Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury
Quarterly of the National School of Judiciary and Public Prosecution
Zeszyt 1 (45)/2022

Aktywność zorganizowanych grup przestępczych w cyberprzestrzeni w czasach pandemii – analiza wybranych podatności i metod anonimizacji

DOI:10.53024/4.1.45.2022

PIOTR ZALEWSKI*, PIOTR SZYMAŃSKI**

STRESZCZENIE
Przedmiotem opracowania jest próba przedstawienia problematyki wybranych metod aktywności przestępców, którzy dzięki intensywnemu rozwojowi Internetu, a także zaawansowanych technologii komputerowych i telekomunikacyjnych, dokonują oszustw na szkodę uczestników sektora e-usług i rynków walutowych, przy wykorzystaniu podatności tych obiektów na wybrane ataki przestępcze. W konkluzjach przedstawiono jeden z modeli postępowania organów ścigania, który pozwala na skuteczne rozpoznanie tego typu zjawisk na etapie wykrywczym i dowodowym.

Słowa kluczowe: cyberprzestępczość, cyberbezpieczeństwo, oszustwo, Internet, współpraca międzynarodowa organów ścigania

1. WPROWADZENIE

Dynamiczne zmiany, jakie zachodzą we współczesnym świecie, stały się impulsem do rewolucyjnych przemian różnych dziedzin życia, które dały społeczeństwom i jednostkom nowe możliwości rozwoju i stają się nieustannie źródłem nieznanych dotąd możliwości. Szczególnym znakiem rozpoznawczym końca XX w. stał się rozwój technologiczny, który wprowadził do otaczającej nas rzeczywistości nowe znaczenia i konteksty znanych już kategorii społecznych. Zmienia się nie tylko sposób funkcjonowania jednostek, społeczeństw i państw, ale i wzajemne relacje, jakie zachodzą na różnych ich poziomach.

* Młodszy inspektor dr Piotr Zalewski – Zastępca Komendanta Wojewódzkiego Policji w Rzeszowie, Uniwersytet Jana Kochanowskiego w Kielcach.
** Młodszy inspektor Piotr Szymański – Naczelnik Wydziału do walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Rzeszowie.

Rozwój technologiczny wytworzył koniunkturę na różne usługi świadczone drogą elektroniczną, co sprawiło, że na przestrzeni ostatnich dwudziestu lat osoby prywatne, przedsiębiorstwa, a nawet w pewnym stopniu administracja państwowa, praktycznie w całości przeniosły swoją aktywność w określonych obszarach ze świata realnego do cyberprzestrzeni[1]. Proces, który odbywał się zgodnie z dynamiką możliwości technicznych i rosnących potrzeb odbiorców, zmierzał nieuchronnie do wykorzystania sieci teleinformatycznych w praktycznie każdej dziedzinie biznesu na coraz większą skalę. Został on zdynamizowany przez pandemię COVID-19 i wynikające z niej ograniczenia ludzkiej aktywności w świecie rzeczywistym.

Wzrostowi zakresu usług świadczonych drogą elektroniczną, a tym samym liczby potencjalnych ich odbiorców, towarzyszy wzrost poziomu nieznanych dotąd ryzyk i zagrożeń bezpieczeństwa użytkowników. Jako poziom bezpieczeństwa należy rozumieć świadomość zagrożeń bezpieczeństwa odbiorców e-usług oraz możliwości adekwatnego zapobiegania i reagowania. Te dwie składowe bezpośrednio określają poziom podatności klientów szeroko rozumianych usług elektronicznych na mechanizmy przestępczego ataku wykorzystywane przez cyberprzestępców[2].

Sprawcy przestępstw popełnianych z wykorzystaniem sieci teleinformatycznych, tzw. cyberprzestępstw, posiadają doskonałe rozpoznanie w zakresie podatności zarówno mechanizmów bezpieczeństwa, stosowanych przy świadczeniu różnego rodzaju e-usług, jak i końcowych odbiorców tych usług. To właśnie zdiagnozowane podatności bezpośrednio wpływają na dobór mechanizmów przestępczych, w tym w szczególności sposobów maskowania tożsamości, technik inżynierii społecznej oraz rodzaju stosowanego ataku, pozwalających skutecznie dążyć do osiągnięcia założonego celu przestępczego, jakim w zdecydowanej większości są pieniądze pokrzywdzonych.

W niniejszym opracowaniu autorzy przybliżą wybrane metody aktywności przestępczej sprawców wykorzystujących możliwości zaawansowanych technologii

---

[1] Cyberprzestrzeń, wg. T. Aleksandrowicza definiowana jest jako „(…) całość powiązań ludzkiej działalności z udziałem ICT (*Information and Communication Technology*) (…), mianem cyberprzestrzeni (*cyberspace*) określa się sieć łączącą systemy komputerowe obejmujące jednostki centralne i ich oprogramowanie, ale także dane, sposoby i środki ich przesyłania. Cyberprzestrzeń obejmuje systemy powiązań internetowych, usługi teleinformatyczne oraz systemy zapewniające prawidłowe funkcjonowanie kraju, tj. systemy transportu, łączności, systemy infrastruktury energetycznej, wodociągowej i gazowej czy ochrony zdrowia (…)" charakteryzuje się ona takimi cechami jak „(…) niezależność od miejsca, niezależność od odległości, niezależność od czasu, niezależność od granic, względna anonimowość, możliwość ustalenia sprzętu, nie osoby" – T. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15(8), s. 11.

[2] M. Hajduk-Stelmachowicz, K. Iwan, *Zarządzanie bezpieczeństwem informacji w obszarze bankowości elektronicznej wobec zjawiska cyberprzestępczości – aspekt indywidualny*, „Roczniki Kolegium Analiz Ekonomicznych" 2018, nr 49, s. 493.

komputerowych i telekomunikacyjnych oraz wskażą rozpoznane podatności obiektów na wybrane ataki przestępcze. Celem artykułu jest zaproponowanie optymalnego modelu działania organów ścigania, tak na etapie wykrywczym i dowodowym, jak i w perspektywie prewencji kryminalnej. Rozpoznanie omawianej problematyki to efekt doświadczenia zawodowego autorów, uzupełnionego analizą opracowań teoretycznych – literatury krajowej oraz zagranicznej, co pozwoliło na praktyczne zastosowanie i wskazanie rozwiązań możliwych w tej płaszczyźnie.

Punktem wyjścia do omówienia wskazanej problematyki jest charakterystyka zjawiska cyberprzestępczości, szczególnie w zakresie przestępstw ukierunkowanych na inwestycje na rynku finansowym – forex[3] kryptowalut[4], 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 wypracowania procedury przeprowadzanej w ramach czynności prewencyjnych oraz procesowych. Wskazane w niniejszym opracowaniu rozwiązania mogą przyczynić się do zwiększenia skuteczności w zakresie przeciwdziałania cyberprzestępczości w omawianym zakresie.

2. ZAGROŻENIA ZWIĄZANE Z OFERTAMI INWESTYCJI. OSZUSTWA NA „ZDALNY PULPIT" – OD PLATFORM INWESTYCYJNYCH DO OSZUSTW „NA BANKOWCA"

Skala zagrożeń i ryzyka związanego z przestępczością w sieci Internet rośnie i będzie rosła wraz z nieuniknionym dalszym rozwojem technologii informacyjno-komunikacyjnych, technologii mobilnych, systemów urządzeń elektronicznych – *Internet*

---

[3] Rynek FOREX, a właściwie *foreign exchange* (ang. *foreign exchange* – wymiana zagraniczna), jest to rynek walutowy, na którym dokonywane są transakcje sprzedaży i kupna walut, najczęściej za pomocą platform transakcyjnych, nie ma fizycznej siedziby ani lokalizacji. Rynek ten umożliwia kupno lub sprzedaż każdej z ponad 150 kwotowanych par walutowych. Aby stać się uczestnikiem tego rynku, wystarczy zarejestrować się na jednej z wielu dostępnych w Internecie platform oraz wpłacić depozyt zabezpieczający. Zob. M. Czekała, A. Szpara, *Metody zabezpieczeń pozycji walutowych – model Garmana-Kohlhagena oraz rynek Forex*, „Zeszyty Naukowe Wyższej Szkoły Bankowej we Wrocławiu" 2013, nr 2(34), s. 93.

[4] Kryptowaluta bitcoin – pierwsza wirtualna kryptowaluta, wprowadzona na rynek walutowy w 2009 r., przez Satoshi Nakamoto. Do dzisiaj nie ma pewności, czy Nakamato rzeczywiście istnieje, czy też jest to pseudonim osoby, a nawet grupy osób podających się za twórców bitcoina. Do tej pory nie wiadomo też, kto wprowadził wirtualną walutę na rynek międzynarodowy. Bitcoin jest to kryptowaluta w dużej mierze oparta na matematyce i algorytmach. Różni się od waluty tradycyjnej choćby całkowitą anonimowością transferów czy brakiem nadzoru ze strony banków centralnych. Nie ma postaci fizycznej, a cała jego infrastruktura opiera się na komunikacji w sieciach *Peer-to-Peer,* w skrócie *P2P* (ang. *peer-to-peer* – dosł. osoba do osoby), to rodzaj sieci i narzędzia (programy, aplikacje) służących do bezpośredniej wymiany plików między użytkownikami Internetu. Zob. M. Gal, A. Pyć, *Rola kryptowaluty bitcoin na rynku walutowym*, „Journal of Capital Market and Behavioral Finance" 2017, Vol. 3(7), s. 19.

of Things[5], a tym samym dalszym rozwojem bankowości elektronicznej i usług umożliwiających inwestowanie *online* na rynku finansowym. Coraz łatwiejszy dostęp do atrakcyjnych usług oferowanych drogą elektroniczną powoduje jednoczesny wzrost zagrożeń z nimi związanych. Mowa tu o szeroko pojętej przestępczości wymierzonej przeciwko bezpieczeństwu danych oraz przeciwko mieniu. Na skalę przestępczości w elektronicznym obrocie ma także wpływ zachowanie indywidualnych uczestników rynku finansowego, którzy nie zawsze w dostatecznym stopniu są świadomi istniejących zagrożeń i ryzyka związanego z inwestycjami. Często osoby te nie mają wiedzy o tym, jak mogą bronić się przed oszustami oraz gdzie szukać pomocy w sytuacji, gdy padną ofiarą oszustwa. Otrzymując ofertę uzyskania dostępu do w rzeczywistości nieistniejących usług lub obietnicę „znaczących zysków" odpowiadają na nie, przesyłając swoje dane osobowe lub płacąc za „usługę"[6].

Trendy i kierunki rozwoju nowoczesnych technologii są wyznaczane potrzebami ich użytkowników. Nowe technologie z jednej strony zwiększają przewagę konkurencyjną firm dzięki dostarczeniu zwinnych rozwiązań biznesowych i zaspokojeniu rosnących potrzeb klientów, z drugiej zaś generują bariery i zagrożenia. Wyniki badania przeprowadzonego przez Ernst & Young wśród 596 firm wskazują na poważne bariery w upowszechnianiu nowych technologii. Wśród najważniejszych przeszkód, które wskazują wiodące przedsiębiorstwa z różnych branż (oprócz wysokich kosztów wdrożenia i braku kapitału na transfer technologii), znalazło się cyberbezpieczeństwo (wskazuje na nie 49% badanych firm). Według raportu, warto wskazać na dwa obszary wymagające szczególnej uwagi. Pierwszym z nich są regulacje prawne dotyczące nowych technologii – w szczególności w zakresie bezpieczeństwa transakcji opartych na łańcuchu bloków (*blockchain* – ang. *block chain – łańcuch bloków*) oraz bezpieczeństwa algorytmów uczenia maszynowego (ang. *machine learning* – uczenie się maszynowe). Drugim istotnym obszarem jest ugruntowanie i ujednolicenie interpretacji przepisów dotyczących odpowiedzialności przedsiębiorców oraz osób fizycznych za przestępstwa popełniane w przestrzeni cyfrowej[7].

Rok 2020 był rokiem wyjątkowym dla wzrostu poziomu cyberprzestępczości. Pandemia COVID-19 spowodowała znaczny wzrost naszej aktywności w cyberprzestrzeni. Dotyczy to zwłaszcza wykorzystania usług związanych z finansami elektronicznymi. Internet nie jest już w większości tylko źródłem informacji oraz

---

[5] *Internet of Things, IoT* (ang. *Internet of things* – Internet rzeczy/przedmiotów), koncepcja sieci połączonych ze sobą „inteligentnych" urządzeń (np. czujników, urządzeń, systemów i sieci zarządzania).

[6] K. Boroszko, *Zwalczanie nielegalnych działań w zakresie pośredniczenia w transakcjach finansowych*, opracowanie niepublikowane.

[7] Raport EY. Law Compass (2020), *Prawo i innowacje. Wyzwania 2020*, [online] https://assets.ey.com/content/dam/ey-sites/ey-com/pl_pl/marketo-assets/gated-pdfs/2021/ey-raport-ey-law-compass-prawo-i-innowacje-wyzwania-2020.pdf.

miejscem spotkań towarzyskich. Staje się dla nas miejscem pracy, zakupów oraz zarządzania naszymi finansami, dlatego największą pod względem liczebności grupę cyberprzestępstw stanowi oszustwo. Wzrost aktywności cyberprzestępców, zwłaszcza w latach 2020-2021 obrazują m.in. dane statystyczne publikowane przez Naukową Akademicką Sieć Komputerową. CERT Polska w latach 2014-2021 w zakresie oszustw komputerowych obsłużył:

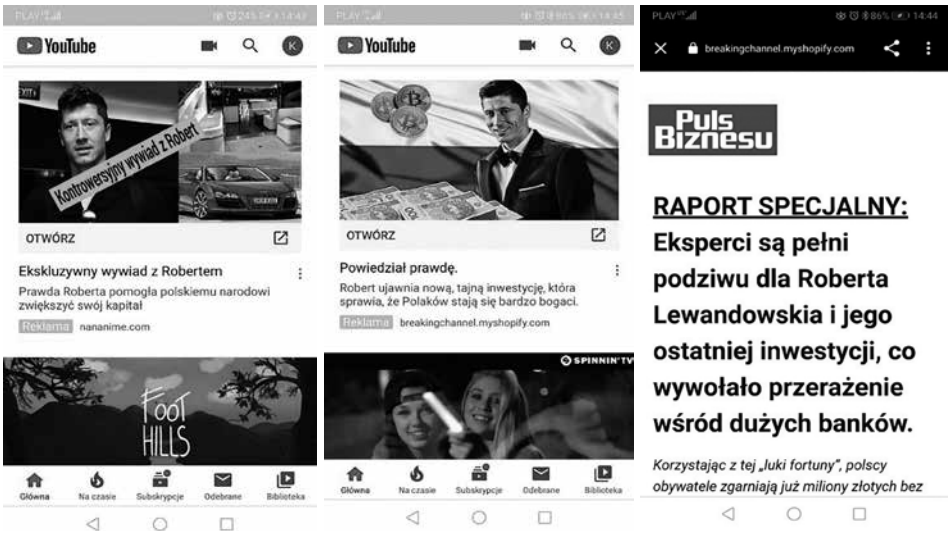
- w 2014 r. – 613 zgłoszeń,
- w 2015 r. – 611 zgłoszeń,
- w 2016 r. – 1069 zgłoszeń,
- w 2017 r. – 1439 zgłoszeń,
- w 2018 r. – 1878 zgłoszeń,
- w 2019 r. – 4086 zgłoszeń,
- w 2020 r. – 8310 zgłoszeń,
- od 1 stycznia do 30 czerwca 2021 r. – 9167 zgłoszeń[8].

Początek 2020 r. to nie tylko początek okresu pandemii, to także czas ewolucji wprowadzonego na rynek w 2018 r. przez grupy cyberprzestępcze nowego mechanizmu przestępczego – oszustwa, które po pewnym czasie otrzymało nazwę oszustwa „na zdalny pulpit". Przestępstwo to, jak się okazuje, zyskuje coraz większą popularność z uwagi na zastosowanie doskonale przemyślanych i wdrożonych zabiegów socjotechnicznych, pozwalających skutecznie manipulować potencjalnymi ofiarami, połączonych z równie skutecznymi narzędziami anonimizacji, w wysokim stopniu utrudniającym realizowanie procesu wykrywczego przez organy ścigania.

Pierwsza odmiana oszustwa na „zdalny pulpit" zbudowana jest wokół inwestycji w waluty wirtualne. Sprawcy tworzą stronę internetową zawierającą ofertę świadczenia usług inwestycyjnych, na której osoba zainteresowana wypełnia formularz kontaktowy, wskazując imię, nazwisko, numer telefonu i kraj zamieszkania. Strona ta jest miejscem, do którego pokrzywdzeni trafiają po przeczytaniu fikcyjnych artykułów, zamieszczanych przez sprawców pod linkami na różnego rodzaju portalach społecznościowych. Artykuły te informują o nieprawdopodobnych zyskach, jakie uzyskały sławne osoby ze świata sportu lub show biznesu w wyniku skorzystania z usług firmy związanej ze stroną internetową. Po wypełnieniu formularza kontaktowego przez osobę zainteresowaną inwestycjami następuje kontakt telefoniczny wywołany przez rzekomego doradcę inwestycyjnego.

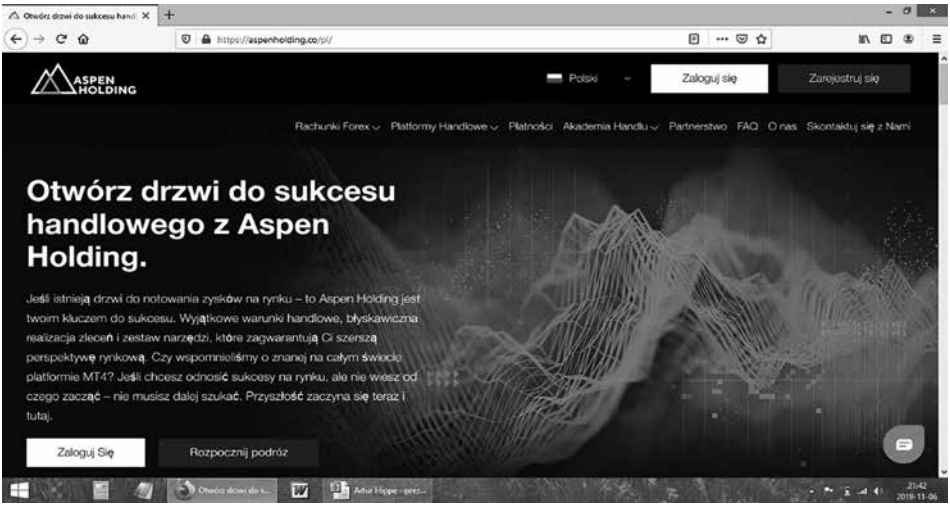
[8] https://www.nask.pl/pl/aktualnosci/4266,CERT-Polska-informuje-o-znacznym-wzroscie-liczby-oszustw-komputerowych.html.

Ryc. 1. Przykładowa strona internetowa zawierająca ofertę świadczenia usług inwestycyjnych



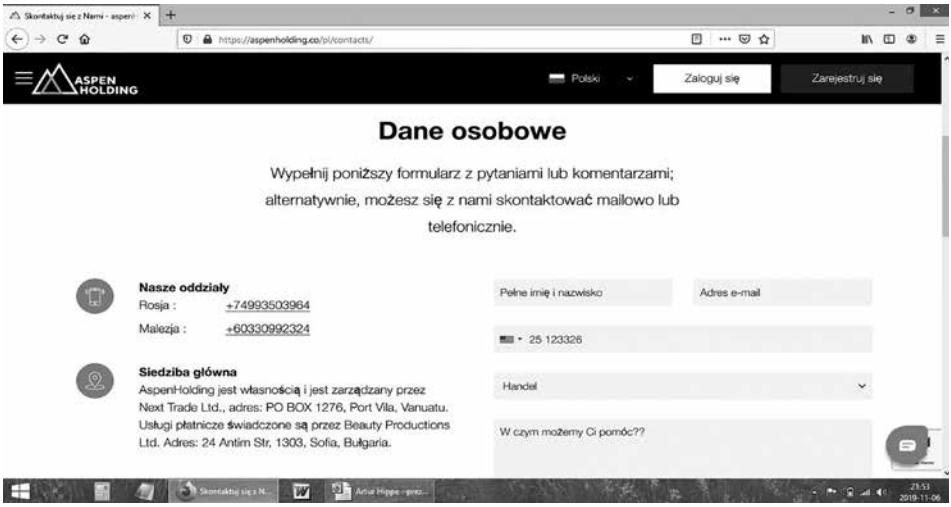
Źródło: Internet, archiwum własne autorów.

Ryc. 2. Przykładowa strona internetowa zawierająca ofertę świadczenia usług inwestycyjnych Aspen Holding



Źródło: Internet: aspenholding.com, archiwum własne autorów.

Ryc. 3. Przykładowa strona internetowa zawierająca formularz kontaktowy Aspen Holding



Źródło: aspenholding.com, archiwum własne autorów.

Poza opisaną metodą naboru, odnotowano również inne:

- sprawca kontaktuje się telefonicznie z potencjalną ofiarą, mimo że pokrzywdzony nie był dotychczas zainteresowany inwestycjami (grupy przestępcze korzystają z dostępnych baz kontaktowych udostępnianych w sieci Internet);
- pokrzywdzony zainteresowany inwestycjami korzysta z for inwestycyjnych, w tym grup społecznościowych utworzonych na portalach społecznościowych, gdzie poznaje tzw. lidera zajmującego się rynkiem Forex oraz kryptowalutami, który zapewnia, że istnieje możliwość szybkiego i łatwego zarobku, oferując jednocześnie swoją pomoc przy inwestowaniu pieniędzy[9].

Pierwsze rozmowy mają na celu zbudowanie u potencjalnej ofiary wizji ogromnych zysków, bez konieczności znajomości mechanizmów funkcjonujących na rynkach finansowych, oczywiście przy zachowaniu pełnego bezpieczeństwa inwestowanych środków. Fikcyjny doradca z reguły identyfikuje się w rozmowie nazwą platformy, którą reprezentuje, w celu uwiarygodnienia i spoufalenia się z pokrzywdzonym. Na tym etapie działania przedstawiciele „platform inwestycyjnych" intensyfikują działania i kontakty z klientem. Stają się bardziej zaangażowani,

[9] K. Boroszko, *Zwalczanie nielegalnych działań…*

często wywierają presję na klientów, strasząc ich stratami lub krótkimi terminami na podjęcie decyzji inwestycyjnej.

Kolejnym etapem jest wpłata przez „inwestora", czyli pokrzywdzonego, określonej kwoty, tzw. opłaty wpisowej, najczęściej w wysokości 250 USD lub 250 EUR. Zakładane jest indywidualne „konto inwestycyjne" pokrzywdzonego, który podejmuje tym samym współpracę w daną „platformą inwestycyjną".

Kolejnym warunkiem przystąpienia do inwestowania jest zainstalowanie na komputerze klienta narzędzia do zdalnej obsługi urządzenia – „AnyDesk", „TeamViewer", dzięki któremu, doradca będzie miał możliwość pełnego dostępu do finansów klienta oraz jego konta inwestycyjnego, a wszystkie transakcje będą odbywać się za wiedzą i zgodą inwestora, który cały proces będzie mógł obserwować na ekranie swojego komputera. Kolejny, najważniejszy z punktu widzenia cyberprzestępców etap to „inwestowanie" pieniędzy ofiary, polegające na:

- otworzeniu fikcyjnego konta inwestycyjnego na nazwisko „klienta",
- założeniu portfeli walut wirtualnych na nazwisko „klienta",
- inwestowaniu w walutę wirtualną, co w rzeczywistości polega na kupnie walut i wyprowadzaniu ich najczęściej na kolejne portfele pozostające już w wyłącznej dyspozycji sprawców. Zakup walut wirtualnych jest finansowany ze środków zgromadzonych na rachunku „klienta", który w czasie inwestowania jest obsługiwany przez sprawców za wiedzą i zgodą pokrzywdzonego, a autoryzowany jest przez „klienta".

Należy podkreślić, że wszystkie działania związane z realizacją etapu „inwestowania" odbywają się już wyłącznie z wykorzystaniem przez sprawców urządzeń „klienta", dzięki narzędziom do zdalnej obsługi, wskutek czego ślady aktywności sprawców znajdują się na tym etapie na urządzeniach pokrzywdzonych.

Pieniądze z rachunków pokrzywdzonych transferowane są również przelewami natychmiastowymi (np. Elixir) na rachunki innych osób fizycznych, które najczęściej są także pokrzywdzonymi, zwerbowanymi w zbieżnym czasie przez innego przedstawiciela danej „platformy inwestycyjnej" lub bezpośrednio tzw. przelewami internetowymi na konta giełd lub kantorów umożliwiających wymianę waluty rynkowej na walutę wirtualną. Na tym etapie dochodzi do wykorzystania danych kart bankowych wydanych do rachunku, takich jak numer karty, data ważności, kod CVV/CVC. Bezpośrednio po wymianie waluty FIAT[10] wychodzącej z rachunku pokrzywdzonego następuje jej przekazanie na portfele kryptowalutowe,

[10] Waluta FIAT, waluta fiducjarna, pieniądz fiducjarny (łac. *fide*s – wiara) to wirtualny pieniądz, który nie ma oparcia w rezerwie zabezpieczającej banku (np. złocie), a jedynie polega na zaufaniu do emitenta. Mocą decyzji władz państwowych jest prawnym środkiem płatniczym na danym terytorium, *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/pieniadz-fiducjarny;3956792.html.

wygenerowane i podstawione przez sprawców w celu dalszego transferu środków w ramach *blockchain*.

W efekcie opisanego procederu, ofiary przestępstwa nie odzyskują środków, a w najgorszym scenariuszu, pozostają nie tylko ze stratami w postaci utraconych oszczędności, ale także z zobowiązaniami kredytowymi zaciągniętymi przez siebie lub przez „doradców inwestycyjnych" platform.

Istotną cechą działania sprawców opisanego przestępstwa jest stałe doskonalenie mechanizmu działania, w szczególności przez uzupełnianie działań o coraz doskonalsze metody maskowania tożsamości. Świadczy o tym wdrożenie na etapie kontaktów „doradców" z „inwestorami" tzw. *spoofingu* telefonicznego, czyli metody podszywania się pod dowolny numer telefonu dzwoniącego. Metoda ta zostanie szczegółowo opisana w dalszej części opracowania.

Wykorzystanie możliwości podszycia się pod każdy numer telefonu wywołującego połączenie spowodowało, że sprawcy w ramach stosowanego przedsięwzięcia socjotechnicznego zaczęli podszywać się pod pracowników banków, którzy z punktu widzenia społeczeństwa są grupą znacznie bardziej godną zaufania niż pracownicy platform inwestycyjnych. Dodatkowo w celu uzyskania oczekiwanej reakcji ofiar sprawcy informują o rzekomym nieautoryzowanym dostępie do ich rachunków bankowych. Celem działania sprawców jest, jak w przypadku poprzednim, doprowadzenie do instalacji narzędzia do zdalnej obsługi urządzenia wykorzystywanego przez ofiarę do obsługi bankowości internetowej, aby uzyskać dostęp do jego rachunku bankowego, lub bezpośrednie wyłudzenie danych wrażliwych, takich jak dane kart płatniczych.

3. WYKORZYSTANIE RYNKU E-COMMERCE PRZEZ CYBERPRZESTĘPCÓW

Grupą użytkowników Internetu szczególnie narażoną na działanie cyberprzestępców są odbiorcy usług w branży e-commerce. Okres pandemii również miał ogromny wpływ na wzrost zainteresowania internautów tym sektorem, a tym samym na wzrost aktywności cyberprzestępców w zakresie udoskonalania znanych i wdrażania nowych mechanizmów oszustw internetowych.

Najbardziej popularna z nowych metod działania cyberprzestępców została ukierunkowana na użytkowników internetowego portalu ogłoszeniowego OLX. Sprawcy, wykorzystując działanie tzw. bota, zautomatyzowanego narzędzia, nawiązują za pośrednictwem komunikatora internetowego WhatsApp kontakt z autorami ogłoszeń dotyczących ofert sprzedaży, deklarują zainteresowanie kupnem oferowanego towaru. W momencie podjęcia korespondencji przez sprzedającego dalsza konwersacja jest już prowadzona przez członka grupy przestępczej. Celem

działania sprawców jest na tym etapie uzyskanie zaufania ze strony sprzedającego, wystarczającego do odwiedzenia strony, ukrytej pod przesłanym przez nich linkiem. Z treści korespondencji wynika, że link ma prowadzić do strony, dzięki której sprzedający otrzyma szybki przelew za oferowany produkt. W rzeczywistości dane karty płatniczej, które użytkownik wprowadza, aby uzyskać środki pieniężne, są przechwytywane przez sprawców w celu uzyskania nieautoryzowanego dostępu do pieniędzy pokrzywdzonego. W innej odmianie ataku następuje instalacja złośliwego oprogramowania na urządzeniu sprzedającego, które umożliwia sprawcom przejęcie kontroli nad zainfekowanym hostem lub przechwycenie danych wrażliwych, takich jak dane dostępowe do rachunku bankowego i in. Przykładowa korespondencja sprawców ze sprzedającym została zobrazowana na ryc. 4.

Ryc. 4. Przykładowa korespondencja sprawców ze sprzedającym

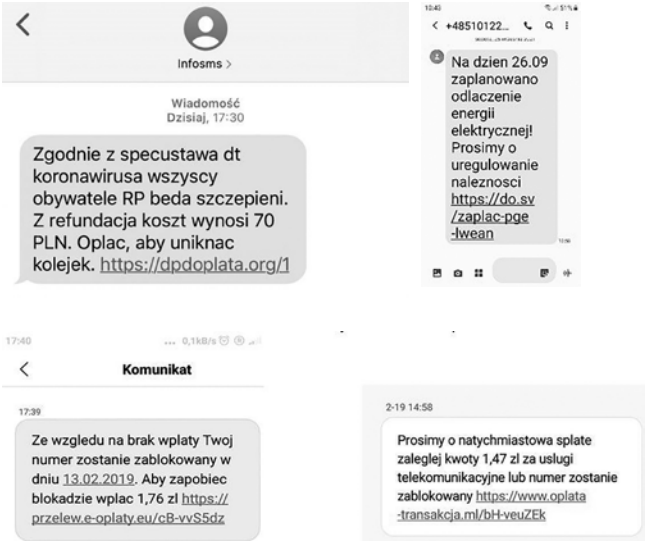
Źródło: archiwum własne autorów

4. OSZUSTWA ZWIĄZANE Z PANDEMIĄ

Kolejny sposób działania sprawców, wdrożony w czasie trwania stanu pandemii, wykorzystuje metodę *sms phishingu*[11]. Sprawcy rozsyłają wiadomości sms, w których, w zależności od zaplanowanej „historii", podszywają się najczęściej pod instytucje godne zaufania lub świadczące usługi o zasięgu ogólnopolskim. Przykładowe wiadomości przedstawiono na ryc. 5:

[11] *Phishing* (ang. *password harvesting fishing* – łowienie haseł) metoda ataku przy wykorzystaniu wiadomości sms lub e-mail, gdzie sprawca podszywa się pod różne osoby lub znane podmioty gospodarcze, starając się wyłudzić dane kart bankomatowych, logowania do kont bankowych, portali społecznościowych lub usług biznesowych.

Ryc. 5. Przykładowa korespondencja sprawców ze sprzedającym – *phishing*



Źródło: archiwum własne autorów

W tym przypadku, podobnie jak w opisywanym powyżej, uruchomiając stronę internetową, znajdującą się pod linkiem przysyłanym w treści SMS-a pokrzywdzeni, którzy próbowali dokonać płatności, utracili poufność swoich danych dostępowych do rachunków bankowych, ponieważ trafili na sfałszowane strony płatności internetowych. W efekcie powyższego sprawcy wyprowadzili w sposób nieautoryzowany pieniądze z rachunków pokrzywdzonych.

Realizując opisane procedery przestępcze, sprawcy bazują na niskim poziomie edukacji internautów. Jak wynika z doświadczenia autorów, użytkownicy Internetu nie dysponują podstawową wiedzą z zakresu weryfikacji wiarygodności innych użytkowników oraz umiejętnością czytania nazw domenowych, będących częścią składową każdego adresu URL.

Zasadnym wydaje się w tym miejscu przybliżenie podstawowych informacji z zakresu organizacji sieci Internet. Każdemu urządzeniu sieci jest przyznawany unikatowy adres IP, zapisywany w następującym formacie, w zależności od wersji protokołu komunikacyjnego:

- IPv4 – np. 101.100.146.147
- IPv6 – np. 2001:0db8:0000:0000:0000:0000:1428:57ab

Adresy IP umożliwiają indywidualizację wszystkich urządzeń w sieci w danej jednostce czasu.

Ze względu na skończoną liczbę adresów oraz konieczność ich agregacji dla celów uproszczenia trasowania powstały Regionalne Rejestry Internetowe – organizacje zajmujące się przydzielaniem puli adresów dla poszczególnych dostawców Internetu.

Organizacją nadrzędną jest Agencja Zarządzania Numeracją Internetową (ang. IANA), która zajmuje się dystrybucją poszczególnych puli adresowych. Do organizacji regionalnych należą:

APNIC (ang. *Asia Pacific Network Information Centre*) – dla rejonu Azji i Pacyfiku,

ARIN (ang. *American Registry for Internet Numbers*) – dla rejonu Ameryki Północnej,

LACNIC (ang. *Regional Latin-American and Caribbean IP Address Registry*) – dla rejonu Ameryki Łacińskiej i wysp Karaibskich,

RIPE (fr. *Réseaux IP Européens*) – dla rejonu Europy, Bliskiego Wschodu i centralnej Azji,

AfriNIC – dla rejonu Afryki[12].

Regionalne rejestry internetowe zajmują się zarządzaniem adresami IP i przechowują bazy danych z informacjami o podmiotach (np. firmach telekomunikacyjnych, dostawcach usług internetowych, a także innych instytucjach i przedsiębiorstwach), którym przydzielone zostały konkretne pule adresów IP. Wśród gromadzonych informacji znajdują się nazwy podmiotów oraz ich adresy geograficzne (w tym: kraj, miasto, ulica).

Każdy serwer, na którym utworzona jest strona internetowa, posiada własny adres IP. Aby ułatwić użytkownikowi zapamiętanie adresu strony, wprowadzono system nazw domenowych DNS (ang. *Domain Name System* – system nazw domen), dzięki któremu znane nam adresy URL są zamieniane na zrozumiałe dla urządzeń wchodzących w skład sieci adresy IP i odwrotnie. Zadanie to realizują serwery DNS.

System DNS opiera się na 13 głównych serwerach, rozmieszczonych w różnych częściach świata, które przy współpracy z innymi „pośrednimi" serwerami DNS realizują żądanie pobrania strony, które użytkownik zgłasza, wpisując adres w pasku adresowym przeglądarki.

Częścią składową adresu URL jest nazwa domenowa strony internetowej (adres DNS) np.: „policja.gov.pl".

Adres DNS składa się z domen internetowych, rozdzielonych kropkami, ułożonych w sposób hierarchiczny, przy czym domena najwyższego poziomu znajduje się na końcu ciągu znaków.

W strukturze hierarchicznej domen rozróżniamy domeny:

- najwyższego poziomu (rozszerzenia) – powyżej których w systemie DNS nie istnieją żadne inne domeny,
- drugiego poziomu,
- subdomeny.

[12] https://www.dipol.com.pl/co_to_jest_adres_ip_maska_sieciowa_brama__bib538.htm.

Istnieją dwa typy domen najwyższego poziomu:

- krajowe – zawsze dwuliterowe, np. Polska – .pl,
- funkcjonalne – np. „.com" (dla celów biznesowych, komercyjnych), „.edu" (do zastosowań edukacyjnych), „.gov" (przeznaczone dla instytucji rządowych), „.net" (przeznaczone dla podmiotów świadczących usługi internetowe lub telefoniczne na dużą skalę).

Administrowaniem wszystkimi światowymi domenami zajmuje się organizacja ICAAN (ang. *Internet Corporation for Assigned Names and Numbers* – Internetowa Korporacja ds. Nadawania Nazw i Numerów). W jej gestii leży określenie budowy domen, ustanawianie nowych rozszerzeń, a także kontrola działalności globalnych serwerów DNS.

Każde rozszerzenie zarządzane jest przez odpowiednią organizację. Europejskim rozszerzeniem „.eu" zarządza EURiD (ang. *European Registry for Internet Domains* – Europejski Rejestr Nazw Domen Internetowych).

Polska domena narodowa „.pl" wraz z subdomenami zarządzana jest przez NASK (Naukowa Akademicka Sieć Komputerowa) – instytut badawczy, który pełni funkcję rejestru domen internetowych[13].

Wszelkie czynności dotyczące nazwy domeny .pl abonent zgłasza bezpośrednio do obsługującego ją rejestratora, którego dane dostępne są w bazie *WHOIS* (ang. etym. *who is* – dosł. kto jest). Zmiany te wykonywane są zgodnie z obowiązującymi u rejestratora procedurami i obejmują w szczególności następujące czynności:

- zmiana delegacji nazwy domeny, tj. zmiana serwerów nazw obsługujących nazwę domeny;
- aktualizacja danych abonenta, np. aktualizacja nazwy abonenta, adresu siedziby lub zamieszkania, adresu korespondencyjnego, numeru telefonu i/lub faksu, adresu e-mail;
- zmiana abonenta nazwy domeny, tj. przeniesienia praw i obowiązków wynikających z umowy o rejestrację i utrzymanie nazwy domeny zawartej z NASK na rzecz innego podmiotu bądź osoby;
- wydanie kodu authinfo, niezbędnego do transferu obsługi nazwy domeny do innego rejestratora;
- rezygnacja z utrzymywania nazwy domeny[14].

Wszystkie powyższe czynności wymagają wyraźnej zgody abonenta nazwy domeny.

Pod adresem: www.dns.pl/cgi-bin/whois.pl można uzyskać szczegółowe informacje na temat zarejestrowanej nazwy domeny z rozszerzeniem „.pl". Każdy regionalny rejestr domen internetowych prowadzi bazę *WHOIS* dla administrowanych przez siebie domen internetowych.

---

[13] https://www.heuristic.pl/blog/e-biznes/Rejestracja-domeny-jakie-rozszerzenie-wybrac;122.html.

[14] https://dns.pl/.

W sieci dostępne są ponadto uniwersalne usługi *WHOIS*. Są to usługi działające na zasadzie pytanie/odpowiedź i są szeroko rozpowszechnione do wysyłania zapytań do baz danych DNS, m.in. po to, by poznać właściciela domeny lub dostawcę Internetu – ISP (ang. *Internet service provider* – dostawca usług internetowych) dzierżawiącego dany adres IP.

Znajomość powyższych zasad organizacji Internetu ma bezpośredni wpływ na bezpieczeństwo użytkowników sieci. Cyberprzestępcy bowiem, aby utrudnić ich identyfikację organom ścigania, stosują bardziej lub mniej zaawansowane metody anonimizacji. Maskowanie tożsamości przez sprawców jest również elementem łańcucha zabiegów socjotechnicznych, których celem jest uzyskanie maksymalnego poziomu zaufania potencjalnej ofiary, co w dalszej kolejności pozwala skutecznie manipulować ich zachowaniami, aż do osiągnięcia założonego celu przestępczego.

5. WYBRANE METODY MASKOWANIA TOŻSAMOŚCI

W całej historii istnienia Internetu oraz ewoluujących równolegle do nowych, coraz skuteczniejszych mechanizmów bezpieczeństwa metod działania cyberprzestępców, jedną z wiodących ról odgrywa anonizmizacja. Jest to element procesu przestępczego, w ramach którego sprawcy ukrywają elementy swojej tożsamości (zarówno cyfrowej, jak i rzeczywistej), aby utrudnić organom ścigania ich identyfikację, przypisanie sprawstwa konkretnego przestępstwa, a w konsekwencji – doprowadzenie do ich ukarania.

Elementami, które pozwalają powiązać aktywność użytkowników sieci teleinformatycznych z ich danymi osobowymi są m. in. numery MSiSDN[15], numer IMEI[16], adres e-mail, adres IP. Dane te, dzięki zastosowanym rozwiązaniom prawnym, są gromadzone przez ich administratorów – podmioty świadczące daną usługę oraz w uzasadnionych przypadkach udostępniane uprawnionym organom państwa wraz z danymi użytkowników – abonentów konkretnej usługi.

Przedsięwzięcia podejmowane przez cyberprzestępców w zakresie maskowania swojej tożsamości stale ewoluują i są przez nich stosowane adekwatnie do popełnianych przestępstw. Do najbardziej charakterystycznych metod anonimizacji, wykorzystywanych w związku z opisanymi w niniejszym opracowaniu przestępstwami, zaliczyć należy:

- Caller ID *spoofing*[17] – *spoofing* telefoniczny,
- e-mail *spoofing*,

---

[15] MSISDN (ang. *Mobile Station International Subscriber Directory Number*) – numer abonenta sieci komórkowej.

[16] IMEI (ang. *International Mobile Equipment Identity*) – indywidualny numer identyfikujący urządzenie mobilne.

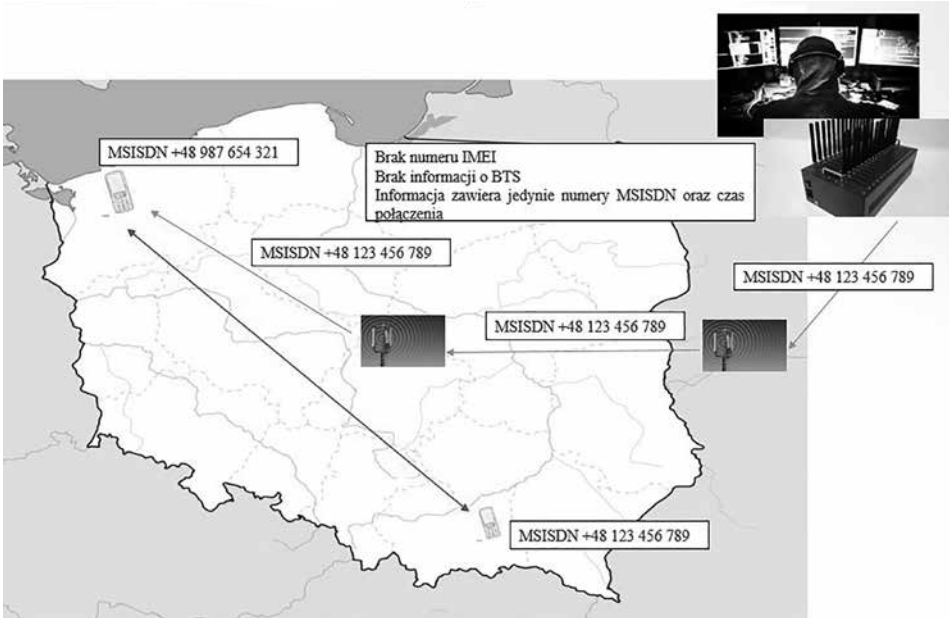
[17] *Spoofing* (ang. *spoof* – naciąganie, szachrajstwo) – podszywanie się pod kogoś lub pod podmiot, numer, dane, w celu oszukania innej osoby. *Spoofing* telefoniczny polega na podszywaniu się numeru telefonicznego dzwoniącego pod inny numer, np. znanej instytucji, podmiotu.

- przejęcia adresów IP (włamania do urządzeń sieciowych, złośliwe oprogramowanie typu klient botnet, podłączenie do cudzej sieci Wi-Fi).

Spoofing jest procesem, w którym sprawcy poprzez ukrycie, a w rzeczywistości podmianę, elementów swojej cyfrowej tożsamości podszywają się pod konkretną osobę lub instytucję, w celu osiągnięcia swoich przestępczych zamierzeń. Dane, które ulegają podmianie to w zależności od metody *spoofingu* numer MSISDN oraz adres e-mail, czyli te dane, które dla odbiorcy korespondencji są elementami widocznymi i w pierwszej kolejności podlegają przede wszystkim wzrokowej weryfikacji.

Na poniższej grafice przedstawiono schemat połączenia telefonicznego, w którym sprawcy, podszywając się pod numer +48 123 456 789, wykorzystując określone uwarunkowania sieci telekomunikacyjnych, wywołują połączenie z numerem +48 987 654 321, gdy w tym samym czasie numer +48 123 456 789 jest użytkowany i zarejestrowany na innego abonenta, który w rzeczywistości nie ma nic wspólnego z danym połączeniem. Zaznaczyć należy, że urządzenie – nazwijmy to legalnego użytkownika numeru – nie bierze udziału w danym zdarzeniu telekomunikacyjnym.

Ryc. 6. Metody maskowania tożsamości – *spoofing* telefoniczny



Źródło: opracowanie własne.

Caller ID spoofing jest metodą wykorzystywaną przez sprawców różnego rodzaju oszustw. Przestępstwa, w których realizacji sprawcy najczęściej sięgają po tę metodę, to oszustwa tzw. pod legendą, a wśród nich:

- „na zdalny pulpit",
- „na policjanta",
- „na bankowca".

Jak zatem zabezpieczyć się przed *spoofingiem* telefonicznym? Jedyną, ale też niezawodną metodą jest wywołanie połączenia na numer wykorzystywany przez sprawców w celu weryfikacji rozmówcy. *Caller ID spoffing* jest procesem jednokierunkowym. Sprawcy nie są w stanie w ramach tej metody przechwycić połączeń kierowanych na numer, pod który się podszywają.

Pomimo podobnych założeń *spoofingu* telefonicznego i e-mail *spoofingu* sposób weryfikacji nadawcy jest różny. Odesłanie maila, z wykorzystaniem przycisku odpowiedz nie pozwoli na sprawdzenie, czy nadawcą jest osoba godna zaufania, przedstawiciel danej instytucji. W tym przypadku odpowiedź znajdziemy w nagłówku wiadomości. Należy zaznaczyć, że nie wszystkie elementy wiadomości e-mail są możliwe do edycji. Najważniejszym elementem wiadomości e-mail jest nagłówek rozszerzony, w którym znajduje się opis drogi, jaką przebyła wiadomość od nadawcy do adresata, zawierający adresy IP urządzeń, które brały udział w transmisji korespondencji oraz czasy konkretnych zdarzeń. Ponadto analiza nagłówka rozszerzonego pozwoli potwierdzić lub wykluczyć, czy adres e-mail, znajdujący się w nagłówku podstawowym wiadomości jest faktycznie tym, z którego wysłano wiadomość.

Istotnym elementem przestępstw popełnianych przez cyberprzestępców z wykorzystaniem spreparowanych wiadomości e-mail jest ukrywanie prawdziwego adresu IP. Na przestrzeni okresu trwania pandemii coraz częściej obserwowane jest zjawisko przychwytywania adresów IP innych użytkowników Internetu, co w konsekwencji prowadzi do wniosków, że to oni są sprawcami przestępstw. Najczęściej czynnikami umożliwiającymi sprawcom przechwycenie cudzego adresu IP jest funkcjonowanie niezabezpieczonych sieci Wi-Fi (najczęściej domowych) oraz niewłaściwe podejście użytkowników do problemu bezpieczeństwa użytkowanych urządzeń sieciowych (infekcja złośliwym oprogramowaniem).

Cyberprzestępczość jest zjawiskiem, które stanowi coraz większe zagrożenie. Pomimo wdrażania coraz nowszych systemów i mechanizmów bezpieczeństwa, sprawcy modyfikują znane lub wprowadzają nowe metody działania, wykorzystujące w coraz większym stopniu inżynierię społeczną oraz w dalszym ciągu wysoki poziom podatności społeczności internetowej.

6. MOŻLIWOŚCI ORGANÓW ŚCIGANIA W ZAKRESIE ZAPOBIEGANIA I ZWALCZANIA CYBERPRZESTĘPCZOŚCI – WSPÓŁPRACA MIĘDZYINSTYTUCJONALNA

Transgraniczny charakter Internetu, jego sposób organizacji oraz fakt, że użytkownicy mogą wykorzystywać usługi świadczone przez podmioty z całego świata stawiają przed organami ścigania nowe wyzwania. Wraz ze wzrostem zagrożenia cyberprzestępczością oraz pojawiającymi się coraz nowszymi metodami działania sprawców niezbędnym jest poszukiwanie i wdrażanie rozwiązań, umożliwiających organom ścigania na całym świecie szybkie i skuteczne pozyskiwanie różnego rodzaju danych, a w szczególności danych telekomunikacyjnych, internetowych oraz stanowiących tajemnicę bankową.

Międzynarodowe kanały wymiany informacji policyjnych realizowane są przy aktywnym udziale międzynarodowych organizacji policyjnych Europol[18] i Interpol[19].

Na etapie współpracy organów wymiaru sprawiedliwości istnieją rozwiązania takie jak międzynarodowa pomoc prawna oraz Europejski Nakaz Dochodzeniowy pomiędzy państwami będącymi jego stronami. Zasadnicze regulacje w tym zakresie zawierają ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego[20] oraz akty międzynarodowe, wyznaczające zakres pomocy międzynarodowej.

Metodykę narzędzia śledczego, jakim jest międzynarodowa pomoc prawna, reguluje rozporządzenie Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. – Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratur[21] w dziale IV zatytułowanym „Współpraca międzynarodowa w sprawach karnych".

Europejski Nakaz Dochodzeniowy (END) definiuje dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych, zgodnie z którą END to orzeczenie sądowe wydane lub zatwierdzone przez organ wymiaru sprawiedliwości jednego państwa członkowskiego (zwanego dalej „państwem wydającym") w celu wezwania innego państwa członkowskiego (zwanego dalej „państwem wykonującym") do przeprowadzenia jednej lub kilku określonych czynności dochodzeniowych

---

[18] Europol jest organem ścigania Unii Europejskiej. Głównym celem Europolu jest przyczynianie się do zwiększenia bezpieczeństwa Europy z korzyścią dla wszystkich obywateli UE. Agencja, z siedzibą w Hadze (Niderlandy), wspiera 27 państw członkowskich w walce przeciwko poważnej przestępczości międzynarodowej i terroryzmowi. Współpracuje również z wieloma państwami partnerskimi spoza UE oraz organizacjami międzynarodowymi. – https://www.europol.europa.eu/pl/about-europol.

[19] Interpol – Międzynarodowa Organizacja Policji Kryminalnej. Organizacja międzyrządowa, skupiająca 195 krajów członkowskich – https://www.interpol.int/Who-we-are/What-is-INTERPOL.

[20] Dz. U. z 2021 r. poz. 534.

[21] Dz. U. z 2017 r. poz. 1206.

w celu uzyskania materiału dowodowego. Państwa członkowskie wykonują END, stosując zasadę wzajemnego uznawania i przestrzegając przepisów dyrektywy[22].

Z punktu widzenia skuteczności podejmowanych w ramach postępowań przygotowawczych przedsięwzięć współpracy międzynarodowej w sprawach dotyczących cyberprzestępstw istotnym jest pojęcie retencji danych. Każde państwo ma w tym zakresie własne, odrębne stanowisko. W Polsce retencja danych telekomunikacyjnych uregulowana jest w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[23], w której zapisany jest obowiązek przechowywania przez usługodawców telekomunikacyjnych określonych danych, związanych ze zdarzeniem telekomunikacyjnym przez okres 12 miesięcy od zaistnienia zdarzenia. Okres retencji danych telekomunikacyjnych w różnych krajach świata wynosi nawet kilka dni. W momencie osiągnięcia ustawowego czasu retencji danych operator telekomunikacyjny bezpowrotnie usuwa gromadzone dane, istotne z punktu widzenia wykrywczego. Fakt ten, w zależności od czasu jaki upłynął od momentu popełniania przestępstwa do pozyskania o nim informacji przez organy ścigania lub wymiaru sprawiedliwości, w wielu przypadkach uniemożliwia nawet próbę podjęcia skutecznych działań ukierunkowanych na ustalenie tożsamości sprawców.

Bardzo przydatne ze względu na nietrwałość danych telekomunikacyjnych i internetowych jest narzędzie „zamrażania danych" wykorzystywane na podstawie Konwencji budapesztańskiej[24], której celem jest wprowadzenie w systemach prawa karnego poszczególnych państw pewnych uniwersalnych rozwiązań w zapobieganiu i zwalczaniu szeroko pojętej cyberprzestępczości. Przewiduje ona niejednolite podejście państw stron konwencji do przedmiotu retencji danych telekomunikacyjnych oraz określa jej rolę w skuteczności zwalczania cyberprzestępczości. Zgodnie z art. 29 Konwencji, policjanci w trakcie realizacji czynności w prowadzonym postępowaniu przygotowawczym, mogą zwrócić się do podmiotów świadczących usługi poza granicami Polski o zabezpieczenie danych teleinformatycznych oraz internetowych. Okres zabezpieczenia – „zamrożenia danych" zgodnie z zapisami Konwencji obejmuje 90 dni i może być przedłużony o kolejne 90 dni, a proces ten przebiega specjalnie do tego celu wdrożonymi kanałami komunikacji. Zabezpieczenie danych wydłuża więc okres ich przechowywania nawet o dodatkowe 180 dni w porównaniu do obowiązującego w danym kraju ustawowego okresu retencji.

---

[22] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32014L0041.

[23] Dz. U. z 2021 r. poz. 576.

[24] Konwencja Rady Europy o cyberprzestępczości sporządzona w Budapeszcie 23 listopada 2001 r.; https://op.europa.eu/pl/publication-detail/-/publication/117bab8e-bae5-4837-9cfc-322490939cbe/language-pl.

W praktyce oznacza to, że prokurator lub sąd, w wyniku zastosowania przez Policję instytucji „zamrożenia danych" otrzymuje 180 dni na wdrożenie procesowych narzędzi międzynarodowej wymiany informacji i pozyskanie danych telekomunikacyjnych bez ryzyka ich utracenia, przy założeniu, że wniosek w tym zakresie zostanie doręczony do organów właściwego kraju w okresie obowiązkowej retencji danych.

Konwencja Rady Europy o cyberprzestępczości w Rzeczypospolitej Polskiej weszła w życie 1 czerwca 2015 r. w wyniku ratyfikowania jej przez Prezydenta RP na mocy ustawy z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości[25]. Autorzy nie zdołali dotrzeć do danych statystycznych, umożliwiających zobrazowanie ilościowego wykorzystania tego narzędzia przez Policję na przestrzeni niespełna siedmiu lat oraz skuteczności jego zastosowania w kontekście wystąpień jednostek prokuratury o udostępnienie danych, niemniej dotychczasowe doświadczenie zawodowe pozwala na stwierdzenie, że uprawnienie to nie jest wykorzystywane na poziomie zadowalającym.

Bardzo istotnym elementem z punktu widzenia przeciwdziałania cyberprzestępczości jest aktywność zarówno instytucji państwowych, sektora prywatnego, jak i wszystkich użytkowników Internetu.

Do najważniejszych przedsięwzięć, jakie winna podejmować Policja w zakresie zapobiegania cyberprzestępczości zaliczyć z pewnością należy różnego rodzaju działania profilaktyczne. Określenia profilaktyka i profilaktyka społeczna oznaczają zapobieganie zarówno problemom zdrowotnym, sytuacjom determinującym pojawianie się potrzeb z zakresu opieki społecznej, katastrofom, jak i negatywnym stanom dotyczącym różnych sfer życia społecznego. Dlatego dążenie do przeciwdziałania, a przynajmniej ograniczania negatywnych zjawisk społecznych, ze szczególnym uwzględnieniem przestępczości, uzasadnia skłanianie się ku określeniu tego rodzaju działań mianem profilaktyki społecznej[26].

W 2017 r., w związku z przeprowadzoną analizą stanu zagrożenia cyberprzestępczością oraz cyberzagrożeniami dla dzieci i młodzieży, Komenda Wojewódzka Policji w Rzeszowie wdrożyła program profilaktyczny „Cyberbezpieczni". Analiza cyberzagrożeń na terenie województwa podkarpackiego dała podstawę do wyodrębnienia najistotniejszych cyberzagrożeń, których skala w okresie poprzedzającym wdrożenie programu zauważalnie wzrastała. Program został skierowany do mieszkańców województwa podkarpackiego, a w szczególności dzieci,

---

[25] Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r.; Dz. U. z 2014 r. poz. 1514.

[26] M. Kordaczuk-Wąs, *Uwarunkowania społeczne działań profilaktycznych policji. Studium socjologiczne.*

młodzieży, rodziców, nauczycieli i pedagogów w celu zwiększenia bezpieczeństwa użytkowników Internetu, poprzez m.in.:

- uświadamianie specyfiki zagrożeń wynikających z korzystania z Internetu,
- upowszechnianie zasad bezpiecznego korzystania z Internetu,
- przedstawianie specyfiki cyberzagrożeń,
- zaangażowanie w walkę z cyberprzestępczością i cyberprzemocą społeczeństwa, władz samorządowych, instytucji oraz mediów[27].

Przebieg programu profilaktycznego „Cyberbezpieczni" w latach 2017-2019 oraz analiza osiągniętych efektów, w tym m.in. spadek czynów karalnych popełnionych za pośrednictwem sieci Internet przez nieletnich na terenie woj. podkarpackiego, dały podstawę do wydłużenia jego realizacji do końca 2022 r.

Stały rozwój mechanizmów wykorzystywanych do popełniania cyberprzestępstw oraz powiększające się grupy odbiorców różnego rodzaju usług, świadczonych z wykorzystaniem sieci teleinformatycznych, np. w wyniku osiągnięcia wieku umożliwiającego dostęp do nich, uzasadnia wniosek, że przedsięwzięcia profilaktyczne, bez względu na podmiot je realizujący, powinny mieć charakter ciągły o jak najszerszym zasięgu. Dodatkowo autorzy takich inicjatyw winni na bieżąco aktualizować informacje o cyberzagrożeniach oraz o możliwościach ochrony z punktu widzenia użytkownika końcowego.

Innym przykładem rozwiązania, które ma ogromny wpływ na bezpieczeństwo finansów i stanowi coraz bardziej niezbędny element weryfikacji stron internetowych związanych z aktywnością cyberprzestępców, jest lista ostrzeżeń przed niebezpiecznymi stronami, prowadzona przez CERT Polska[28]. Lista funkcjonuje na podstawie podpisanego 23 marca 2020 r. „Porozumienia o współpracy w zakresie szczególnej ochrony użytkowników Internetu przed stronami wyłudzającymi dane, w tym dane osobowe, w okresie stanów nadzwyczajnych, m.in. stanu epidemii", którego stronami są Prezes Urzędu Komunikacji Elektronicznej wraz Ministrem Cyfryzacji, Naukowa Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy oraz Orange Polska S.A., Polkomtel Sp. z o.o., P4 Sp. z o.o., T-Mobile Polska S.A.

Celem porozumienia jest stworzenie i sprawne prowadzenie listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników Internetu. Przykładowy fragment listy ostrzeżeń przedstawiono na ryc. 7.

---

[27] http://bip.rzeszow.kmp.policja.gov.pl/287/programy-prewencyjne/29774,Program-profilaktyczny-Cyberbezpieczni.html.

[28] https://www.cert.pl/posts/2020/03/ostrzezenia_phishing/.

Ryc. 7. Fragment listy ostrzeżeń przed niebezpiecznymi stronami

```
# CERT.PL's Warning List
# Homepage: https://www.cert.pl/news/single/ostrzezenia_phishing/
# Source: http://hole.cert.pl/domains/
# Version: 202112051056
# START HOSTS LIST
195.187.6.35 www.remarkablequest.top
195.187.6.35 remarkablequest.top
195.187.6.33 notablenephew.top
195.187.6.33 sleaver-com.preview-domain.com
195.187.6.33 resources.purefan.org
195.187.6.33 olx.pl-process-safegate24.xyz
195.187.6.34 www.appleid-account.com
195.187.6.34 appleid-account.com
195.187.6.34 olx-pl.zapitan-ie.rest
195.187.6.34 kaszelktj.pl
195.187.6.34 www.kaszelktj.pl
195.187.6.34 squaredistributor.com
195.187.6.33 www.pastelguess.com
195.187.6.34 pastelguess.com
195.187.6.35 www.portionprofessional.com
195.187.6.34 portionprofessional.com
195.187.6.35 www.innpetty.com
195.187.6.34 innpetty.com
195.187.6.33 www.patchdriver.com
195.187.6.34 patchdriver.com
195.187.6.33 www.squaredistributor.com
195.187.6.35 www.barrellink.com
195.187.6.35 barrellink.com
195.187.6.33 www.filthsdeferrals.com
195.187.6.33 filthsdeferrals.com
195.187.6.34 www.gingelydespondency.com
195.187.6.34 gingelydespondency.com
195.187.6.33 www.awestrickenfarraginous.com
195.187.6.35 awestrickenfarraginous.com
```

Źródło: https://hole.cert.pl/domains/domains_hosts.txt

Cyberprzestępczość jest zjawiskiem stawiającym coraz to nowe wyzwania przed organami ścigania. Możliwości jakie Internet daje przestępcom powodują bardzo dynamiczny wzrost zagrożenia zjawiskiem cyberprzestępczości zorganizowanej. Jest to niewątpliwie wyzwanie, z którym już dziś muszą się mierzyć przedstawiciele wymiaru sprawiedliwości i organów ścigania na całym świecie. Skuteczne zwalczanie tego zagrożenia możliwe jest tylko dzięki wdrożeniu właściwych mechanizmów gromadzenia i wzajemnego udostępniania danych niezbędnych na poziomie międzynarodowym, co pozwoli na skuteczną deanonimizację cyberprzestępców, a w konsekwencji umożliwi wykazanie sprawstwa i pociągnięcie do odpowiedzialności karnej.

BIBLIOGRAFIA

Literatura

Aleksandrowicz T., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15(8).

Boroszko K., *Zwalczanie nielegalnych działań w zakresie pośredniczenia w transakcjach finansowych*, opracowanie niepublikowane.

Czekała M., Szpara A., *Metody zabezpieczeń pozycji walutowych – model Garmana-Kohlhagena oraz rynek Forex*, „Zeszyty Naukowe Wyższej Szkoły Bankowej we Wrocławiu" 2013, nr 2(34).

Gal M., Pyć A., *Rola kryptowaluty bitcoin na rynku walutowym*, „Journal of Capital Market and Behavioral Finance" 2017, Vol. 3(7).
Hajduk-Stelmachowicz M., Iwan K., *Zarządzanie bezpieczeństwem informacji w obszarze bankowości elektronicznej wobec zjawiska cyberprzestępczości – aspekt indywidualny*, „Roczniki Kolegium Analiz Ekonomicznych" 2018, nr 49.
Kordaczuk-Wąs M., *Uwarunkowania społeczne działań profilaktycznych policji. Studium socjologiczne,* Warszawa 2017.

Akty normatywne

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego; Dz. U. z 2021 r. poz. 534.
Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; Dz. U. z 2021 r. poz. 576.
Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r.; Dz. U. z 2014 r. poz. 1514.
Rozporządzenie Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. – Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratur; Dz. U. z 2017 r. poz. 1206.

Zasoby internetowe

Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/pieniadz-fiducjarny;3956792.html.
Raport EY. Law Compass (2020), *Prawo i innowacje. Wyzwania 2020*, <https://assets.ey.com/content/dam/ey-sites/ey-com/pl_pl/marketo-assets/gated-pdfs/2021/ey-raport-ey-law-compass-prawo-i-innowacje-wyzwania-2020.pdf.
https://www.dipol.com.pl/co_to_jest_adres_ip_maska_sieciowa_brama__bib538.htm
https://www.heuristic.pl/blog/e-biznes/Rejestracja-domeny-jakie-rozszerzenie-wybrac;122.html
https://dns.pl/
https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32014L0041,
https://www.cert.pl/posts/2020/03/ostrzezenia_phishing/
http://bip.rzeszow.kmp.policja.gov.pl/287/programy-prewencyjne/29774,Program-profilaktyczny-Cyberbezpieczni.html
https://www.nask.pl/pl/aktualnosci/4266,CERT-Polska-informuje-o-znacznym-wzroscie-liczby-oszustw-komputerowych.html

SPIS RYCIN:

The activity of organized crime groups in a cyberspace in times of the pandemic – the analysis of selected susceptibilities and anonymization methods

SUMMARY

The subject of the study is an attempt to present the problems of the selected methods of activity of criminals who, thanks to the intensive development of the Internet, as well as advanced computer and telecommunications technologies, fraud to the detriment of participants in the e-services sector and currency markets, while exploiting the vulnerability of these objects to selected criminal attacks. In conclusion one of the models of law enforcement proceedings that allows for effective recognition of this type of phenomena at the detection and evidence stage.

Keywords: cybercrime, cybersecurity, fraud, Internet, international cooperation of law enforcement agencies.