PAULINA ŁOJEWSKA*

CHARAKTERYSTYKA WSPÓŁCZESNEJ CYBERPRZESTĘPCZOŚCI ZORGANIZOWANEJ

Abstrakt

Nieustanny rozwój i postępująca rewolucja technologiczna wpływa na wszystkie sfery życia współczesnego człowieka. Możliwość wykorzystania nowoczesnych technologii w celu czerpania zysków z prowadzenia działalności przestępczej została dostrzeżona przez międzynarodowe zorganizowane grupy przestępcze. Poniższa analiza traktuje o charakterze zorganizowanych grup cyberprzestępczych oraz wykorzystywaniu technologii IT do nielegalnej działalności w cyberprzestrzeni. Ukazuje także powody dla których ściganie i zapobieganie tym przestępstwom jest wyzwaniem dla społeczności międzynarodowej.

Słowa kluczowe: cyberprzestępczość, zorganizowana grupa przestępcza, technologia.

Internet stał się nieodzowną częścią życia, prowadzenia biznesu. Posiada on dużo zalet wynikających z korzystania z niego, jednakże pełen jest również wielu zagrożeń. Korzyści mogące płynąć z popełniania przestępstw w intrenecie oraz zyski z tego płynące zostały dostrzeżone przez zorganizowane grupy przestępcze[1]. Rewolucja informacyjna, której jesteśmy świadkami to niezwykle dynamiczny proces. Od momentu gdy wprowadzono pierwszy komputer osobisty oraz uruchomiono pierwszą sieć komputerową – ARPAnet do chwili obecnej postęp informatyczny objął już wszystkie dzieciny życia współczesnego człowieka. Szacuje się, że dziennie użytkownicy sieci Internet wysyłają 144 mld e-maili, zaś na samych tylko urządzeniach mobilnych przetwarza się około 1.3 EB danych[2].

Wzrost przestępczości zorganizowanej w cyberprzestrzeni wiąże się z brakiem ujednoliconych uregulowań w prawie międzynarodowym. Wynikają z tego rozbieżności oraz niespójności, które ułatwiają sprawcom unikanie odpowiedzialności za przestępstwa popeł-

* Paulina Łojewska – absolwentka studiów licencjackich i magisterskich na kierunku bezpieczeństwo wewnętrzne INP UW. Aktualnie funkcjonariusz Komendy Miejskiej Policji we Włocławku. Kontakt e-mail: pjlojewska@gmail.com

1 A. Boszko, *Finanse przestępczości zorganizowanej*, Toruń 2014, s. 147.

2 P. Ciszek, *Cyberprzestępczość (z)organizowana*, [w:] W. Zubrzycki (red.), *Przez przestępczość zorganizowaną do terroryzmu*, Szczytno 2015, s. 49.

niane w sieci z wykorzystaniem urządzeń multimedialnych[3]. Zagrożenie zorganizowaną cyberprzestępczością jest problemem na tyle istotnym, że Federalne Biuro Śledcze umieściło ją wysoko na liście priorytetów działania zaraz po terroryzmie i działalności antyamerykańskiej. Ukazuje to skalę problemu oraz wskazuje, że ten rodzaj popełnianych przestępstw charakteryzuje się dużą dynamiką rozwoju oraz znacznym potencjałem możliwości osiągania zysków[4]. Konwencja Rady Europy określa cztery formy cyberprzestępczości, której dopuszczają się sprawcy:

- przestępstwa związane z pornografią z udziałem małoletnich (oferowanie oraz udostępnianie materiałów, przesyłanie, wytwarzanie w celu udostępniania, posiadanie na nośnikach danych bądź w systemie informatycznym, pozyskiwanie dla siebie lub innej osoby);
- przestępstwa z wykorzystaniem komputera (oszustwa i fałszerstwa komputerowe – modyfikowanie, usuwanie danych bądź ingerowanie w systemy komputerowe);
- przestępstwa dotyczące poufności, dostępności i integralności danych, systemów komputerowych (zakłócanie pracy systemu komputerowego, ingerencje w całość bądź część danych, ich przechwytywanie w trakcie transmisji, umyślne usuwanie bądź niszczenie danych);
- przestępstwa przeciwko własności intelektualnej (rozpowszechnianie utworów, wykonań artystycznych bez zgody twórcy)[5].

Zorganizowana cyberprzestępczość posiada charakter elastyczny, dostosowuje się do zmian oraz rozwoju technologicznego. Dzięki globalnemu ukierunkowaniu sieci Internet ułatwione jest stworzenie grupy przestępczej o zasięgu międzynarodowym[6]. Fakt, iż trudno jest ujednolicić definicyjnie ramy zjawiska przestępczości zorganizowanej ukazuje, że aktualnie dochodzi do dynamicznych oraz gwałtownych zmian nie tylko w kontekście przemian społeczno-gospodarczych, ale także technologicznych, do których adaptują się również grupy przestępcze[7]. Członkowie zorganizowanych grup przestępczych, analogicznie do gospodarki, nieustannie ewoluują oraz dostosowują się do panującej sytuacji, a także w dużym stopniu korzystają ze zdobyczy współsennej techniki. Do swoich potrzeb przestępcy adaptują narzędzia dostępne w sieci komputerowej[8]. W związku z rozwojem technologicznym oraz postępującą globalizacją grupy przestępcze dostosowują zakres swojej działalności oraz formę strukturalną do otoczenia, w jakim muszą funkcjonować. Prowadzi to do powstania różnorodności form działalności przestępczej oraz czasowego działania sprawców[9].

Przestępstwa w cyberprzestrzeni są domeną głównie grup przestępczych o zasięgu międzynarodowym. Dla ochrony przed atakiem hackerskim, kradzieżą danych, zainfe-

---

3 D. Krawczyk, *Internet zagrożeniem dla bezpieczeństwa wewnętrznego*, „Horyzonty Bezpieczeństwa" 2016, nr 2 (1) 2, s. 43.

4 W. Mądrzejowski, *Przestępczość zorganizowana. System zwalczania*, Warszawa 2015, s. 108.

5 Tamże, s. 108–109.

6 Tamże, s. 109.

7 W. Krukowski, *Pojęcie organizacji przestępczej i przestępczości zorganizowanej*, „Prokuratura i Prawo" 2006, nr 1, s. 26.

8 P. Ciszek, dz. cyt., s. 51.

9 W. Krukowski, dz. cyt., s. 26.

kowaniem szkodliwym oprogramowaniem nie wystarczą typowe systemy zabezpieczające. Sprawcy przestępstw, którzy są członkami grup przestępczych, to grupa przestępców wyspecjalizowanych. Ich działalność skupia się na osiągnięciu maksymalnego zysku, a ich działania nie posiadają ideologicznego charakteru[10]. Wśród zmian w zorganizowanych grupach przestępczych można również zaobserwować łączenie potencjału posiadanego przez grupę z wiedzą oferowaną przez specjalistów od informatyki, nowoczesnych technologii[11]. Zorganizowane grupy przestępcze korzystają z dostępu do oprogramowania oraz usług funkcjonujących w chmurze. Programy oraz oprogramowania z jakich korzystają, poziomem skomplikowania dorównują tym, które używane są przez międzynarodowe korporacje oraz wysoko rozwinięte firmy[12].

Cyberprzestępcy nie stwarzają nowych rodzajów czynów zabronionych. Nowoczesne technologie dostarczają nowych rozwiązań i sposobów do popełniana przestępstw dobrze znanych organom ścigania. Nowoczesna technika wykreowała jedynie nowy rodzaj obszaru, przestrzeni w której popełnianie mogą być przestępstwa[13]. Członkowie zorganizowanych grup mogą za pośrednictwem sieci dokonywać przestępstw z obszaru handlu narkotykami, przestępstw ekonomicznych. Wykorzystanie komputera oraz dostępu do sieci nie musi być równoznaczne z popełnianiem przestępczości cybernetycznej np. oszustw internetowych[14]. Grupy przestępcze prowadzą działalność o różnorodnym charakterze: działania nielegalne, półlegalne – w tzw. „szarej strefie", zgodną z prawem, legalną działalność gospodarczą. Różnokierunkowość działalności pozwala ukryć czyny nielegalne, przeprowadzić „pranie brudnych pieniędzy" pochodzących z działalności przestępczej, ułatwia także zdobywanie kontaktów z osobami z innych państw[15].

Grupę przestępczą tworzą jej członkowie, którzy przyczyniają się do realizacji zamierzonych celów oraz zapewniają zyski z prowadzonej działalności. Działalność prowadzona przez zorganizowane organizacje przestępcze przypomina przedsiębiorstwo[16]. Cechami grupy przestępczej są:

- posiadanie wewnętrznej struktury, podziału ról, zbioru zasad, hierarchii w strukturze organizacji oraz wewnętrzna dyscyplina wśród członków grupy;
- celowe działanie;
- działanie o charakterze rozmyślnym, modyfikowanie poczynań aby jak najszybciej doszło do osiągnięcia celu;
- osiąganie celów końcowych poprzez wykorzystanie różnego rodzaju środków;
- posiadanie osób koordynujących działania członków grupy, zarządzających;
- współdziałanie w realizacji określonego celu;
- dążenie do zwiększenia efektywności w realizacji określonego celu;
- trwałość grupy;

10 A. Boszko, dz. cyt., s. 157.

11 J. Kosiński, *Paradygmaty cyberterroryzmu*, Warszawa 2015, s. 260.

12 P. Ciszek, dz. cyt., s. 51.

13 W. Mądrzejowski, dz. cyt., s. 109.

14 Tamże, s. 109.

15 W. Krukowski, dz. cyt., s. 26–27.

16 Tamże, s. 31.

- wykonywanie działań przestępczych zarówno w sposób bezpośredni w celu osiągniecia korzyści finansowych oraz w sposób pośredni w celu zdobycia wpływów;
- używanie różnych form przemocy w celu zrealizowania celu;
- korzystanie podczas realizacji celu z usług specjalistów, wysokiej klasy konsultantów;
- prowadzenie działalności o charakterze międzynarodowym, mobilność w działaniu, wykorzystywanie różnic w prawie poszczególnych państw[17].

W zorganizowanych grupach przestępczych nie tylko działania mają charakter zorganizowany, jest to także cecha samych sprawców. Zaplanowane działanie ma na celu zgromadzenie dużych zysków w przemyślany sposób, w podejmowanych przedsięwzięciach nie ma przypadkowego, impulsywnego działania[18].

Pierwsze cyberprzestępstwa obejmowały ataki skierowane na komputery bądź sieci komputerowe oraz dane, które się w nich znajdowały. W późniejszym etapie przestępstwa te polegały na ataku na integralność systemów teleinformatycznych. Aktualnie dochodzi do cyberprzestępstw trzeciej generacji, charakteryzują się one używaniem specjalistycznego oprogramowania do popełniania przestępstw. Ewolucja działań przestępczych doprowadziła do tego, że czyny zabronione nie są popełniane bezpośrednio przez sprawców, lecz za pomocą oprogramowania stworzonego w danym celu[19]. Podział aktualnie popełnianych cyberprzestępstw przyjęty przez międzynarodową Organizację Policji Interpol:

- oszustwa dokonane przy pomocy komputera;
- przestępstwa popełniane w sieci;
- dokonywanie sabotażu oprogramowania i sprzętu;
- naruszenie dostępu do zasobów, nieupoważnione wejście do systemu informatycznego[20].

Początki przestępczej działalności w cyberprzestrzeni to czas, gdy dominującą grupą były osoby indywidualne. Aktualnie za większością przestępstw, które są dokonywane stoją zespoły sprawców, które przybierają nowatorską do tej pory formę. Zespół, grupa składa się z osób, które kontaktują się ze sobą w niespotykany do tej pory sposób. Sprawcy prowadzą wymianę informacji poprzez korzystanie z komunikatorów gier online. Grupy, które komunikują się w wyżej przedstawiony sposób charakteryzują się małą liczebnością, skupiają jednak osoby posiadające określoną wiedzę oraz umiejętności, a ich sposób współpracy przypomina funkcjonowanie przedsiębiorstwa[21]. W zespole panuje odpowiedzialność za poszczególne elementy działalności oraz realizowanie określonych zadań. W przypadku gdy grupa przestępcza posiada wystarczające środki, staje się samowystarczalna w zakresie zapewnienia sobie wszystkich usług niezbędnych do popełnienia przestępstwa. Nie musi ona zlecać poszczególnych zadań osobom indywidualnym, które do grupy nie należą. Dzięki posiadaniu odpowiednich środków grupa może stać się na tyle hermetyczna i samodzielna, by znacznie zmniejszyć prawdopodobieństwo rozpracowania, identyfikacji przez służby oraz organy ścigania[22]. Grupy przestępcze przy planowaniu przedsięwzięcia przestępczego

17 Tamże, s. 36–37.

18 Tamże, s. 38.

19 M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8, s. 244.

20 Tamże, s. 249.

21 P. Ciszek, dz. cyt., s. 55.

22 Tamże, s. 55.

współpracują ze sobą, lecz ta współpraca przybiera nową formę. Nad zaplanowaniem oraz realizacją zadania czuwa zespół złożony z osób, które są ekspertami z dziedziny informatyki, używają one pseudonimów podczas kontaktowania się ze sobą, używają sieci Tor, która zapewnia anonimowość w czasie korzystania z zasobów Internetu bądź komunikatorów gier internetowych. Zorganizowane grupy przestępcze, które w swoich szeregach posiadają ekspertów z dziedziny informatyki, świadczą także usługi w tzw. „podziemiu internetowym", wyróżnia się cztery rodzaje usług internetowych świadczonych przez grupy przestępcze:

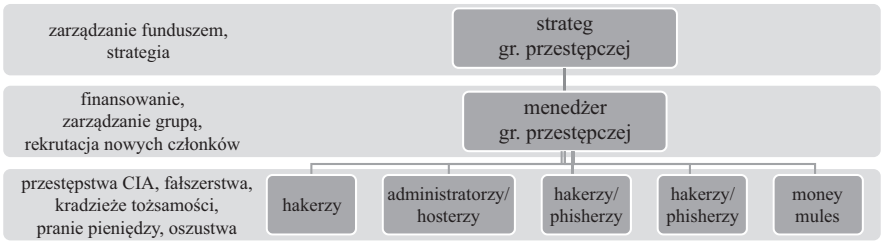
1. Stwarzanie narzędzi służących do popełniania przestępstw internetowych („crimeware as a service") – w tę kategorie usług wpisuje się tworzenie oprogramowania, które wychwytuje luki oraz błędy programów, które następnie sprawcy wykorzystują do popełniania konkretnych przestępstw. Jest to także tworzenie oprogramowania, które ma funkcję pomocniczą podczas ataku, popełniania przestępstwa oraz narzędzi, które mają ukryć obecność złośliwego oprogramowania, konstruowanie sprzętu służącego do pozyskiwania danych np. skimmery kart płatniczych a także urządzeń ułatwiających włamania np. podsłuchy.
2. Zlecanie wykonania cyberprzestępstwa („hucking as a service") – czyli zlecenie wykonania konkretnego przestępstwa innym osobom, należy pamiętać, że w tym przypadku zleceniodawca usług nie musi posiadać wiedzy specjalistycznej dotyczącej ataku, koszt takiej usługi przewyższa koszt nabycia poszczególnych programów oraz narzędzi służących do popełnienia czynu zabronionego. Ten rodzaj usług oferowanych przez cyberprzestępców obejmuje także dostarczanie informacji służących do kradzieży tożsamości, dane dotyczące logowania.
3. Badania („research as a service") – jest to oferowanie podatności oprogramowania, nim na rynku pojawi się poprawka, ulepszony program który naprawił tę podatność. W przeciwieństwie do pozostałych rodzajów usług świadczonych przez grupy przestępcze badania nie muszą pochodzić ze źródeł nielegalnych.
4. Infrastruktura cyberprzestępstw („cybercrime infrastructure as a service") – opracowanie narzędzi służących do popełnienia przestępstwa i ich wykorzystanie np. wynajęcie sieci komputerów w celu przeprowadzenia ataku. Jest to zapewnienie sobie narzędzi niezbędnych do popełnienia przestępstwa, w poczet tych działań wchodzi wymiana narzędzi bądź ich odpowiednia konfiguracja poprzez posiadanie odpowiedniej platformy do tego służącej[23].

Zorganizowane grupy cyberprzestępcze stwarzają pomiędzy członkami powiązania o charakterze funkcjonalnym, następuje także rozdział zadań w sieci przestępczej. Grupa przestępcza musi posiadać osobę, która pełni role stratega, to ona wyznacza podejmowane działania aktualne oraz przyszłe, zarządza też finansami. Tak jak w przypadku współczesnych korporacji oraz przedsiębiorstw, w strukturze grupy przestępczej wykształciła się rola menedżera, który zajmuje się zarządzaniem bezpośrednim, to on kontaktuje się osobami, które wykonują zlecone przez niego zadania, polecenia. Określenie zadań scedowanych na poszczególnych wykonawców jest zależne od ich obszaru działania. Wyraźnie określona hierarchia każdemu z członków grupy jasno przydziela jego rolę w procederze przestęp-

[23] Tamże, s. 52–53.

czym. Na najniższym szczeblu znajdują tzw. „mules" – „muły", które odpowiedzialne są za całość przygotowań. Na średnim szczeblu hierarchii znajdują się osoby świadczące usługi takie jak pranie pieniędzy, wynajem botnetów. Najwyższy szczebel grupy stanowią osoby, które są specjalistami, wysokokwalifikowanymi ekspertami dziedzinowymi, administratorami, doskonalą narzędzia przestępcze. Członkowie grupy, którzy należą do najwyższego poziomu czerpią największe zyski z działalności przestępczej[24].

Rysunek 1. Poziomy oraz funkcje pełnione przez członków grupy cyberprzestępczej



Źródło: J. Kosiński, *Paradygmaty cyberterroryzmu*, Warszawa 2015.

Popełnianie przestępstw w sieci Internet, bądź za pomocą komputera zostało określone mianem cyberprzestępstwa. Termin ten jest szeroko definiowany jako działanie w sferze IT podmiotów niepaństwowych o charakterze nielegalnym, gdzie celem jest zdobycie zysku. Nie zawsze jest to jedyny cel sprawcy, ale zawsze jest to główny czynnik jego działania[25]. Pierwsze przestępstwa, których dopuszczano się w cyberprzestrzeni były popełniane przez hakerów, którzy kierowali się w swoich działaniach chęcią pokazania swoich umiejętności lub pomocą przyjacielską dla innych hakerów. Włamania na strony internetowe bądź kradzieże danych usprawiedliwiali niekiedy większym dobrem np. chęcią by jak najwięcej osób poznało prawdę o danym wydarzeniu[26]. Wraz z rozwojem technologii oraz możliwości popełniania przestępstw w sieci doszło do przekształcenia się pojedynczego sprawcy w grupę, która dostrzegła korzyści płynące z popełniania przestępstw w sieci. W 2012 roku oszacowano, że zyski cyberprzestępczości wynosiły 1 bilion dolarów[27]. Aktualnie około 80% przestępstw popełnianych w intrenecie jest popełnianych przez zorganizowane gangi, grupy przestępcze. Cechami przestępczości w przestrzeni cybernetycznej są:

- międzynarodowy zasięg;
- niskie koszty działalności przestępczej, duże korzyści;
- nieświadomość ofiary oraz rzadko składane doniesienie z wyłączeniem przypadków w których doszło do dużych strat;
- łatwość w obsłudze technologii informatycznej;
- krótki czas potrzebny do popełnienia przestępstwa[28].

24 J. Kosiński, dz. cyt., s. 262–263.

25 D. Krawczyk, dz. cyt., s. 44.

26 P. Ciszek, dz. cyt., s. 50.

27 Tamże, s. 50.

28 Tamże, s. 50.

Wyżej przytoczone cechy przestępstw w cyberprzestrzeni były powodami dla których zainteresowanie tą formą działalności przestępczej zbudziło zainteresowanie zorganizowanych grup przestępczych. Należy jednak zauważyć, że działalność zorganizowanych grup w cyberprzestrzeni nie zawsze spełnia wszystkie przesłanki potrzebne do sklasyfikowania jej jako przestępczość zorganizowaną z uwagi na fakt, iż brak jest w nich jednego wyraźnego przywódcy oraz z uwagi na to, że w realizacji swoich celów nie zawsze sięgają po przymus fizyczny[29]. Cyberprzestępczość zorganizowana to dziedzina działalności nielegalnej zdominowana przez grupy przestępcze o charakterze transnarodowym, nie jest to jednak reguła gdyż działalność tego typu prowadzić mogą również grupy o mniejszym zorganizowaniu, które nie posiadają tak rozległego zaplecza finansowego oraz naukowego, których zasięg działalności ogranicza się do terytorium jednego państwa[30]. Dzięki rozwiniętej komunikacji oraz różnorodności kanałów do niej służących kontakt z osobami na innej części globu nie jest problemem, także w kontekście planowania działań przez grupę przestępczą. Posługując się stosownym oprogramowaniem oraz dostępem do sieci, sprawca jest zdolny do popełnienia przestępstwa na terenie jednego państwa będąc jednocześnie na terenie innego. Z uwagi na różnorodność przestępstw popełnianych w cyberprzestrzeni powstają grupy przestępcze, które odchodzą od multiprzestępczości, specjalizując się w tej konkretnej dziedzinie[31]. Grupy te skupiają osoby, które posiadają identycznie motywy działania oraz niezbędne umiejętności i wiedzę by popełniać przestępstwa w cyberprzestrzeni. Przestępczość komputerowa to działalność przynosząca duże dochody. Jej dochodowość znacznie przewyższa zyski narkotykowych karteli. W roku 2011 straty poniesione w wyniku działania cyberprzestępców zostały w Stanach Zjednoczonych określone na 12 mld USD. Równocześnie ze wzrostem przestępczości w cyberprzestrzeni, FBI odnotowało znaczny spadek tradycyjnych form przestępczości o charakterze fizycznym[32]. Poprzez wykorzystanie technologii oraz narzędzi komunikacji w sferze biznesowej, a także gospodarczej dochodzi do ułatwień w procesie popełniania przestępstw z katalogu zainteresowań zorganizowanych grup przestępczych popełnianych dotychczas poza cyberprzestrzenią. Dzięki wykorzystaniu komunikatorów internetowych, e-maili, telefonii internetowej w przepływie informacji wzrasta anonimowość członków grupy przestępczej oraz maleje prawdopodobieństwo wykrycia rozmów[33]. Przestępstwa komputerowe to głównie przestępstwa o tradycyjnym charakterze, do których używa się komputera. Dzięki zastosowaniu najnowszej dostępnej technologii ich popełnianie jest znacznie ułatwione. Do tej kategorii zalicza się także wyłudzenia kwot pieniędzy poprzez przesyłanie na telefon płatnych wiadomości sms[34]. Do korzystania z dostępnych narzędzi dochodzi w zależności od rodzaju planowanego ataku. Jakość narzędzi, jakie posiadają sprawcy przestępstw pozwala na niewidoczną penetrację sieci komputerowej z możliwością braku wykrycia przestępstwa przez

29 Tamże, s. 50.

30 D. Krawczyk, dz. cyt., s. 44.

31 Z. Płoszyński, *Przestępczość internetowa*, „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2012, nr 3, s. 42.

32 P. Ciszek, dz. cyt., s. 48.

33 J. Kosiński, dz. cyt., s. 261.

34 Tamże, s. 59.

miesiące lub nawet lata. W swojej działalności przestępczej zorganizowane grupy niejednokrotnie korzystają z tzw. botnetów, czyli grup komputerów zainfekowanych szkodliwym oprogramowaniem. Sam handel botnetami jest działalnością wysokodochodową[35]. Sposoby popełniania przestępstw w cyberprzestrzeni można podzielić na 3 rodzaje:

- posłużenie się dostępną technologią IT w celu usprawnienia przepływu informacji pomiędzy członkami grupy, bardziej zaawansowanego zorganizowania grupy;
- użycie technologii IT bezpośrednio w celu realizacji procederu przestępczego;
- wykorzystanie posiadanej technologii IT w kontekście ofensywnym jako działanie wymierzone przeciwko użytkownikom cyberprzestrzeni[36].

Na ataki cyberprzestępców narażone są głównie systemy, w których dochodzi do przesyłania informacji, ich wymiany, głównie oprogramowania zarówno użytkowników indywidualnych jak i organizacji, przedsiębiorstw a także aplikacje[37]. Wzrost zorganizowanej przestępczości w cyberprzestrzeni spowodował, że wyodrębniono nowy rodzaj zagrożeń – *Advanced Presistent Threats*. Jest to atak na wybrany cel np. bank, który charakteryzuje się swoistym skoncentrowaniem oraz wielowymiarowością. Podczas ataku dochodzi do prób sforsowania zabezpieczeń, wyszukiwania luk w oprogramowaniu a także wykorzystania wszelkich czynności mających miejsce w systemie organizacji np. wejście na portal społecznościowy przez pracownika. Ten rodzaj ataku został sklasyfikowany jako osobna kategoria zagrożeń przestępstw komputerowych, z uwagi na fakt wykorzystania podczas ataku każdego urządzenia, które posiada dostęp do infrastruktury organizacji, przy czym tym urządzeniem nie musi być komputer. Poprzez uzyskanie dostępu do urządzeń multimedialnych używanych przez pracobiorców można dokonać przesłania pracownikowi wiadomość email, która będzie zainfekowana, w takim stopniu poddaną spreparowaniu, że jej zawirusowanie nie zostanie rozpoznawane przez system bezpieczeństwa oprogramowania ochronnego. Tak przesłany wirus nie musi się uaktywnić od razu po otworzeniu wiadomości. Może przebywać w systemie będąc w trybie uśpienia i dopiero w sprzyjającym momencie rozpocząć infiltrację i atak na system. Wirus ten może także w odpowiednim momencie przygotować dane a następnie dokonać ich wysłania za pomocą transmisji szyfrowanej z wcześniej zidentyfikowanym serwerem. Po ukończonym zadania dochodzi do samozniszczenia wirusa, co doprowadza do tego, że użytkownik pozostaje w niewiedzy o wykonanej operacji oraz w przeświadczeniu bezpieczeństwa danych i systemu na którym pracuje[38]. Inwestowanie w środki ochrony komputera podczas korzystania z sieci stwarzają fałszywe poczucie bezpieczeństwa nie tylko wśród użytkowników indywidualnych, ale również w organizacjach komercyjnych. Mimo daleko idących przedsięwzięć mających na celu zabezpieczenie przed atakiem, nie są one w stanie uchronić systemu przed cyberprzestępcami. Dzieje się tak dlatego, że pojawiają się coraz to nowe formy ataków, przy których sprawcy korzystają z wyspecjalizowanych narzędzi bardziej zaawansowanych niż przyjęte formy ochrony[39]. Jako przykład w wykorzystywaniu przez przestępczość zorganizowaną

35 P. Ciszek, dz. cyt., s. 52.

36 D. Krawczyk, dz. cyt., s. 44.

37 Z. Płoszyński, dz. cyt., s. 38.

38 P. Ciszek, dz. cyt., s. 54.

39 Tamże, s. 53.

nowoczesnych technologii można podać funkcjonowanie tzw. botnetów. Warto zaznaczyć, że nie są one wykorzystywane jedynie jako rozwiązanie o charakterze informatycznych, lecz również należą do biznesowej platformy sprawców przestępstw[40]. Grupy przestępcze używające botnetów w swoim działaniu nie posiadają wszystkich cech charakteryzujących zorganizowaną przestępczość, działają poza przyjętymi do tej pory schematami. Rodzi to trudności w ich identyfikacji oraz w procesie zwalczania oraz ścigania. W ich strukturach często brakuje wyraźnego lidera, nie sięgają po przymus fizyczny. Należy jednak zaznaczyć, że spełniają 4 podstawowe kryteria identyfikacji zorganizowanej przestępczości tj.:

- współpraca więcej niż 2 osób;
- stosowanie form dyscypliny/ kontroli;
- wyznaczenie zadań do realizacji dla każdej z osób;
- współdziałanie osób w grupie przez czas nie określony bądź określony (kryterium to służby ukazaniu stabilności oraz trwałości grupy)[41].

Zarówno w sferze gospodarczo-biznesowej, jak i sferze użytkowników indywidualnych poprzez korzystanie z sieci można dotrzeć ze swoim komunikatem w dowolnie wybrany przez nas rejon świata. Międzynarodowe firny większość spraw związanych ze swoją działalnością realizują za pośrednictwem komunikowania się w sieci. Aby ułatwić transakcje internetowe stworzono wirtualną walutę tj. bitcoin, która nie posiada swojej materialnej wersji. Bitcoin nie jest jako waluta przypisany do żadnego państwa, nie jest również zależny od polityki jakiegokolwiek banku. Obrót wirtualną walutą opiera się na technologiach informatycznych, gdzie w sieci dochodzi do transakcji pomiędzy poszczególnymi użytkownikami[42]. Każdy z użytkowników programu może liczyć na anonimowość, gdyż zawartość jego wirtualnego portfela nie jest przypisana do konkretnej osoby. Transakcje pomiędzy użytkownikami oparte są na zasadzie węzłów „Peer-to-Peer". Waluta wirtualna jest w zainteresowaniu zorganizowanych grup przestępczych z uwagi na zalety wynikające z przeprowadzania nim transakcji[43]. Zainteresowanie prowadzeniem transakcji poprzez używanie bitcoina jest spowodowane maksimum anonimowości, która zapewniana jest podczas wykonywanej transakcji. Przepływ pieniądza realizowany za pośrednictwem programu, nie jest w żaden sposób kontrolowany, śledzony bądź archiwizowany, a dane które należy wpisać w potwierdzeniu przelewu są ograniczone do absolutnego minimum. Także szybkość wykonywanych transakcji jest niewątpliwą zaletą tego programu. Niemożliwym także staje się ustalenie stron uczestniczących w transakcji, gdy w krótkim czasie dochodzi do wielu operacji. Dużym atutem wirtualnej waluty jest swoboda dostępu do niej z dowolnego miejsca oraz bezpieczeństwo posiadanego wirtualnego portfela[44].

W kręgu zorganizowanych grup przestępczych pozostają także spamy. Są to niepożądane wiadomości głównie o charakterze marketingowym, które przesyłane są na skrzynkę email lub na telefony komórkowe. Z uwagi na fakt, że Internet jest miejscem, gdzie marketing się nieustannie rozwija, niemożliwym jest obecnie nie mieć choćby najmniejszego

40 J. Kosiński, dz. cyt., s. 261.

41 Tamże, s. 261.

42 A. Boszko, dz. cyt., s. 148.

43 Tamże, s. 148.

44 Tamże, s. 148–149.

kontaktu ze spamem. Spamy rozsyłane przez grupy przestępcze dotyczą zakupu leków, podrabianej markowej odzieży, bądź elektroniki. Do wysyłania tych wiadomości są wykorzystywane komputery umiejscowione głównie na terenie Azji. Dziennie komputery te są w stanie wysłać około 10 milionów spamów co przynosi miesięczny dochód wahający się w granicach 4000000 USD[45].

Nie tylko spamy są formą internetowej działalności zorganizowanych grup przestępczych. Zagrożenie związane jest z wirusami, trojanami, a także programami: spywere, adwere. Przesyłanie zainfekowanych plików, bądź oferowanie zainfekowanego programu ma na celu kradzież posiadanych przez użytkownika danych. Dane te dotyczą wszelkich operacji, które są wykonywane przez użytkownika w sieci, począwszy od haseł logowania i kodów kończąc na danych logowania do rachunku bankowego. Posiadając powyższe dane z łatwością można się podszyć pod daną osobę w sieci. Z uwagi na fakt, iż wiele z transakcji realizowanych jest poprzez internetowe przelewy prawdopodobieństwo użycia skradzionych danych związanych z rachunkiem bankowym staje się realne. Programy typu spywere są także umieszczane w różnego rodzaju gadżetach komputerowych np. grach komputerowych oraz dyskach zewnętrznych. Programy typu spywere są często używanym narzędziem służącym do wyłudzania danych. Natomiast programy typu adwere zazwyczaj ukryte są w ogłoszeniach o charakterze marketingowym, gdzie otworzenie przesłanej wiadomości powoduje automatyczne zakończenie pracy komputera. Po przechwyceniu danych oraz dokonaniu transakcji z użyciem skradzionych danych logowania, kradzieży tożsamości w ostatecznej fazie dochodzi do lokowania środków finansowych na bezpiecznych kontach bankowych sprawców przestępstwa[46].

Najczęstszym rodzajem cyberprzestępstw są te popełniane przy pomocy internetowych, elektronicznych metod płatniczych tzw. phishing. Przestępstwo to polega na uzyskaniu danych dotyczących logowania się na internetowe kontro bankowe tj. loginów, haseł, które umożliwiają wykonywanie transakcji internetowych. Przestępstwo to może być wykonywane przez międzynarodową grupę przestępczą i mieć charakter globalny a skradzione dane wrażliwe mogą dotyczyć użytkowników bankowości elektronicznej w różnych częściach globu[47]. Przestępczość związana z elektronicznymi sposobami płatności może być popełniana także na zasadzie skimmingu, czyli fałszowania kart płatniczych poprzez ich przerabianie, kopiowanie, podrabianie. Dane dotyczące kart płatniczych pozyskiwane są poprzez zakładanie w bankomatach urządzeń mających na celu zeskanowanie danych z pasków magnetycznych karty[48]. Do pozyskania danych w przestępstwie phishingu dochodzi także poprzez podszywanie się pod strony banków, które funkcjonują oficjalnie. Osoba, która myśli, że znajduje się na stronie swojego banku, w sposób nieświadomy podaje przestępcom swoje dane potrzebne do zalogowania się na swoje konto – login i hasło, kody dostępu[49]. Próby wyłudzenia danych wrażliwych konta internetowego polegają na:

45 Tamże, s. 151.

46 Tamże, s. 151.

47 W. Mądrzejowski, dz. cyt., s. 109.

48 Tamże, s. 110.

49 A. Boszko, dz. cyt., s. 152.

- wysyłaniu fałszywych wiadomości email posiadających odnośnik do nieprawdziwej strony banku, serwisu płatności on-line;
- rozsyłania oprogramowania komputerowego który jest zainfekowany poprzez np. konie trojańskie, programy spywere;
- zmiany w pliku hosts, który odpowiada za interpretowanie adresów IP i domen;
- zmiany w adresie IP, przekierowywanie użytkownika na inny serwer, na którym znajduje się podstawiona fałszywa strona np. banku;
- przesyłanie fałszywych wiadomości email, które mają udawać wiadomości dotyczące bezpieczeństwa podczas operacji elektronicznych w banku, emaile te posiadają w swojej treści prośbę o przesłanie kodów, pinów w celu wykonania weryfikacji[50].

Phishing to nie tylko kradzież danych potrzebnych do zalogowania się na konto bankowe, to również kradzież tożsamości użytkownika. Poprzez działania przestępcze sprawca pozyskuje dane osób, by wykorzystać je w dalszym procederze przestępczym. Do przestępstwa dochodzi dzięki wykorzystaniu odpowiednich środków technicznych oraz technologii informatycznej. W przypadku phishingu kradzież tożsamości może zostać poprzedzona oszustwem internetowym[51]. W Internecie funkcjonuje wiele forów internetowych, na których możliwe jest dokonanie zakupu szkodliwego oprogramowania, bądź danych niezbędnych do autoryzacji internetowych rachunków bankowych, cena dostępu zależy od lokalizacji konta oraz wysokości środków na nim dostępnych[52]. Także kradzież praw autorskich jest domeną zorganizowanych grup przestępczych, które czerpią zyski z nielegalnego upowszechniania w sieci utworów pozyskanych bez zgody ich twórców. Dodatkowo sprawcy dokonują ściągnięcia utworów z Internetu i przenoszą je na urządzenia przenośne, które trafiają do nielegalnej sprzedaży[53].

Z wirtualną działalnością zorganizowanych grup przestępczych związane są również gry hazardowe online. Firmy, które prowadzą tego rodzaju działalność zarejestrowane są w krajach, w których nie trzeba odprowadzać podatku np. Kajmany, Cypr. Z uwagi na fakt, iż gra odbywa się za pośrednictwem Internetu bądź drogą telefoniczną, trudno jest oszacować, jaka dokładnie jest skala zjawiska. Wysokość dochodów osiąganych przez grupy przestępcze trudniące się hazardem online są znane dopiero gdy dochodzi do zatrzymania sprawców procederu, gdy zapadają wyroki, a wysokie grzywny są natychmiastowo regulowane przez sprawców przestępstw. Świadczy to o tym, iż dochody uzyskane tytułem hazardu muszą być znacznie wyższe[54].

Cyberprzestępczość jest obecnie zjawiskiem dynamicznym, nieustannie ewoluującym. Przekształcenia oraz zmiany jakie mają miejsce wiążą się z dostępem do najnowszych technologii. Zorganizowane grupy przestępcze trudniące się procederem działają na zasadach syndykatu z międzynarodowym zasięgiem. Dla tych grup nie istnieją ograniczenia finansowe oraz legislacyjne z uwagi na fakt, iż do popełniania przestępstw używają one narzędzi

---

50 K. Ciulkin-Sarnocińska, *Phishing- specyficzna forma pozyskiwania danych newralgicznych*, [w:] E. Guzik-Makaruk, E. Pływaczewski, *Współczesne oblicza bezpieczeństwa*, Białystok 2015, s. 114.

51 Tamże, s. 116.

52 P. Ciszek, dz. cyt., s. 48.

53 A. Boszko, dz. cyt., s. 152.

54 Tamże, s. 155.

i rozwiązań technologicznych opartych na legalnej działalności. Uzależnienie współczesnego świata od technologii oraz postępująca informatyzacja wszystkich sektorów gospodarki, sfer życia czyni cyberprzestępczość problemem istotnym w kontekście międzynarodowym. Przekształcenia grup przestępczych jakie nastąpiły spowodowały utrudnienia w zidentyfikowaniu sprawców przestępstw z uwagi sposób komunikacji pomiędzy członkami grupy oraz wyspecjalizowanych narzędzi służących do popełniania procederu przestępczego. Walka z tym procederem jest wyzwaniem dla państw oraz organizacji międzynarodowych z uwagi na fakt, iż niektóre z państw nie są w posiadaniu narzędzi, które ułatwiłby reagowanie na cyberprzestępczość, nie mają stosownych uregulowań prawnych oraz nie posiadają odpowiednich rozwiązań technicznych. Niezbędne jest wypracowanie międzynarodowego porozumienia, gdyż żaden kraj nie jest sam bezpieczny w sieci globalnej[55].

Tytuł w języku angielskim:
CHARACTERISTICS OF CONTEMPORARY ORGANIZED CRIME

Bibliografia

Publikacje zwarte

Boszko A., *Finanse przestępczości zorganizowanej*, Toruń 2014.

Guzik-Makaruk E., Pływaczewski E. (red.), *Współczesne oblicza bezpieczeństwa*, Białystok 2015.

Kosiński J., *Paradygmaty cyberterroryzmu*, Warszawa 2015.

Mądrzejowski W., *Przestępczość zorganizowana. System zwalczania*, Warszawa 2015.

Zubrzycki W. (red.), *Przez przestępczość zorganizowaną do terroryzmu*, Szczytno 2015.

Artykuły

Krawczyk D., *Internet zagrożeniem dla bezpieczeństwa wewnętrznego*, „Horyzonty Bezpieczeństwa" 2016, nr 2 (1) 2.

Krukowski W., *Pojęcie organizacji przestępczej i przestępczości zorganizowanej*, „Prokuratura i Prawo" 2006, nr 1.

Płoszyński Z., *Przestępczość internetowa*, „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" 2012, nr 3.

Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8.

[55] P. Ciszek, dz. cyt., s. 57.