeszcze w trakcie negocjacji.

Należy przy tym zauważyć, że Rosjanie pomimo braku zgody przez EMA o dopuszczeniu do użytku szczepionki byli w stanie przekonać kilka krajów europejskich do importu Sputnika V w ramach bilateralnych umów z konkretnymi państwami, co zdecydowanie można potraktować jako ich sukces w toczonej przez nich grze względem UE i Zachodu. FR ponadto toczyła szeroko zakrojone operacje informacyjne w celu siania zamętu wewnątrz społeczeństw zachodnich poprzez rozpowszechnianie teorii spiskowych związanych z pandemią COVID-19, które wzmagają strach i niepewność w grupach społecznych, które poddają się tego typu teoriom. Na przestrzeni I kwartału roku 2021 mieliśmy do czynienia z wieloma tego typu teoriami spiskowymi. Zarówno USA jak i Wielka Brytania oskarżały Rosję o szerzenie dezinforma-

cji i propagandy wymierzonej w ich szczepionki – Pfizer, Moderna i AstraZeneca, czemu Kreml – zaprzecza, a zamiast temu wysuwa oskarżenia pod adresem Stanów Zjednoczonych, że ich działania polityczne i szantaż, jakiemu poddają inne państwa, a tym samym uniemożliwia im zakupu Sputnika V, np. Brazylii.

Krótkoterminowym celem rosyjskich działań i zmasowanych operacji informacyjnych jest dopuszczenie Sputnika V do sprzedaży za granicą, zwłaszcza w krajach Unii Europejskiej (zatwierdzenie przez EMA). W Rosji szczepionka została zarejestrowana 11 sierpnia 2020 roku i wprowadzono ją na rynek wewnętrzny 8 września, jeszcze przed rozpoczęciem III fazy badań klinicznych, jako produkt, który ma znaczenie strategiczne wobec ogólnoświatowego kryzysu. 2 lutego 2021 r. ukazał się Lancet Journal, gdzie opisano, m.in. wyniki badań III fazy, szczegółowe wyniki oraz standardową metodologię badań, wykorzystaną przy określaniu jakości, skuteczności i bezpieczeństwa szczepionki dla populacji FR. Na podstawie tych danych oszacowano, że szczepionka jest skuteczna w 91,6%, jednak publikacja w medycznym czasopiśmie jest w zasadzie jedyną publicznie dostępną informacją o produkcie. Społeczność międzynarodowa naukowców wskazywała na kilka nieścisłości w badaniu, a przede wszystkim zarzucano Rosjanom, że nie udostępnili bardziej szczegółowych danych, w szczególności protokołów z badań.

Pierwszym krajem, który otrzymał szczepionkę Sputnik V była Białoruś (21 grudnia 2020 r.). W następnych miesiącach – ponad 60 krajów (w tym Rosja) zatwierdziło szczepionkę Sputnik V. Ze względu na sytuację pandemiczną, proces dopuszczania nowego produktu medycznego do użytku w innych krajach miał charakter przyspieszony – podobnie jak na Zachodzie, a odbywało się to głównie na podstawie badań klinicznych przeprowadzonych w FR. Szczepionka rosyjska została zaakceptowana głównie przez państwa postsowieckie, kraje Ameryki Łacińskiej, Półwysep Arabski, Azję i Afrykę. W Europie został zarejestrowany przez Węgry, Słowację, Serbię, Czarnogórę

i Macedonię Północną, a także Bośniacką Republikę Serbską. W początkowej fazie – początek 2021 r., Sputnik V konkurował głównie ze szczepionką chińską, ponieważ zachodnie firmy farmaceutyczne początkowo koncentrowały swoje wysiłki na realizacji zamówień i dostaw do krajów Zachodu, a większość krajów, w których zarejestrowany jest Sputnik V, to kraje rozwijające się, a więc nie mające tak dużych środków na zakup wystarczającej ilości szczepionek zachodnich lub ich zamówienia były na tyle małe, że koncerny zachodnie nie realizowały w pierwszej kolejności zamówień do tych krajów, co więcej oczekiwały one na dostawy zachodnich szczepionek w ramach koordynowanego przez WHO programu solidarności COVAX (do którego Rosja nie przystąpiła), który ma na celu w sposób sprawiedliwy i równomierny zapewnić dostęp całej ludzkości do szczepionek zachodnich.

Czy Federacja Rosyjska ponosiła porażki w swoich działaniach względem zachodu?

Podczas, gdy postępowanie przed Europejską Agencją Leków, mające na celu dopuszczenie Sputnika V do obrotu na terenie UE zakończy się prawdopodobnie w roku 2022, a FR w tym czasie zawarła szereg kontraktów i umów bilateralnych z poszczególnymi państwami UE to EMA wzywa państwa członkowskie UE do powstrzymania się od rejestracji Sputnika V na szczeblu krajowym do momentu, kiedy nie zostanie zakończony przez urząd proces sprawdzania bezpieczeństwa i skuteczności szczepionki oraz testowania jej pod kątem zgodności z normami europejskimi (tak jak w przypadku preparatów zachodnich i innych produktów medycznych). W połowie marca 2021 r. dyrektor generalna EMA – Christa Wirthumer-Hoche porównała decyzje Budapesztu i Bratysławy o zatwierdzeniu szczepionki Sputnik V na własnym terytorium z grą hazardową „rosyjska ruletka". W odpowiedzi Moskwa oskarżyła ją o stronniczość wobec produktu. Rzecznik Kremla Dmitrij Pieskow nazwał jej wypowiedź niestosowną i godną pożałowania, a twórcy rosyjskiej szczepionki kwestionowali neutralność EMA i zażądali oficjalnych

przeprosin od Szefowej EMA i całej instytucji, natomiast szef RDIF Kirill Dmitriew oskarżył P. Christę Wirthumer-Hoche o celowe opóźnianie procesu rejestracji produktu na terenie UE.

Rosja od momentu opracowania preparatu boryka się z problemami z produkcją szczepionek, zarówno od strony technologii, ilości i możliwości dostosowania fabryk, logistyki i wielu innych aspektów, które składają się na sytuację, że Federacja Rosyjska nie była i nie jest do dnia dzisiejszego w stanie sprostać produkcji na skale otrzymanych zamówień – setek milionów sztuk szczepionki. Dlatego postanowiono wytransferować technologię poza obszar Federacji Rosyjskiej np. do Korei Południowej lub krajów europejskich. gdzie to firmy farmaceutyczne miałyby produkować szczepionkę Sputnik V, ponieważ w IV kwartale 2020 r., I oraz II kwartale 2021 r. wyprodukowano na terenie FR zaledwie dziesiątki milionów sztuk szczepionki, podczas gdy obecne zapotrzebowanie wynosi miliardy sztuk.

Kolejnym problemem potencjalnych odbiorców rosyjskiej szczepionki jest nierzetelność informacyjna ze strony Rosji, ponieważ wszelkie dane o ilości dostarczonych szczepionek Sputnik V pochodzą od krajów trzecich, a FR nie udostępniała w początkowej fazie żadnych statystyk. Nastepnym ciosem w dyplomację szczepionkową FR i jej działania polityczne i informacyjne, mające ocieplać stosunek do własnego produktu w Europie była sytuacja z dostarczoną szczepionką Sputnik V na Słowację. W kwietniu 2021 r. Słowackie media opublikowały pełną wersję opinii Słowackiego Urzędu Kontroli Leków (ŠÚKL), gdzie stwierdzono, że otrzymane szczepionki nie były identyczne z produktem, który jest poddawany ocenie przez EMA lub tymi, których wyniki badań klinicznych zostały opisanym Lancecie. Według ŠÚKL rosyjskie szczepionki stosowane w różnych krajach na całym świecie mają „tylko wspólną nazwę", a różnice dotyczą fundamentalnych kwestii, takich jak skład chemiczny, a nawet budowa anatomiczna. ŠÚKL zwrócił uwagę, że mimo wielokrotnych próśb strona rosyjska nie dostarczyła około 80% wymaganych informacji. Słowacja ostatecznie zwróciła całą partię

szczepionek do Rosji, a po początkowych protestach Rosji oraz rzucanych oskarżeniach, np. oskarżające Słowacki Urząd ds. Kontroli Leków, że nie miał on formalnego prawa poddawać badaniu laboratoryjnemu dostarczonych szczepionek – Rosja ostatecznie przyjęła zwrot szczepionek. Był to duży cios zarówno w politykę i dyplomację szczepionkową FR, która nieustannie starała się ocieplać wizerunek własnego produktu, zwłaszcza na terytorium UE. Dużym echem odbiło się również to wydarzenie w mediach społecznościowych, co było poważnym ciosem w działania informacyjne wymierzone w społeczeństwa UE i pozostałych krajów Zachodu.

Działalność rosyjska w sferze informacyjnej państw zachodu

FR już od czasów ZSRR, a nawet i wcześniej doskonale opanowała sztukę działań informacyjnych, zarówno tych ofensywnych jak i działań względem własnego społeczeństwa. Należy podkreślić, że Rosjanie w sferze informacyjnej zawsze działają według ustalonych przez siebie wcześniej celów, które chcą osiągnąć, a których odgadnięcie przez stronę atakowaną lub poddawaną działaniom informacyjnym nie zawsze jest łatwe i oczywiste, ponieważ w klasycznych działaniach informacyjnych, szczególnie agresywnych chodzi o spowodowanie u przeciwnika niemożności podejmowania jasnych i dokładnych decyzji, opartych na twardych i sprawdzonych danych, a zamiast tego decyzje powinny być podejmowane na podstawie danych niepełnych/ błędnych/ specjalnie przygotowanych (spreparowanych)/ bazujących na emocjach itd.

Należy również pamiętać, że Rosjanie dostosowują swój przekaz do poszczególnych krajów, regionów, a nawet grup społecznych – szczególnie w dobie mediów społecznościowych, gdzie poziom rzetelności informacji nierzadko jest dramatycznie niski, a jej sprawdzalność zazwyczaj sprowadza się

jedynie do „społecznego poparcia”[6] czyli skali aktywności innych użytkowników względem danej informacji np. ilości udostępnień/ polubień itd. Dlatego przekaz względem szczepionek jak i Sputnik V będzie diametralnie różny w różnych krajach europejskich, np. w Polsce promocja szczepionki rosyjskiej jest znikoma, granicząca z jej brakiem, dlatego, że społeczeństwo Polskie w przeważającej większości nie chciało stosować i nie miało zaufania do rosyjskiego produktu medycznego, a działania informacyjne były ukierunkowane na deprecjonowanie skuteczności pozostałych szczepionek, wzbudzanie lub prowokowanie zachowań antyszczepionkowych, czy pogłębiania strachu przed pandemią, wirusem, samotnością czy śmiercią. Natomiast w innych krajach UE przekaz w wielu aspektach był diametralnie inny – pozytywny względem szczepionki Sputnik V, np. w Niemczech, w sytuacji braku możliwości szybkiego dostępu do szczepień, ze względu na wprowadzenie określonej selekcji przy brakach zaopatrzeniowych, biura podróży, zaczęły oferować wycieczki do Moskwy i innych miast FR z możliwością szczepienia rosyjską szczepionką, co zaowocowało wyborem tego typu opcji przez Niemców, którzy nie byli w przewidziani jako ta grupa, która jako pierwsza otrzyma szczepienie, dzięki czemu stopniowo zaczęła być tworzona grupa „ambasadorów” rosyjskich szczepień w niemieckim społeczeństwie.[7]

Słowenia czy Węgry były krajami należącymi do UE, które jako pierwsze zakupiły większe ilości szczepionek z Rosji, do czego przyczyniły się opisane wyżej czynniki – skuteczna dyplomacja FR i skuteczne działania w przestrzeni informacyjnej tych państw.

---

[6] K. Nash, A Johansson, K. Yogeeswaran, Social Media Approval Reduces Emotional Arouser for People High in Narcissism: Electrophysiological Evidence, Brief Research Report, 2019, [dostęp: grudzień 2021].

[7] K. Giles, Handbook of Russian Information Warfare, NATO Defence College, 2016, [dostęp: grudzień 2021].

Poszczególne cele działań informacyjnych FR niewątpliwie różnią się względem konkretnych krajów, regionów czy organizacji międzynarodowych, jednakże zawsze są podporządkowane głównym celom politycznym FR.

Wykorzystanie mediów społecznościowych do realizacji Własnych celów politycznych i informacyjnych przez Rosję

Gwałtowny rozwój nowoczesnych społeczeństw informacyjnych, a następnie mediów społecznościowych, pozwolił, aby Federacja Rosyjska oddziaływała na społeczeństwa w sposób wcześniej nieznany i nowatorski, stosując nowoczesne metody, które opierają się na sprawdzonych działaniach, które wpływają na percepcję ludzi. Olbrzymią i pożądaną zmianą w stosunku do czasów Zimnej Wojny jest to, że FR nie musi, a przynajmniej na zdecydowanie mniejszą skalę ukrywać swojego współautorstwa danej informacji, ponieważ w czasach Zimnej Wojny, jakakolwiek wzmianka na temat pochodzenia informacji z ZSRR natychmiast całkowicie ją dyskredytowała w oczach opinii publicznej społeczeństw Zachodu.

Przykładem na to może być operacja dezinformacyjna, jaką ZSRR przeprowadził na temat AIDS w latach ’80 XX w., gdzie przypisywano pochodzenie tego wirusa z tajnych laboratoriów CIA lub II dekady później FR próbuje rozpowszechniać informacje w niektórych częściach świata, np. niektórych krajach Afryki, że Stany Zjednoczone są odpowiedzialne za wytworzenie i późniejsze rozpowszechnianie wirusów Ziki i Eboli, posługując się niemal tymi samymi technikami oddziaływania na społeczeństwa, grupy społeczne i pojedynczych ludzi.

Dzisiaj – w czasie pandemii Sars-Cov-2 FR również w niektórych częściach świata próbuje zastosować podobne działania – przedstawić USA jako kraj, który jest odpowiedzialny za wybuch pandemii i stworzenie koronawirusa. Techniki jakimi się przy tym posługuje są niezmienna – a opierają się na tym, że podawana i rozpowszechniana informacja musi być odpowiednio przygotowana i dostosowana do percepcji grupy odbiorczej, w następnym

kroku jest rozpowszechniana za pomocą mediów społecznościowych poprzez wykorzystanie szeregu kont do tego przeznaczonych, które mogą być „hodowane" przez lata, a które to zgromadziły pokaźną grupę obserwatorów lub kont obserwujących które są kreatorami opinii w określonych społecznościach – a to jest główny cel działań informacyjnych, czyli dotarcie do jak największej liczby osób i/lub grup w danym społeczeństwie/ grupie etnicznej/ społeczności międzynarodowej itd.[8]

Jak pokazują badania, od kilkunastu lat, ilość czasu spędzanego przed ekranami smartfonów, przeglądając w tym czasie media społecznościowe przez użytkowników nieustannie rośnie, co stwarza niepowtarzalne okazje, aby wykorzystać to do działań informacyjnych przez kraje takie jak FR. Korporacja Meta Inc. – Facebook posiada obecnie 3 miliardy aktywnych użytkowników w ujęciu miesięcznym, dzięki czemu jest obecnie najpotężniejszym medium społecznościowym na świecie. Tak duża ilość użytkowników posiada szereg potrzeb, m.in. potrzeby dostępu do informacji, które szereg portali próbuje zaspokoić, jednak poważnym zagrożeniem dla użytkowników korzystających i posługujących się informacjami zaczerpniętymi z Facebook-a lub innych mediów społecznościowych jest ich znikoma weryfikowalność, co stwarza olbrzymie pole do działania dla krajów, których celem jest próba wpłynięcia na percepcję opinii publicznej danego kraju.[9]

Jak pokazują badania, przy przesadnym wyeksponowaniu jednostek na zbyt dużą ilość bodźców informacyjnych, mogą one prowadzić do swoistej „niewrażliwości" informacyjnej, czyli zatracenia przez jednostki lub grupy społeczne zdolności do odróżniania fikcji, fałszu i zjawisk rzeczywistych,

[8] Ibidem
[9] IAB Polska, Przewodnik po Social Mediach w Polsce, 2019 [dostęp: grudzień 2021].

a ten stan świadomości jednostek oznacza zdolność do zaakceptowania wszelkich form rzeczywistości jako tych rzeczywistych, nawet istnienia zjawisk całkowicie paranaukowych, paranormalnych czy przeczących wszelkim prawom fizyki, chemii, matematyki itd. Ten stan świadomości jednostek występuje również, kiedy dochodzi do hejtu i jest on również wynikiem tych samych założeń, które są nieco inaczej ukierunkowane, ponieważ w sytuacji występowania lub pisania hejterskich treści, użytkownicy niejako eliminują ze swojej świadomości element istnienia rzeczywistego istnienia osoby/treści hejtowanej. Niemożność spotkania się z osobą w świecie rzeczywistym i obserwacji jej emocji powoduje zastąpienie rzeczywistości pewnym obrazem w świadomości hejtera i uzewnętrznienie własnych emocji i odczuć względem tego wytworzonego obrazu. Kolejnym istotnym czynnikiem, który wpływa na zachowania hejterskie jest chęć zmiany posiadanego obrazu – negatywnego we własnej świadomości, stąd również często następuje tak zaciekła obrona własnej racji w „walce na komentarze", która niemal zawsze kończy się fiaskiem.

Kolejnym etapem „padania ofiarą" działań informacyjnych jest tzw. „znieczulica informacyjna", czyli utrata chęci na przyswajania lub akceptację jakichkolwiek informacji i następuje utrata zaufania do jakichkolwiek źródeł informacyjnych spoza obszaru własnej bańki informacyjnej nawet bezsprzecznych faktów, potwierdzonych w pełni z metodologią badań naukowych lub osób, które dana jednostka uważa za „autorytet" to jednak w zderzeniu z inną opinią danego autorytetu niż dana jednostka lub grupa społeczna posiada, dany autorytet zostaje uznany za zdezawuowany. Doskonałymi przykładami powyższego stanu rzeczy jest ruch społeczny „wyznawców" płaskiej ziemi oraz ruch „antyszczepionkowy". Te ruchy społeczne w obecnej konfiguracji pozostają głuche na argumenty lub pomimo istnienia oczywistych i niezbitych faktów naukowych „na wyciągnięcie ręki" np. poprzez podróż samolotem przez Atlantyk z Europy do Ameryki lub możli-

wości obserwacji Ziemi z przestrzeni kosmicznej w czasie rzeczywistym, nadal utrzymuje, że Ziemia jest płaska. Antyszczepionkowcy natomiast potrafią wewnątrz własnych baniek informacyjnych utrzymywać, że szczepionki zawierają mikro-chipy, dzięki którym ludzkość będzie kontrolowana przez niektórych miliarderów.

Powyższe całkowicie abstrakcyjne stwierdzenia podziela jakaś część ludzi na Ziemi i pomimo, że odsetek ten jest nadal marginalny, to dzięki istnieniu mediów społecznościowych jest tak pokaźny. Naukowcy upatrują występowania tego typu zjawisk w wielu przyczynach, głównymi z nich są oczywiste działania informacyjne krajów, których celem jest destabilizacja społeczeństw Zachodu, np. FR, kolejnym aspektem będącym przyczyną tych zjawisk jest gwałtowny rozwój społeczeństw informacyjnych w ciągu kilku lat i powstania mediów społecznościowych, jednak jak uważają naukowcy badający opisywane zjawiska, podstawowym czynnikiem decydującym o tak dużej podatności na tego typu operacje informacyjne są deficyty edukacyjne oraz umiejętności analizy informacji i sprawdzania źródeł występujące u jednostek, grup społecznych itd., jednak nie tylko w konkretnej sferze, np. medycznej, ale przede wszystkim w sferze rozumienia funkcjonowania naszych umysłów jako ludzi, które działają i postrzegają rzeczywistość w sposób liniowy, czyli taki, który dąży do jak najprostszego wytłumaczenia otaczającego świata, a występowanie skomplikowanych i wielopłaszczyznowo złożonych zjawisk np. pandemii COVID-19 powoduje, że niektóre jednostki lub grupy społeczne odmawiają na poziomie biologicznym przyswojenia określonych informacji, gdyż jest to zbyt skomplikowane i nie pasujące do ich codziennego sposobu postrzegania rzeczywistości.

Dobrym przykładem powyższego stanu rzeczy są działania Fundacji Open Estonia, która prowadzi wiele badań w Estonii, kilka lat przeprowadziła szereg badań z zakresu operacji informacyjnych, przeprowadzonych przez FR względem obywateli Estonii, a którzy etnicznie są Rosjanami (stanowią oni

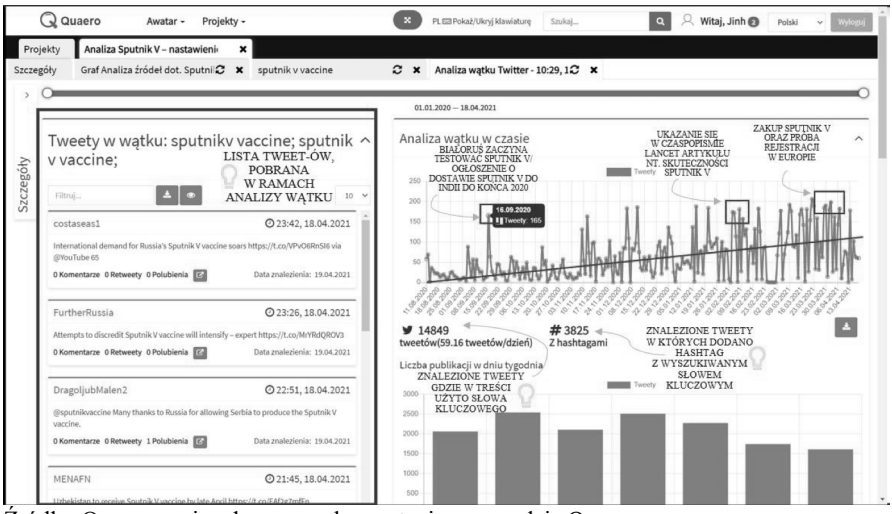
ok. 25% populacji Estonii). Przebadano wpływ wpływu informacji otrzymywanych ze źródeł estońskich, aby po pewnym czasie informacje były przez grupę badawczą czerpane tylko ze źródeł rosyjskich – skutkiem takich działań było to, że zdecydowana większość respondentów po pewnym czasie utraciła możliwości formułowania i wyrażania własnych poglądów i zaczęła traktować informacje pozyskiwane z obu źródeł jako nieprawdziwe. Wnioski z tych samych badań pokazują również, że treści nadawane przez źródła rosyjskojęzyczne są bardziej atrakcyjne i angażujące emocjonalnie, a uwaga widza jest przyciągana poprzez „silne oddziaływanie na emocje" poprzez publikacje, np. szokujących treści lub takich, które silnie polaryzują grupy społeczne.[10]

Medium Twitter, badania własne nad problematyką i oddziaływaniem FR względem zachodu poprzez Sputnik V11

W tym podrozdziale zostaną przedstawione wyniki badań i analiz własnych zagadnienia szczepionki Sputnik V na przykładzie medium Twitter.

[10] K. Giles, Handbook of Russian Information Warfare, NATO Defence College, 2016, [dostęp: grudzień 2021].

[11] Badania przeprowadzono za pomocą autorskiego narzędzia QUAERO, które służy do zbierania i analizowania danych z social mediów (oprogramowanie QUAERO należy do Inseqr Sp. z o.o.).

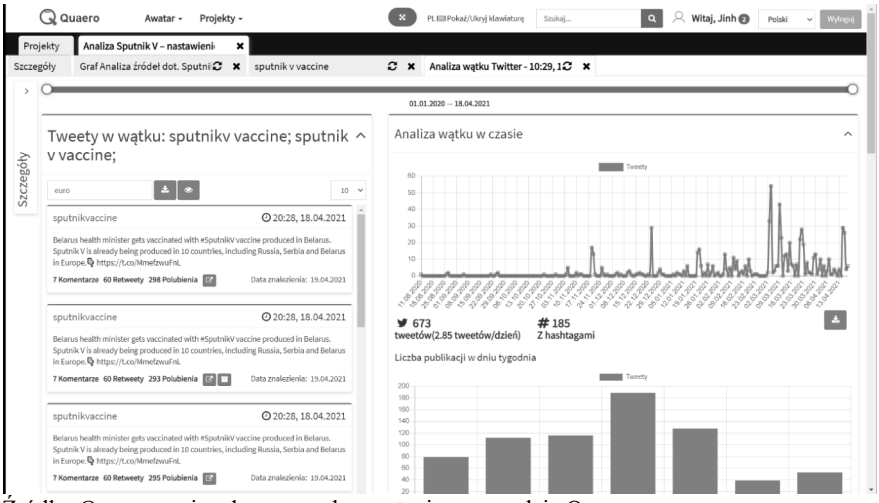


Źródło: Opracowanie własne z wykorzystaniem narzędzia Quaero.
Rys. 1. Zakres danych zebranych od stycznia 2020 r. do kwietnia 2021 r.

Powyższy rysunek (Rys. 1) przedstawia zakres danych zebranych od stycznia 2020 r. do kwietnia 2021 r. – jak możemy zaobserwować, mediana popularności tematu szczepionki Sputnik V nieustannie rosła, aby w ostatnim kwartale 2020 r. oraz I kwartale 2021 r. przybrać duże natężenie. Kiedy analizujemy dane z social mediów w sposób na zasadzie metodologii big data, ważnym jest, aby zwracać uwagę na rzeczy mniej oczywiste. Na wykresie głównym mogliśmy zaobserwować określone peek'i działalności użytkowników Twitter, ale kiedy włączymy do analizy wykresy ze słowami kluczowymi wyraźnie wskazującymi na inne języki, np. polski, arabski, rosyjski to wyraźnie wtedy można zaobserwować, które informacje miały charakter „ogólny", przekaz, np. pozytywny – jak w przypadku publikacji wyników badań I, II oraz III fazy badań klinicznych nad szczepionką Sputnik V – odbiło się to

echem we wszystkich krajach, zauważalnie wzmacniając popularność rosyjskiej szczepionki, zwłaszcza w sytuacji, kiedy nie były jeszcze dostępne szczepionki Zachodu.

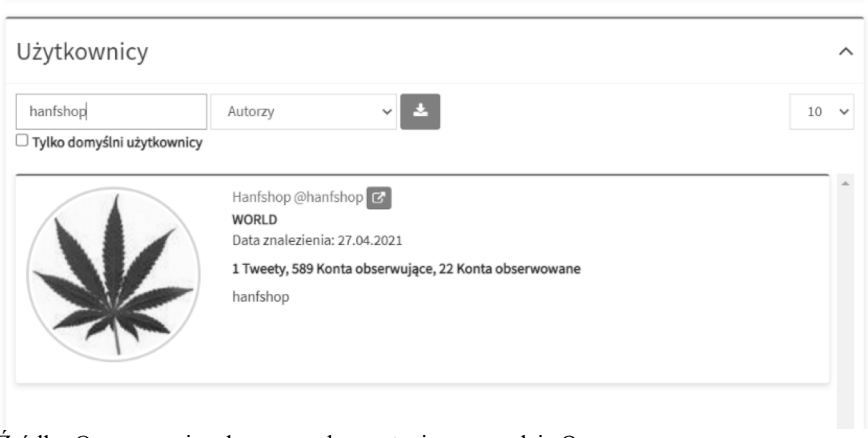
Należy mieć również na uwadze, że FR przygotowując operacje informacyjne i dostosowując je do konkretnych państw/ społeczeństw czy grup społecznych wykorzystuje bardzo często emocjonalne elementy, które wpływają w sposób znaczny na opinię publiczną, a czym bardziej spolaryzowane jest społeczeństwo, tym łatwiej takie operacje prowadzić. Wspomniane powyżej peek'i aktywności użytkowników powtarzają się w wielu krajach – jest to informacja ogólna – skierowana do, np. społeczności międzynarodowej itd., ale zazwyczaj, jesteśmy w stanie również zidentyfikować informacje skierowane tylko i wyłącznie do danej społeczności, a poniżej przykład takiego działania (Rys. 2).



Źródło: Opracowanie własne z wykorzystaniem narzędzia Quaero.

Rys. 2. Aktywności wątku „sputnikv vaccine"

Przy analizie social mediów należy również poszukiwać charakterystycznych słów kluczowych i filtrować dane w celu zwiększenia szansy wykrywania potencjalnych siatek botów lub trolli internetowych. Na powyższym przykładzie (Rys. 2) wyfiltrowaliśmy dane, zawężając ich obszar do grup społecznych zamieszkujących Europę, a tym samym mogliśmy przeanalizować tweet'y i ich treść oraz ton i nastawienie do szczepionki, jakie publikują osoby będące członkami tych grup społecznych. Po znalezieniu ciekawych kont, które mogły być kreatorami opinii publicznej, można określić ich siłę oddziaływania informacyjnego poprzez sprawdzenie ilości osób je obserwujących oraz powiązań i najczęstszych interakcji pomiędzy tymi kontami.



Źródło: Opracowanie własne z wykorzystaniem narzędzia Quaero.
Rys. 3. Przykład konta oddziałowującego

Jak możemy zaobserwować na powyższym przykładzie (Rys. 3) wytypowaliśmy potencjalne konto, które w danym wątku opublikowało Tweeta, który bardzo gorąco popierał jak najszybsze wprowadzenie szczepionki Sputnik V do użytku w Europie, a do tego był pisany łamaną angielszczyzną i sprawiał wrażenie bezpośredniego tłumaczenia na język angielski poprzez

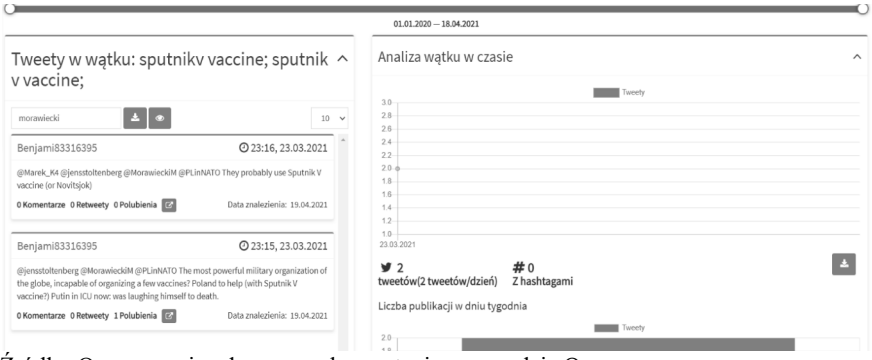
translator internetowy. Jak możemy od razu zaobserwować, to konto posiada pewne możliwości oddziaływania informacyjnego, gdyż obserwuje je 589 użytkowników, w dalszej kolejności należało tylko ustalić, powiązania z innymi kontami oraz częstotliwość oraz miejsca dyskusyjne, w których to konto zabiera głos. Dzięki zdobyciu powyższych informacji można byłoby określić, czy może być to potencjalnie konto publikujące tendencyjne informacje, które w określonych przypadkach może być wykorzystywane do wrogich działań informacyjnych, jeżeli przy dalszych analizach potwierdziłaby się część z powyższych informacji, to wówczas należałoby objąć stałym monitoringiem dane konto i obserwować jego działania, tak aby w przyszłości móc reagować natychmiast przy próbie uruchomienia określonej operacji informacyjnej.

Dalsze analizy aktywności powyższego konta nie przyniosły potwierdzenia hipotez, które mogłyby wskazywać na działalność informacyjną tego konta w sposób odbiegający od działań „typowych" użytkowników, zostały jednak znalezione inne ciekawe poszlaki. Opisywane konto posiadało wśród obserwujących konto z Rys. 4 i nadzwyczaj często wchodziło w interakcje z powyższym kontem.

Źródło: Opracowanie własne z wykorzystaniem narzędzia Quaero

Rys. 4. Przykład konta powiązanego

Konto zaprezentowane powyżej (Rys. 4), w momencie pisania niniejszego artykułu – pod koniec IV kwartału 2021 r. zostało już zawieszone przez serwis Twitter. Jednakże jego działalność była nadzwyczajnie ciekawa, ponieważ to konto publikowało zarówno w języku polskim, jak i angielskim oraz rosyjskim. Dodatkowo było wrogo i agresywnie nastawione do działań europejskich, NATO-wskich (NATO jako sojusz wojskowy, w żadnym momencie ani elemencie nie uczestniczyło w negocjacjach, produkcji itd. szczepionek) oraz polskich władz względem szczepionki Sputnik V (w Polsce przytłaczająca większość opinii publicznej nie chciała, nawet potencjalnie zaszczepić się szczepionką rosyjską), której to polskie władze nawet w sferze rozważań i w sytuacji deficytu innych szczepionek nie zamierzały zamówić.
Poniżej (Rys. 5) możemy zapoznać się z małym wycinkiem Tweet-ów opublikowanych przez powyższe konto:



Źródło: Opracowanie własne z wykorzystaniem narzędzia Quaero
Rys. 5. Przykładowe tweet'y

W świetle powyższych danych oraz tego, że dane konto z dużą dozą prawdopodobieństwa było rodzajem konta bota lub trolla internetowego, o czym dodatkowo świadczy fakt, że sam serwis Twitter również je zablokował, konto nr 1 - @hanfshop należy również objąć monitoringiem, ponieważ

prezentowało zbyt ścisłą relację z kontem, które prowadziło i uczestniczyło w operacjach informacyjnych wymierzonych w Zachód.

Podsumowanie – Social Media

Prześledzone i zaprezentowane wyniki badań nad działalnością w social mediach w medium Twitter użytkowników i potencjalnych „trolli internetowych", dowodzą, jak w społeczeństwach silnie spolaryzowanych, czyli takich, gdzie poziom emocji opinii publicznej jest na bardzo wysokim poziomie oddziaływanie informacyjne staje się stosunkowo proste, a zwłaszcza w mediach, które umożliwiają publikację dowolnych informacji, które nie muszą być w żaden sposób weryfikowane czy sprawdzane.

Dzięki wykorzystaniu odpowiednich narzędzi możemy z powodzeniem monitorować social media, a zwłaszcza kreatorów opinii, warto przy tym zwracać uwagę na grupy odbiorcze i ich liczebność wobec kreatorów opinii i m.in. na tej podstawie szacować skalę grup odbiorczych i wpływu danych informacji na konkretne grupy społeczne. Należy przy tym tworzyć siatki powiązań i obserwować zachowania konkretnych kreatorów opinii, ich odbiorców oraz użytkowników, którzy trafiają na daną informację „przypadkowo". Śledzenie i obserwowanie aktywności w social mediach może dostarczyć wielu informacji, które można wykorzystać w celu przeciwdziałania dezinformacji i fake newsom, a pozyskane tam informacje można wykorzystać w kampaniach informacyjnych ze strony rządów poszczególnych państw, których celem byłaby edukacja społeczeństwa w kontekście wzmożonych działań informacyjnych, które np. wrogie państwo prowadzi w social mediach względem opinii publicznej danego państwa. Śledzenie i obserwacja social mediów może być również działaniem, dzięki któremu możliwe jest rozpoznanie odpowiednio wcześnie wrogich działań informacyjnych i dezinformacyjnych, dzięki czemu można im skutecznie przeciwdziałać.

Wydaje się, że jest to realne działanie, które oprócz solidnej edukacji społeczeństw co do zagrożeń występujących w cyberprzestrzeni oraz przestrzeni informacyjnej związanej, m.in. z social mediami ma szansę przynieść namacalne korzyści, dzięki czemu realne przeciwdziałanie dezinformacji i wrogim działaniom informacyjnym będzie mogło odnieść pożądany skutek, a nie koncentrować się na działaniach defensywnych w momencie, gdzie już znaczne szkody mogły zostać poczynione przez agresora. Dzięki odpowiedniemu monitorowaniu własnej przestrzeni informacyjnej możliwe staje się podjęcie działań defensywnych w momencie ataku, a nie w momencie, kiedy wroga operacja informacyjna zdołała już się „rozpędzić".

Podsumowując, na powyższym przykładzie badań nad problematyką i zagadnieniem szczepionki Sputnik V i jej obecności w social mediach oraz aktywności FR w tychże w opinii autora, nie ulega najmniejszej wątpliwości, że Rosjanie w sposób wyrafinowany i wyrachowany nieustannie prowadza walkę informacyjną z Zachodem z wykorzystaniem social mediów, a im większe napięcia zostają wygenerowane na świecie lub wewnątrz poszczególnych krajów wobec których FR ma określone plany i cele polityczne, tym łatwiej jest przeprowadzać tego typu działania. Niewątpliwym jest również fakt, że operacje informacyjne prowadzone przez FR są obliczone długoterminowo, a obecna architektura social mediów im w tym pomaga, ponieważ tworząc wielopoziomową i szeroką siatkę powiązań i kont, które mogą stopniowo włączać do swojej działalności w miarę, jak konta zyskują popularność w cyklu wielomiesięcznym lub wieloletnim, powoduje to, ze social media stają się głównym polem walki informacyjnej prowadzonej między FR a Zachodem.

Zakończenie

Trudna sytuacja epidemiologiczna w Europie w roku 2020 i w pierwszych kwartałach 2021 r. – w połączeniu ze stosunkowo powolną kampanią

szczepień w UE wywoływały i wywołują po dziś dzień niezadowolenie społeczne co przekładało się na wywieranie dużej presji na europejskich polityków, aby pilnie znaleźli skuteczniejsze sposoby walki z pandemią, zwłaszcza jeżeli weźmiemy pod uwagę tempo i stopień wyszczepialności społeczeństw w Izraelu, Wielkiej Brytanii czy USA. W rezultacie byliśmy świadkami powszechnego w całej UE spadku zaufania do instytucji unijnych za obecną sytuację i wymuszania poprzez opinię publiczną oraz rządy poszczególnych państw konkretnych działań Komisji Europejskiej i znalezienia rozwiązań co do importu szczepionek, które nie zostały jeszcze zatwierdzone.

Kreml starał się wykorzystać trudną sytuację do zintensyfikowania promocji Sputnika V i nakłonienia państw członkowskich do jego zakupu. W ten sposób strona rosyjska stwarza wrażenie, że jej przygotowanie mogłoby rozwiązać obecne problemy UE z niedoborami szczepionek, podczas gdy w rzeczywistości jakiekolwiek większe dostawy byłyby wysoce nieprawdopodobne, ze względu na własne problemy Rosjan z produkcją szczepionek. Poza tym dostawy mogłyby rozpocząć się najwcześniej w drugiej połowie 2021 r., kiedy – zgodnie z prognozami UE – nie byłyby już potrzebne (które to prognozy się sprawdziły), ponieważ produkty zachodnie zaspokoją popyt. Ponadto dostawy zakontraktowanych ilości Sputnika V (m.in. do Serbii, Węgier i Argentyny) były opóźnione. Ambitne plany produkcyjne Rosjan, zwłaszcza dla terytoriów poza Federacją Rosyjską (Indie, Korea Południowa, Brazylia) niezostały wypełnione i zrealizowane.

Poza tym FR musiała poradzić sobie z kolejnymi problemami wizerunkowymi, ponieważ pod koniec II kwartału 2021 r. Brazylijski Urząd Kontroli Leków opublikował komunikat, że niegroźny, genetycznie zmodyfikowany adenowirus wykorzystany do produkcji Sputnika V sam się namnaża i to w organizmie osoby zaszczepionej jak i poza nią. Oczywiście taka sytuacja nigdy nie powinna mieć miejsca w prawidłowo przygotowanej szczepionce, a powyższa sytuacja spowodowała, że Brazylia zażądała zwrotu

szczepionki do FR, ze względu na wadliwość produktu. Standardową odpowiedzią FR były oskarżenia wysuwane pod adresem władz brazylijskich, jednak ostatecznie część dostarczonej partii szczepionek – te wadliwe zostały przyjęte i uznane przez FR. Niewątpliwie był to kolejny duży cios wizerunkowy wymierzony w rosyjską dyplomację szczepionkową i działania w sferze informacyjnej państw.

Kreml wykorzystywał rosyjską szczepionkę jako instrument softpower w celu osiągnięcia własnych celów politycznych oraz poprawy swojego wizerunku w Unii Europejskiej, a ponadto rozbicia jej jedności, zwłaszcza między państwami członkowskimi a Brukselą. Rosyjskie oskarżenia o stronniczość EMA stanowiły poważne wyzwanie dla spójności UE oraz jej wizerunku, zwłaszcza w kontekście silnej presji ze strony kilku państw UE, aby jak najszybciej zakończyć proces weryfikacji Sputnika V i umożliwić jego import. Wynikało to z wielu różnych zmiennych, a główną był stosunek opinii publicznej tych krajów i stopnia zaufania do Rosji. Pod koniec roku 2021 Sputnik V nadal nie został zatwierdzony przez EMA, a więc presja Kremla nie przyniosła spodziewanego rezultatu, a Europejska Agencja Leków pomimo wielu nacisków realizuje swoje zadania zgodnie z obowiązującymi procedurami. Kolejne wpadki wizerunkowe, np. na Słowacji czy w Brazylii oraz stopniowe zwiększanie realizacji zamówień przez zachodnie koncerny spowodowały, że działania informacyjne FR oraz intensywna dyplomacja szczepionkowa zostały zepchnięte na boczny tor, nawet w krajach początkowo przychylnych Sputnikowi V, np. na Węgrzech i na Słowacji.

Wartym podkreślenia jest również fakt, że Rosja nie posiadała ani obecnie nie posiada wystarczających mocy produkcyjnych, ani tym bardziej zapasów Sputnika V, aby w sposób realny mogła wpłynąć na kampanię szczepień w Europie, a jak się w końcówce roku 2021 okazuje – również na świecie. Nawet plany produkcyjne Sputnika V w Korei Południowej nie zostały w pełni zrealizowane w określonych terminach, a tym samym oddziaływanie informacyjne FR pod względem wizerunkowym oraz szeroko rozumianej

walki informacyjnej w stosunku do krajów Zachodu oraz wybranych krajów Ameryki Łacińskiej i Azji – np. Indii, gdzie sytuacja epidemiczna była w II i III kwartale 2021 dramatyczna, ostatecznie nie powiodły się, a było to spowodowane niewystarczającymi mocami produkcyjnymi oraz niewystarczającą jakością samego produktu – szczepionki Sputnik V.

Bibliografia

1. Arquilla J., *Can information warfare ever be just*?, Kluver Academic Publisher 2009.
2. Bankauskaite D., *Lithuania Report*, CEPA, 2016
3. Bittman L., *The KGB and Soviet Disinformation. An Insider's view*, Washington 1985.
4. Darczewska J., *Anatomia Rosyjskiej wojny informacyjnej. Operacja Krymska – studium przypadku*, OSW Maj 2014.
5. Darczewska J., *Diabeł tkwi w szczegółach*, OSW Maj 2015.
6. Davenport i Prusak, Working knowledge, 1998.
7. Dieckmann Ch., *Deutsche Besatzungspolitik in Litauen 1941 – 1944*, Wallstein 2011 (angielskie tłumaczenie).
8. Fedchenko Y., *Kremlin Propaganda: Soviet Active Measures by Other Means,* StopFake.org, 2016.
9. Gajlewicz-Korab K., Konarska K., *Koncentracja kapitału w mediach i jej zapobieganie we Francji oraz Niemczech*, Instytut Staszica, Warszawa 2015.
10. Giles K., *Handbook of Russian Information Warfare*, NATO Defence College Nr 9, październik 2016.
11. Grabowski M., Zając A., *Dane, Informacje i Wiedza – próba definicji*, Akademia Ekonomiczna w Krakowie 2013.
12. Hajduk J., Stępniewski T., *Russia's Hybrid War with Ukraine: Determinants, Instruments, Accomplishments, and Challenges*, Studia Europejskie luty 2016.

13. Hajduk J., Władza i media we współczesnej Ukrainie, Pułtusk 2011.
14. Helma S., *Dezinformacja i wojna psychologiczna jako element polityki Związku Sowieckiego i Federacji Rosyjskiej*, UJ Kraków 2018.
15. Janda J., *Czech President is Russia's Trojan Horse*, Obserwator PE, czerwiec 2016.
16. Jundo-Kaliszewska B., *Etnolingwistyczna istota nacjonalizmu litewskiego i antypolonizm Litwinów na przełomie lat osiemdziesiątych i dziewięćdziesiątych XX w*., Uniwesytet Łódzki 2013.
17. Laurinavicius M., *Is Russia Winning the Information War in Lithuania?,* Raport CEPA 2016.
18. Libicki M., *What is information warfare*, AON 1995.
19. Liik K., *The Bronze Year of Estonia-Russia relations*, Rocznik MSZ Estonii 2007.
20. Lucas E., Pomeranzev P., *Winning the information war*, Raport CEPA, sierpień 2016 r.
21. Mattiisen M., Żurawski vel Grajewski P., Supinska A., *Russia's Influence and Presence in Estonia*, New Direction Fundacja UE, 2010
22. Modrzejewski Z., Markiewicz Sz., Współczesna walka informacyjna, AON 2016.
23. Nord P., Psychosocjotechnika, dezinformacja – oręż wojny, Komorów 1999.
24. Pac B., *Wojna informacyjna jako skuteczne narzędzie destabilizacji państw i rządów*, Raport Defence24.pl i Ośrodka Analiz Strategicznych, luty 2016.
25. Patyna M., *Problem integracji Rosjan w Estonii w latach 1989 – 2005*, Muzeum Historii Polski 2007.
26. Pynnoniemi K., Racz A., *Fog of Falsehood*, Raport FIAA nr 45, 2016
27. Senge, „The dance of change: The Challenges to Sustaining Momentum in Learning Organizations", 1999.

28. Smolenova I., *The Pro-Russian Disinformation Campaign in the Czech Republic and Slovakia*, Prague Security Studies Institute, czerwiec 2015 r.
29. Stępniewski T., *Unia Europejska, Ukraina i Rosja: kryzysy i bezpieczeństwo*, Studia Europejskie nr. 76, 2015.
30. Tibor R., *NATO Information Operations in Theory and in Practice Battling for Hearts and Minds in Afghanistan*, AARMS Nr 1, 2013.
31. Wasiuta O., Wasiuta S., *Wojna informacyjna zagrożeniem dla ludzkości*, Uniwersytet Pedagogiczny w Krakowie 2014.
32. Wilson A., Ukraine Crisis. *What it Means for the West*, Yale University, New Haven and London 2014.

Abstract

INFORMATIONAL AND DIPLOMATIC IMPACT RUSSIAN FEDERATION DURING THE COVID-19 PANDEMIC. CASE STUDY ON THE EXAMPLE OF USE OF RUSSIAN SPUTNIK VACCINE V AS AN ARGUMENT IN INFORMATION WARFARE

Summary: This chapter presents and describes the methods and techniques used by the Russian Federation to conduct information activities towards the West - including the use of social media. The authors also made an attempt to define and analyze the goals of the Russian Federation in terms of informing and achieving its own political goals, and the Sputnik V vaccine was one of the key elements that the Russian Federation had and operated to achieve its own goals. In the last part of the publication, the authors presented the methodology of preparing analyzes based on information activities in social media, using the example of the Sputnik V vaccine, and attempted to answer the questions about the legitimacy and reaction time to hostile information influence from Russia.

Keywords: information warfare, Sputnik V, information interaction, Covid-19, Russia.

Rozdział 11

Usiłowanie dokonania oszustwa na platformie OLX

dr hab. Jacek BIL[1]

STRESZCZENIE: Powszechna dostępność użytkowników do dokonywania sprzedaży
i zakupów za pomocą dedykowanych do tego celu platform internetowych jest wygodną i skuteczną metodą pozyskiwania i sprzedawania produktów. Operatorzy tego rodzaju serwisów będący świadomi zagrożeń związanych z pozyskiwaniem danych osobowych, przejmowaniem kont użytkowników, czy też uzyskiwaniem danych uwierzytelniających, wprowadzają skuteczne rozwiązania, które minimalizują (po stronie serwisu) ryzyka oszustw kierowanych przeciwko użytkownikom. Wskazane ograniczenia użyteczne są wyłącznie przy zachowaniu należytej staranności w trakcie dokonywania transakcji przez klientów. Sprawcy oszustw stosują zabiegi o podłożu socjotechnicznym, które w konsekwencji wprowadzają w błąd potencjalnych sprzedawców i kupujących. Niejednokrotnie popełnienie błędu przez użytkownika prowadzi do phishingu, w ramach którego sprawcy dokonują przestępstwa oszustwa. Niniejszy rozdział jest studium przypadku dotyczącego usiłowania oszustwa na szkodę osoby sprzedającej produkt za pomocą platformy OLX.

SŁOWA KLUCZOWE: oszustwo, socjotechnika, phishing, przejęcie danych, internetowe platformy zakupowe.

Socjotechnika

Termin socjotechnika przypisany jest ogółowi metod i działań zmierzających do uzyskania pożądanego zachowania jednostek i grup ludzkich. To

[1] prof. WAT, Wydział Bezpieczeństwa, Logistyki i Zarządzania, Wojskowa Akademia Techniczna w Warszawie, ryszardpio@wp.pl, ORCID:

także nauka o sposobach i wynikach świadomego wpływania na rzeczywistość społeczną[2]. Christopher Hadnagy wskazuje, iż w ramach stosowania socjotechniki dostarczane są człowiekowi określone informacje. Treści kierowane do adresata zawierają olbrzymi ładunek emocjonalny i uczuciowy oraz odwołują się do intelektu. Skuteczne działania socjotechniczne ukierunkowane są zatem na stosowanie następujących metod:

1) sytuacji deprawacyjnych – agresor wysyła komunikaty odbiorcy uniemożliwiające lub utrudniające zaspokojenie podstawowych potrzeb,

2) potęgowanie potrzeb nieelementarnych - metoda stosowana w przypadku wytwarzania chęci osiągnięcia określonego dobra (materialnego i niematerialnego), które mogą być spełnione przez ofertę agresora,

3) kanalizacji ideałów – w tym przypadku agresor ukierunkowuje przekaz na wiarę, ideały i wartości atakowanego,

4) intensyfikacji lęku: metoda stosowana w przypadku groźby i strachu, kiedy atakowany w trosce o zapewnienie bezpieczeństwa skłonny jest do podporządkowania się zabiegom agresora.

Socjotechnika, a zwłaszcza oddziaływanie socjotechniki ukierunkowane jest na dokonywanie świadomych przekształceń (społecznych), w celu uzyskania zaplanowanego celu. Przywołany proces (oddziaływanie) wymaga udziału podmiotu i przedmiotu oddziaływania[3]. ***Zdobywanie informacji*** to podstawowe zadanie socjotechnika. Intensywność i skuteczność podejmowanych ataków zależy od ilości posiadanych informacji i od praktykowanej metody infiltracji. Informacje można wyszukać w Internecie oraz poprzez osobiste ich uzyskiwanie w ramach bezpośredniej działalności (np. obserwacja), czy też podejmowania różnego rodzaju kombinacji sytuacyjnych. Bogate

---

[2] Socjotechnika, https://sjp.pwn.pl/slownik/socjotechnika.html, [dostęp: 11.07.2021].

[3] Ł. Scheffs, Socjotechnika władzy, http://cejsh.icm.edu.pl, [dostęp: 11.07.2021].

zasoby Internetu sprawiają, iż socjotechnicy chętnie podejmują działania właśnie w tym obszarze, w którym pozyskują bardzo dużo informacji. Oprócz umiejętności zdobywania informacji równie ważnym jest zdolność ich analitycznej obróbki i przechowywania. Osoby stosujące socjotechnikę prowadzą swojego rodzaju ***katalog***, w którym umieszczane zostają informacje na temat celu zakładanego efektu, tj. rodzaj zdobytych informacji, zaobserwowane działanie, zachowanie oraz uwagi na temat uzyskania informacji. W późniejszym etapie socjotechnik zestawia informacje i spostrzeżenia (ujęte w katalogu) z atakami, które chce przeprowadzić, co umożliwia wykonanie planu działania przewidzianego dla każdego celu. Kolejnym krokiem do przeprowadzenia ataku (np. oszustwa) jest ***wytworzenie pretekstu***, roli jaką agresor planuje odegrać w planowanym przedsięwzięciu. Najczęściej jest to określenie osoby jaką chce odgrywać (w analizowany studium przypadku jest to potencjalny nabywca obuwia) agresor. Jest to swojego rodzaju aktorstwo uprawiane zarówno w świecie rzeczywistym, jak i w przestrzeni wirtualnej. Pretekst socjotechnika, niezależnie czy jest prowadzony za pomocą rozmów telefonicznych, w ramach kontaktów bezpośrednich, czy też w Internecie, musi odwoływać się do języka, doboru słów oraz innych niezbędnych zabiegów, w celu wytworzenia sytuacji, w których atakowany obiekt (osoba) nie będzie miała żadnych wątpliwości, że socjotechnik jest tą właściwą osobą. Właściwie przeprowadzony etap pretekstu umożliwia przejście do zdobywania informacji bez zadawania pytań wprost podczas prowadzenia zwykłej wymiany zadań. Etap ten zwany jest ***wzbudzaniem***, czyli prowadzeniem rozmów, w wyniku których agresor zdobywa sympatię, zaufanie, konieczne dla przeprowadzenia skutecznego ataku. Prowadzone rozmowy (również w formie przesyłania tekstu) umożliwiają nawiązanie relacji mających na celu wywołanie poczucia bliskości i zaufania, które powstają, gdy ktoś psychologicznie

otwiera się na druga osobę i nie obawia się podać istotnych informacji[4]. Następnym etapem zmierzającym do uzyskania zamierzonego celu jest ***wpływ i manipulacja***, w ramach których agresor nakłania atakowany obiekt (osobę), by zrobiła to czego od niej oczekuje socjotechnik. Kluczowym aspektem tego etapu działania jest zabieg prowadzący do tego, by atakowana osoba podejmowała działania z własnej woli, z przekonaniem autorstwa pomysłu. W tym obszarze stosowanych jest szereg zasad, do których można zaliczyć: wzajemność, ustępstwo, przyzwolenie, niedobór, autorytet, zobowiązanie i konsekwencja, lubienie kogoś – czegoś oraz dowód społeczny. W tym miejscu należy podkreślić istotną różnicę pomiędzy wpływem a manipulacją. Wpływanie na obiekt ataku jest działaniem polegającym na przekonaniu go, żeby chciał zrobić to czego agresor oczekuje. Manipulacja jest działaniem polegającym na skłonieniu atakowanego do czegoś, czego on nie chce zrobić. W trakcie podejmowania zabiegów polegających na wpływaniu na druga osobę, celem agresora jest to, by atakowany poczuł się lepiej, że poznał agresora. Podczas stosowania manipulacji celem działania jest osiągnięcie zamierzenia, bez względu na samopoczucie drugiej osoby. Kontynuując kategoryzację działań socjotechnicznych wskazanych przez Christophera Hadnagy kolejnym etapem działań agresora jest **ramowanie**, które polega na znajdowaniu wspólnych wartości dla atakującego i atakowanego. Wartości te zależą od tego w jaki sposób atakowany postrzega świat wokół siebie i jak reaguje na różnego rodzaju wydarzenia[5].

Podstawowe formy socjotechniki to: ***łowienie ludzi na haczyk, wzbudzanie w rozmowach telefonicznych, wcielanie się w obcą osobę***. Mając na uwadze przedmiot niniejszego opracowania wydaje się, iż formą socjotechniki przypisaną temu zdarzeniu jest tzw. ***łowienie ludzi na haczyk***. Z tego też

---

[4] Ch. Hadnagy, Socjotechnika. Metody manipulacji i ludzki aspekt bezpieczeństwa, Wyd. Helion, Gliwice 2020, s. 57-64.
[5] Ibidem, s. 65-66

powodu ta forma zostanie przybliżona szerzej niż pozostałe dwie. Z uwagi na wszechstronny zakres aktywności społecznej w przestrzeni Internetu najpopularniejszą formą socjotechniki jest phishing, w ramach którego wysyłane są na skrzynkę e-mail do wytypowanych odbiorców socjotechniczne wiadomości lub też wiadomości zawierające złośliwe pliki. Nie jest tajemnicą, iż otworzenie pliku lub kliknięcie w przesłany link umożliwi agresorowi, np. włamanie się do systemu, wykradzenie danych, pozyskanie danych uwierzytelniających i inne niepożądane działania. Obecnie e-maile phishingowe są niezwykle często stosowaną metodą przez agresorów. Ch. Hadnagy podaje (powołując się na bliżej nieokreślone źródło), iż jeden na 300 odebranych e-maili to działanie phishingowe. W tym zakresie należy przywołać metodę *spear phising*, która polega na wysyłaniu spersonalizowanych wiadomości zawierających szczegóły nawiązujące do tego, co odbiorca lubi lub nie. Kolejną metodą jest *whaling*, której istotą jest ukierunkowanie ataku na ważny dla agresora cel, np. przedstawiciela najwyższego kierownictwa spółki prawa handlowego (lub też indywidualnego użytkownika platformy zakupowej - przyp. autora). Niezależnie od przyjętej metody, socjotechnik wykorzystywał będzie okoliczności wywołujące strach, ciekawość oraz władzę, w celu nakłonienia do realizacji przyjętego zamierzenia. Phishing jest skuteczną metodą nieuczciwych socjotechników z uwagi na szeroki wachlarz jego zastosowania w Internecie oraz poprzez wykorzystywanie widomości, które wyglądają jak prawdziwy e-mail, do tego ma takie same kolory, styl i układ jak te pochodzące z oryginalnego źródła. Warto jednak zwrócić uwagę na wybrane szczegóły, które odkrywają fałszywość przekazu:

1) błędy literowe w adresach stron, portali, co często jest niezauważalne przez użytkowników, z uwagi na podobieństwo do oryginału,

2) powitanie zaczynające się od „Cześć”„, Witam”, gdzie normalnie powinno się pojawić nazwisko i imię,

3) ważną wskazówką jest link, ponieważ jak zostanie umieszczony nad nim znacznik okaże się, że wcale nie przekieruje użytkownika na oczekiwany adres, ale na specjalnie przygotowaną stronę przez agresora,

4) oprócz przygotowanych linków także stosowane są elementy graficzne, np. przycisk z napisem kopiuj link, prowadzący do strony pułapki.

Ważnym elementem socjotechniki jest używanie komunikacji niewerbalnej. Wydawać by się mogło, iż tego rodzaju komunikacji nie można wykorzystać w przypadku stosowania wyłącznie słowa pisanego. Okazuje się jednak, iż jest to możliwe. Socjotechnik odwołując się do ramowania (budowania mostów pomiędzy atakującym a atakowanym) stosował będzie słowa wywołujące w myśli atakowanej osoby obrazy, dlatego też słowa zdolne są do kreowania wizualnych scenariuszy, pod wpływem których użytkownik podejmuje działanie mogące wyrażać cel agresora. Socjotechnik działając w celu wyłudzenia informacji używał będzie słów, które wywołują określone emocje, by skłonić ofiarę do podjęcia pożądanego działania. W tego rodzaju przedsięwzięciach socjotechnik (agresor) wykorzystuje emocje strachu, smutku lub inną, na której mu zależy. Dodatkowym narzędziem socjotechnika w ramach komunikacji niewerbalnej jest wykorzystywanie emotikonów, które są dla wielu użytkowników nieodzownym dopełnieniem (dodatkiem) słowa pisanego. W określonych scenariuszach gry socjotechnicznej agresor używa emotikonów, w celu zaprezentowania swojej osoby jako radosnej, przyjaznej i otwartej, co w konsekwencji ułatwi realizację zamierzonego planu[6].

Jak wspomniano powyżej w obszarze zainteresowania nieetycznych socjotechników znajdują się także działania ***prowadzone przy wykorzystaniu telefonu***. W tym zakresie niezwykle aktywnym sposobem jest podszywanie się pod określony numer dzwoniący (spoofing), czyli udawanie, że rozmowa nawiązywana jest z innego numeru niż w rzeczywistości (np. dzwoni ktoś ze

[6] Ibidem, s. 67-72

wsparcia technicznego operatora, firmy, itp.), co umożliwia socjotechnikowi wykreowanie dogodnej pozycji do realizacji planu. Spoofing informacji dzwoniącego sprzyja szybkiemu uzyskaniu zaufania, ponieważ wyświetlany numer jest pewnego rodzaju gwarantem wiarygodności. Atakujący będący nawet w sporej odległości od ofiary może za pomocą przygotowanej legendy wzbudzić zaufanie, a w konsekwencji wyłudzić interesujące go dane. Podobnie jak w przypadku wiadomości tekstowych, również w przypadku rozmów prowadzonych telefonicznie możliwe jest stosowanie komunikacji niewerbalnej, służącej wyłudzaniu informacji przez telefon. Narzędziami stosowanymi w tej metodzie jest uśmiech – który zwiększa poziom zaufania w relacjach z nieznajomymi, ale też postawa w stosunku do rozmówcy, ton i wysokość głosu, a także, czy osoba mówi głośno, czy cicho[7]. Trzecią z przywołanych form socjotechnicznych jest ***podszywanie się pod określoną osobę***. Jak wskazuje Christopher Hadnagy przyjęcie tożsamości innej osoby ułatwia zdobycie informacji, zwłaszcza w sytuacji, kiedy ktoś okazuje legitymacje, plakietkę z nazwiskiem, posiada dostosowany do sytuacji ubiór (np. roboczy), mówi i zachowuje się jako osoba, za którą się podaje. W takich przypadkach umysł ludzki dostaje odpowiedź na pytania, których nawet nie zadał:

1) Kim jest ta osoba?

2) Jakie ma dowody, na udowodnienie tego co mówi?

3) Czy znajduje się w stanie niebezpieczeństwa, czy też nie?

Atakowana osoba uzyskująca odpowiedź na frapujące je pytania uspokaja się i staje się mniej czujna, z czego korzysta agresor.

Ataki hackerskie zaczynają się głównie od wiadomości phishingowych, ale są to również operacje inicjowane rozmowami telefonicznymi oraz przy wykorzystaniu sprzętu komputerowego. Kluczowym dla powodzenia nielegalnych operacji jest stosowanie metod socjotechnicznych, zarówno w

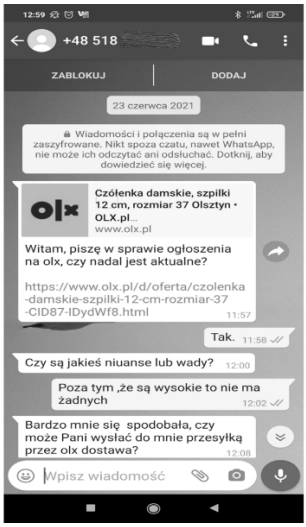
[7] Ibidem, s. 73-75.

sprawach dotyczących ataków na organizacje publiczne, duże firmy czy też dotyczących codziennych czynności – transakcji sprzedaj, kup. Wszystkie te przedsięwzięcia wymagają planowania, zdobywania informacji oraz bardzo dużej dawki zabiegów socjotechnicznych, zarówno werbalnych, jak i pozawerbalnych[8].

Studium przypadku

Przedmiotem tej części opracowania jest przypadek związany z usiłowaniem wyłudzenia danych uwierzytelniających do bankowości elektronicznej. Analizowana sprawa datowana jest na miesiąc czerwiec 2021 roku i dotyczyła oferty sprzedaży obuwia damskiego. Osoba, mieszkająca w Olsztynie, chcąc sprzedać buty umieściła za pomocą platformy OLX ofertę, w której dokonała opisu przedmiotu sprzedaży, podając wymagane informacje, w tym m. in. numer telefonu. Agresor przyjmując plan działania wytypował osobę (prawdopodobnym kryterium przyjętym przez atakującego była cena butów, płeć osoby, sprawdzenie historii transakcji, posługiwanie się aplikacją WhatsApp). Kolejnym działaniem sprawcy było wspomniane wcześniej wytworzenie pretekstu, czyli w tym przypadku przyjęcie postawy osoby – potencjalnego nabywcy towaru.

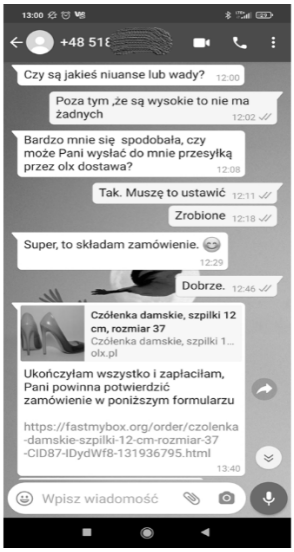
[8] Ibidem, s. 72-81.



Zdjęcie nr 1. Informacja dotycząca zainteresowania przedmiotem sprzedaży

Analiza treści informacji zawartych w pierwszym kontakcie jasno wskazuje, iż agresor przyjął plan polegający na wytworzeniu pretekstu do kolejnych działań. Sprawca stosuje opisywaną wcześniej metodykę postępowania, która polega na sformułowaniu zwrotu „*Witam*", tak charakterystycznego dla działania socjotechników (wiele osób stosuje ten zwrot powitania, nie mając zamiaru podejmowania negatywnych działań, należy jednak zadać sobie pytanie, czy ja sam(a) nie stosuję socjotechniki wobec rozmówców?). Ogólny obraz przekazu w tej części korespondencji nie budzi podejrzeń. Ale czy na pewno? Inicjowany przez agresora dialog wiąże strony wspólną sprawą – etap wzbudzania, podczas którego potencjalny kupujący wyraża troskę o jakość towaru. Po udzieleniu odpowiedzi od osoby atakowanej (zapewne scenariusz odpowiedzi był znany na podstawie opisu przedmiotu), agresor stosuje dalsze zabiegi socjotechniczne, które dodatkowo budują więź pomiędzy aktorami tego wydarzenia. Wyrażenie uznania towaru w oczach sprzedawcy, ma na celu uśpienie czujności osoby atakowanej, treść wiadomości „*bardzo mnie się*

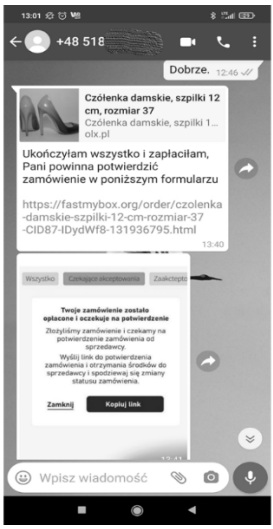
spodobała" jest potencjalną zachętą do dalszych, szybkich działań sprzedającego. Należy jednak w tym miejscu się zatrzymać, w celu dokonania analizy przywołanego zapisu. Niniejszy zapis powinien zwrócić uwagę osób zajmujących się problematyką ujawniania nieetycznych działań socjotechnicznych, ponieważ sposób formułowania zdania wskazuje, iż potencjalny kupujący może korzystać z dostępnych aplikacji tłumaczenia tekstu, a jego prawdziwa tożsamość jest zakamuflowana.



Zdjęcie nr 2. Informacja wskazująca na kontynuację zakupu

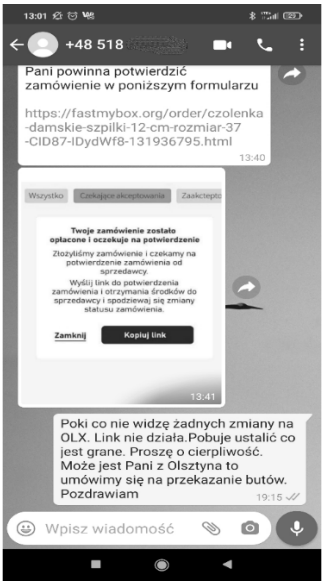
Na podstawie analizy zdjęcia numer 2, zauważalny jest etap podjętej przez agresora manipulacji, wyrażony wskazaniem sposobu dostarczenia przesyłki. Oczywiście nie sama metoda przesyłki stanowi o manipulacji, a potencjalna deklaracja zakupienia butów, potwierdzona sposobem dokonania dostawy. Jak wynika z analizy zapisów należy zauważyć, iż obie strony – potencjalna kupująca (jeśli rzeczywiście jest kobietą) oraz sprzedająca, już na

tym etapie są stronami wyrażającymi wspólne wartości, tj. szybkie działanie i chęć dokonania transakcji. Dodatkowo uwagę zwraca zastosowanie emotikonu (w postaci uśmiechniętej buźki), który w powszechnym odczytaniu nie jest niczym niezwykłym, jednak mając na uwadze wskazane w tym artykule zasady odwoływania się do pozawerbalnych środków dla pozyskania uwiarygodnienia, zastosowanie przedstawionej formy graficznej przekonuje o słuszności podejrzenia stosowania nielegalnych działań, wykorzystujących narzędzia socjotechniki. Umieszczenie tego rodzaju obrazu graficznego miało na celu przekonać sprzedającą, iż po drugiej stronie transakcji znajduje się osoba wiarygodna, dążąca do szybkiej finalizacji sprawy. Istotna jest także treść wiadomości umieszczonej przed emotikonem o treści „*Super, to składam zamówienie*", która jest zabiegiem zapewniającym sprzedającą o ostatecznej decyzji, co do zakupienia towaru. Wystosowana odpowiedź od sprzedającej o treści „*Dobrze*" utwierdza agresora o trafności podejmowanych kroków.



Zdjęcie nr 3. Wskazanie sposobu zakończenia transakcji

Dalsza analiza przesyłanych treści tekstowych ujawnia kolejne mechanizmy działania sprawcy. Na zdjęciu nr 3 zaprezentowano wpis agresora o treści „*Ukończyłam wszystko i zapłaciłam, Pani powinna potwierdzić zamówienie w poniższym formularzu*". Dobór słów użytych w tej części korespondencji jest doskonałym przykładem manipulacji socjotechnicznej, w ramach której agresor informuje o załatwieniu sprawy po swojej stronie, z jednoczesnym wywarciem wpływu na postępowanie sprzedającej, w myśl założenia – jeśli tak dobrze się znamy i rozumiemy to należy dochować umowy. Formułowane w ten sposób treści utrudniają logiczną analizę postepowania, w ramach której powinno pojawić się pytanie, czy proponowany sposób finalizacji sprawy jest zgodny z procedurami OLX? Oczywiście, że nie jest! Dążąc do uwiarygodnienia podejmowanych działań, sprawca przesłał kolejną wiadomość, w której umieścił spreparowany na wzór oryginału formularz, zawierający ukryty przycisk, za pomocą którego sprzedająca mogła „potwierdzić" podjętą transakcję. Uwagę zwraca sposób wykonania przesłanej platformy, w której sprzedająca informowana jest o postępie realizowanej transakcji oraz umieszczone są dwa pola, jedno pod nazwą „*kopiuj link*", a drugie „*zamknij*". Zabiegiem socjotechnicznym jest danie wyboru sprzedającej jeszcze na tym etapie, co do odstąpienia od transakcji, w ramach opcji „*zamknij*". Agresor mając na uwadze sposób procedowania transakcji i fakt, że zazwyczaj sprzedający jest bardziej zainteresowany doprowadzeniem sprawy do końca, jest pewien, że atakowany wybierze opcję „*kopiuj link*".



Zdjęcie nr 4. Informacja od sprzedającej o niedziałaniu linku

Zgodnie z zabiegami agresora sprzedająca skorzystała z przesłanego formularza i kliknęła w opcję „*kopiuj link*”, co też było celem sprawcy. Jak uwidoczniono na zdjęciu nr 4 link jednak nie został aktywowany, o czym informuje sprzedająca w ostatniej części korespondencji. Powstanie błędu podczas aktywacji linku spowodowane zostało (na szczęście) decyzją sprzedającej, co do wyboru opcji połączenie z siecią. W tym przypadku skorzystano z możliwości aktywacji linku poprzez narzędzia systemowe platformy OLX, która uniemożliwiła dalsze procedowanie aktywacyjne oraz jak się okazało, wywołało podejrzenia sprzedającej co do możliwości wyłudzenia danych uwierzytelniających.

Monitoring zdarzeń wywołanych przez oszustów wskazuje, iż przeprowadzony atak nie jest odosobniony. Na stronie internetowej dobreprogramy.pl, umieszczona została w dniu 12 lipca bieżącego roku informacja

dotycząca działania oszustów, którzy śledzą oferty na OLX, a następnie dokonują wyłudzenia pieniędzy. Opisywane zdarzenie wydaje się być tożsame z przywołanym studium przypadku, ponieważ wykorzystane mechanizmy sprawcze oraz przedmiot sprzedaży – buty, są takie same. Pokrzywdzona z Legnicy nie miała tyle szczęścia, co sprzedająca z Olsztyna, bowiem na skutek wyłudzenia danych uwierzytelniających sprawcy ukradli z jej konta jedenaście tysięcy złotych[9].

Podsumowanie

Świadomość społeczna zagrożeń wynikających z wyłudzenia danych poprzez stosowanie phishingu wydaje się być na wysokim poziomie. Zjawisko chętnie jest definiowane oraz bardzo często staje się przedmiotem dyskursu publicznego i naukowego. Stanowi także stały punkt rozważań w ramach prowadzenia przedmiotów z obszaru bezpieczeństwa, realizowanych na różnego rodzaju poziomach kształcenia. Podmioty organizujące sprzedaż internetową dbają o zabezpieczenie techniczne przed nieuprawnionymi atakami oraz informują klientów o konieczności zachowania szczególnej ostrożności przy realizacji podejmowanych transakcji. Jak się okazuje, stosowanie jedynie zabezpieczeń technicznych, nie jest wystarczające dla ochrony wartości pieniężnych użytkowników. Instrumenty socjotechniki używane dotychczas w przestrzeni politycznej oraz w obszarze szeroko rozumianego wywierania wpływu, zagospodarowane zostały na dobre przez sprawców przestępstw operujących w Internecie. Poznanie ludzkich potrzeb, ich słabości oraz nadmiernej skłonności do realizacji celu, stanowi doskonałe podłoże dla nieetycznych działań socjotechnicznych. Przywołane w ramach

[9] Sprzedaż butów na OLX i problem: z konta zniknęło 11 tys. złotych, https://www.dobreprogramy.pl/sprzedaz-butow-na-olx-i-problem-z-konta-zniknelo-11-tys-zlotych,6660367423588896a, [dostęp: 12.07.2021].

niniejszego artykułu zdarzenie utwierdza w przekonaniu, iż sprawcy tego rodzaju przestępstw operują dojrzałym warsztatem wywierania wpływu i manipulacji. Wydaje się być zasadnym stwierdzenie, iż dla wypracowania skutecznych metod przeciwdziałania zdarzeniom, w ramach których wyłudzane są istotne dane, należy rozpoznać i zneutralizować mechanizmy techniczne umożliwiające dokonywanie tego typu przestępstw oraz prowadzić działania demaskujące nieuczciwych socjotechników. W obszarze poznawczym niniejszego artykułu umieszczono studium przypadku, które dotyczy ważnej sprawy z punktu zapewnienia bezpieczeństwa personalnego obywatela. Należy jednak mieć na uwadze, że wykorzystywane wcześniej mechanizmy walki politycznej odwołujące się do socjotechniki, zaadaptowane zostały na potrzeby szeroko rozumianej walki informacyjnej, w ramach której istnieje wysokie ryzyko wyłudzania informacji ważnych dla bezpieczeństwa państwa. Obszar podejmowanego działania nie ma granic, ponieważ obejmuje wrogą aktywność zarówno w przestrzeni tradycyjnych kontaktów i oddziaływania międzyludzkiego oraz doskonale rozwijany jest w sieci informacyjnej z Internetem włącznie.

Bibliografia

1. Hadnagy, Ch., *Socjotechnika. Metody manipulacji i ludzki aspekt bezpieczeństwa*, Wyd. Helion, Gliwice 2020.
2. Scheffs, Ł., *Socjotechnika władzy*, http://cejsh.icm.edu.pl.
3. Socjotechnika, https://sjp.pwn.pl/slownik/socjotechnika.html.
4. Sprzedaż butów na OLX i problem: z konta zniknęło 11 tys. złotych, https://www.dobreprogramy.pl/sprzedaz-butow-na-olx-i-problem-z-konta-zniknelo-11-tys-zlotych,6660367423588896a.

Jacek BIL

Abstract

THE "BLIK" CRIME

Summary: The author of this chapter describes what the "BLIK" crime is about. He draws attention to the characteristic elements of such fraud and presents the mechanisms used by criminals.

Keywords: BLIK, fraud, hacking, identity, spoofing.

Rozdział 12

Wybrane cyberzagrożenia w dobie pandemii COVID-19

Dorota HUMECKA-LICHOSIK[1]

STRESZCZENIE: W rozdziale przedstawiono przykłady wykorzystania przez przestępców zdarzeń o dużej wadze emocjonalnej do popełniania cyberprzestępstw.

SŁOWA KLUCZOWE: COVID-19, cyberprzestępczość.

Wstęp

Pandemia COVID-19 oraz cyberataki zdecydowanie w sposób destrukcyjny wpływają zarówno na ludzi jak i na globalną gospodarkę. COVID-19 odciska piętno nie tylko na mechanizmach oraz metodach działania sprawców, ale również na wykorzystywaną przez nich socjotechnikę. Analiza krajowych oraz międzynarodowych raportów dotyczących cyberbezpieczeństwa pozwala na zaobserwowanie znacznego wzrostu ilości incydentów.

W 2020 r. problemy cyberbezpieczeństwa unaocznił i wyeksponował związany z pandemią COVID-19 lockdown, który spowodował nagłe przejście do wykonywania pracy, świadczenia usług, jak również do realizacji zadań publicznych w trybie online. Do nowych warunków bardzo szybko

[1] Szef Sekcji Systemów Teleinformatycznych, RCI Gdynia, d.humecka-lichosik@ron.mil.pl.

dostosowali się również sprawcy cyberprzestępstw, uznawanych za najbardziej dynamiczną formę przestępczości. Cyberprzestępcy tworzą nowe sposoby działania, jak również dostosowują już istniejące do nowej sytuacji wykorzystując innowacyjne wektory ataków, którymi obejmują nowe kategorie osób. Przestępcy potrzebują tylko niewielkiego okna możliwości, aby zachęcić użytkownika do otworzenia przesłanego załącznika lub kliknięcia w łącze, które może spowodować natychmiastowe spustoszenie w danym środowisku. Czy jesteśmy przygotowani do zdalnej pracy, do zdalnej nauki, do realizacji zadań publicznych z wykorzystaniem środków komunikacji elektronicznej? Zdecydowanie zarządzanie cyberbezpieczeństwem stało się kluczowym elementem dla komunikacji w sieci. Tylko wyważone podejście do wzmacniania cyberochrony może zaradzić rosnącemu ryzyku i umożliwić realizację wszelkich zamierzonych działań w tych niekonwencjonalnych czasach. COVID-19 stał się nie tylko problemem zdrowotnym, ale zaczął generować obszerne ryzyko dla cyberbezpieczeństwa. Niewątpliwie cyberprzestępcy szybko skorzystali z rozprzestrzeniania się wirusa i zaczęli prowadzić szereg działań nakierowanych na popyt informacyjny, jak również na zasoby. Dla cyberprzestępców pandemia jest idealną okazją do zwiększenia skuteczności ataków opartych na socjotechnice.

Podczas wprowadzania kolejnych faz obostrzeń można było zaobserwować różnego rodzaju scenariusze ataków. W Polsce najczęstszymi incydentami bazującymi na lęku w obawie przed pandemią są przestępstwa ukierunkowane na nadużycia finansowe w sieci.

Regularne zamykanie galerii handlowych spowodowały, że ludzie coraz chętniej zaczęli kupować produkty z wykorzystaniem sklepów elektronicznych.

Należy mieć na uwadze, iż załamanie które pojawiło się wraz z nadejściem pandemii dotknęło nie tylko pojedynczych osób, ale również małych, średnich oraz dużych firm, które w obawie o utratę klientów, stanowisk pracy, czy zachowania płynności finansowej próbują podjąć walkę z przetrwaniem

zastoju gospodarczego. Ponadto kryzys oddziałuje na instytucje, które za cel stawiają sobie utrzymanie swojej pozycji sprzed pandemii, jak również na całe państwa próbujące podjąć odpowiednie starania w celu ograniczenia skutków zaistniałej sytuacji w wymiarze zdrowotnym, społecznym i gospodarczym. Wszystkie powyższe podmioty mogą stać się potencjalnie celem cyberataków.

Jednym z zasobów interesujących każdego kto śledził wybuch i przebieg epidemii koronawirusa, jest interaktywny portal internetowy zarządzany przez Uniwersytet Johnsa Hopkinsa (ryc. 1), który w czasie rzeczywistym dostarcza aktualnych informacji na temat rozprzestrzeniania się choroby COVID-19[2].

Źródło: https://coronavirus.jhu.edu/map.html.

Ryc.1. Interaktywna mapa Uniwersytetu Johnsa Hopkinsa dostarczająca informacji o koronawirusie

[2] https://www.pwpw.pl/Czlowiek_i_dokumenty, nr 57,"C&C-Coronavirus i Cyberprzestępczość.

Portal ten również został wykorzystany przez cyberprzestępców do manipulowania ofiarami. Hakerzy spreparowali e-maile o treści „Raport WHO o sytuacji COVID-19", które wyglądały identycznie jak wysłane z Centrum Johnsa Hopkinsa. Podczas gdy użytkownik klikał w link, automatycznie uruchamiał się plik programu Excel, w którym zawarty był wykres obrazujący sytuacje epidemiczną w danym kraju. W tym samym czasie jedno z makr w arkuszu pobierało oprogramowanie typu RAT, które pozwalało przejąć kontrolę nad sprzętem ofiary.

To pokazuje, jak schemat działania cyberprzestępców jest bezlitosny, jak potrafią bazować na nieszczęściu innych i żadna krzywda ludzka nie jest w stanie ich zatrzymać.

Wybrane cyberzagrożenia

Fałszywe zbiórki i smishing

Po wprowadzeniu w Polsce ograniczeń związanych z COVID-19 w sieci pojawiło się wiele fałszywych zbiórek z przeznaczeniem na szczytne cele. Przestępcy próbują wyłudzać środki finansowe na walkę z koronawirusem podszywając się pod różne organizacje społeczne. Często ofiary są okradane nie tylko z pieniędzy, ale również z danych osobowych oraz tożsamości.

Jednym z pierwszych przykładów takiego oszustwa w dobie pandemii, było podszycie cyberoszustów pod prawdziwą zbiórkę prowadzoną w serwisie „siepomaga.pl". Sprawcy tworząc fałszywą stronę internetową chcieli doprowadzić osoby do niekorzystnego rozporządzenia mieniem poprzez wprowadzenie ich w błąd, że pieniądze które wpłacają, w rzeczywistości trafią na walkę z wirusem. Polacy otrzymywali smsy o następującej treści „Wspieramy polską służbę zdrowia w czasie walki z epidemią COVID-19! Wesprzyj szpitale w Polsce przekazując datek! https://pomoc.sie-pomaga.net/koronawirus?SS52".

Załączony w treści wiadomości link prowadził do fałszywej strony. Nieautentyczna zbiórka znajdowała się pod adresem się-pomaga[.]net,

z myślnikiem i w domenie „.net”.Te prawdziwe kwesty są pod nazwą bez myślnika i w domenie „.pl” tj.siepomaga.pl[3].
Adres fałszywej strony: https://pomoc[.]sie-pomaga[.]net/koronawirus?SS52 (ryc.2)

Źródło: https://zaufanatrzeciastrona.pl/post/zlodziejskie-hieny-kradna-pod-szyldem-pomocy-sluzbie-zdrowia/.

Ryc.2. Przykład fałszywej strony zbiórki

Przy pomocy tej fałszywej platformy internetowej, która imitowała zbiórkę na pomoc w walce z COVID-19, przestępcy pozyskiwali loginy i hasła do bankowości mobilnej.

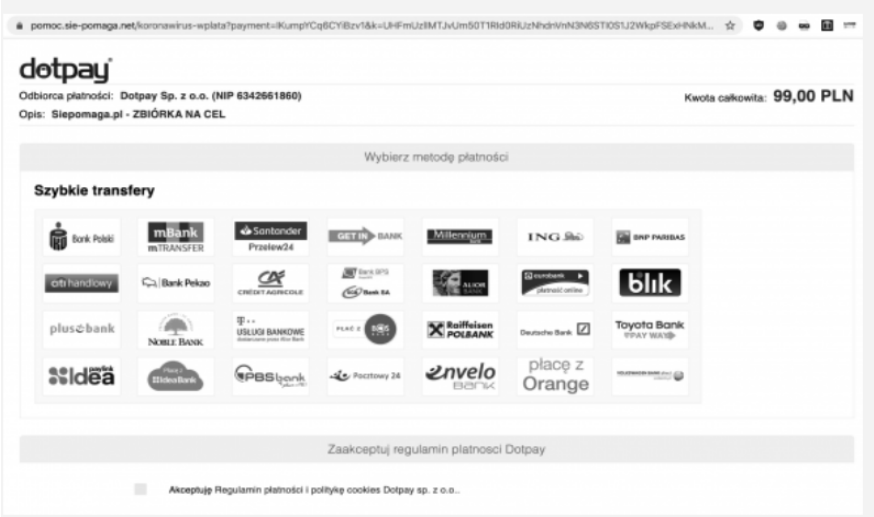
Podrabiane były także kolejne podstrony związane z wpłatą środków (ryc.3), a odbiorca ataku zostawał przekierowany na stronę fałszywego panelu

[3] CERT Polska

pośrednika płatności (ryc.4), gdzie następowało wyłudzenie od niego loginu oraz hasła do banku.

Źródło: https://zaufanatrzeciastrona.pl/post/zlodziejskie-hieny-kradna-pod-szyldem-pomocy-sluzbie-zdrowia.

Ryc.3. Przykład fałszywej podstrony zbiórki



Źródło: https://zaufanatrzeciastrona.pl/post/zlodziejskie-hieny-kradna-pod-szyldem-pomocy-sluzbie-zdrowia.

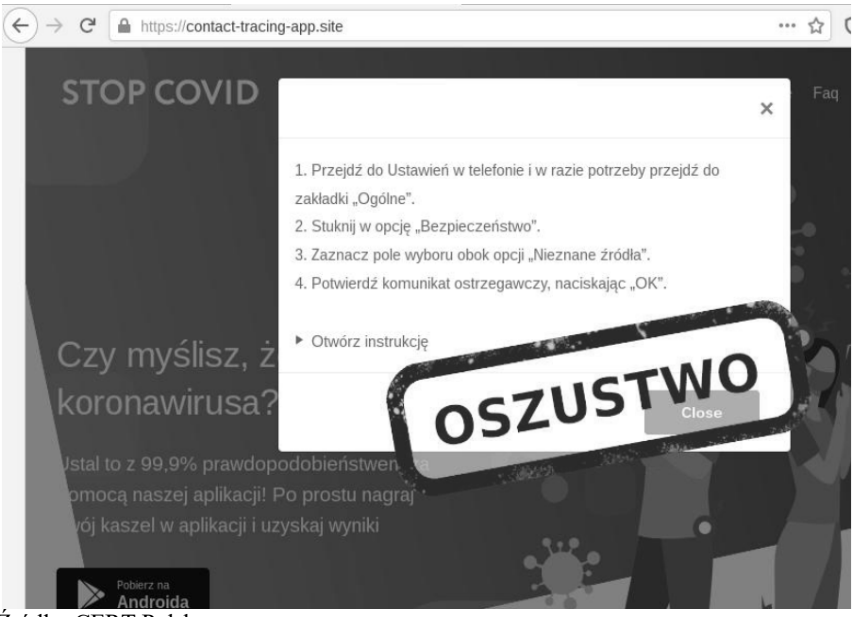
Ryc.4. Przykład fałszywego panelu pośrednika płatności

Podczas trwania pandemii COVID-19 dał się zaobserwować wzmożony atak tzw. smishing- atak SMS-phishing, który polega na przesyłaniu wiadomości tekstowych, mających skłonić ofiarę do podjęcia określonego działania. Zazwyczaj celem atakujących jest zmuszenie odbiorcy do połączenia się ze złośliwą stroną. Wykradzione dane hakerzy w prosty sposób wykorzystują do celów oszustw tożsamościowych. W momencie kliknięcia w przesłany link, urządzenie zostaje zainfekowane złośliwym oprogramowaniem lub też użytkownik zostaje przeniesiony na symulowaną stronę internetową. Cyberprzestępca w ten sposób osiąga swój cel, zdobywając ważne informacje, niezbędne do popełniania oszustwa.

W czasie lockdownu, pojawiło się również bardzo dużo oszustw związanych z tematem szczepień przeciwko COVID-19. Oszustwa te polegały na żądaniu zapłaty za szczepionki lub stymulowały do rozpoczęcia SMS-owej rejestracji na szczepienie przeciwko koronawirusowi.

Cyberprzestępcy zdobyli się również na stworzenie dedykowanej aplikacji (ryc.6), której zadaniem było sprawdzenie czy użytkownik jest zainfekowany COVID-19. Przestępcy próbowali podszyć się pod rządową aplikację „ProteGO Safe", znaną również jako STOP COVID. Stworzyli oni stronę, która imituje witrynę z domeny „gov.pl" na której umieścili złośliwe oprogramowanie. Za pośrednictwem wiadomości sms rozsyłali treści nakłaniające do zainstalowania programu, który na podstawie nagrania kaszlu miał stwierdzić czy dany użytkownik jest zakażony koronawirusem czy też nie (ryc.7). Instalacja fałszywej aplikacji STOP COVID, wymuszała na odbiorcy przyznanie dostępu do powiadomień jak również umożliwiała sprawdzanie zawartości okna, z którego korzysta użytkownik. W ten sposób cyberoszuści pozyskiwali poufne dane logowania do bankowości mobilnej i potwierdzenia transakcji.

Źródło: CERT Polska.
Ryc.6. Przykład fałszywej strony aplikacji



Źródło: CERT Polska.

Ryc.7. Przykład fałszywej strony aplikacji

Ataki związane ze zdalną edukacją

W związku z COVID-19 edukacja zdalna rozpoczęła się zupełnie nieplanowanie. Grono publicznych placówek takich jak przedszkola, szkoły czy uczelnie wyższe zmuszone były zmierzyć się z trybem nauczania online. W użytku jest wiele narzędzi cyfrowych, które umożliwiają przeprowadzenie lekcji w trybie zdalnym. Zdalna edukacja stała się wyzwaniem nie tylko dla w/w placówek, ale również dla uczniów, nauczycieli oraz rodziców, którzy poniekąd zmuszeni zostali do jej eksploatacji w życiu codziennym. Wachlarz narzędzi elektronicznych z jakich w obecnych czasach korzystamy jest ogromny: od komputera, tabletu, telefonu, po narzędzia konferencyjne. Należy mieć na uwadze, że każdy z nich jest potencjalnie podatny na przyjęcie cyberataku.

W związku ze zdalną edukacją pojawiło się również wiele problemów związanych z nieprawidłowym wyskalowaniem usług. Tuż po rozpoczęciu obowiązkowych lekcji w trybie online, zaprzestał działać jeden z najbardziej popularnych dzienników elektronicznych - Librus. Jest on narzędziem wykorzystywanym do komunikacji między nauczycielami a uczniami. Służy do rejestracji przebiegu nauczania, wglądu do obecności ucznia w szkole oraz jego ocen. Podczas zaistniałej awarii często zawieszał się lub wczytywał dane z ogromnym opóźnieniem, co uniemożliwiało poprawne wykonywanie pracy jego użytkownikom (ryc.7).

Bardzo podobna sytuacja miała też miejsce z innym dziennikiem elektronicznym jakim jest Vulcan. Wzmożony ruch, który był spowodowany wielokrotnością logowań, przyczynił się do zaistniałej awarii (ryc.8).

Librus padł pierwszego dnia obowiązkowych lekcji online. Mamy KOMENTARZ MEN

Dorota Kalinowska

25 marca 2020, 12:14

Ten tekst przeczytasz w mniej niż minutę

Udostępnij na Facebooku

Udostępnij na Twitterze

komputer / fot.Shutterstock

Tego samego dnia, kiedy rozpoczęły się obowiązkowe lekcje online, padł Librus, czyli popularny dziennik elektroniczny.

Źródło: https://edukacja.dziennik.pl/aktualnosci/artykuly/6467598,librus-szkola-lekcje-online-epidemia-covid-19-koronawirus-men.html.

Rys.7. Zaprzestanie funkcjonalności dziennika elektronicznego

Dziennik Zachodni › Wiadomości › Vulcan i Librus nie...

Vulcan i Librus nie działają. Brak możliwości logowania więc korzystamy z Google. Oświadczenie: szkolne dzienniki elektroniczne przeciążone

MCH 30 marca 2020, 7:25

Środa, 25 marca, miała być pierwszym dniem obowiązkowej nauki zdalnej, którą MEN wprowadził rozporządzeniem. Uczniowie nie mogą jej jednak rozpocząć, bo padły dzienniki elektroniczne - alarmują w Internecie nauczyciele. pixabay

Źródło: https://dziennikzachodni.pl/vulcan-i-librus-nie-dzialaja-brak-mozliwosci-logowania-wiec-korzystamy-z-google-oswiadczenie-szkolne-dzienniki-elektroniczne/ar/c1-14878571.

Ryc.8. Zaprzestanie funkcjonalności dzienników elektronicznych

W maju 2020 r. pojawiły się również ataki ukierunkowane na wyłudzanie danych do logowania do portalu Librus Rodzina. Została utworzona bardzo podobna domena phishingowa o nazwie „portalibrus[.]pl" różniąca się tylko jedną literką „–l" (ryc.9).

źródło: https://sekurak.pl/wyciagaja-w-banalny-sposob-loginy-hasla-od-uczniow-i-nauczycieli-falszywy-portalibrus-pl.

Ryc.9. Przykład podrobionej domeny

W marcu 2020 r. w Polsce doszło do ataku hakerskiego na serwery największego internetowego dziennika szkolnego. Sprawcy przez kilka godzin zakłócali jego funkcjonowanie przez co uniemożliwiali nauczycielom prowadzenie zajęć online. Na podstawie ustaleń śledczych z Komendy Wojewódzkiej Policji w Katowicach, wynika,że sprawcami ataków jest grupa nastolatków z różnych części Polski. Na prośbę śląskich policjantów zlecono przeszukanie mieszkań nieletnich, jak również zabezpieczono sprzęt.

Śledczy wpadli na trop hakerów po około dwumiesięcznej pracy. Okazało się nimi kilku nastolatków, którzy skontaktowali się ze sobą poprzez internet, postanawiając przeprowadzić wspólny atak na platformę e-dziennika. Z uwagi na fakt, że byli to mieszkańcy różnych województw, o pomoc

poproszono policjantów z komórek „cyber" w poszczególnych komendach wojewódzkich w Gdańsku, Krakowie, Poznaniu i Radomiu, którzy przeprowadzili m.in. przeszukania w mieszkaniach wytypowanych sprawców, zabezpieczając ich sprzęt komputerowy. Zebrany materiał dowodowy pozwolił już na przestawienie jednemu z nich - 18-latkowi z Warszawy - zarzutu ataku na infrastrukturę o szczególnym znaczeniu dla jednostek samorządu terytorialnego, za co może mu grozić do 8 lat więzienia[4]. (ryc.10).


cyberprzestępczość

Nastolatkowie włamali się do dziennika elektronicznego. Grozi im 8 lat więzienia

Marcin Pietraszewski 31 sierpnia 2020 | 09:40

1 ZDJĘCIE

©Agencja Gazeta

Dziennik elektroniczny (Fot. Dawid Chalimoniuk / Agencja Gazeta)

Źródło: https://katowice.wyborcza.pl/katowice/7,35063,26254257,nastolatkowie-wlamali-sie-do-dziennika-elektronicznego-grozi.html.

Ryc.10. Artykuł dot. włamania do dziennika elektronicznego- nastolatkowie wła-mali się do dziennika elektronicznego

[4] https://www.policja.pl/pol/aktualnosci/193077,Zarzuty-za-atak-hakerski-na-serwery-e-dziennika-podczas-pandemii-koronawirusa.html.

Czynu zabronionego związanego z włamaniem do elektronicznego dziennika dopuścił się również szesnastoletni uczeń z Mysłowic. Wykorzystał on nielegalnie zdobyte dane, zalogował się do systemu i napisał sobie zwolnienie z dwóch ostatnich lekcji. Niestety, ale wzbudził podejrzenia nauczyciela popełniając błędy ortograficzne. Sprawa znalazła swój finał w sądzie rodzinnym.

W kwietniu 2021 r. we Francji odnotowano ataki ukierunkowane na państwową sieć nauczania zdalnego. Po ponad siedmiu miesiącach zajęć stacjonarnych, kiedy uczniowie powrócili do nauki online, pojawiły się problemy z połączeniem internetowym. Sprawcami byli najprawdopodobniej „zagraniczni hakerzy”[5]. Analogiczny problem pojawił się również ponad rok wcześniej, podczas pierwszego lockdownu we Francji. Wówczas za cyberataki zostali oskarżeni Rosjanie.

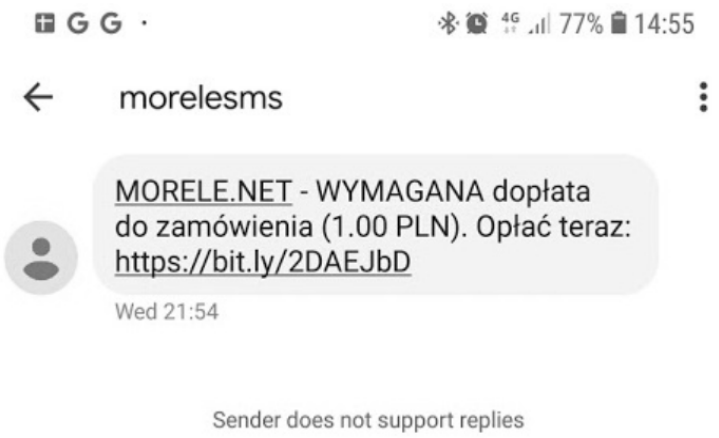
Ataki z wyorzystnaiem fałszywych stron agentów rozliczeniowych i banków

Już od 2017 r. można było zaobserwować pierwsze ataki z wykorzystaniem fałszywych stron agentów rozliczeniowych oraz banków. W dobie pandemii COVID-19 problem ten niestety nieustająco narasta.

Mechanizm sprawców polega na przesyłaniu smsów lub maili do osób z konkretną prośbą o dopłatę lub zapłatę do przeróżnego rodzaju przesyłek. W treści przesyłanej wiadomości znajduje się link do fałszywego panelu płatności. (ryc.20). W dobie pandemii pojawiło się wiele wiadomości z prośbą o dopłatę do przesyłek, ze względu na np. przekroczenie ich ciężaru oraz dopłatę do ogłoszeń umieszczonych w portalach takich jak olx.pl czy otomoto.pl.

[5] https://apnews.com/article/lifestyle-paris-distance-learning-coronavirus-pandemic-france-fabdd0fdd0c96d8d9618dcc1a48dff99

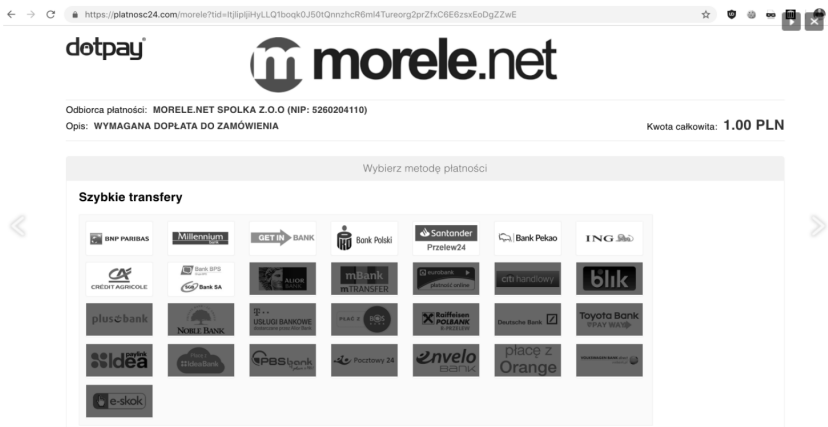
Pojawił się również atak związany z wyciekiem danych na stornie morele.net. Klienci sklepu internetowego po dokonaniu zakupu, otrzymywali wiadomości sms z prośbą o dopłatę do zamówienia kwoty w wysokości 1zł (ryc.11).



Źródło: https://zaufanatrzeciastrona.pl/post/uwaga-na-duza-fale-atakow-udajacych-posrednikow-szybkich-platnosci/.

Ryc.11. przykład oszukańczego SMS-a

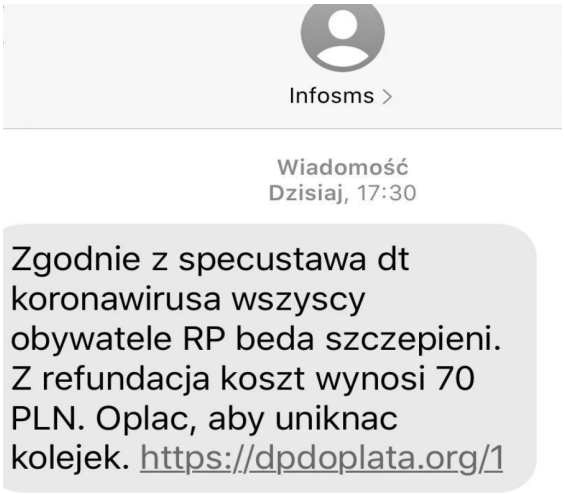
Po kliknięciu w umieszczony w smsie link odbiorca był przekierowywany na stronę (ryc.12) dzięki której przestępcy uzyskiwali poufne dane.



Źródło: https://zaufanatrzeciastrona.pl/post/uwaga-na-duza-fale-atakow-udajacych-posrednikow-szybkich-platnosci/.

Ryc.12. Przykład fałszywego panelu płatności

Tuż po wprowadzeniu obostrzeń związanych z lockdownem 13 marca 2020 r. pojawiły się dystrybucje wiadomości sms o n/w treści (ryc.13).

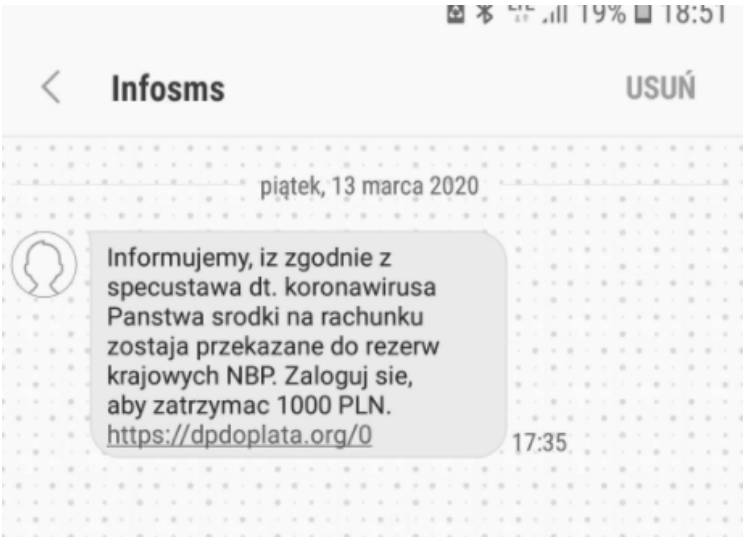


Źródło: CERT Polska.

Ryc.13. Przykład oszukańczego smsa

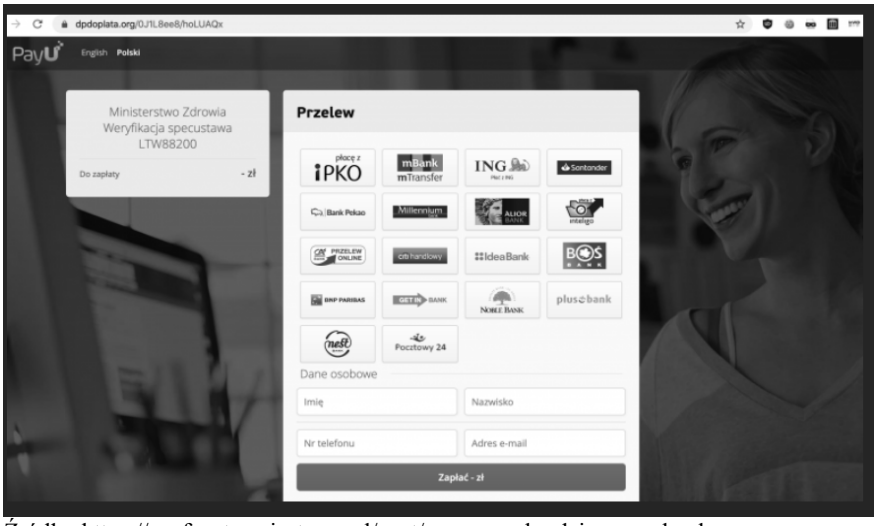
Oszuści zastosowali tu nową socjotechnikę związaną z koronawirusem. Domena, którą wykorzystali związana była z wcześniejszymi mechanizmami działania oszustów.

W tym samym okresie w tematyce związanej z pandemią, zaobserwowano atak, w którym cyberprzestępcy informowali o blokadzie środków na koncie, które miały być przekazane do rezerw krajowych NBP (ryc. 14). Przestępcy wykorzystali tą samą nazwę domenową oraz podszyli się pod agenta rozliczeniowego -spółkę payU (ryc.15).



Źródło: CERT Polska.

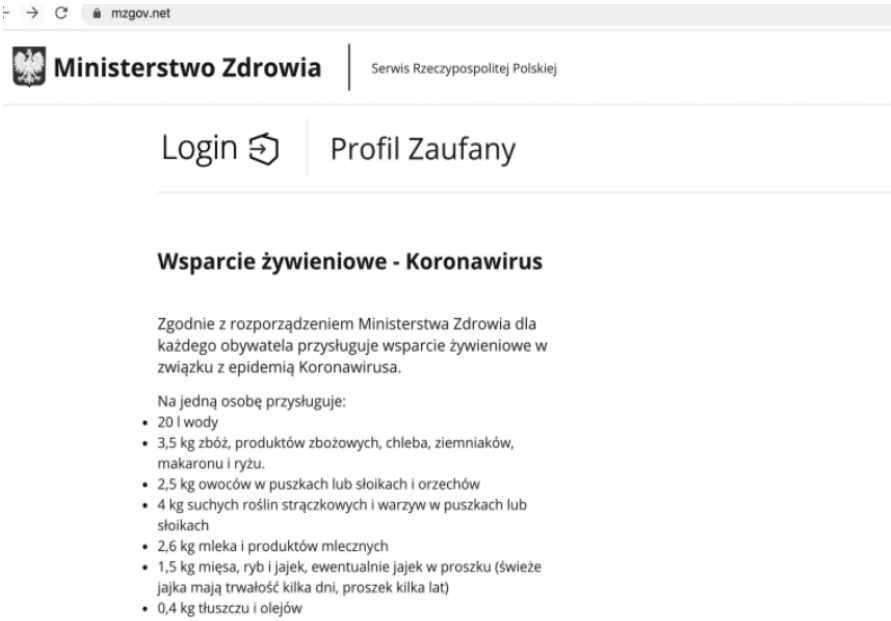
Ryc.14. Przykład oszukańczego smsa



Źródło: https://zaufanatrzeciastrona.pl/post/uwaga-na-kradziez-z-rachunku-na-koronawirusa/.

Ryc.15. Przykład fałszywego panelu płatności

Na początku pandemii można było zaobserwować również informacje o możliwości uzyskania od Ministerstwa Zdrowia wsparcia żywieniowego w związku z epidemią koronawirusa (ryc.16). Przestępcy wykorzystując odpowiednie narzędzia socjotechniki wyłudzali dane poprzez wejście za pośrednictwem banku do profilu zaufanego (rys.17).



Źródło: CERT Polska.

Ryc.16. Przykład fałszywej strony oferującej wsparcie żywieniowe

Źródło: https://zaufanatrzeciastrona.pl/post/nowy-atak-z-koronawirusem-w-tle-wsparcie-zywnosciowe-z-ministerstwa-zdrowia/.

Rys.17. Potwierdzanie danych osobowych poprzez profil zaufany za pomocą jednego z banków

Odnośnie dopłat do przesyłek, głównym działaniem sprawców było wymuszenie dopłaty do dezynfekcji paczki lub też dopłaty za przekroczenie ciężaru nadanej przesyłki. W sieci pojawiło się wiele fałszywych smsów (ryc.18).

Źródło: Internet.
Ryc.18. Przykłady fałszywych sms

Po kliknięciu w załączony w treści wiadomości link użytkownik wybierając logo swojego banku przekierowywany był na nieautentyczną stronę logowania dostosowaną do wybranego banku (ryc.19). Szablon tej witryny został stworzony celem umożliwienia przestępcom wyłudzenie danych. Dane wpisane przez ofiarę trafiały prosto do przestępców.

Źródło: https://www.cert.pl/uploads/docs/Raport_CP_2019.pdf.

Ryc.19. Przykładowa fałszywa strona logowania do bankowości ING

Źródło: Internet.
Ryc.20. Mechanizm działania cyberoszustów

Ransomware skierowany na służbę zdrowia

W ciągu ostatniej dekady świat stanął w obliczu wielu zagrożeń. Źródła tych zagrożeń nie są jednorodne. Co więcej granice między światem fizycznym a „cyber-światem" stają się coraz bardziej zatarte, ponieważ praktycznie wszystkie urządzenia są już podłączone do internetu.

W dobie pandemii COVID-19 coraz bardziej popularnym atakiem stało się infekowanie placówek ochrony zdrowia, oprogramowaniem ransomware w celu wyłudzenia okupu. Ataki na placówki medyczne stały się niezwykle istotne, z uwagi na możliwość wpływania na bezpieczeństwo, jak również zdrowie i życie ludzkie.

Sytuacja pandemiczna jest jednak permanentnie wykorzystywana przez cyberprzestępców, którzy jak podkreślają eksperci, atakują ten sektor z

uwagi na większą skłonność spełnienia żądań okupu biorąc pod uwagę okoliczności. Główną motywacją są względy finansowe. Na szczycie listy atakowanych regionów znajduje się Europa Środkowa, gdzie odnotowano rekordowy wzrost ataków o 145% w listopadzie 2020 r. Tuż za nią znajduje się Azja Wschodnia ze wzrostem 137% oraz Ameryka Łacińska z wynikiem 112% względem poprzedniego miesiąca. Analizując poszczególne kraje najbardziej dramatyczny wzrost odnotowano w Kanadzie, gdzie liczba ataków wzrosła o ponad 250%, a następnie w Niemczech - o 220%. Hiszpania natomiast odnotowała podwojenie liczby ataków[6].

We wrześniu 2020 r. w Wielkiej Brytanii oraz w Stanach Zjednoczonych nastąpił atak na systemy Universal Health Services Inc., który jest jednym z największych operatorów, obsługujących około 400 szpitali i ośrodków opiekuńczych. W wyniku powyższego cyberataku, niektóre szpitale musiały wypełniać informację o swoich pacjentach „ręcznie".

Jak wielka jest skala cyberataków ukierunkowanych w służbę zdrowia przedstawia projekt Safecare, który wskazuje i monitoruje incydenty bezpieczeństwa w szpitalach w miarę postępu kryzysu. Celem planu działania serwisu Safecare jest dostarczenie rozwiązań, które poprawiają bezpieczeństwo fizyczne i cyberbezpieczeństwo, w bezproblemowy i efektywny kosztowo sposób[7].

Na stronie internetowej „safecare-project.eu" umieszczane są ataki, które wymierzone zostały w placówki służby zdrowia na całym świecie (tabela 1).

[6] https://www.cyberdefence24.pl/pandemia-cyberprzestepczosci-dotyka-placowki-medyczne
[7] https://www.safecare-project.eu/

Date	Country	City	Cyber/Physical	Link
22/03/2020	USA	Wheeling	Physical	https://fox2now.com/news/national/dozens-of-masks-stolen-from-west-virginia-hospital-amid-coronavirus-pandemic/
18/03/2020	Germany	Weidenau	Physical	https://www.siegener-zeitung.de/siegen/c-lokales/25-jaehriger-klaut-unter-anderem-desinfektionsmittel_a196342
15/04/2021	USA	Washington DC	Cyber	https://healthitsecurity.com/news/hackers-steal-data-of-200k-during-carefirst-bluecross-dc-cyberattack
16/03/2020	UK	Warwick	Physical	https://www.leamingtoncourier.co.uk/news/people/people-steal-hand-sanitisers-warwick-hospital-2451776
15/02/2021	France	Villefranche	Cyber	https://www.francebleu.fr/infos/sante-sciences/l-hopital-de-villefranche-sur-saone-victime-d-une-attaque-informatique-apres-celui-de-dax-1613421523
19/03/2020	Italy	Verona	Physical	https://www.larena.it/territori/citt%C3%A0/continui-furti-di-gel-nei-reparti-una-cosa-indegna-1.7999039
26/11/2020	USA	Vermont	Cyber	https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html
16/03/2020	Italy	Verduno (CN) Piedmont	Physical	https://www.regione.piemonte.it/web/pinforma/notizie/apre-nuovo-ospedale-verduno-per-diventare-covid-hospital-piemonte
28/02/2020	Romania	Vaslui	Physical	https://www.digi24.ro/stiri/angajati-ai-spitalului-de-urgenta-vaslui-prinsi-cand-incercau-sa-fure-produse-sanitare-si-alimente-1267483
24/04/2020	Germany	Valer	Physical	https://www.presseportal.de/blaulicht/pm/68442/4585092

Tabela 1. Zestawienie wybranych cyberataków na placówki medyczne. Źródło: https://www.safecare-project.eu/?p=588

Jednym z pierwszym ataków, w dobie pandemii, było zainfekowanie szpitala klinicznego w Brnie w Czechach, który miał miejsce w marcu 2020 r. Personel szpitala prowadził testy na obecność koronawirusa i analizował wówczas około 20 próbek dziennie. Informacje o ataku zostały oficjalnie potwierdzone przez czeskiego premiera Andreja Babisza.

„Atak cybernetyczny nastąpił około drugiej w nocy. Stopniowo poszczególne systemy ulegały awarii, więc koniecznym było wyłączenie wszystkich komputerów" - powiedział dyrektor szpitala Jarosław Sterba[8].

Oprócz brneńskiego szpitala klinicznego cyberatakiem została również dotknięta jednostka dziecięco-położnicza. Placówka medyczna zmuszona była odwołać zaplanowane operacje, a część pacjentów zostało przetransportowanych do pobliskich szpitali.

[8] https://ct24.ceskatelevize.cz/domaci/3061748-fakultni-nemocnice-v-brne-celi-kybernetickemu-utoku-pise-idnescz

W szpitalu klinicznym przestały działać komputery przetwarzające dane pacjentów, co spowodowało również paraliż karetek pogotowia ratunkowego. Personel szpitala otrzymał całkowity zakaz uruchomiania wszelkich urządzeń zainfekowanych złośliwym oprogramowaniem.

Zdaniem niezależnego badacza i konsultanta ds. cyberbezpieczeństwa dr Łukasza Olejnika sytuacja była bardzo poważna, gdyż w dobie pandemii szpitale są w stanie przeciążenia a ryzyko paraliżu, z powodu infekcji złośliwym oprogramowaniem oraz utratą dostępu do danych, mogą nieść za sobą poważne konsekwencje.

Zdaniem byłego doradcy ds. cyberwojny Międzynarodowego Komitetu Czerwonego Krzyża w Genewie zdarzenia tego rodzaju "powodują wydłużenie czasu wykonywania procedur, a więc pośrednio mogą obecnie prowadzić nawet do utraty życia". Olejnik podkreślił, że ryzyko dla cyberbezpieczeństwa placówek medycznych w sytuacji zagrożenia epidemicznego wzrosło bardzo mocno, gdyż pandemia koronawirusa to "wcześniej zupełnie nieznana nam sytuacja, z której cyberprzestępcy i inne zorganizowane grupy niestety mogą próbować skorzystać"[9].

Ataki ransomware niosą za sobą nie tylko spustoszenie w systemach teleinformatycznych, ale również przynoszą śmiertelne ofiary. Za pierwszą śmiertelną ofiarę takiego ataku uznaje się kobietę w Niemczech, której na czas nie udzielono pomocy medycznej.

We wrześniu 2020 r. hakerzy zaszyfrowali dane co uniemożliwiło poprawne działanie systemów komputerowych, w Szpitalu Uniwersyteckim w Dusseldorfie. Systemy te były zakłócane przez tydzień, ulegały stopniowej awarii przez co nie było możliwości uzyskania dostępu do danych pacjentów. Na 30 serwerach zostało zaimplementowane szkodliwe oprogramowanie,

[9] https://www.pap.pl/pap-technologie/604452%2Chakerzy-zaatakowali-szpital-kliniczny-w-czeskim-brnie-nie-dzialaja-komputery

w wyniku, którego cyberprzestępcy przejęli całkowitą kontrolę nad systemami placówki. Decyzją władz szpitala koniecznym było przewiezienie pacjentki, która była w stanie krytycznym do placówki medycznej oddalonej o około 30 kilometrów. Nie było możliwości udzielenia jej pomocy na miejscu, gdyż sprzęt został zhakowany. Pacjentka wymagająca natychmiastowej pomocy medycznej zmarła po przewiezieniu w inne miejsce[10].

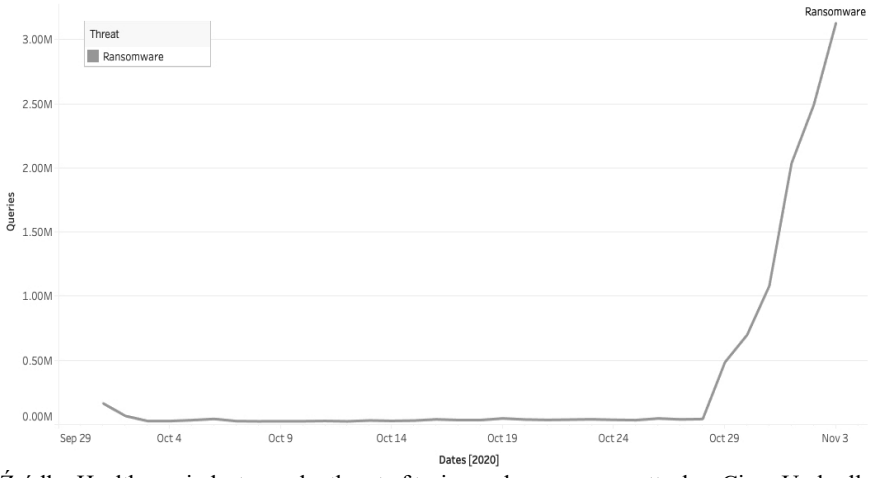
W grudniu 2020 r. miał miejsce atak hakerski na wrocławskie pogotowie. Informacja została potwierdzona przez dyrektor pogotowia-Zbigniewa Miądzkiego. Przez kilka godzin nie działał system komputerowy, którego zadaniem jest wspomaganie pracy dyspozytorów placówki. Prawdopodobnie cyberoszuści wykorzystali słabość zabezpieczeń systemów. Szczególnie istotnym jest fakt utraty ważności specjalistycznego oprogramowania. Personel Pogotowia Ratunkowego we Wrocławiu został powiadomiony o zdarzeniu dopiero po upływie 10 dni. Pracownicy pogotowia zostali poproszeni o utworzenie rachunków bankowych w Biurze Informacji Kredytowej. Miało to na celu zminimalizowanie ryzyka wykorzystania ich danych dla prawdopodobnego zaciągnięcia kredytów[11].

Niestety celem hakerów nie są tylko podmioty publiczne, wielkie koncerny, ale także instytucje ochrony zdrowia: placówki medyczne oraz szpitale. Podczas trwania pandemii COVID-19 jest to tendencja wyjątkowo niepokojąca, gdyż jednostki mające za zadanie ochronę zdrowia i życia stoją na „pierwszej linii frontu" w walce z koronawirusem (ryc.21).

---

[10] https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94

[11] https://gazetawroclawska.pl/atak-hakerow-na-wroclawskie-pogotowie-zablokowali-komputery-i-zazadali-okupu/ar/c1-15366679



Źródło: Healthcare industry under threat of trojan and ransomware attacks - Cisco Umbrella.

Ryc.21. Przykład ruchu ransomware, który wzrósł 7,8-krtonie w sektorze opieki zdrowotnej w ciągu jednego tygodnia w październiku 2020 r.

Zakończenie

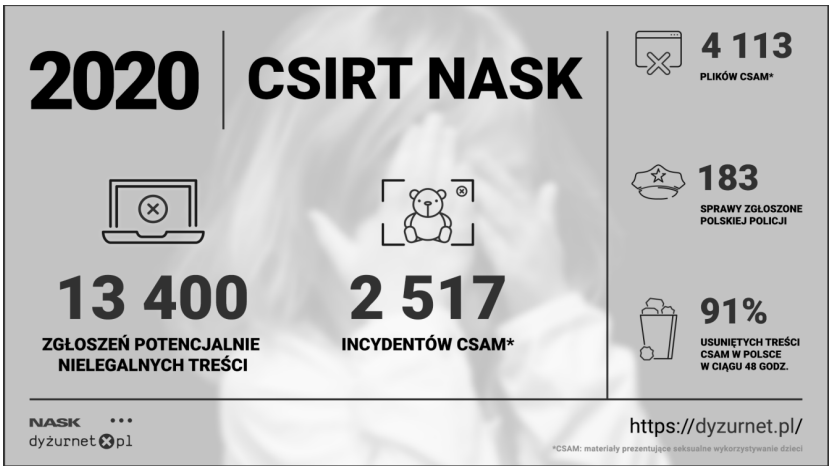
Sytuacjom kryzysowym towarzyszy często wzmożona aktywność oszustów i przestępców, którzy wykorzystują zamieszanie związane z funkcjonowaniem człowieka w nietypowych warunkach, a szczególnie w sytuacjach zagrożenia życia czy zdrowia. Nie inaczej jest w cyberprzestrzeni.

W przedstawionym rozdziale zostały opisane wybrane cyberzagrożenia z jakimi społeczeństwo zmaga się w dobie pandemii COVID-19. Powyższe treści nie wyczerpują wszystkich działań cyberprzestępców, którzy tak prężnie działają w sieci w obecnych czasach. Oprócz wymienionych powyżej zagrożeń rozwój pandemii spowodował stworzenie idealnego gruntu dla rozprzestrzeniania się fałszywych informacji tzw. „fake newsów". Według danych Instytutu Monitorowania Mediów liczba publikacji w mediach na temat

„fake newsów", w 2020 roku, wzrosła aż o 177 procent w porównaniu z rokiem poprzednim. Z uwagi na strach jaki towarzyszy podczas pandemii, ludzie są bardziej podatni na fałszywe informacje.

Wraz z pandemią COVID-19 wzrosła również liczba incydentów cyberprzemocy i zjawiska „sextortion" (szantaż online na tle seksualnym).

Niestety, ale widoczny jest również wzrost liczby incydentów związanych z seksualnym wykorzystaniem dzieci. Pod koniec 2020 r. liczba zgłoszeń dot. nielegalnych treści wynosiła 13,4 tys., a liczba zarejestrowanych incydentów CSAM (materiałów prezentujących seksualne wykorzystanie dzieci) przekroczyła 2,5 tys. (ryc.22). 183 sprawy zgłoszono policji, a zdecydowaną większość (91%) treści CSAM usunięto w ciągu 48 godzin[12].



Źródło: https://www.nask.pl/pl/aktualnosci/4151,CSIRT-NASK-w-2020-roku-coraz-wiecej-wyludzen-danych-i-oszustw-w-sieci.html.

Ryc.22. Liczby incydentów dot. nielegalnych treści

[12] https://www.nask.pl/pl/aktualnosci/4151,CSIRT-NASK-w-2020-roku-coraz-wiecej-wyludzen-danych-i-oszustw-w-sieci.html.

Jak wynika z analizy ekspertów CSIRT NASK, w 2020 r. zarejestrowano ponad 34,5 tys. zgłoszeń o potencjalnych zagrożeniach cyberbezpieczeństwa, w tym przeanalizowano ponad 10,4tys. incydentów bezpieczeństwa. Szczególne zainteresowania przestępców zwróciły urządzenia związane z Internetem Rzeczy (IoT). W tym samym czasie odnotowano niemal 6 tys. powiadomień o infekcjach tego typu urządzeń (ryc.23).

Źródło: https://www.nask.pl/pl/aktualnosci/4151,CSIRT-NASK-w-2020-roku-coraz-wiecej-wyludzen-danych-i-oszustw-w-sieci.html.

Ryc.23. Ilość incydentów zgłoszonych w 2020 r

Pandemia obecnie jest największym globalnym wyzwaniem. Jako że posiadamy nieskrępowany, swobodny dostęp do informacji musimy należycie weryfikować ich źródła i polegać na tych, które są wiarygodne i rzetelne. Przekazane w internecie treści wydają się zawsze być łatwo dostępne i wiarygodne. Niestety, ale jest to problem, z którym nie wszyscy sobie radzą - należy nauczyć się weryfikacji tychże treści.

Konieczność wdrażania przez firmy nowych technologii oraz narastające zainteresowanie bezpieczeństwem IT wiąże się z coraz częstszym korzystaniem z sieci 5G, urządzeniami IoT (ang. *Internet Of Things*), pracą zdalną, czy też korzystaniem z systemów opartych na rozwiązaniach chmurowych.

Według ekspertów Trend Micro wzrosła skala ataków na przedsiębiorstwa stosujące model AaaS (ang. *Access as a Service*), których celem są sieci domowe kluczowych pracowników, korporacyjne sieci IT i aplikacje działające w ramach internetu rzeczy[13].

Poza stosowaniem uniwersalnych środków ostrożności w sieci, w czasie pandemii warto:

1. Zawsze weryfikować organizatorów zbiórek internetowych - należy sprawdzić czy organizator danej zbiórki jest wiarygodny, zanim zapadnie decyzja o wsparciu jakiegoś celu,
czy jest to organizacja o ugruntowanej pozycji, czy figuruje w oficjalnych rejestrach (np. KRS). Jednym z przykładów sytuacji, która powinna budzić wątpliwości to: strona internetowa uruchomiona na potrzeby organizacji zbiórki pod pretekstem zebrania pieniędzy w bliżej nieokreślonym celu posługując jedynie tematem koronawirusa lub COVID-19.

2. Nie ryzykować przy zakupach w internecie - zakupy w sieci zawsze warto robić u znanych i sprawdzonych dystrybutorów, a najlepiej u takich, którzy mają program ochrony kupujących – można to sprawdzić w internecie . Lepiej poczekać na dostawę trochę dłużej niż stracić pieniądze, płacąc nieznanemu dostawcy za towar niewiadomego pochodzenia, którego można nigdy nie otrzymać. Należy być ostrożnym również z dzieleniem się swoimi danymi z przypadkowymi sprzedawcami.

3. Uważać na próby wyłudzenia danych z wykorzystaniem „fake news" - jak wspomniałam powyżej fałszywe informacje pojawiają się cały

[13] http://it-filolog.pl/cyberbezpieczenstwo-w-dobie-pandemii/

czas, prowadząc do dezinformacji i/lub paniki. Towarzyszą im nagłówki sformułowane w taki sposób, aby wywołać emocje i sprowokować do kliknięcia w dany link lub banner. Należy zawsze sprawdzić źródło informacji, nie klikać w przypadkowe linki i nie logować się za pomocą danych uwierzytelniających (np. do Facebooka), żeby obejrzeć filmik lub zobaczyć fotorelację.

4. Zachować zasadę ograniczonego zaufania przy korzystaniu z emaili, smsów i wszelkich komunikatorów - w sieci pojawia się bardzo dużo spamu ze „złośliwą" zawartością (np. o tytule „wypełnij formularz kwarantanny"). W sytuacji silnego stresu człowiek często podejmuje nieracjonalnie decyzje, czego następstwem może być otworzenie zainfekowanego załącznika. Przestępcy to wiedzą i wykorzystują. Jeśli otrzymamy emaila lub wiadomość z nieznanego źródła, należy być ostrożnym.

5. Otoczyć bliskich szczególną cyberopieką - należy uczulić bliskich na emaile czy smsy ze złośliwą zawartością, fałszywe zbiórki internetowe, sklepy i informacje. Jeżeli zauważy się ryzykowne, z perspektywy cyberbezpieczeństwa, zachowania bliskich osób w mediach społecznościowych (np. na Facebooku), warto skontaktować się z nimi bezpośrednio (np. przez telefon), wyjaśnić sytuację i zalecić ostrożność. Możliwe, że ich konto zostało przejęte i jest używane do propagowania złośliwych treści.

Niestety, ale wiele incydentów związanych z cyberbezpieczeństwem nadal pozostaje niezauważonych lub ich wykrycie zajmuje dużo czasu. Tylko dzięki zaangażowaniu wszystkich użytkowników sieci istnieje możliwość ograniczenia liczby incydentów bezpieczeństwa.

Abstract

SELECTED CYBER THREATS IN THE ERA OF COVID-19 PANDEMIC

Summary: The chapter presents examples of how criminals use emotionally significant events to commit cybercrimes.

Keywords: COVID-19, cybercrime.

Rozdział 13

Analyzing ransomware negotiations with CONTI: An in-depth analysis

DFIR Research Group, Team Cymru[1]

SUMMARY: CONTI is a ransomware group that uses a double extortion attack to force its victims into paying. The group has more than $14m confirmed payments in bitcoin and has several high-profile victims in its portfolio. The latter is verified by the publication of the exfiltrated data of the victims who do not pay the requested ransom. Given the modus operandi of the group, we managed to intercept many of their negotiations, which provided us with intelligence into how they operate. The studied interactions correspond to more than a third of their earnings and are therefore quite indicative of how they work as a group.

KEYWORDS: ransomware, CONTI, cybercrime, blockchain forensics.

1. Introduction

CONTI is a ransomware that uses the double extortion model to force their victims pay the ransom. In essence, the attackers will not only lock up

[1] Rozdział jest pracą zbiorową wymienionych dwóch organizacji. W razie pojawienia się konieczności kontaktu z autorami można to zrobić z: Anargyros Chryssanthou, Athena Research Center - a.chrysanthou@athenarc.gr, Constantinos Patsakis, University of Piraeus - kpatsak@gmail.com, Joshua Hopkins, Team Cymru - jhopkins@cymru.com.

a victim's files by encrypting them and demand ransom for their decryption, but they will also steal files and threaten to publish them on a website or otherwise leak them if their initial ransom request is not met. This model is not novel, as it has been introduced by MAZE and then used in other ransomware campaigns such as REvil, Ragnar, and Egregor, to name a few. The group is being operated in the Ransomware as a Service (RaaS) model. Therefore, there is a group of developers who have developed the ransomware and distribute it to some affiliates that they recruit. These affiliates will use it once they penetrate a host. Each party keeps a share of the paid ransom, which are paid in some cryptocurrency.

The confirmed earnings of the CONTI group, based on a specialised Open-Source Intelligence (OSINT) source that tracks ransomware - ransomwhere[2], are currently $14,740,000. These earnings position CONTI among the most highly paid ransomware and due to the high impact on USA-based organisations "caused" the Federal Bureau of Investigations (FBI) to issue a dedicated flash alert[3] and more recently the Cybersecurity and Infrastructure Security Agency (CISA) has also issued a dedicated alert[4]. In what follows, we provide an insight on the transactions of more than a third (34.96%) of CONTI earnings. According to the dedicated CONTI news site, which is currently available through the "open" web[5] and through TOR[6], there are more than 450 organisations that have been hacked, and some of their data are now publicly available.

The basic phases of the means of infiltration, which are utilized by

[2] https://ransomwhe.re/
[3] https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impacthealthcare-and-first-responder-networks-5-20-21.pdf
[4] https://us-cert.cisa.gov/ncas/alerts/aa21-265a
[5] https://continews.click
[6] https://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion

CONTI, are illustrated in Figure 1.

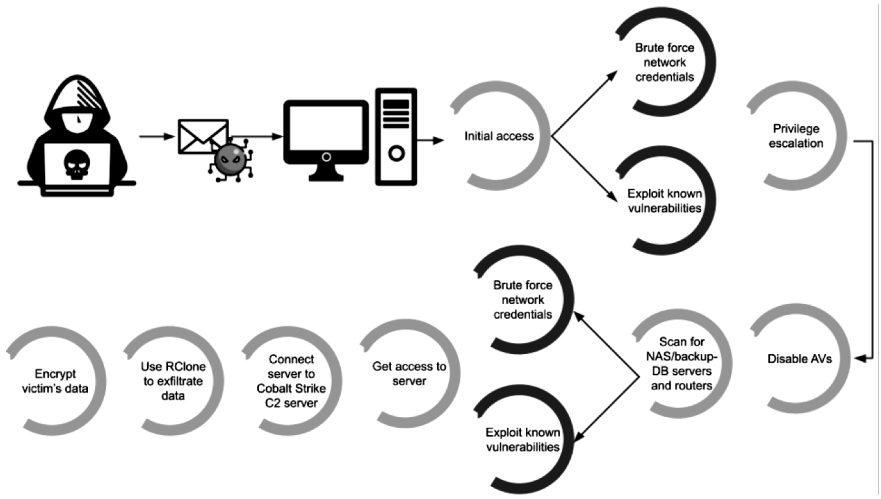


Figure 1. Overview of the CONTI Infiltration Process

In principle, infiltration starts with the attackers sending a phishing email to the potential victim. Once the victim opens the email and unbeknown to him/her runs the malicious dropper, the attackers get initial access to the victim's network and can execute code. Having gained initial access, the attackers try to establish a better foothold and perform lateral movement to perform the aimed objectives, with the end goal being to hold the victim hostage and force the victim to pay a ransom (a) to regain access to his/her data, which at the final stage of the attack are encrypted by CONTI, (b) to prevent publication/selling of his/her data.

In this context, the attackers try to brute force credentials, perform an LSASS memory dump, or even exploit some existing vulnerabilities to elevate privileges. Once this is done, the attackers try to turn off infected/infiltrated

systems' antivirus solutions (AVs) as well as other existing security mechanisms. Subsequently, the attackers will scan the network for other servers/workstations to gain additional access.

Then, the infected/infiltrated host(s) is (are) attached to a Cobalt Strike C2 server controlled by the attackers. Afterwards, the attackers use RClone[7] to upload the exfiltrated data to a cloud service (usually Mega[8]).

Finally, the attackers launch the ransomware "encryptor" to lock the victim's files. After the encryption, CONTI leaves a "README" file in each folder that it encrypts, which notifies the victim of the attack that his/her data have been encrypted and provides means to contact the CONTI team to pay the ransom and get the decryption software. In prior versions, the team used email addresses as means of communication. However, they developed a portal later, where users could contact CONTI using an ID that they were assigned. In these cases, the template of the ransomware notice is in the form of Figure 2.

[7] https://rclone.org/

[8] https://www.hhs.gov/sites/default/files/analyst-note-conti-ransomware-tlp-white.pdf

```
All of your files are currently encrypted by CONTI ransomware. If you try to use
any additional recovery software - the files might be damaged or lost.

To make sure that we REALLY CAN recover data - we offer you to decrypt samples.

You can contact us for further instructions through:

Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION :

https://contirecovery.xyz

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready
to publish it on out news website if you do not respond. So it will be better
for both sides if you contact us ASAP


---BEGIN ID---
1234abcd1234ABCD1234abcd1234ABCD1234abcd1234ABCD1234abcd1234ABCD
---END ID---
```

Figure 2. A Sample of the Ransomware Notice Left by CONTI

CONTI has been used in several attacks of high-profile organizations, has been deployed along BazarLoader[9], and is considered a stakeholder of the ransomware cartel, as a member of the Wizard Spider threat group (ClearSky Cyber Security 2021; DiMaggio 2021).

Up to now, there are many detailed technical reports about several ransomware and how they operate. Among them, many of these reports deal

[9] https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/

with CONTI[10]. Moreover, there are reports which showcase how CONTI works operates when infiltrating an organization[11].

More generally, there are studies about ransomware payments, economics (Laszka, Farhang, and Grossklags 2017; Hernandez-Castro, Cartwright, and Cartwright 2020) or theoretical strategies (Caporusso, Chea, and Abukhaled 2018; Cartwright, Hernandez Castro, and Cartwright 2019; Li and Liao 2020; Hofmann 2020).

To the best of our knowledge, this is the first public report about the actual negotiation process used in a ransomware campaign and not just about a small fragment of the process, e.g. (ClearSky Cyber Security 2021). The basic reason is that up to now, this intelligence was internal. Besides the perpetrator, only the victim and the delegated victim's personnel would have access to this information, while there would not be any further communication of this exchange beyond perhaps the payment wallet address.

Therefore, operational information, statistics about the steps of the performed negotiations, possible ransom discounts, errors, or even other requests of both sides are not publicly documented nor discussed. Filling this gap, this report provides a good insight into the internal operations of such processes and can be considered rather representative based on the profiles of the compromised organisations. Several patterns emerge from both negotiating sides (victims and ransomware operators) in terms of followed processes, existing pitfalls, and provided services.

We argue that this report sheds light on a very shady topic which, despite all technical and legal measures to counter it, remains a very thorny issue

[10] https://www.sentinelone.com/labs/conti-unpacked-understanding-ransomware-development-as-a-response-todetection/and https://unit42.paloaltonetworks.com/conti-ransomware-gang/

[11] https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/

for cybersecurity professionals and continues to grow as ransomware groups evolve their tactics.

Data collection methodology

To collect the samples for conducting our research, we used various open malware repositories and analysis services including, but not limited to Malware Bazaar, Triage, Hybrid Analysis, CAPE, JOE Sandbox, and VirusShare. Note that in all cases, we used publicly available samples.

Finally, it is worth highlighting that many web pages that discuss CONTI infections contain images that depict the ransomware notice without obfuscating the ID (see Figure 3).

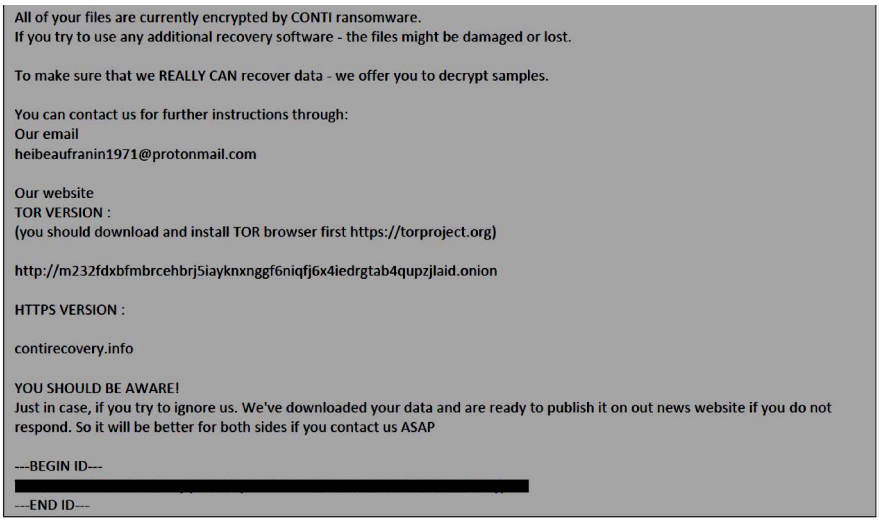


Figure 3. An Example of a CONTI Ransomware Note Including the Victim ID (Redacted)

The latter implies that the security consultants who shared these screenshots did not understand how they were publicly exposing their clients

for the sake of publicity. The same applies to security consultants or internal IT/security teams, who uploaded the collected samples to malware analysis services, to have them analysed, without realizing that in this way they put the targeted organisations at risk by revealing potentially targeted / maybe even internal not publicly available information[12], as well as useful intelligence to any attackers, which might attempt a newer attack to the organisations, on how the latter handle malware-related incidents.

While there are several hundreds of CONTI samples online, the number of unique IDs is quite limited, which implies that during several campaigns, the spear-phishing emails may have contained different droppers; however, the encryptor (delivered in the final stage of the attack - the encryption phase -) that was used contained a specific ID per victim at a time, which we later noticed that was reused. Notably, in many of the collected samples, one may notice that the ransomware notice asks the victim to contact the attacker by using ProtonMail, an email service provider which is well-known for the provided privacy and security features and provides also an "open" web[13] and a TOR website URL[14] [15]. This is especially relevant for the first versions of CONTI.

---

[12] see for example https://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/, https://krebsonsecurity.com/wp-content/uploads/2014/01/POSWDS-ThreatExpert-Report.pdf and https://www.qualityplusconsulting.com/res/pos/2014-1-24_InsideTargetBreach_Dell.pdf, where in Target data breach incident the used POS malware, based on relevant reports, was uploaded to Symantec, and contained an internal IP address and as believed by information security researchers, a domain name in Target's network

[13] https://contirecovery.info

[14] http://m232fdxbfmbrcehbrj5iayknxnggf6niqfj6x4iedrgtab4qupzjlaid.onion

[15] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5759-ccn-cert-id-02-21-conti-v3-ransomware-1/file.html

Table 1 illustrates some of these email addresses used by the earlier versions of CONTI. In many of the most recent collected samples, the ID is hardcoded within the binary and, in most cases, can be extracted by simply collecting the strings of the binary. The same applies to the used Protonmail email addresses[16].

Email address
elsleepamlen1988@protonmail.com
southbvilolor1973@protonmail.com
maxgary777@protonmail.com
ranosfinger@protonmail.com
polzarutu1982@protonmail.com
flapalinta1950@protonmail.com
xersami@protonmail.com
heibeaufranin1971@protonmail.com

Table 1. Some of the ProtonMail email addresses used by CONTI

In total, we extracted 115 unique IDs that we used to connect to the CONTI negotiation platform and extract the relevant negotiations in HTML format. From these IDs, 68 were valid, and 47 contained negotiations or confirmed victims, i.e., the CONTI operators expected input from the victims.

Negotiations

The CONTI negotiations in general are relatively short, but they may last several weeks. The victims are communicating with the CONTI team

[16] More ProtonMail email addresses used by Conti exist in various OSINT sources, ex. https://www.pcrisk.com/removalguides/17011-conti-ransomware

through the provided CONTI Recovery Service links that are left in the ransomware notice and discuss the means of infiltration and encryption of their data. Please note that in the first versions of CONTI, the negotiations were initiated through email exchanges. Gradually, in the later versions, the CONTI team developed a specialised platform for the negotiations. The webpage was available on the "open" web with various TLDs (.top, .xyz, .best, etc.) and also through TOR. At the time of writing, it is available through web[17] and through TOR[18].

The site's design changes over time from the form of Figure 4 to the form of Figure 5.

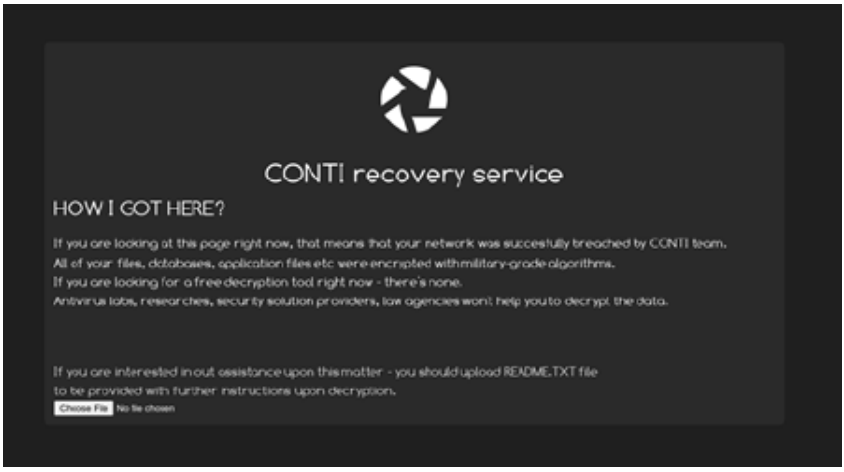


Figure 4. Recovery Site of CONTI (contirecovery.best - contirecovery.info)

[17] https://contirecovery.ws

[18] https://http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

In principle, each victim is assigned with an ID that consists of 64 alphanumeric characters, and the victim must upload the README file to the web form as displayed in Figure 5.

In most cases, the CONTI team requires the representative of the victim to identify himself/herself as well as the victim organization. The latter implies that the people performing the negotiations are not always the same ones who penetrated the victim as the attacker should already know who the victim is.

Nevertheless, on several occasions, the chat is prepared, welcoming the victim organization with their title. If there is no interaction from the victims, the CONTI team starts issuing threats, which initially concern the publication of the collected data on the CONTI News site, with additional threats to sell access to the data. See Figure 6.

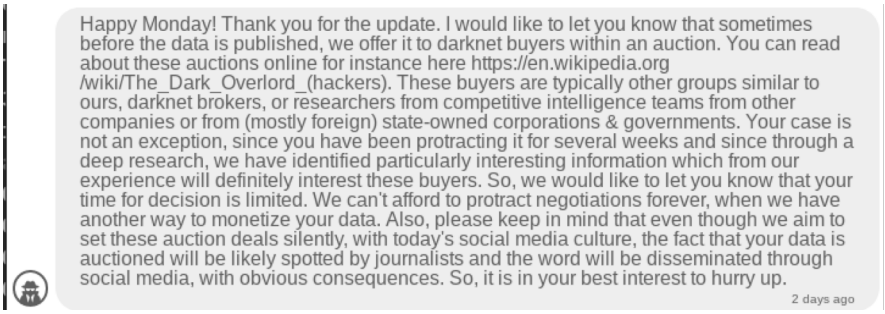


Figure 6. CONTI Team Threatening to Sell the Victim's Data

On several occasions, the CONTI team notifies the victims, which did not give in to their threats before the deadline provided by the CONTI team, that the publication of their data has started/finished and/or that a buyer for the data has been found. The chat activity is occasionally monitored by the operators, e.g., that a person logged in, see Figure 7.

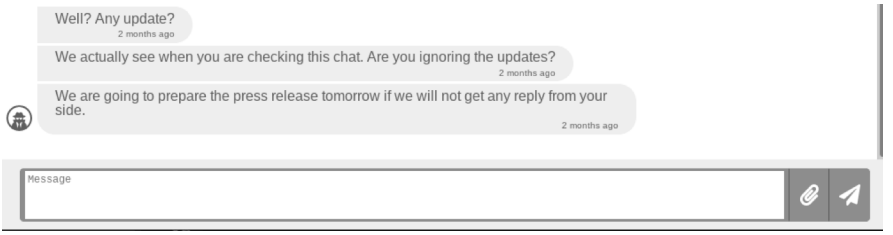


Figure 7. Excerpt from the CONTI Negotiation Platform

The threats for publication/selling of the data, in the beginning, do not have a strict nor specific deadline. Depending on the interaction of the victim with the CONTI team (or lack of it), they evolve from generic to 'soon', 'next week', etc. Refer to Figure 7 for an example of a generic deadline.

When victims decide to negotiate the price, typically, they require a guarantee that their files will be recovered. Therefore, CONTI operators provide a 'data pack' as they call it, which shows through the contained files the name of the victim and usually 30% of the directory listing tree for the encrypted files. Moreover, they might ask the victim to "provide two files for a test decryption", which they subsequently decrypt. The decrypted files as well as the 'data pack' are provided to the victims through various usually "obscure" file services. More precisely, for exchanging files with the victims, the CONTI team uses the following services:

https://qaz.im/
https://transfer.sh/
https://dropmefiles.com/
https://www.sendspace.com/

The main reason for using these services is probably some of their features, e.g., the services provide a deletion mechanism for the recipient of the uploaded files, they are free, they do not require strong authentication.

The exchanged files are encrypted by using default mechanisms (e.g., the embedded encryption mechanism of compression programs) and simple

passwords (e.g., 123123) to prevent compatibility issues for the recipients of the files.

After the introductions, the negotiation starts with an initial ransom price from the CONTI team. Since all the negotiations did not lead to a deal, we report in Table 2 the initially requested ransom and the agreed one that was paid for the payments that we could verify through the bitcoin transactions.

Initially requested ransom	Paid ransom	Steps	BTC
1,250,000	1,000,000	1	20.05326047
3,000,000	800,000	6	17.084
5,000,000	746,500	6	15.43
999,000	512,000	8	10.22997602
900,000	450,000	6	8.00275566
1,500,000	350,000	10	9.69536871
900,000	325,000	15	8.90692000
980,000	300,000	7	7.87000000
400,000	200,000	9	5.42840261
1,700,000	120,000	8	2.61000000
300,000	150,000	5	2.46426081
200,000	100,000	7	2.46426081
150,000	100,000	3	2.65200000
Total:	3,607,000	7 (average)	112.8912051

Table 2. Statistics from the confirmed payments of the collected negotiations

Moreover, we report in sum the negotiation steps (how many different ransom amounts were asked by CONTI team and how many counteroffers the victims performed) as well as the ransom amounts in Bitcoin, which were paid to the corresponding wallets.

It should be highlighted that the attackers use the financial status and public reports of each separate victim to assess the requested ransom and stress this information through the discussions to press for increased prices. The latter is verified by the operational/training documents of the group, which were leaked in August by a "disgruntled employee", who "left" the group.

After the payment is made by the victims, CONTI operators provide the victim with a decryptor. A typical issue of the decryptor, which is reported by the victims, is that many files, subsequent to have been decrypted, keep the added ransomware extension (e.g., LSNWX as in the intercepted chats and according to other sources[19]), which the victim has to manually remove, to access the decrypted files.

On some occasions, the victims requested feedback on how the attack was made. The response from the operators was rather generic as, e.g., the corresponding person was "inaccessible". The operators notified that an employee opened a malicious link/attachment on an email that gave them access to the host to execute malicious code. From there, they only report the use of Mimikatz and other tools, as well as that they performed lateral movement to extract the domain/admin passwords. The latter is also aligned with the leaked operational/training documents of the group.

In some instances, the operators recommend their victims to use SentinelOne, Kaspersky, or Symantec security solutions, see Figure 8. Note again that the leaked operational/training documents of the group contained instructions on how to turn off Microsoft Defender and Sophos AV solutions. Apart from the decryptor, they often provide the log file of gshred, which they used to shred the files that they exfiltrated from their victim.

[19] https://www.splunk.com/en_us/blog/security/conti-threat-research-update-and-detections.html.

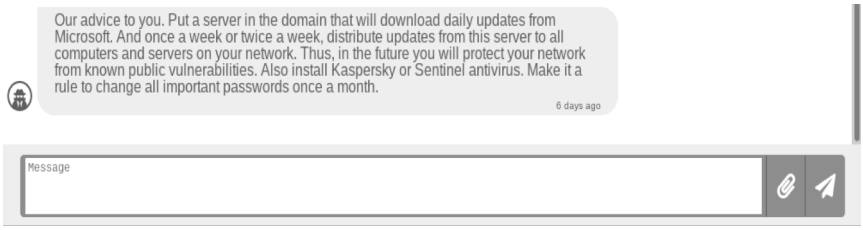


Figure 8. Security 'Advice' From the Negotiators After the Payment

It should be noted that in one negotiation the team admitted having lost the files during exfiltration. Therefore, since the extortion for publishing the files could not work for them, they proposed a discount of 50% to the victim for the decryption tool, see Figure 9.

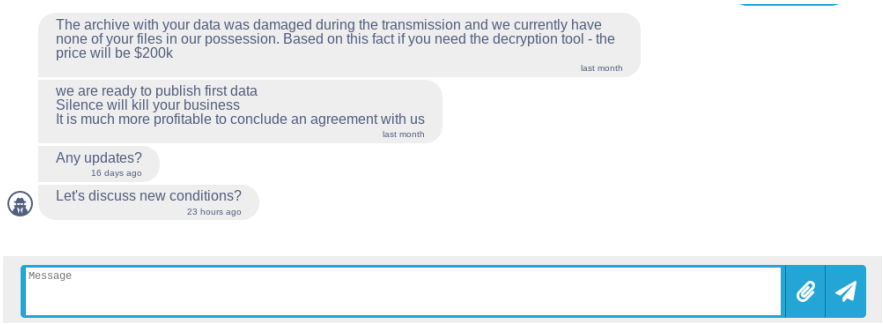


Figure 9. Notification of Losing the Victim's Files

Examples have also been observed where the victims have successfully negotiated the payment of the ransom in smaller chunks, see Figure 10.

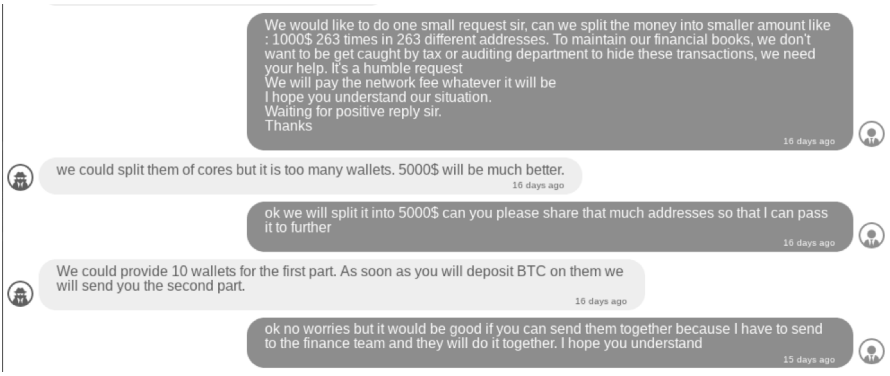


Figure 10. Request for payments in smaller chunks

We should also highlight that some negotiators seem to be aware that people may monitor these negotiations. Therefore, they may specifically request the deletion of these chats, see Figure 11.

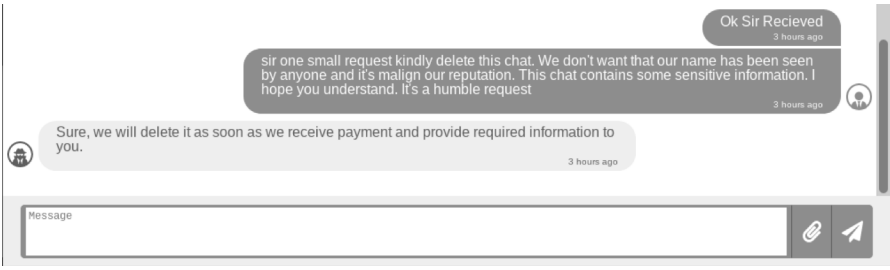


Figure 11. Request for Chat Deletion

Finally, of specific interest is the very well-known case of the Irish Health Service Executive (HSE)[20]. The initially requested price was $19,999,000. The HSE representative asked the team only for proof that they

[20] https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/

indeed had access to the data. After the proof was provided, it is probable that the public outcry forced the CONTI team to provide the decryptor for free without any further discussion. Then, the HSE side proceeded with notifying the perpetrators of the legal actions that had been initiated against them.

Since there was no payment, CONTI team notified that they would try to sell the collected data. Notably, this negotiation was trolled by another person who accessed the relevant ID negotiation page.

Discussion

While it is rather common to share malware samples, it is rather odd to have such samples in the open. Clearly, the infected organizations or the tasked analysts opted toupload the samples as public samples without thinking of the consequences. In essence, without prior analysis, this is a rather lousy practice since, in targeted attacks, this may leak sensitive information.

Indeed, despite the fact this allows for snooping of the negotiations, it also impedes the process. As observed, third parties had intervened and 'trolled' the negotiations twice (not only in the HSE case) or made the perpetrators see that there is traffic and expect interactions from their victims when this was not the case. In an isolated case, the negotiations were continued in another platform since they were conducted with someone that according to the victim, should not have access to them. Even more, in several cases, the victims did not request proof of the decryption of their files or the shredding log, which shows a lack of capacity in handling such cases.

We should report that we have three cases where we do not have the full negotiations. Therefore, we do not know how they ended nor any bitcoin address to determine whether the victims paid the requested ransom. However, the victims are not listed in the exposure web page.

A very interesting finding has to do with the handling of the negotiations. As discussed, one would expect that each ID is targeted to a single organization, as this would be a result of a spear-phishing campaign. However,

the latter is not actually the case as we have noticed that the same IDs are used with new victims. Therefore, previous victims may look at the negotiations of new victims.

Moreover, we have observed that the negotiation chat is occasionally cleared. More precisely, not all chats are available continuously and not to their full extent. In fact, we have observed the removal of fragments of the discussion, with the most noticeable being the removal of bitcoin addresses. This implies that the operator of each negotiation has the option to clear part of the chat and that different operators could be assigned per ID. The reuse of IDs may imply the use of the same encryption key, so decryptors may work for other victims; however, with the ones at hand, this claim cannot be verified.

It should also be noted that the operators reuse a lot of wordings for, e.g., salutation, requesting interaction, ransom bidding. For instance, the exact same wording as in

Figure 12 has been intercepted more than once. Indicatively, we point out that the exact same text with Figure 8 is used in another chat with the sole change that instead of Kaspersky, it was referring to Symantec. The above implies that apart from the leaked training/operational manuals, there is another 'playbook' for the negotiations, which includes what should be said and how.

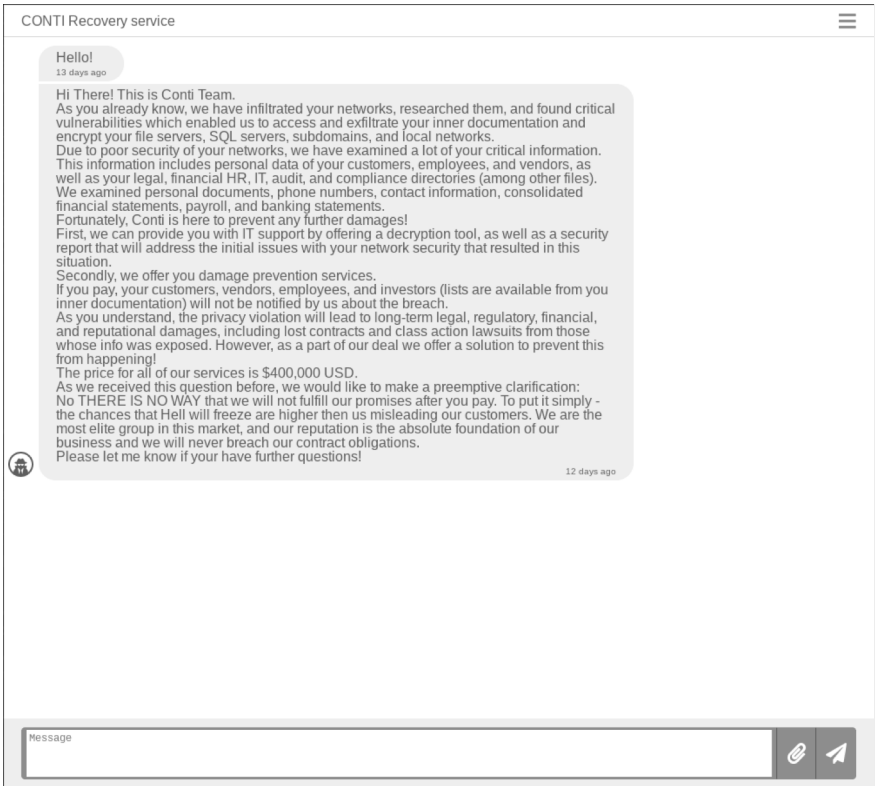


Figure 12. Reused salutation by the CONTI team

During the negotiations, the operators try to appear as professionals, to belong to a greater group as in a formal organization and to be friendly to the victim without initiating further discussions. In fact, the group has been reported to be recruiting people through advertisements[21]. The negotiation de-

[21] https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-one/

pending on the organization, may take several iterations and immediate payments are favored and discounted. The negotiators of the CONTI group, appearing as professionals, sometimes mention their victims as customers/clients and not as victims.

Finally, after the recent leaks of chats on the media, CONTI has introduced a CAPTCHA mechanism in the negotiation site.

Conclusion

The authors of this work do not by any means promote the payment of ransom. On the contrary, we illustrate how this trend has evolved into a multi-million industry worldwide and made organizations suffer. We illustrate in this research that several practices, such as sharing malware samples without proper sanitization of the binary, may have a boomerang effect on the victim by further exposing him/her.

Indeed, one can understand how such negotiations could be derailed by third parties entering the negotiations. Moreover, even if the victim paid for the ransom, third parties had access to the sensitive data and that the exposure could be even more augmented.

In a wilder scenario, another adversary could jump in the conversation and convince the victim of being the original adversary and luring him/her into paying the ransom in another wallet or double encrypting the victim's files.

Given the public leaks and their size, an obvious question that should be investigated is whether the victim organizations have reported these attacks appropriately, as legal obligations of, e.g., GDPR, set specific deadlines for these actions. The question is even more relevant for the cases of organizations that paid the ransom and whose data leakages cannot be verified through the public leaks. In fact, the legal implications are an aspect that the CONTI team is often trying to use to convince their victims in paying the ransom, see Figure 13.

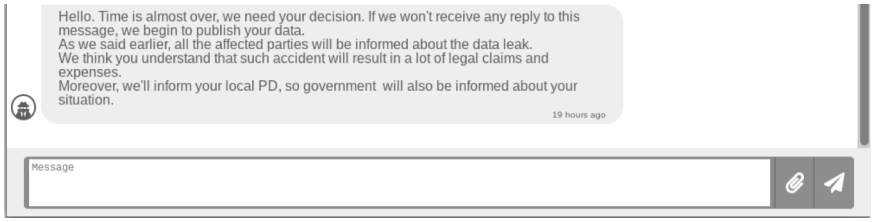


Figure 13. Stressing of Legal Obligations by the CONTI Negotiator

References

1. Caporusso N., Singhtararaksme Ch., and Raied A. 2018. "A Game- Theoretical Model of Ransomware." In International Conference on Applied Human Factors and Ergonomics, 69–78. Springer.
2. Cartwright E., Hernandez Castro J., and Cartwright A. 2019. "To Pay or Not: Game Theoretic Models of Ransomware." Journal of Cybersecurity 5 (1): tyz009.
3. Clearsky Cyber Security. 2021. "Conti Modus Operandi and Bitcoin Tracking." https://www.clearskysec.com/wp-content/uploads/2021/02/conti-ransomware.pdf.
4. Dimaggio J. 2021. "Ransom Mafia. Analysis of the World's First Ransomware Cartel." https://analyst1.com/file-assets/ransom-mafia-analysis-of-theworld%E2%80%99s-first-ransomware-cartel.pdf.
5. Hernandez Castro J., Cartwright A., and Cartwright E. 2020. "An Economic Analysis of Ransomware and its Welfare Consequences." Royal Society Open Science 7 (3): 190023.
6. Hofmann T. 2020. "How Organizations Can Ethically Negotiate Ransomware Payments." Network Security 2020 (10): 13–17.
7. Laszka A., Farhang S., and Grossklags J. 2017. "On the Economics of Ransomware." In International Conference on Decision and Game Theory for Security, 397–417. Springer.
8. Zhen L., and Liao Q. 2020. "Ransomware 2.0: To Sell, Or Not To Sell a Game-Theoretical Model of Data-Selling Ransomware." In Proceedings

of the 15th International Conference on Availability, Reliability and Security, 1–9.

Abstrakt

ANALIZOWANIE NEGOCJACJI RANSOWAREOWYCH Z CONTI: POGŁĘBIONA ANALIZA

Streszczenie: Celem niniejszego rozdziału jest przedstawienie wybranych cyberzagrożeń mogących wpływać na bezpieczeństwo systemów teleinformatycznych wywołanych atakami pochodzącymi z cyberprzestrzeni, a także analiza wybranych zagrożeń w kontekście tematów poruszanych podczas międzynarodowej konferencji na temat cyberbezpieczeństwa morskiego.

Słowa Kluczowe: ransomware, CONTI, cyberprzestępczość, analiza kryminalistyczna blockchain.