WYKRYWANIE CYBERZAGROŻEŃ I ZAPOBIEGANIE IM

Publikacja sfinansowana z funduszy Komisji Europejskiej w ramach programu Erasmus+. Publikacja została zrealizowana przy wsparciu finansowym Komisji Europejskiej. Publikacja odzwierciedla jedynie stanowisko jej autorów i Komisja Europejska oraz Narodowa Agencja Programu Erasmus+ nie ponoszą odpowiedzialności za jej zawartość merytoryczną. PUBLIKACJA BEZPŁATNA

Spis treści

1. Wprowadzenie

2. Pojęcie cyberprzestępczości i pojęcia pokrewne
2.1. Cyberprzestępczość
2.2. Klasyfikacja form cyberprzestępczości
2.3. Cyberatak
2.4. PODSUMOWANIE ROZDZIAŁU

3. Ochrona karna przed cyberprzestępczością
3.1. Cyberprzestępczość w dokumentach międzynarodowych i WE/UE
3.2. Merytoryczne aspekty cyberprzestępczości w Republice Czeskiej
3.3. Merytoryczne aspekty cyberprzestępczości w Polsce
3.4. Merytoryczne aspekty cyberprzestępczości w Portugalii

4. Przejawy cyberprzestępczości
4.1. Inżynieria społeczna (socjotechnika)
4.2. Botnet
4.3. Złośliwe oprogramowanie
4.4. Ransomware
4.5. Spam
4.6. Spam
4.7. Phishing, Pharming, Spear Phishing, Vishing, Smishing
4.8. Prześladowanie użytkowników poczty elektronicznej (BEC)
4.9. Nieuczciwe strony internetowe (firmy)
4.10. Hacking
4.11. Cracking
4.12. Piractwo internetowe (komputerowe)
4.13. Sniffing (wąchanie)
4.14. Ataki DoS, DDoS, DRDoS
4.15. Rozpowszechnianie szkodliwych treści
4.16. Cyberataki na sieci społecznościowe
4.17. Kradzież tożsamości
4.18. APT (Advanced Persistent Threat - zaawansowane trwałe zagrożenie)
4.19. Cyberterroryzm
4.20. PODSUMOWANIE

5. Wnioski

6. Wykorzystana literatura

1. Wprowadzenie

W dzisiejszych czasach nie sposób uciec od technologii informacyjnych i komunikacyjnych. Wkład tych technologii w życie społeczne we wszystkich dziedzinach działalności ludzkiej (np. medycyna, badania naukowe, bezpieczeństwo, transport itp.) jest niezaprzeczalny. Technologie informacyjno-komunikacyjne to najszybciej i najgwałtowniej rozwijający się sektor działalności człowieka.

Należy zdać sobie sprawę, że informacje i dane oraz ich wykorzystanie niosą ze sobą znaczny potencjał gospodarczy i polityczny. Informacja i jej treść mogą nie tylko decydować o istnieniu lub nieistnieniu jednostki czy firmy, ale w rzeczywistości mogą wpływać na rozwój świata.

Korzystanie z technologii informacyjnych i komunikacyjnych ma jednak swoje minusy. Jednym z nich jest niewątpliwie gigantyczny i dynamiczny rozwój "nowego rodzaju" przestępczości, z którą należy walczyć w taki sposób, aby nie stwarzać zagrożenia i nie naruszać interesów społeczeństwa. Przestępstwa te można zbiorczo określić mianem cyberprzestępczości. [1]

Należy zauważyć, że na całym świecie podejmowane są znaczne wysiłki, zarówno na poziomie prawnym, jak i instytucjonalnym, aby podjąć odpowiednie środki w odpowiedzi na to nowe i dynamiczne zjawisko naszych czasów. [2]

Trzy fakty stały się kluczowe dla rozwoju cyberprzestępczości. [3] Pierwszym z nich jest połączenie komputerów uniwersyteckich i utworzenie sieci komputerowej służącej do wymiany danych. [4] Drugim jest stworzenie pierwszego komputera osobistego (PC) przez firmę IBM pod koniec lat 80. Trzecim, i moim zdaniem najważniejszym, kamieniem milowym jest udostępnienie Internetu społeczeństwu, w tym dostosowanie poszczególnych aplikacji do formy bardziej przyjaznej dla użytkownika.

Rozwój dzisiejszego społeczeństwa cyfrowego nie opiera się bezpośrednio na rozwoju gospodarczym związanym z zasobami materialnymi, lecz na rozwoju technologii informatycznych, na podłączaniu coraz większej liczby użytkowników do Internetu, a zwłaszcza do aplikacji jako takich, a także na czerpaniu zysków z informacji i danych pochodzących od samych użytkowników. Zmiany te, związane z rozwojem technologii informatycznych, zachodzą zarówno w wymiarze społecznym, jak i ekonomicznym i są jedną z przyczyn powstawania cyberprzestępczości.

Cyberprzestrzeń jest obecnie najskuteczniejszą i najniebezpieczniejszą bronią w rękach cyberprzestępców. Nie chodzi o to, że cyberprzestrzeń, czy sam Internet, jest niebezpieczny lub niepewny. Chodzi o to, że system jest tylko tak silny, jak jego najsłabsze ogniwo. W tym przypadku, bardziej niż kiedykolwiek, najsłabszym elementem jest użytkownik. W rzeczywistości to użytkownik jest największym "zagrożeniem" dla siebie i swojego otoczenia, bo choć posiada osobowość prawną [5], to często ma jedynie minimalną wiedzę na temat swoich praw i obowiązków.

Internet stał się częścią naszego codziennego życia, a jego multimedialny aspekt rozwija się bardzo szybko. Czy tego chcemy, czy nie, Internet jest medium potężniejszym i bardziej drapieżnym niż telewizja czy jakiekolwiek inne medium masowe. Nawet zwykły użytkownik może teraz przekazywać lub narzucać swoje pomysły i opinie całej populacji świata za pomocą prostego interfejsu. I nie ma znaczenia, czy te idee są normalne, czy w jakikolwiek sposób wypaczone.

Z jednej strony Internet oferuje praktycznie nieograniczone możliwości pozyskiwania i przetwarzania informacji o niemal wszystkim, bez konieczności spędzania czasu w bibliotekach czy centrach informacyjnych poza domem (uzyskanie danej informacji to kwestia kilku sekund).

Google i Wikipedia stały się ważnymi, a często jedynymi źródłami informacji, na podstawie których podejmujemy decyzje. Internet umożliwia komunikację, zbliża ludzi do siebie, ułatwia wiele czynności dzięki możliwości znalezienia rozwiązań lub instrukcji, oferuje wiele różnych kanałów informacyjnych itp. Dzięki temu można to wszystko robić w zaciszu własnego domu i z poczuciem niemal całkowitej anonimowości.

Z drugiej strony, działania w tym wirtualnym środowisku mogą powodować duże straty finansowe, obawy przed naruszeniem prywatności przez obce osoby, utratę cennych danych osobowych, komunikację w sieci osób zaburzonych psychicznie (pedofilów, narkomanów, osób zdezorientowanych filozoficznie itp.), komunikowanie się tych osób z naszymi własnymi dziećmi za naszymi plecami, organizowanie grupom przestępczym nielegalnych działań bez możliwości przechwycenia przez osoby trzecie, oszustwa, nieuprawnione wkraczanie w sferę prywatną firm, przekierowywanie zleceń biznesowych, kradzież cudzych kont, niszczenie danych i baz danych, naruszanie praw autorskich itp.

Nie można dopuścić do tego, by cyberprzestrzeń stała się środowiskiem, w którym sprawcy mogą de facto bezkarnie popełniać wszelkie przestępstwa. Jest jednak tylko jeden punkt wyjścia do walki z przestępczością w cyberprzestrzeni - jest nim sama cyberprzestrzeń. Należy zrozumieć, czym tak naprawdę jest cyberprzestrzeń, na jakich zasadach funkcjonuje, jakie rodzaje przestępstw mogą mieć miejsce w tym wirtualnym świecie i co organy ścigania, a przede wszystkim sam użytkownik, mogą zrobić, aby zapobiec tej nielegalnej działalności.

Rzeczywiste zapobieganie wyżej wymienionym negatywnym zjawiskom musi koniecznie rozpocząć się od użytkowników końcowych, ponieważ w cyberprzestrzeni to właśnie oni są typowymi pierwszymi ofiarami napastnika. Opierając się na moim doświadczeniu jestem przekonany, że kształcenie i szkolenie użytkowników powinno być istotną częścią procesu wprowadzania technologii informacyjnych i komunikacyjnych do naszego życia. Uważam, że budowanie kompetencji informacyjnych powinno być nierozerwalnie związane z tworzeniem, dystrybucją i promocją produktów lub usług związanych z technologiami informacyjno-komunikacyjnymi. Rzeczywista edukacja w tym zakresie, a raczej zapoznanie z możliwymi zagrożeniami, ryzykiem i negatywnymi aspektami informatyki, powinna być częścią nauczania wszystkich form studiów na wszystkich poziomach edukacji.

W przypadku osób, które zajmują się tą problematyką w ramach swojego zawodu, przed tymi specjalistami stawiane są jeszcze wyższe wymagania, ponieważ muszą oni stale doskonalić się i szkolić, aby móc stawić czoła coraz to nowym i dynamicznie rosnącym atakom dokonywanym za pomocą i w środowisku TIK.

---

[1] Cyberprzestępczość jest często określana różnymi nazwami. Uważam, że cyberprzestępczość jest najbardziej opisowym określeniem tego bezprawnego działania. W niniejszej monografii w odniesieniu do tego zjawiska stosowane będą terminy: cyberprzestępstwo, cyberprzestępczość.

Jeśli przyjmiemy dosłowne tłumaczenie angielskiego tytułu Cybercrime, to tłumaczenie "cyberprzestępczość" nie jest dokładne, ponieważ dosłowne tłumaczenie tego połączenia dwóch słów można przetłumaczyć jako: cyberprzestępstwo (lub przestępstwa). W Republice Czeskiej powszechnie stosuje się również tłumaczenie Konwencji o cyberprzestępczości, choć nie jest ono, jak stwierdzono powyżej, dosłowne. Dlatego uważam, że nawet w

świetle tego tłumaczenia używanie terminu cyberprzestępczość nie jest błędem.

W kolejnej części publikacji zostanie przedstawiona definicja różnic pomiędzy cyberprzestępczością a działalnością przestępczą w tym obszarze, a także zarysowane zostaną poglądy różnych autorów na temat precyzyjnego określenia tego przestępstwa. W szczególności w niniejszej publikacji terminy cyberprzestępstwo i cyberprzestępczość będą używane synonimicznie.

[2] Np. walka z cyberprzestępczością: patrole cybernetyczne i internetowe zespoły dochodzeniowo-śledcze w celu wzmocnienia strategii UE. [online]. [cyt. 10.7.2016]. Dostępny pod adresem: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827

[3] Fakty te zostały następnie poparte szeregiem innych okoliczności (np. brakiem regulacji prawnych dotyczących Internetu, niemożnością egzekwowania prawa, poczuciem anonimowości użytkowników itp.)

[4] Więcej szczegółów można znaleźć w ARPANET lub NSFNET. Jest to okres końca lat sześćdziesiątych. Por. Historyczne mapy sieci komputerowych. [online]. [cyt. 2016-07-10]. Dostępne: https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html

[5] Mają prawa i obowiązki. Użytkownicy nawiązują, modyfikują i, w razie potrzeby, rozwiązują stosunki prawne.

2. Pojęcie cyberprzestępczości i pojęcia pokrewne

- 💻 Cyberprzestępczość
- 🖥️ Klasyfikacja form cyberprzestępczości
- 💻 Cyberatak

2.1. Cyberprzestępczość

Wykorzystanie komputerów, systemów informatycznych i technologii informacyjnych oraz ich integracja z niemal wszystkimi sektorami działalności człowieka jest zjawiskiem charakterystycznym dla naszych czasów. Można stwierdzić, że praktycznie niemożliwe jest znalezienie takiego obszaru działalności człowieka w którym informatyka, systemy informatyczne lub technologie informacyjne i komunikacyjne nie byłyby bezpośrednio lub pośrednio wykorzystywane.

Niestety, wraz z rosnącymi możliwościami korzystania z tych nowoczesnych udogodnień i postępem naukowo-technicznym, rosną też możliwości i częstotliwość ich nadużywania do popełniania przestępstw.

W latach 90. ubiegłego wieku ukuto termin "przestępczość komputerowa" (Computercrime, Computerkriminalität) na określenie przestępstw popełnianych z wykorzystaniem technologii informatycznych. W swojej publikacji Smejkal definiuje w połowie lat 90. przestępczość komputerową jako różnorodną mieszaninę przestępstw, których wspólnym czynnikiem jest komputer, program i dane. Termin przestępczość komputerowa "...należy rozumieć jako popełnianie czynów przestępczych z udziałem komputera jako zbioru sprzętu i oprogramowania, nie wyłączając danych, lub dużej liczby komputerów, zarówno oddzielnie, jak i połączonych w sieć komputerową, albo jako przedmiotu takich czynów przestępczych, z wyjątkiem jednak tych czynów przestępczych, których przedmiotem są opisane urządzenia jako mienie ruchome lub narzędzia przestępstwa. "[1] Z powyższej definicji jasno wynika, że przestępczość komputerowa odnosiła się wyłącznie do systemów komputerowych jako celów ataku.

Termin "przestępstwo komputerowe" kojarzy się z tym, że przestępstwo musi być popełnione na komputerze lub za jego pośrednictwem, najczęściej na komputerze osobistym (PC). Takie rozumienie jest obecnie uproszczone, a także w pewien sposób ogranicza ilościowo liczbę zjawisk, które można objąć terminem przestępstwa popełniane z wykorzystaniem technologii informacyjno-komunikacyjnych. Wiele współczesnych urządzeń technicznych, dzięki zastosowaniu mikroprocesorów i ich miniaturyzacji, już dawno przejęło funkcje komputerów osobistych (PC), nie nazywając ich jednak komputerami osobistymi. Są to urządzenia hybrydowe wykonujące różne funkcje, które wcześniej były wykonywane przez specjalne urządzenia. Współczesne urządzenia techniczne, które umożliwiają komunikację między sobą a użytkownikiem i których projektowaniu przyświeca idea ALL-IN-ONE, osiągają znacznie większą moc obliczeniową niż najnowocześniejsze jednostki obliczeniowe z pierwszej połowy lat 90. ubiegłego wieku. I nawet te urządzenia[2], choć nie nazywa się ich komputerami, mogą być celem przestępstw lub środkiem do ich popełnienia. Z tych powodów termin "przestępstwo komputerowe" lub "przestępczość komputerowa" jest obecnie rzadko używany w literaturze przedmiotu. Zamiast terminu "komputer" używa się obecnie terminu "technologia informacyjno-komunikacyjna" (ICT) lub "przestępczość teleinformatyczna"[3].

W 2000 r. Rada Europy opublikowała definicję przestępstwa komputerowego, zaczerpniętą ze Statutu Komisji Ekspertów ds. Przestępczości w Cyberprzestrzeni: "Przestępstwo skierowane przeciwko integralności, dostępności lub poufności systemów komputerowych lub przestępstwo w tradycyjnym rozumieniu, związane z wykorzystaniem nowoczesnych technologii informacyjnych i komunikacyjnych"[4].

Decyzja ramowa Rady UE 2002/584/WSiSW w sprawie europejskiego nakazu aresztowania definiuje "przestępstwa komputerowe" jako działania skierowane przeciwko komputerowi lub działania, w których komputer jest środkiem do popełnienia przestępstwa. Definicja cyberprzestępczości opiera się wówczas na treści europejskiego nakazu aresztowania.

W konwencjach międzynarodowych termin "cyberprzestępczość" jest najczęściej używany w odniesieniu do przestępstw popełnianych za pomocą technologii informatycznych, a stosowanie tego terminu zostało przeniesione ze sfery normatywnej do słownictwa społeczności zawodowej. Termin "cyberprzestępczość" jest podobny do terminów "przestępstwa z użyciem przemocy", "przestępstwa młodocianych", "przestępstwa gospodarcze" itp. Nazwy takie stosuje się w odniesieniu do grup przestępstw, które mają pewien wspólny czynnik, np. sposób wykonania, osobę sprawcy (przynajmniej pod względem rodzaju) itp. W gruncie rzeczy mogą one stanowić bardzo zróżnicowany zestaw przestępstw powiązanych wspólnym czynnikiem (komputer, program, dane)"[5].

Definiując treść terminu cyberprzestępczość, należy zauważyć, że wraz ze wzrostem możliwości wykorzystania środków informacyjno-komunikacyjnych rośnie również możliwość ich użycia (nadużycia) do popełniania przestępstw. Dlatego też w zasadzie nie istnieje uniwersalna, ogólnie przyjęta definicja, która w pełni oddawałaby zakres i głębię tego pojęcia.

Jedną z możliwych definicji przestępstwa komputerowego lub cyberprzestępstwa można znaleźć w Interpretive Dictionary of Cybersecurity[6]:

Cyber crime

„Criminal activity in which a computer appears in some way as an aggregate of hardware and software (including data), or only some of its components may appear, or sometimes a larger number of computers either standalone or interconnected into a computer network appear, and this either as the object of interest of this criminal activity (with the exception of such criminal activity whose objects are the described devices considered as immovable property) or as the environment (object) or as the instrument of criminal activity (See Computer crime).“

Przestępstwa komputerowe / cyberprzestępczość

"Przestępstwo popełnione przy użyciu systemu przetwarzania danych lub sieci komputerowej albo bezpośrednio z nimi związane".

W tych dwóch definicjach widać próbę zdefiniowania wszystkich aspektów cyberprzestępczości, ale autorzy popełnili pewne nieścisłości. Po pierwsze, używa się tych dwóch terminów synonimicznie, ale w definicji cyberprzestępczości pomija się fakt, że komputer jest zarówno celem, jak i środkiem ataku. Podobne problemy związane z faktycznym zdefiniowaniem cyberprzestępczości można znaleźć w innych miejscach.

Biorąc pod uwagę wysiłki zmierzające do zdefiniowania pojęcia cyberprzestępczości, należy posłużyć się Konwencją Rady Europy nr 185 o cyberprzestępczości z 23 listopada 2001 r. [7] Konwencja ta nie definiuje jednak faktycznego pojęcia cyberprzestępczości. Określa ona jedynie środki, które powinny zostać podjęte przez stronę ratyfikującą na poziomie krajowym. Te środki w dziedzinie prawa karnego materialnego określają następnie przybliżone ramy przestępstw uznawanych za cyberprzestępstwa. Ta ramowa definicja (wraz z innymi przestępstwami zawartymi w Protokole dodatkowym nr 189 Rady Europy do Konwencji o cyberprzestępczości[8]) stanowi podstawową przestrzeń dla ujednolicenia prawnego przestępstw,

które można uznać za cyberprzestępstwa w różnych krajach. Rzeczywista, często bardzo ścisła, definicja omawianych przestępstw jest raczej na korzyść, ponieważ nie ogranicza ona krajowej (bardziej szczegółowej lub rozbudowanej) implementacji tych przestępstw, ale jednocześnie zapewnia spełnienie minimalnych wymagań (standardów) przez wszystkie strony ratyfikujące.

Również z powodu znacznej różnicy zdań na temat tego, co jest, a co nie jest cyberprzestępstwem, w dalszej części tego rozdziału zdefiniujemy to pojęcie, zarówno w sensie pozytywnym, jak i negatywnym.

W najbardziej ogólnym ujęciu cyberprzestępczość można zdefiniować jako czyn skierowany przeciwko komputerowi lub sieci komputerowej albo czyn, w którym komputer jest wykorzystywany jako narzędzie do popełnienia przestępstwa. Fakt, że sieć komputerowa lub cyberprzestrzeń jest środowiskiem, w którym odbywa się ta działalność, jest niezbędnym elementem, aby definicja cyberprzestępstwa miała zastosowanie.

Definiując pojęcie cyberprzestępczości, należy przede wszystkim zdefiniować pojęcie przestępstwa w ogóle. W związku z funkcjonowaniem systemów informatycznych, technologii komputerowej lub środków komunikacji dochodzi do szeregu działań, które z pewnością są niepożądane, ale nie są karalne z punktu widzenia prawa karnego, mimo że mogą być bardzo niebezpieczne (szkodliwe) dla społeczeństwa. Czyny takie nie mogą być a priori kwalifikowane jako przestępstwa komputerowe, informacyjne lub jakiekolwiek inne - nie są one w ogóle przestępstwami. Definiując pojęcie przestępstwa (które może być definiowane z kilku perspektyw - socjologicznej, prawnokarnej itd.), opieramy się na definicji przestępstwa jako ogółu czynów, które można zakwalifikować do określonego przestępstwa regulowanego przez prawo karne. Tak więc zgodnie z tą definicją nie są przestępstwem czyny, które nie spełniają żadnego z elementów przestępstwa, czyli nawet wykroczenia lub innego przestępstwa administracyjnego. Taka definicja przestępczości jest dość precyzyjna i może być stosowana nawet w dziedzinie technologii informacyjno-komunikacyjnych.

Charakterystyczne dla popełniania przestępstw w dziedzinie ICT jest jednak to, że przy ich popełnianiu wykorzystywane są takie procedury lub środki, których użycie nie wypełnia żadnego z elementów przestępstwa, ale które stanowią integralną część lub warunek wstępny innych czynów, które są już karalne na mocy prawa karnego. [9] Ponadto te niekaralne procedury lub środki stanowią ważne elementy w procesie wykrywania i wyjaśniania działalności przestępczej, których identyfikacja i zrozumienie odgrywa istotną rolę w wykrywaniu sprawców tego typu przestępstw.[10]

Cyberprzestępczość stanowi swego rodzaju najszerszy zbiór wszystkich działań przestępczych, które mają miejsce w środowisku technologii informacyjnych i komunikacyjnych. Przestępstwa popełnione w ramach tego zestawu można dalej klasyfikować i określać różnymi terminami w zależności od różnych aspektów. Na przykład "przestępstwa internetowe", "e-przestępstwa", "cyberterroryzm" lub "piractwo" mogą stanowić podzbiory cyberprzestępczości, a wyliczenie to nie wyczerpuje możliwych podzbiorów zachowań, które można objąć terminem cyberprzestępczość.

Termin cyberprzestępczość najczęściej odnosi się do czynów przestępczych związanych z technologiami informacyjnymi i komunikacyjnymi:

(a) wykorzystywane jako narzędzie do popełnienia przestępstwa,

(b) jest celem ataku sprawcy, przy czym atak ten stanowi przestępstwo.

Jednak taka definicja cyberprzestępczości nie jest już dziś aktualna. Obejmowałby on również przestępstwa, w których technologia informatyczna jest wykorzystywana, ale nie w kontekście jej normalnego użycia lub przeznaczenia (np. przypadki, w których sprawca wyrządza ofierze szkodę, uderzając monitor lub inną część komputera w tył głowy z zamiarem spowodowania obrażeń ciała; kradzież ciężarówki przewożącej podzespoły komputerowe itp.) Są to przestępstwa, w których ICT są używane niezgodnie z ich przeznaczeniem - np. jako broń, przedmiot o pewnej wartości pieniężnej, niezależnie od celu, jakiemu służą lub mają służyć. Do wykrywania i wyjaśniania takich przestępstw będą stosowane inne metody dochodzeniowe (np. metodyka dochodzeń w sprawie kradzieży itp.), a nie metodyka dochodzeń w sprawie cyberprzestępczości.

Aby można było mówić o cyberprzestępczości, należy umieścić technologie informacyjno-komunikacyjne, które zostały wykorzystane do popełnienia przestępstwa lub były jego celem, w określonym kontekście. W związku z tym do dwóch powyższych punktów należy dodać kolejny, zawierający ten warunek. Cyberprzestępczość to przestępczość, w której wykorzystuje się środki technologii informacyjnej i komunikacyjnej:

(a) wykorzystywane jako narzędzie do popełnienia przestępstwa,

(b) są celem ataku ze strony sprawcy, który to atak stanowi przestępstwo, pod warunkiem, że środki te są wykorzystywane lub nadużywane w środowisku informatycznym, systemowym, programowym lub komunikacyjnym (tj. w cyberprzestrzeni).

Taka definicja cyberprzestępczości jest jednak wciąż niewystarczająca. Stosując ustalone w ten sposób kryteria określania, czy dany czyn można uznać za cyberprzestępstwo, stwierdzamy, że na przykład w rozumieniu definicji udziału (organizacja, instrukcja i pomoc) w rozumieniu art. 24 ustawy nr 40/2009 Sb., Kodeks karny, z późniejszymi zmianami[11], każde przestępstwo umyślne można popełnić za pomocą informacji (np. osoba nakłania inną osobę do popełnienia umyślnego przestępstwa zabójstwa za pomocą wiadomości e-mail). Podobnie będą miały zastosowanie inne formy współpracy przestępczej (np. podżeganie, przyzwolenie na popełnienie czynu zabronionego). Można je również realizować za pomocą technologii informacyjnej. Takie działania nie mogą być jednak klasyfikowane jako cyberprzestępczość. W związku z tym przyjęcie przeciwnego poglądu prowadziłoby do jedynego możliwego wniosku - cyberprzestępstwem jest każde przestępstwo, w popełnieniu którego sprawca w jakikolwiek sposób wykorzystał technologie informacyjno-komunikacyjne. Z tego punktu widzenia trudno byłoby znaleźć przestępstwa, których nie można by uznać za cyberprzestępstwa.

Z powyższego wynika, że nie wystarczy zdefiniować cyberprzestępstwo tylko w kategoriach pozytywnych, ale trzeba je również zdefiniować poprzez wymienienie czynów, które z zasady nie mogą być uznane za cyberprzestępstwo.

W tym duchu możliwe będzie sklasyfikowanie trzech różnych kategorii przestępstw pod pojęciem cyberprzestępczości:

1) przestępstw, których indywidualnym przedmiotem charakteryzującym przestępstwo jest bezpośrednio ochrona systemu komputerowego, jego sprzętu i komponentów przed określonymi rodzajami ataków lub uzasadnione interesy osób w niezakłóconym korzystaniu z tych środków technicznych,

2) przestępstw, w przypadku których sposób popełnienia za pomocą technologii informacyjno-komunikacyjnych stanowi jedną z cech charakterystycznych przestępstwa,

3) inne istotne przestępstwa, które nie należą do pierwszej lub drugiej kategorii, ale które w konkretnym przypadku mogą być również popełnione z wykorzystaniem technologii informacyjnej i które odpowiadają powyższej definicji, ponieważ przy ich wykrywaniu i wyjaśnianiu można stosować procedury podobne do tych stosowanych w dochodzeniach w sprawie przestępstw z kategorii 1 i 2 (np. podobnie ukierunkowane ekspertyzy).

---

[1] SMEJKAL, Vladimír, Tomáš SOKOL i Martin VLČEK. *Počítačové právo.* Praha: C. H. Beck, 1995, s. 99

[2] Obecnie istnieje wiele urządzeń, które określa się mianem systemu komputerowego.

[3] Na przykład:

GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 32 a násl.

Smejkal, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue, 2003, roč. 2, č. 6, s. 161.

POŽÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, s. 249.

[4] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 5

[5] SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 19

[6] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 57 a 73. [online]. [cit.10.7.2016]. Dostępne: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

[7] Zwana dalej Konwencją o cyberprzestępczości. Więcej informacji można znaleźć na stronie: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[8] Zwany dalej Protokołem dodatkowym. ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

Bliże viz: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

[9] Na przykład wysyłanie wiadomości śmieci (SPAM). Spam może czasami być tylko wiadomością reklamową (handlową). Takie postępowanie nie jest karalne na mocy prawa karnego. Można sobie wyobrazić na przykład wysyłanie SPAM-u o podłożu politycznym, religijnym lub innym. W innych przypadkach SPAM może zawierać złośliwe oprogramowanie, które umożliwia uzyskanie nazwy użytkownika i hasła do konta bankowego klienta (co w pewnych okolicznościach może być kwalifikowane jako np. przygotowanie do przestępstwa).

[10] Przykładowo, dzięki komunikacji sprawcy z otoczeniem możliwe jest namierzenie adresu IP jego komputera, a następnie zlokalizowanie miejsca połączenia z Internetem.

[11] Zwany dalej Kodeksem Karnym lub KK.

2.2. Klasyfikacja form cyberprzestępczości

Uważam, że jeśli chcemy zająć się kwestią cyberprzestępczości, należałoby przynajmniej ogólnie określić, co może wchodzić w zakres tego przestępstwa. Dlatego na zakończenie tego podrozdziału chciałbym przedstawić czytelnikowi kilka klasyfikacji cyberprzestępczości (lub przestępczości komputerowej) w ujęciu różnych norm prawnych, różnych autorów oraz organizacji zajmujących się zwalczaniem cyberprzestępczości. Chcę też pokazać, jak na tych klasyfikacjach opiera się pogląd na cyberprzestępczość.

1. Klasyfikacja zgodnie z Konwencją o cyberprzestępczości i Protokołem dodatkowym.

Konwencja o cyberprzestępczości dzieli cyberprzestępstwa na cztery kategorie:

1. przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych,

2. przestępstwa komputerowe,

3. przestępstwa związane z treścią,

4. przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

W protokole dodatkowym określono dodatkowe przestępstwa związane z cyberprzestrzenią:

1. rozpowszechnianie materiałów rasistowskich i ksenofobicznych za pośrednictwem systemów komputerowych,

2. groźby o podłożu rasistowskim i ksenofobicznym,

3. zniewagi o podłożu rasistowskim i ksenofobicznym,

4. zaprzeczanie, rażące minimalizowanie, aprobowanie lub usprawiedliwianie ludobójstwa lub zbrodni przeciwko ludzkości.

2. Klasyfikacja Komitetu Ekspertów ds. Przestępczości w Cyberprzestrzeni

Zgodnie ze Statutem Komisji Ekspertów ds. Przestępczości w Cyberprzestrzeni Rady Europy z 2000 r., cyberprzestępczość można podzielić na:

1) W zależności od pozycji komputera w czasie popełniania przestępstwa:

- cel ataku;

- środki (narzędzia) ataku.

2. W zależności od rodzaju przestępstwa:

- tradycyjne przestępstwa (np. fałszowanie banknotów itp.)

- nowe przestępstwa (np. phishing, DDoS itp.)[1].

3. Klasyfikacja według eEurope+

Dokument ten dzieli przestępstwa komputerowe na:

1. przestępstwa naruszające prywatność

- Nielegalne gromadzenie, przechowywanie, modyfikowanie, ujawnianie i rozpowszechnianie danych osobowych.

2. przestępstwa związane z zawartością komputera

- Pornografia dziecięca, rasizm, podżeganie do przemocy itp.

3. ekonomiczne

- Nieuprawniony dostęp, sabotaż, hakerstwo, rozprzestrzenianie wirusów, szpiegostwo komputerowe, fałszerstwa komputerowe i oszustwa.

4. Przestępstwa związane z własnością intelektualną[2]

4. Klasyfikacja przestępstw komputerowych według kryminologii

Porada i Konrad[3] dzielą przestępczość komputerową na pięć podstawowych grup.

1. Nieuprawniona ingerencja w dane wejściowe

- zmiana dokumentu wejściowego do przetwarzania komputerowego,

- tworzenie dokumentu zawierającego fałszywe dane do późniejszego przetwarzania komputerowego.

2. Nieuprawnione zmiany w przechowywanych danych

   - ingerencja w dane, nieuprawniona ingerencja w dane, a następnie powrót do normalnego stanu.

3. Nieuprawnione instrukcje dotyczące obsługi komputera

   - bezpośrednia instrukcja wykonania operacji lub instalacja oprogramowania, które wykonuje operacje automatycznie.

4. Nieuprawnione włamanie do komputera, systemu komputerowego i jego baz danych

   - informacyjne wprowadzanie danych do bazy danych, bez wykorzystywania informacji,

   - nieuprawnione wykorzystanie informacji do użytku osobistego,

   - zmienianie, niszczenie lub zastępowanie informacji innymi informacjami,

   - nielegalne "przechwytywanie" i rejestrowanie ruchu w komunikacji elektronicznej.

5. Ingerowanie w cudzy komputer, oprogramowanie i pliki oraz dane w bazach danych

   - tworzenie programów w celu atakowania,

   - wprowadzenie wirusa do oprogramowania komputerowego,

   - zainfekowanie wirusami lub innymi programami.

5. Skupienie się Europolu na określonych rodzajach cyberprzestępstw według stopnia ich nasilenia

Europol przestrzega konwencji o cyberprzestępczości i stosuje się do zawartej w niej klasyfikacji przestępstw. Aby wspierać walkę z cyberprzestępczością i pomagać państwom członkowskim, w ramach Europolu utworzono europejskie centrum ds. walki z cyberprzestępczością (EC3)[4]. Zespół ten jasno zadeklarował zakres swoich kompetencji w walce z cyberprzestępczością i określił trzy punkty centralne (PR):

1. FP TERMINAL - oszustwo płatnicze. Grupa zajmująca się oszustwami internetowymi i udzielająca wsparcia w ich zwalczaniu.

2. FP Cyborg - Zbrodnie zaawansowane technologicznie. Grupa zajmująca się i zapewniająca wsparcie w różnych atakach cybernetycznych na infrastrukturę krytyczną[5] i systemy informatyczne. W szczególności ataki następujących typów: złośliwe oprogramowanie, oprogramowanie ransomware, hakerstwo, phishing, kradzież tożsamości itp.

3. Bliźniaki FP - wykorzystywanie seksualne dzieci. Grupa zajmująca się prowadzeniem dochodzeń w sprawie przestępstw związanych z seksualnym wykorzystywaniem dzieci i udzielająca wsparcia w tym zakresie.

6. Klasyfikacja cyberprzestępstw według ich związku ze środowiskiem cyfrowym

Wraz z rozwojem cyberprzestępczości jako takiej, w ostatnich latach coraz częściej pojawia się pogląd, że cyberprzestępczość można postrzegać jako zachowania, które można określić jako "czyste" lub "czysto" cyberprzestępcze. Takim postępowaniem można objąć wyłącznie ataki cybernetyczne, które miały miejsce w cyberprzestrzeni, a ich celem i narzędziem był system komputerowy lub dane. Zazwyczaj ataki te mają charakter hakerski, DoS, DDoS, ataki na infrastrukturę krytyczną itp.

Inne przestępstwa popełniane w środowisku cyberprzestrzeni uważa się jedynie za przeniesienie "starych" lub "zwykłych" zachowań przestępczych do nowego środowiska cyfrowego.

Zgodnie z powyższym podziałem, cyberprzestępczość można rozumieć w następujący sposób:

   - węższe pojęcie ("czysta" cyberprzestępczość);

   - szersze pojęcie ("zwykłe" zachowanie przestępcze w nowym środowisku).

7. Inne możliwe klasyfikacje cyberprzestępczości

Istnieje wiele innych sposobów klasyfikowania cyberprzestępczości, dlatego dla celów ilustracyjnych podajemy inne możliwe klasyfikacje cyberprzestępczości[6].

W tym miejscu pozwolę sobie również przedstawić klasyfikację, którą opracowałem na podstawie własnej wiedzy zdobytej głównie podczas interpretowania problematyki cyberprzestępczości na różnego rodzaju seminariach czy konferencjach.

W dużym uproszczeniu można stwierdzić, że cyberprzestępczość można podzielić na trzy aspekty:

1. w zależności od częstotliwości (charakteru) ataków:

(a) naruszenie praw autorskich (zob. piractwo internetowe (komputerowe)). Jest to czyn dominujący w cyberprzestrzeni, w którym dochodzi do naruszenia własności intelektualnej. Widoczne są wysiłki na rzecz zwalczania tego zjawiska, zwłaszcza ze strony prywatnych organizacji broniących praw autorów);

b) inne ataki cybernetyczne (zob. Przejawy cyberprzestępczości. Z wyjątkiem piractwa internetowego (komputerowego)).

2. W zależności od karalności wg prawa karnego:

(a) działanie prawnokarne - każde z wymienionych działań, które można powiązać z czynami zabronionymi pod groźbą kary;

b) zachowania nieobjęte przepisami prawa karnego (niekaralne) (niektóre z wymienionych zachowań nie mogą zostać objęte ustawowymi znamionami przestępstwa, nawet przy zastosowaniu dopuszczalnej analogii[7]).

3. W zależności od stopnia tolerancji ze strony większości społeczeństwa:

(a) zachowanie tolerowane przez społeczeństwo (najbardziej tolerowane jest zachowanie polegające na naruszeniu praw autorskich);

b) zachowania nieakceptowane przez społeczeństwo (np. pornografia dziecięca itp.).

---

[1] [online]. [cyt. 11.3.2010]. Dostępny pod adresem: http://assembly.coe.int/documents/WorkingDocs/doc01/edoc9263.htm

Por. MATĚJKA, Michał. Przestępstwa komputerowe. Praga: Computer Press, 2002, s. 49.

[2] Więcej informacji na ten temat można znaleźć w: JIROVSKÝ, Václav. Cyberprzestępczość to nie tylko hakerstwo, cracking, wirusy i trojany bez tajemnic. Praga: Grada, 2007, s. 92.

[3] Więcej informacji: STRAUS, Jiří et al. Kryminalistyczna metodologia. Pilzno: Aleš Čeněk, 2006, s. 272-274.

[4] Zwalczanie cyberprzestępczości w erze cyfrowej. [online]. [cyt. 7.5.2018]. Dostępny pod adresem: https://www.europol.europa.eu/ec3

[5] Jeśli chodzi o definicję terminu infrastruktura krytyczna, w Republice Czeskiej (w przypadku cyberprzestrzeni) należy oprzeć się na ustawie o bezpieczeństwie cybernetycznym i o zmianach w powiązanych ustawach (ustawa o bezpieczeństwie cybernetycznym zwana dalej ustawą o cyberbezpieczeństwie). W rozdziale 2 lit. b) ustawy zdefiniowano termin "krytyczna infrastruktura informatyczna" oraz "element lub system elementów infrastruktury krytycznej".

Definicja krytycznej infrastruktury informatycznej opiera się na przepisach regulujących zarządzanie kryzysowe. Krytyczna infrastruktura informatyczna jest częścią infrastruktury krytycznej w rozumieniu ustawy nr 240/2000 Sb. o zarządzaniu kryzysowym i o zmianach niektórych ustaw (ustawa o kryzysie), z późniejszymi zmianami ("ustawa o kryzysie"). Aby system lub usługa informatyczna oraz sieć łączności elektronicznej mogły zostać włączone do krytycznej infrastruktury informatycznej, muszą spełniać kryteria definicyjne infrastruktury krytycznej oraz element infrastruktury krytycznej określone w ustawie o kryzysie, a także kryteria przekrojowe i sektorowe określone w rozporządzeniu rządu nr 432/2010 Sb. w sprawie kryteriów określania elementu infrastruktury krytycznej.

W kryteriach sektorowych dotyczących wyznaczania elementu infrastruktury krytycznej, pkt VI. "Systemy łączności i informacji", punkt G.: obszar bezpieczeństwa cybernetycznego. Określa on sektorowe kryteria wyznaczania danego systemu informatycznego, usługi lub sieci łączności elektronicznej jako krytycznej infrastruktury informatycznej.

Definicja ta dotyczy jednak tylko obszaru cyberbezpieczeństwa. Ogólnie rzecz biorąc, infrastrukturę krytyczną można zdefiniować w następujący sposób:

1. Infrastruktura krytyczna oznacza element infrastruktury krytycznej lub system elementów infrastruktury krytycznej, których zakłócenie funkcjonowania miałoby poważny wpływ na bezpieczeństwo państwa, zabezpieczenie podstawowych potrzeb życiowych ludności, zdrowie ludzi lub gospodarkę państwa.

2. Element infrastruktury krytycznej oznacza budynek, urządzenie, zasób lub infrastrukturę publiczną określone zgodnie z kryteriami przekrojowymi i sektorowymi zawartymi w rozporządzeniu rządu nr 432/2010 Sb. w sprawie kryteriów określania elementu infrastruktury krytycznej.

3. Kryterium przekrojowym dla wyznaczenia elementu infrastruktury krytycznej jest aspekt:

(a) wypadki, których próg wynosi ponad 250 ofiar śmiertelnych lub ponad 2 500 osób z następującą po nich hospitalizacją przez ponad 24 godziny,

(b) skutki gospodarcze o progu strat gospodarczych dla państwa przekraczającym 0,5% produktu krajowego brutto; lub

(c) wpływ na społeczeństwo, którego progiem jest rozległe ograniczenie świadczenia podstawowych usług lub inne poważne zakłócenia życia codziennego dotyczące więcej niż 125 000 osób.

[6] Por. PROSISE, Chris i Kevin MANDIVA. Incident response & computer forensics, second ed. Emeryville: McGraw-Hill, 2003, s. 22ff.

Ponadto, np. Cyberprzestępczość. [online]. [cyt. 2015 luty 1].
Dostępne: http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime; id.

[7] Przez analogię rozumie się objęcie przypadku, który nie został wyraźnie wymieniony w ustawie karnej, podobnym przepisem ustawowym wymienionym w ustawie. W odróżnieniu od wykładni rozszerzającej, w analogii stosuje się przepis, który ze względu na swoje znaczenie nie ma zastosowania do sprawy będącej przedmiotem subsumcji. Wykładnia rozszerzająca jest dokonywana zgodnie z celem prawa karnego i w jego granicach, natomiast analogia przekracza te wyobrażone granice. Analogię stosuje się w celu wypełnienia luk w prawie. Dotyczy ona przypadków, których ustawodawca nie uregulował normą prawną. W warunkach Republiki Czeskiej nie może być ona wykorzystywana na niekorzyść (na szkodę) sprawcy (in malam partem).

Więcej informacji można znaleźć na stronie NOVOTNÝ, František, Josef SOUČEK et al. Prawo karne. 3. wydanie rozszerzone. Pilzno: Aleš Čeněk, 2010, s. 83.

2.3. Cyberatak

Prosise i Mandiva charakteryzują **"zdarzenie związane z bezpieczeństwem komputerowym"** (które może być rozumiane jako atak komputerowy lub przestępstwo komputerowe) jako nielegalne, nieuprawnione, niedopuszczalne działanie dotyczące systemu komputerowego lub sieci komputerowej. Działania te mogą mieć na celu np. kradzież danych osobowych, rozsyłanie spamu lub inne formy nękania, sprzeniewierzenie, rozpowszechnianie lub posiadanie pornografii dziecięcej itp.[1]

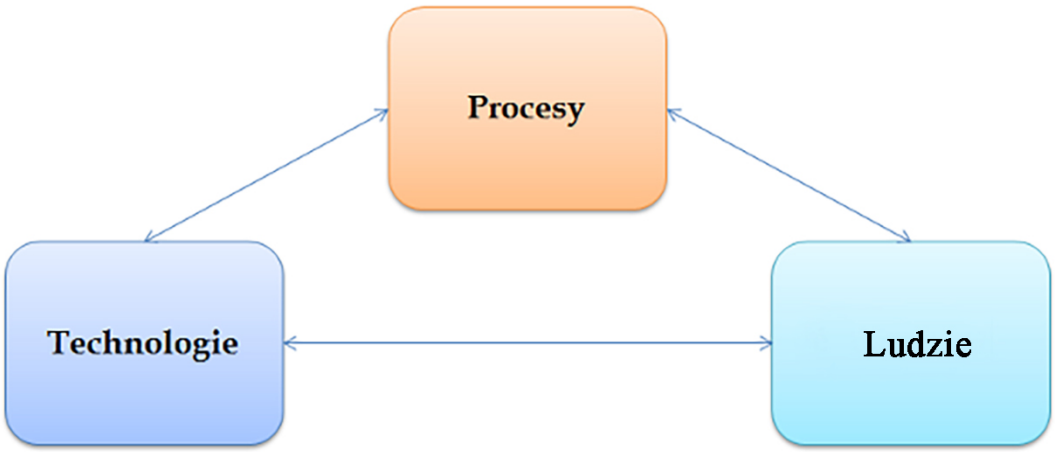
Jirásek i in. definiują cyberatak jako *"atak na infrastrukturę informatyczną w celu spowodowania szkód i uzyskania wrażliwych lub strategicznie ważnych informacji". Jest on najczęściej używany w kontekście ataków o podłożu politycznym lub militarnym."*[2]

Taka definicja cyberataku byłaby bardzo restrykcyjna i nie obejmowałaby wszystkich negatywnych działań użytkowników cyberprzestrzeni[3] , zwłaszcza że łączy w sobie warunki uszkodzenia systemu informatycznego i pozyskania informacji. Cyberatak może być również działaniem socjotechnicznym, w którym jedynym celem jest uzyskanie informacji, lub odwrotnie - atakiem DoS lub DDoS, w którym jedynym celem może być zablokowanie (tj. nieuszkodzenie) funkcjonalności jednego lub kilku systemów komputerowych lub świadczonych usług.

Na podstawie powyższych rozważań **atak cybernetyczny**[4] można zdefiniować jako **każde bezprawne działanie napastnika w cyberprzestrzeni, skierowane przeciwko interesom innej osoby**. Czyny te nie zawsze muszą przybierać formę przestępstwa, ważne jest, by zakłócały normalny tryb życia ofiary. Atak cybernetyczny może być zakończony, jak również znajdować się w fazie przygotowań lub prób.[5]

Cyberprzestępstwo musi być również atakiem cybernetycznym, ale nie każdy atak cybernetyczny musi być przestępstwem. Wiele ataków cybernetycznych może, nawet przy braku normy prawnokarnej, zostać zaliczonych do czynów, które będą miały charakter przestępstw cywilnych lub administracyjnych, lub też mogą nie być czynami karalnymi na podstawie jakiejkolwiek normy prawnej (np. mogą to być tylko czyny niemoralne lub nieumyślne).

Powodzenie ataku cybernetycznego zależy zazwyczaj od naruszenia jednego z elementów składających się na bezpieczeństwo cybernetyczne (**ludzie, procesy i technologia**). **Elementy te muszą być stosowane lub modyfikowane w całym cyklu życia. W szczególności zapobieganie, wykrywanie i reagowanie na atak.**[6] Bezpieczeństwo technologii informatycznych, informacji i danych jest również bezpośrednio uzależnione od przestrzegania zasad "C", "I", "A".



Elementy bezpieczeństwa cybernetycznego

Chcąc zdefiniować pojęcie cyberataku, należy posłużyć się definicjami wynikającymi z ustawy nr 181/2014 Sb. o cyberbezpieczeństwie i o zmianach w powiązanych ustawach (ustawa o cyberbezpieczeństwie).[7] W sekcji 7 ustawy zdefiniowano pojęcia "zdarzenie zagrażające bezpieczeństwu cybernetycznemu" i "incydent zagrażający bezpieczeństwu cybernetycznemu". **Incydent bezpieczeństwa cybernetycznego** to *"zdarzenie, które może spowodować naruszenie bezpieczeństwa informacji w systemach informatycznych lub naruszenie bezpieczeństwa usług albo bezpieczeństwa i integralności sieci łączności elektronicznej".* De facto jest to zdarzenie, które nie ma realnych negatywnych konsekwencji dla danego systemu komunikacyjnego lub informatycznego, ale w istocie jest to tylko zagrożenie, które musi być realne**.**

Incydent bezpieczeństwa cybernetycznego to *"naruszenie bezpieczeństwa informacji w systemach informatycznych lub naruszenie bezpieczeństwa usług i/lub bezpieczeństwa i integralności sieci łączności elektronicznej w wyniku zdarzenia związanego z bezpieczeństwem cybernetycznym".* Incydentem związanym z bezpieczeństwem cybernetycznym jest zatem naruszenie bezpieczeństwa informacji w systemach informatycznych lub naruszenie bezpieczeństwa usług albo bezpieczeństwa i integralności sieci łączności elektronicznej, tj. zakłócenie działania systemu informacyjnego lub komunikacyjnego o negatywnych skutkach.

---

[1] PROSISE, Chris i Kevin MANDIVA. *Reagowanie na incydenty i informatyka śledcza, wydanie drugie.* Emeryville : McGraw-Hill, 2003, s. 13.

Por. dalej CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* Londyn: Academic Press, 2004, s. 9 i nast.

[2] JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [Wydanie 2. zaktualizowane. 2. edycja: AFCEA, 2015, s. 59. Dostępny w Internecie: http://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/

[3] W szczególności w definicji brakuje określenia jakiejkolwiek innej motywacji atakującego niż ta, która miałaby na celu ...*spowodowanie szkód lub zdobycie strategicznie ważnych informacji*. Przykładem nieobjętym tą definicją są ataki o podłożu ekonomicznym, których liczba obecnie gwałtownie wzrasta.

[4] Należy odróżnić pojęcie **incydentu bezpieczeństwa** od pojęcia cyberataku, który stanowi naruszenie bezpieczeństwa IS/IT i zasad zdefiniowanych w celu jego ochrony (polityka bezpieczeństwa).

[5] Przykładem może być atak wirusa Conficker stworzonego przez botnet. To kończy atak. Pozostaje jednak pytanie, do jakich celów ostatecznie zostanie wykorzystana ta sieć (być może jest to przygotowanie do znacznie poważniejszego ataku cybernetycznego).

[6] Więcej informacji na ten temat można znaleźć w artykule SVOBODA, Ivan. *Rozwiązania w zakresie cyberbezpieczeństwa.* Wykład w Akademii CRIF. (23. 9. 2014)

[7] Zwana dalej **ustawą o bezpieczeństwie cybernetycznym**

2.4. PODSUMOWANIE ROZDZIAŁU

ℹ️

PODSTAWOWE INFORMACJE

· Aby zrozumieć problematykę cyberataków i cyberprzestępczości, należy poznać podstawową terminologię bezpośrednio związaną z wybraną dziedziną. W niniejszym rozdziale przedstawiono wybrane terminy techniczne i prawne.

· Nie sposób znaleźć dziedziny działalności ludzkiej, w której technologia komputerowa, system informatyczny lub technologia informacyjna czy komunikacyjna nie byłyby bezpośrednio lub pośrednio wykorzystywane.

· Pojęcie cyberprzestępczości jest podobne do takich pojęć jak "przestępstwa z użyciem przemocy", "przestępstwa młodocianych", "przestępstwa gospodarcze" itp. Nazwy takie stosuje się w odniesieniu do grup przestępstw, które mają pewien wspólny czynnik, np. sposób wykonania, osobę sprawcy (przynajmniej pod względem rodzaju) itp. Jednocześnie mogą one stanowić bardzo zróżnicowaną grupę przestępstw powiązanych wspólnym czynnikiem (komputer, program, dane).

· Cyberprzestępczość można zdefiniować jako działanie skierowane przeciwko komputerowi lub sieci komputerowej albo działanie, w którym komputer jest wykorzystywany jako narzędzie do popełnienia przestępstwa. Fakt, że sieć komputerowa lub cyberprzestrzeń jest środowiskiem, w którym odbywa się ta działalność, jest niezbędnym elementem, aby definicja cyberprzestępstwa miała zastosowanie.

· Cyberprzestępczość to działalność przestępcza, w której wykorzystywane są technologie informacyjne i komunikacyjne:

  o wykorzystywane jako narzędzie do popełniania przestępstw,

  o cel ataku sprawcy, co jest przestępstwem.

  o pod warunkiem, że środki te są wykorzystywane lub nadużywane w środowisku informatycznym, systemowym, programowym lub komunikacyjnym (tj. w cyberprzestrzeni).

· Nie wystarczy zdefiniować cyberprzestępstwo tylko w sposób pozytywny, ale trzeba je również zdefiniować, wymieniając czyny, które z zasady nie mogą być uznane za cyberprzestępstwo.

· Atak cybernetyczny można zdefiniować jako każde bezprawne działanie napastnika w cyberprzestrzeni, skierowane przeciwko interesom innej osoby.

· Zdarzenie związane z bezpieczeństwem cybernetycznym to "zdarzenie, które może spowodować naruszenie bezpieczeństwa informacji w systemach informatycznych lub naruszenie bezpieczeństwa usług i/lub bezpieczeństwa i integralności sieci łączności elektronicznej".

· Dane komputerowe oznaczają "dowolne wyrażenie faktów, informacji lub pojęć w formie nadającej się do przetwarzania przez system komputerowy, w tym program mogący spowodować wykonanie funkcji przez system komputerowy".

· Informacja "to dane, które zostały przetworzone do postaci użytecznej dla odbiorcy. Tak więc każda informacja to dane, dane, ale wszelkie przechowywane dane niekoniecznie stają się informacją".

🗝️

SŁOWA KLUCZOWE, KTÓRE WARTO ZAPAMIĘTAĆ

· cyberprzestępczość

· cyberatak

· wydarzenie związane z bezpieczeństwem cybernetycznym

· działalność przestępcza

· cyberprzestrzeń

❓

PYTANIA KONTROLNE

· Co to jest cyberprzestępczość?

· Co nie jest cyberprzestępstwem?

· Co to jest cyberatak?

· Jaka jest różnica między cyberprzestępczością a cyberatakiem?

· Jaka jest różnica między danymi a informacjami?

- Co symbolizuje triada CIA?

3. Ochrona karna przed cyberprzestępczością

Wysiłki zmierzające do prawnego uregulowania i karania przestępstw popełnianych za pomocą technologii informacyjno-komunikacyjnych można zaobserwować de facto od samego początku tej negatywnej działalności. Cyberprzestępczość bardzo różni się od innych rodzajów przestępstw, a różnica ta polega przede wszystkim na możliwości jej dynamicznego rozwoju i natychmiastowej zmiany (w zależności od powodzenia lub niepowodzenia danego rodzaju ataku), co może stwarzać pewne problemy w odniesieniu do prawodawstwa.

W prawie karnym materialnym obowiązuje zasada, że analogii nie można stosować na niekorzyść sprawcy (*in malam partem)*. Niemniej jednak często możliwe jest objęcie cyberataków przepisami ustawowymi dotyczącymi danego przestępstwa, nawet jeśli pierwotnie przestępstwo to dotyczyło bardziej "tradycyjnych sposobów" jego popełniania (na przykład ataków związanych z naruszeniem praw autorskich, wykorzystywaniem dzieci do produkcji pornografii itp.) Istnieje jednak szereg nowych ataków, w przypadku których nie jest to możliwe. W takich przypadkach ustawodawcy krajowi próbowali do tej pory głównie reagować *ad hoc* na te nowe rodzaje przestępstw, wypełniając luki w ustawodawstwie krajowym.

Przed przystąpieniem do analizy istniejących i skutecznych przepisów w dziedzinie cyberprzestępczości należy zauważyć, że nie tylko w Unii Europejskiej istnieje wyraźne dążenie do wdrożenia skuteczniejszych instrumentów prawnych, które umożliwiłyby reagowanie na cyberprzestępczość w sposób terminowy i adekwatny. W ten sposób stopniowo eliminowane są sprzeczności i niedociągnięcia w normach prawnych państw członkowskich UE i innych państw, które postanowiły aktywnie zaangażować się w walkę z cyberprzestępczością.

Jednym z pierwszych dokumentów dotyczących cyberprzestępczości przyjętych na szczeblu międzynarodowym jest **Podręcznik ONZ dotyczący zapobiegania i kontroli przestępczości komputerowej** (Hawana, 1990).[1]

"Metody ochrony danych i systemów informatycznych są obecnie przedmiotem wielu badań naukowych, ale sama techniczna ochrona tych systemów i danych bez podstawy prawnej może okazać się nieskuteczna ze względu na niejasne definicje, jak daleko może sięgać taka ochrona. W tym kontekście w pełni widoczna jest niespójność prawa krajowego z prawem innych krajów. Rozwój technologii komputerowych i informatycznych, który decyduje o międzynarodowym charakterze cyberprzestępczości, sprawia, że skuteczna ochrona systemów komputerowych i danych jest nie do pomyślenia bez międzynarodowych lub ponadnarodowych ram prawnych, nie tylko między państwami członkowskimi UE, ale w skali globalnej."

---

[1] *Podręcznik Organizacji Narodów Zjednoczonych dotyczący zapobiegania i kontroli przestępczości komputerowej.* [online]. [cyt. 2016-08-20]. Dostępny pod adresem: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

3.1. Cyberprzestępczość w dokumentach międzynarodowych i WE/UE

Przede wszystkim należy wspomnieć o Konwencji o cyberprzestępczości i jej protokole dodatkowym, ponieważ są to dwa najważniejsze dokumenty prawne, które przyczyniają się do ochrony społeczeństwa przed cyberprzestępczością, określając podstawowe ramy kryminalne cyberprzestępczości oraz ustanawiając środki wykrywania cyberprzestępstw i prowadzenia dochodzeń w ich sprawie. Przedstawione zostaną również dokumenty prawne UE i WE dotyczące cyberprzestępczości.

3.1.1 Konwencja Rady Europy nr 185 o cyberprzestępczości

Konwencja o cyberprzestępczości jest najważniejszym dokumentem prawnym dotyczącym cyberprzestępczości, a jej głównym celem jest ujednolicenie przepisów krajowych w dziedzinie cyberprzestępczości. Świadczy o tym fakt, że Konwencja o cyberprzestępczości zobowiązuje umawiające się strony do wprowadzenia do swoich krajowych systemów prawnych takich instrumentów, które umożliwią karanie określonych przestępstw cybernetycznych. To właśnie dokładne określenie okoliczności przestępstwa jest warunkiem wstępnym stosowania norm prawa karnego w cyberprzestrzeni. Ponadto Konwencja o cyberprzestępczości ustanawia ramy prawne dla jednolitego i wspólnego podejścia wobec sprawców tych przestępstw, niezależnie od miejsca ich popełnienia.

Konwencja o cyberprzestępczości została zatwierdzona przez Komitet Ministrów Rady Europy na 109. sesji w dniu 8 listopada 2001 r. Konwencja o cyberprzestępczości została otwarta do podpisu w dniu 23 listopada 2001 r. w Budapeszcie.[1] Konwencja weszła w życie 1 lipca 2004 r.

Republika Czeska podpisała Konwencję o cyberprzestępczości 9 lutego 2005 r., a ratyfikowała ją 22 sierpnia 2013 r., przy czym Konwencja weszła w życie 1 grudnia 2013 r. Państwa członkowskie UE zobowiązały się do ratyfikacji Konwencji o cyberprzestępczości oraz do wprowadzenia do swoich systemów prawnych przepisów, które umożliwią wyjaśnianie i ściganie tego przestępstwa.[2] Konwencja o cyberprzestępczości została również podpisana i ratyfikowana przez takie kraje, jak Stany Zjednoczone Ameryki, Japonia i inne.

Konwencja o cyberprzestępczości[3] składa się z **preambuły** i **48 artykułów,** które podzielono na 4 rozdziały:

1. **Stosowanie terminów** (*Stosowanie terminów*)
2. **Środki, które należy podjąć na poziomie** *krajowym*

Część 1 - Prawo karne materialne (*Prawo karne materialne.* Art. 2 -13)

Część 2 - Prawo proceduralne (art. 14-21)

Część 3 - *Jurysdykcja* (*Judrisdiction.* Art. 22**)**

3. **Współpraca międzynarodowa** (**International** *Co-operation*)

Część 1 - Zasady ogólne (*Zasady ogólne.* Art. 23-28)

Część 2 - *Postanowienia* **szczegółowe** (art. 29-35)

4. **Postanowienia końcowe**

Ważnym krokiem w kierunku ujednolicenia prawa jest zdefiniowanie czterech podstawowych grup przestępstw (zob. Rozdział II; art. 2-13) oraz włączenie innych ogólnych instytucji prawa karnego materialnego. To właśnie jednolita definicja (nazewnictwo) cyberataków pozwoli na ich skuteczniejsze ściganie w krajach, które ratyfikowały Konwencję o cyberprzestępczości. W szczególności:

1) **Przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych**. Art. 2-6),

2) **Przestępstwa komputerowe** (*Przestępstwa komputerowe.* Art. 7-8),

3) **Przestępstwa** *związane z treścią* (art. 9),

4) **Przestępstwa związane z** *naruszeniem* **praw autorskich i praw pokrewnych** (art. 10).

Jeśli chodzi o ogólne zasady prawa materialnego, bardziej szczegółowo określono odpowiedzialność karną za *usiłowanie* i *pomocnictwo* (art. 11)[4] oraz odpowiedzialność karną osoby prawnej (*odpowiedzialność korporacyjna*)[5] za przestępstwo w ramach konwencji o cyberprzestępczości.

3.1.2 Protokół dodatkowy nr 189 Rady Europy do Konwencji o cyberprzestępczości

Protokół dodatkowy Rady Europy nr 189 do konwencji o cyberprzestępczości[6] , przyjęty 28 stycznia 2003 r.[7] , określa szereg przestępstw nieobjętych konwencją o cyberprzestępczości. W konwencji o cyberprzestępczości nie ma przestępstw polegających na rozpowszechnianiu pewnych *"szkodliwych materiałów"*.[8] Protokół dodatkowy definiuje przestępstwa, które polegają przede wszystkim na rozpowszechnianiu materiałów o treści rasistowskiej, ksenofobicznej lub w inny sposób naruszającej tolerancję rasową. Głównym powodem nieuwzględnienia omawianych przestępstw w Konwencji o cyberprzestępczości było podpisanie, a następnie przyjęcie Konwencji o cyberprzestępczości przez USA.[9]

Protokół dodatkowy składa się z **preambuły** i **16 artykułów,** które podzielono na 4 rozdziały:

1. **Postanowienia ogólne** (Postanowienia *wspólne*)
2. **Środki, które należy podjąć na poziomie** *krajowym*

· Artykuł 3 - *Rozpowszechnianie* materiałów rasistowskich i ksenofobicznych za pośrednictwem systemów komputerowych

· Artykuł 4 - Groźba *motywowana* rasizmem i ksenofobią

· Artykuł 5 - *Zniewaga* motywowana rasizmem i ksenofobią

· Artykuł 6 - Zaprzeczanie, rażące pomniejszanie, aprobata lub *usprawiedliwianie* ludobójstwa lub zbrodni przeciwko ludzkości

3. **Relacje między Konwencją o cyberprzestępczości a niniejszym** *protokołem*

4. **Postanowienia końcowe**

W rozdziale pierwszym zmodyfikowano cel Protokołu dodatkowego i zdefiniowano pojęcie materiałów rasistowskich i ksenofobicznych. Zgodnie z art. 1 ust. 1 Protokołu dodatkowego, materiały rasistowskie i ksenofobiczne oznaczają *"wszelkie materiały pisemne, obrazy lub inne formy wyrażania idei lub teorii, które propagują, popierają lub podżegają do nienawiści, dyskryminacji lub przemocy wobec jakiejkolwiek osoby lub grupy osób, ze względu na rasę, kolor skóry, pochodzenie albo przynależność narodową lub etniczną, lub religię, jeśli są używane jako pretekst zamiast któregokolwiek z tych atrybutów".*

3.1.3 Dokumenty UE/WE mające na celu harmonizację ram prawnych w zakresie zwalczania cyberprzestępczości

W szczególności specyfika cyberprzestępczości i potrzeba skutecznej współpracy międzynarodowej sprawiają, że UE stara się ujednolicić przepisy poszczególnych państw członkowskich, aby skuteczniej walczyć z tym negatywnym zjawiskiem. Środkami konwergencji prawa unijnego są przede wszystkim decyzje ramowe, dyrektywy i inne dokumenty UE/WE. Z punktu widzenia zwalczania cyberprzestępczości najważniejsze są następujące dokumenty:

· *Dyrektywa Rady 91/250/EWG* w sprawie ochrony prawnej programów komputerowych

· *Decyzja Rady 92/242/EWG* w sprawie bezpieczeństwa systemów informacyjnych

· *Dyrektywa 98/34/WE Parlamentu Europejskiego i Rady* ustanawiająca procedurę udzielania informacji w zakresie norm i przepisów technicznych, zmieniona dyrektywą *98/48/WE*

· *Dyrektywa 2000/31/WE* w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego, w ramach rynku wewnętrznego ("dyrektywa o handlu elektronicznym")

· *Decyzja ramowa Rady 2000/375/WSiSW* w sprawie zwalczania pornografii dziecięcej w Internecie

· *Decyzja ramowa Rady 2001/413/WSiSW* w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi

· *Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady* w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa)

· *Dyrektywa 2002/19/WE Parlamentu Europejskiego i Rady* w sprawie dostępu do sieci łączności elektronicznej i urządzeń towarzyszących oraz wzajemnych połączeń (dyrektywa o dostępie)

· *Dyrektywa 2002/20/WE Parlamentu Europejskiego i Rady* w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (dyrektywa o zezwoleniach)

· *Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady* w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej)

· *Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady* dotycząca przetwarzania danych osobowych i ochrony prywatności w dziedzinie łączności elektronicznej (dyrektywa o ochronie danych w łączności elektronicznej)

· *Dyrektywa Komisji 2002/77/WE* w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej (dyrektywa o konkurencji)

· *Decyzja ramowa Rady UE 2002/584/WSiSW* w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między państwami członkowskimi

· *Decyzja ramowa Rady 2004/68/WSiSW* dotycząca zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej

· ***Decyzja ramowa Rady 2005/222/WSiSW* w sprawie ataków na systemy informatyczne**

· *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów* - Zwalczanie spamu, oprogramowania szpiegującego i złośliwego *z dnia 15.11.2006 r.*

· *Komunikat Komisji do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Regionów* w sprawie ogólnej strategii zwalczania cyberprzestępczości z 22.*5.2007 r.*

· *Konkluzje Rady* w sprawie wspólnej strategii roboczej i konkretnych środków zwalczania cyberprzestępczości z 27.*11.2008 r.*

· *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów* w sprawie ochrony krytycznej infrastruktury informatycznej "Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności" *z 30.3.2009 r.*

· *Komunikat Komisji do Rady i Parlamentu Europejskiego*, Zwalczanie przestępczości w erze cyfrowej: ustanowienie europejskiego centrum ds. walki z cyberprzestępczością. 2012.

· *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r.* w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) i uchylające rozporządzenie (WE) nr 460/2004

· *Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r.* w sprawie ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW

· *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 513/2014 ustanawiające*, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument finansowy na rzecz wspierania współpracy policyjnej, zapobiegania i zwalczania przestępczości oraz zarządzania kryzysowego, a także uchylające decyzję Rady 2007/125/WSiSW z dnia 16 kwietnia 2014 r.

· *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r.* w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (eIDAS lub rozporządzenie eIDAS)

· *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794* w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) oraz uchylające i zastępujące decyzje 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW, z dnia 11 maja 2016 r.

· *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia* 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

· *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.* w sprawie środków zapewniających wysoki wspólny poziom bezpieczeństwa sieci i systemów informatycznych w Unii (dyrektywa NIS)[10]

· *Konkluzje Rady w sprawie wspólnej strategii roboczej i konkretnych środków zwalczania cyberprzestępczości z dnia 27* listopada 2008 r.

· *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej "Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności"* z 30.3.2009 r.[11]

3.1.4 Normy prawne obowiązujące w Republice Czeskiej

W związku z cyberprzestępczością i cyberbezpieczeństwem należy wspomnieć o normach prawnych Republiki Czeskiej, które bezpośrednio odnoszą się do tego zagadnienia:

· Ustawa nr 40/2009 Dz.U., Kodeks karny

· Ustawa nr 141/1961 Zb., o postępowaniu przed sądem karnym

· Ustawa nr 218/2003 Zb., ustawa o sądownictwie dla nieletnich

· Ustawa nr 121/2000 Dz.U., Ustawa o prawie autorskim

· Ustawa nr 127/2005 Sb. o łączności elektronicznej

· Ustawa nr 480/2004 Zb. o niektórych usługach społeczeństwa informacyjnego

· Ustawa nr 273/2008 Sb. o policji Republiki Czeskiej

· Ustawa nr 89/2012 Dz.U., Kodeks cywilny

· Ustawa nr 110/2019 Dz.U. o przetwarzaniu danych osobowych

· Ustawa nr 14/1993 Zb. o środkach ochrony własności przemysłowej

· Ustawa nr 441/2003 Dz.U. o znakach towarowych

· Ustawa nr 527/1990 Sb. o wynalazkach, wzorach przemysłowych i propozycjach ulepszeń

· Ustawa nr 300/2008 Dz.U., o aktach elektronicznych i dozwolonej konwersji dokumentów, z późniejszymi zmianami

· Ustawa nr 297/2016 Dz.U. o usługach zaufania dla transakcji elektronicznych

· Ustawa nr 160/1999 Sb. o swobodnym dostępie do informacji

· Ustawa nr 181/2014 Dz.U. o cyberbezpieczeństwie i zmianach w powiązanych ustawach (ustawa o cyberbezpieczeństwie)

3.1.5. Normy prawne obowiązujące w Polsce

W polskim prawie główne przepisy dotyczące cyberprzestępczości to:

- Nielegalny dostęp do systemu (hacking) - Art. 267 § 1 i 2 Kodeksu karnego. Przestępstwo to jest ścigane na wniosek pokrzywdzonego. Są one zagrożone karą grzywny, ograniczenia wolności lub pozbawienia wolności do 2 lat.

- Naruszenie tajemnicy komunikowania się (sniffing) - art. 267 § 3 Kodeksu karnego. Ten typ przestępstwa polega na uzyskaniu zastrzeżonych informacji, np. poprzez sniffery, czyli programy przechwytujące dane (hasła i identyfikatory użytkowników). Taki czyn jest zagrożony karą do 2 lat pozbawienia wolności.

- Naruszenie integralności danych (wirusy, trojany), 268 Kodeksu Karnego, Art. 268a Kodeksu Karnego Przestępstwo to dotyczy m.in. kradzieży danych osobowych, udostępniania ich osobom trzecim bez zgody właściciela, a także wykorzystywania ich w sposób nieuprawniony. Za popełnienie tych czynów grożą sankcje finansowe (do 100.000 zł).

- Naruszenie integralności systemu - Art. 269 Kodeksu Karnego 269 Kodeksu karnego Przykładem takiego przestępstwa są np. ataki typu Ping flood, które polegają na przeciążeniu łącza internetowego. Mogą one prowadzić np. do niedostępności niektórych usług. Polski ustawodawca przewidział za ten czyn maksymalną karę do 8 lat pozbawienia wolności (w przypadku naruszenia bezpieczeństwa państwa).

- Tworzenie "narzędzi hakerskich" - Art. 269a Kodeksu karnego, Art. 269b Kodeksu karnego 269b Kodeksu karnego Popełnienie tego przestępstwa jest zagrożone karą od 3 miesięcy do 5 lat pozbawienia wolności.

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

---

[1] Listę państw, które podpisały i ratyfikowały Konwencję o cyberprzestępczości, można znaleźć na stronie:

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=F6wSLE5D.

[2] Zobowiązanie to zawarto w art. 14-21 Konwencji o cyberprzestępczości.

[3] Pełny tekst Konwencji można znaleźć pod adresem: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[4] Wymóg ten jest w pełni realizowany w czeskim prawie karnym poprzez instytucje *usiłowania (*§ 21 i 111 TZK) oraz *współudziału* (§ 24 i 111 TZK).

[5] W czeskim środowisku prawnym odpowiedzialność karna osób prawnych jest realizowana na podstawie ustawy nr 418/2011 Sb. o odpowiedzialności karnej osób prawnych i postępowaniu wobec nich, z późniejszymi zmianami.

[6] *ETS nr 189 Protokół dodatkowy do Konwencji o cyberprzestępczości, dotyczący kryminalizacji czynów o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych* [online]. [cyt. 20.8.2016]. Dostępny pod adresem: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081 60f

[7] Listę państw, które podpisały i ratyfikowały Protokół dodatkowy, można znaleźć na stronie:

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=F6wSLE5D

[8] Z wyjątkiem pornografii dziecięcej, która jest bezpośrednio objęta art. 9 Konwencji o cyberprzestępczości.

[9] Kwestia rasizmu i ksenofobii jest w USA "szarą strefą", ponieważ niektóre wypowiedzi mogą być uznane za przestępstwo, a inne nie. Na przykład w **USA** nie wszystkie przejawy rasizmu są uznawane za przestępstwo, patrz **Pierwsza Poprawka do Konstytucji USA** - *Kongres nie będzie stanowił ustaw szanujących wolność wyznania, zabraniających swobodnego jej praktykowania, ograniczających wolność słowa i prasy, ani prawo ludzi do spokojnego gromadzenia się i wnoszenia petycji do rządu w celu uzyskania zadośćuczynienia***. Aby groźba stanowiła wykroczenie lub przestępstwo, należy wykazać jej realność, w przeciwnym razie byłoby to naruszenie Pierwszej Poprawki. Z kolei we Francji** i **Niemczech**, a także w **Czechach,** przejawy rasizmu są uznawane za przestępstwo.

[10] O niektórych z tych dokumentów zob. VOLEVECKÝ, Petr. W: *Trestní právo,* 2009, t. 12, nr 7-8, s. 26-39. Wszystkie przepisy prawa UE są również dostępne w wersji czeskiej na stronie *EUR-lex.* [online]. [cit.20.8.2016]. Dostępny pod adresem: http://eur-lex.europa.eu/homepage.html

[11] KOLOUCH, Jan i Petr VOLEVECKÝ. *Ochrona prawnokarna przed cyberprzestępczością.* Praga: Akademia Policyjna Republiki Czeskiej w Pradze, 2013, s. 76.

3.2. Merytoryczne aspekty cyberprzestępczości w Republice Czeskiej

3.2.1 Cyberprzestępstwa w części szczególnej kodeksu karnego

Jeśli chodzi o cyberprzestępczość, kodeks karny zawiera specjalne przestępstwa, które dotyczą cyberprzestępczości lub określonych ataków cybernetycznych.

Cyberprzestępstwa klasyfikuje się w najbardziej ogólnym ujęciu pod względem wykorzystania technologii informacyjno-komunikacyjnych na przestępstwa, w których elementy te są wykorzystywane jako narzędzie umożliwiające popełnienie przestępstwa, przy czym fakty przestępstwa obejmują wykorzystanie tych środków jako cechę stanu faktycznego, oraz przestępstwa, w których elementy technologii informacyjno-komunikacyjnych są celem ataku sprawcy, tj. stanowią indywidualny przedmiot lub materialny obiekt ataku.

Ustawodawca umieścił w specjalnej części Kodeksu karnego szereg przestępstw, które albo zawierają znamiona związane z technologiami informacyjno-komunikacyjnymi, albo mogą być wypełnione przez atak cybernetyczny. Przestępstwa te mogą obejmować:

- § 180 nieuprawnione posługiwanie się danymi osobowymi
- § 181 Naruszenie praw innych osób
- § 182 naruszenie tajemnicy przesyłanych wiadomości
- § 183 naruszenie tajemnicy dokumentów i innych dokumentów przechowywanych w pomieszczeniach prywatnych
- § 184 zniesławienie
- § 191 rozpowszechnianie pornografii
- § 192 produkcja i inne formy dysponowania pornografią dziecięcą
- § 193 wykorzystywanie dziecka do produkcji pornografii
- § 193b niezgodne z prawem kontaktowanie się z dzieckiem
- § 205 kradzież
- § 206 nieuprawnione korzystanie z cudzej własności
- § 209 oszustwo
- § 213 prowadzenie nieuczciwych gier i zakładów
- § 214 udział w kapitale zakładowym
- § 216 pranie dochodów z przestępstwa
- § 228 Szkody w mieniu zagranicznym
- § 230 nieuprawniony dostęp do systemu komputerowego i nośnika informacji
- § 231 udostępnianie i przechowywanie urządzenia dostępowego i hasła do systemu komputerowego oraz innych tego typu danych
- § 232 Uszkodzenie zapisu w systemie komputerowym i na nośniku informacji oraz niedbała ingerencja w sprzęt komputerowy
- § 234 niedozwolone udostępnianie, podrabianie i przerabianie środków płatniczych
- § 236 wytwarzanie i posiadanie narzędzi służących do podrabiania towarów
- § 264 podawanie nieprawdziwych danych i nieprzechowywanie dokumentów dotyczących eksportu towarów i technologii podwójnego zastosowania
- § 268 Naruszenie praw do znaków towarowych i innych oznaczeń
- § 267 podawanie nieprawdziwych danych i nieprowadzenie rejestrów dotyczących handlu zagranicznego materiałami wojskowymi
- § 269 Naruszenie chronionych praw przemysłowych
- § 270 Naruszenie praw autorskich, praw pokrewnych oraz praw do baz danych
- § 272 niebezpieczeństwo ogólne
- § 276 uszkodzenie i zagrożenie funkcjonowania obiektu użyteczności publicznej
- § 287 Rozprzestrzenianie się toksemii
- § 290 przejmowanie kontroli nad pojazdem powietrznym, statkiem cywilnym i stałą platformą
- § 291 Zagrożenie bezpieczeństwa pojazdu powietrznego i statku cywilnego

- § 311 atak terrorystyczny
- § 316 szpiegostwo
- § 317 narażanie na szwank informacji niejawnych
- § 345 fałszywe oskarżenie
- § 348 Podrabianie i przerabianie dokumentu publicznego
- § 353 Niebezpieczne zagrożenia
- § 354 niebezpieczne prześladowanie
- § 355 Zniesławienie narodu, rasy, grupy etnicznej lub innej grupy osób
- § 356 Podżeganie do nienawiści wobec grupy osób lub do ograniczania praw i wolności
- § 357 rozpowszechnianie wiadomości alarmowych
- § 361 udział w zorganizowanej grupie przestępczej
- § 364 podżeganie do popełnienia przestępstwa
- § 365 zgoda na popełnienie przestępstwa
- § 400 ludobójstwo
- § 403 Zakładanie, popieranie i promowanie ruchu mającego na celu ograniczenie praw i wolności człowieka
- § 404 wyrażanie sympatii dla ruchu mającego na celu tłumienie praw i wolności człowieka
- § 405 zaprzeczanie, kwestionowanie, aprobowanie i usprawiedliwianie ludobójstwa
- § 407 Podżeganie do wojny napastniczej

Zgodnie z kodeksem karnym cyberprzestępstwa można klasyfikować według wielu różnych kryteriów. Do najczęściej stosowanych klasyfikacji cyberprzestępstw należy wspomniana wcześniej klasyfikacja na:[1]

a) przestępstwa, w **których przedmiotem ochrony są środki technologii informacyjno-komunikacyjnych** (tzn. są one celem ataku cybernetycznego):

- § 182 naruszenie tajemnicy przesyłanych wiadomości
- § 183 naruszenie tajemnicy dokumentów i innych dokumentów przechowywanych w pomieszczeniach prywatnych
- § 206 nieuprawnione korzystanie z cudzej własności
- § 228 Szkody w mieniu zagranicznym
- § 230 nieuprawniony dostęp do systemu komputerowego i nośnika informacji
- § 232 Uszkodzenie zapisu w systemie komputerowym i na nośniku informacji oraz niedbała ingerencja w sprzęt komputerowy
- § 234 niedozwolone udostępnianie, podrabianie i przerabianie środków płatniczych
- § 264 podawanie nieprawdziwych danych i nieprzechowywanie dokumentów dotyczących eksportu towarów i technologii podwójnego zastosowania
- § 267 podawanie nieprawdziwych danych i nieprowadzenie rejestrów dotyczących handlu zagranicznego materiałami wojskowymi
- § 270 Naruszenie praw autorskich, praw pokrewnych oraz praw do baz danych
- § 290 przejmowanie kontroli nad pojazdem powietrznym, statkiem cywilnym i stałą platformą
- § 291 Zagrożenie bezpieczeństwa pojazdu powietrznego i statku cywilnego
- § 311 atak terrorystyczny
- § 317 narażanie na szwank informacji niejawnych
- przestępstw, przy popełnianiu **których do popełnienia przestępstwa wykorzystuje się środki technologii informacyjno-komunikacyjnych:**
- § 180 nieuprawnione posługiwanie się danymi osobowymi
- § 181 Naruszenie praw innych osób
- § 182 naruszenie tajemnicy przesyłanych wiadomości
- § 184 zniesławienie

- § 191 rozpowszechnianie pornografii
- § 192 produkcja i inne formy dysponowania pornografią dziecięcą
- § 193 wykorzystywanie dziecka do produkcji pornografii
- § 193b niezgodne z prawem kontaktowanie się z dzieckiem
- § 205 kradzież
- § 209 oszustwo
- § 213 prowadzenie nieuczciwych gier i zakładów
- § 214 udział w kapitale zakładowym
- § 216 pranie dochodów z przestępstwa
- § 230 nieuprawniony dostęp do systemu komputerowego i nośnika informacji
- § 231 udostępnianie i przechowywanie urządzenia dostępowego i hasła do systemu komputerowego oraz innych tego typu danych
- § 234 niedozwolone udostępnianie, podrabianie i przerabianie środków płatniczych
- § 236 wytwarzanie i posiadanie narzędzi służących do podrabiania towarów
- § 268 Naruszenie prawa do znaku towarowego i innych oznaczeń
- § 269 Naruszenie chronionych praw przemysłowych
- § 272 niebezpieczeństwo ogólne
- § 276 uszkodzenie i zagrożenie funkcjonowania obiektu użyteczności publicznej
- § 287 Rozprzestrzenianie się toksemii
- § 316 szpiegostwo
- § 345 fałszywe oskarżenie
- § 348 Podrabianie i przerabianie dokumentu publicznego
- § 353 Niebezpieczne zagrożenia
- § 354 niebezpieczne prześladowanie
- § 355 Zniesławienie narodu, rasy, grupy etnicznej lub innej grupy osób
- § 356 Podżeganie do nienawiści wobec grupy osób lub do ograniczania praw i wolności
- § 357 rozpowszechnianie wiadomości alarmowych
- § 361 udział w zorganizowanej grupie przestępczej
- § 364 podżeganie do popełnienia przestępstwa
- § 365 zgoda na popełnienie przestępstwa
- § 400 ludobójstwo
- § 403 Zakładanie, popieranie i promowanie ruchu mającego na celu ograniczenie praw i wolności człowieka
- § 407 Podżeganie do wojny napastniczej

Oprócz powyższych przepisów Części Specjalnej Kodeksu Karnego, problematykę cyberprzestępczości reguluje również paragraf 120 Kodeksu Karnego, który stanowi, że "*wprowadzenie kogoś w błąd lub wykorzystanie czyjegoś błędu może nastąpić poprzez ingerencję w* ***informacje lub*** *dane komputerowe, ingerencję w* ***oprogramowanie komputerowe lub*** *wykonanie* ***innej operacji na komputerze****, ingerencję w* ***urządzenia elektroniczne lub inne urządzenia techniczne,*** *w tym ingerencję w* ***przedmioty służące do sterowania takimi urządzeniami,*** *lub wykorzystanie takiej operacji lub takiej ingerencji wykonanej przez inną osobę*".

[1] Ze względu na brzmienie przepisów dotyczących przestępstw, możliwe jest zaklasyfikowanie niektórych z nich do obu kategorii (przepisy te chronią technologie informacyjno-komunikacyjne, ale jednocześnie zawierają znamiona niewłaściwego wykorzystania tych technologii).

3.3. Merytoryczne aspekty cyberprzestępczości w Polsce

Ustawodawca włączył do kodeksu karnego szereg przestępstw, które albo zawierają znamiona związane z technologiami informacyjnymi i komunikacyjnymi, albo mogą być wypełnione przez cyberatak. Przestępstwa te mogą obejmować:

- Art. 126a. Publiczne nawoływanie do popełnienia czynu zabronionego
- Art. 130. Szpiegostwo
- Art. 132. Dezinformacja wywiadowcza
- Art. 133. Znieważenie Narodu lub Rzeczpospolitej Polskiej
- Art. 135. Czynna napaść lub znieważenie Prezydenta RP
- Art. 136. Czynna napaść lub znieważenie przedstawiciela obcego państwa
- Art. 137. Publiczne znieważenie znaku lub symbolu państwa
- Art. 151. Namowa do samobójstwa i udzielenie pomocy
- Art. 165. Sprowadzenie niebezpieczeństwa powszechnego
- Art. 190. Groźba karalna
- Art. 190a. Stalking
- Art. 191. Zmuszanie do określonego zachowania, zaniechania lub znoszenia
- Art. 191a. Utrwalanie wizerunku nagiej osoby
- Art. 196. Obrażanie uczuć religijnych innych osób
- Art. 200a. Elektroniczny kontakt z osobą małoletnią w celach pedofilskich
- Art. 200b. Publiczne propagowanie treści o charakterze pedofilskim
- Art. 202. Prezentacja i rozpowszechnianie pornografii
- Art. 212. Zniesławienie
- Art. 216. Znieważenie osoby
- Art. 224a. Fałszywe zawiadomienie o zagrożeniu
- Art. 226. Znieważenie funkcjonariusza publicznego lub organu konstytucyjnego RP
- Art. 227. Przywłaszczenie funkcji funkcjonariusza publicznego
- Art. 228. Łapownictwo pełniącego funkcję publiczną
- Art. 229. Przekupstwo
- Art. 230. Płatna protekcja bierna
- Art. 230a. Płatna protekcja czynna
- Art. 232. Wywieranie wpływu na czynności sądu
- Art. 234. Fałszywe oskarżenie
- Art. 235. Tworzenie fałszywych dowodów
- Art. 236. Zatajanie dowodów niewinności osoby podejrzanej
- Art. 238. Fałszywe zawiadomienie o popełnieniu przestępstwa
- Art. 239. Poplecznictwo
- Art. 240. Karalne niezawiadomienie o czynie zabronionym
- Art. 241. Bezprawne rozpowszechnienie wiadomości z postępowania przygotowawczego lub rozprawy
- Art. 244. Niestosowanie się do orzeczonych przez sąd środków karnych
- Art. 245. Używanie przemocy lub groźby w celu wywarcia wpływu na uczestnika postępowania
- Art. 246. Wymuszanie przez funkcjonariusza publicznego zeznań, wyjaśnień, informacji lub oświadczenia
- Art. 250. Bezprawne wywieranie wpływu na sposób głosowania osoby uprawnionej
- Art. 251. Naruszenie tajności głosowania
- Art. 255. Publiczne nawoływanie do popełnienia lub pochwalanie występku lub przestępstwa skarbowego
- Art. 255a. Rozpowszechnianie treści ułatwiających popełnienie przestępstwa o charakterze terrorystycznym
- Art. 256. Propagowanie faszyzmu lub innego ustroju totalitarnego
- Art. 257. Rasizm
- Art. 265. Ujawnienie lub wykorzystanie informacji niejawnej o klauzuli „tajne" lub „ściśle tajne"
- Art. 266. Ujawnienie lub wykorzystanie informacji uzyskanej w związku z wykonywaną funkcją lub czynnościami służbowymi
- Art. 267. Bezprawne uzyskanie informacji
- Art. 268. Utrudnianie zapoznania się z informacją osobie uprawnionej
- Art. 268a. Niszczenie, uszkadzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych
- Art. 269. Niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu
- Art. 269a. Zakłócanie pracy systemu informatycznego, teleinformatycznego lub sieci teleinformatycznej
- Art. 269b. Bezprawne wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie programów komputerowych
- Art. 270. Fałszowanie dokumentu i używanie go za autentyczny
- Art. 270a. Fałszowanie faktury i używanie jej za autentyczną
- Art. 271. Poświadczenie nieprawdy
- Art. 271a. Podawanie nieprawdy w fakturze
- Art. 272. Podstępne wyłudzenie poświadczenia nieprawdy w dokumencie
- Art. 273. Używanie dokumentu poświadczającego nieprawdę
- Art. 275. Posługiwanie się cudzym dokumentem tożsamości
- Art. 276. Niszczenie lub ukrywanie dokumentu bez prawa do jego rozporządzaniem
- Art. 277a. Fałszowanie faktury lub używanie sfałszowanej faktury z kwotą określającą mienie wielkiej wartości
- Art. 278. Kradzież
- Art. 282. Wymuszenie rozbójnicze
- Art. 284. Przywłaszczenie
- Art. 285. Uruchomienie na cudzy rachunek impulsów telefonicznych

- Art. 286. Oszustwo
- Art. 287. Oszustwo komputerowe
- Art. 291. Paserstwo umyślne
- Art. 292. Paserstwo nieumyślne
- Art. 293. Paserstwo komputerowe
- Art. 296. Wyrządzenie szkody w obrocie gospodarczym
- Art. 296a. Łapownictwo na stanowisku kierowniczym
- Art. 297. Wyłudzenie kredytu
- Art. 298. Wyłudzenie odszkodowania
- Art. 299. Pranie brudnych pieniędzy
- Art. 300. Utrudnianie zaspokojenia wierzyciela
- Art. 303. Nieprowadzenie lub niezgodne z prawdą prowadzenie dokumentacji działalności gospodarczej
- Art. 304. Wyzysk kontrahenta
- Art. 305. Zakłócanie przetargu publicznego
- Art. 306. Usuwanie, podrabianie lub przerabianie znaków identyfikacyjnych
- Art. 310. Fałszowanie pieniędzy, środków płatniczych lub papierów wartościowych
- Art. 311. Fałszowanie informacji w obrocie papierami wartościowymi
- Art. 312. Puszczanie w obieg przerobionych albo podrobionych pieniędzy, środków płatniczych lub dokumentów płatniczych
- Art. 313. Fałszowanie urzędowych znaków wartościowych
- Art. 314. Fałszowanie znaków urzędowych w celu użycia w obrocie gospodarczym
- Art. 346. Przemoc lub groźba bezprawna żołnierza wobec przełożonego
- Art. 347. Znieważenie przełożonego przez żołnierza

3.4. Merytoryczne aspekty cyberprzestępczości w Portugalii

Fix me

4. Przejawy cyberprzestępczości

Cyberprzestępczość zazwyczaj przejawia się poprzez ataki cybernetyczne, ale wiele ataków wymaga również wykorzystania aspektów czysto nietechnicznych, aby odnieść sukces.

Niektóre czyny zabronione w cyberprzestrzeni lub czyny związane z cyberprzestępczością można zakwalifikować na podstawie odpowiednich przepisów obowiązującego kodeksu karnego, ale istnieją pewne rodzaje czynów, których zakwalifikowanie jako przestępstwa może być znacznie trudniejsze lub wręcz niemożliwe (w wielu przypadkach są to po prostu czyny niemoralne).

Bardzo często cyberprzestępczość jest uważana za nowy rodzaj przestępstw, jednak znaczna część cyberprzestępczości wykorzystuje lub przenosi powszechnie znane rodzaje przestępstw (np. oszustwa, naruszenie praw autorskich, kradzież, nękanie itp.) do środowiska cyfrowego, gdzie można je popełnić "lepiej, szybciej i skuteczniej" niż w świecie rzeczywistym. Czyste ataki cybernetyczne mogą obejmować np. hakerstwo, ataki DoS i DDoS, botnety itp.

Charakterystyczne dla świata wirtualnego jest to, że większość użytkowników ma do niego - moim zdaniem - niezrozumiałe, niemal bezgraniczne zaufanie. Trzeba przyznać, że świat wirtualny staje się dla nas coraz ważniejszy. Osobiście uważam, że wiele osób przestaje myśleć o ewentualnym ryzyku lub zagrożeniach podczas korzystania z usług świadczonych w Internecie. Przede wszystkim urzekają ich pozornie nieskończone możliwości "nowych technologii"; jak inaczej można wytłumaczyć brak podstawowych zasad i mechanizmów obronnych w świecie wirtualnym, skoro w świecie rzeczywistym zachowywalibyśmy się zupełnie inaczej. Z drugiej strony, czasami użytkownicy cyberprzestrzeni przypominają mi *"Dziwny przypadek doktora Jekylla i pana Hyde'a"* [oryg. Dziwny przypadek doktora Jekylla i pana Hyde'a - Robert Louise Stevenson (1886)]. Pozornie przyzwoici ludzie w świecie rzeczywistym, w "pseudoanonimowym" środowisku cyberprzestrzeni wyrażają siebie bez żadnych ograniczeń prawnych czy moralnych. Można więc na przykład natknąć się na przypadek sędziego, który pobiera "pornografię dziecięcą"[1] , użytkowników, którzy nigdy nie ukradli niczego w świecie rzeczywistym, ale nie mają problemu z kradzieżą w świecie wirtualnym[2] , lub naruszających inne prawa chronione przez prawo danego kraju.

W przeszłości wielu czołowych ekspertów wypowiadało się na temat prognoz dotyczących cyberprzestępczości, w tym Schneier, który w 2002 r. przewidywał, że przestępczość będzie kolejnym dużym trendem w dziedzinie bezpieczeństwa w Internecie. "*Nie będą to już wirusy, trojany i ataki DDoS przeprowadzane dla zabawy lub w celu popisania się swoimi umiejętnościami. Będzie on dotyczył prawdziwych przestępstw. Internet. Przestępcy zwykle pozostają w tyle za rozwojem technologii o pięć lub dziesięć lat, ale w końcu zdadzą sobie sprawę z jej możliwości. Tak jak Willie Sutton zaczął napadać na banki, "bo tam były pieniądze", tak współcześni przestępcy zaczną atakować za pośrednictwem sieci komputerowych. Coraz większa wartość (funduszy) jest w Internecie niż w prawdziwych pieniądzach*". [3]

W 2007 r. FBI przedstawiło statystykę, w której porównano zwykły "napad na bank" (rabunek) z czynem o charakterze ataku phishingowego.[4]

Parametr	Średnia liczba napadów z bronią w ręku	Przeciętny atak cybernetyczny
Ryzyko	Sprawca ryzykuje, że zostanie ranny lub zabity.	Brak ryzyka uszkodzenia ciała
Zysk	Średnio 3 - 5 tys. USD.	Średnio 50 - 500 tys. USD.
Prawdopodobieństwo schwytania	50-60% napastników zostaje trafionych.	Trafiono około 10% napastników.
Prawdopodobieństwo skazania	95% schwytanych napastników zostało skazanych.	Spośród tych, którzy zostali złapani, tylko 15% napastników staje przed sądem, a tylko 50% z nich zostaje skazanych.
Zaufanie	Średnio 5 - 6 lat, jeśli sprawca nie zranił nikogo podczas napadu.	Średnio od 2 do 4 lat.

W 2012 roku Goodman stwierdza w odniesieniu do technologii informacyjno-komunikacyjnych, że "*zdolność jednostki do wpływania na masy dzięki tym technologiom rośnie w postępie geometrycznym.* Rośnie *w tempie wykładniczym zarówno w "dobrym, jak i złym celu".* Ilustracją tego wzrostu jest rozwój przestępczości rozbójniczej, która w przeszłości polegała początkowo tylko na posługiwaniu się nożem lub pistoletem, a de facto na rozbojach dokonywanych przez pojedyncze osoby lub małe grupy. *"Poważna 'innowacja' miała miejsce, gdy cały pociąg został obrabowany z 200 osób".* Internet pozwala na przeprowadzenie ataku na jeszcze większą skalę przez pojedynczą osobę. Kradzież dużej liczby użytkowników dobrze ilustruje sprawa Sony Playstation z około 100 milionami ofiar: *"Kiedy w historii ludzkości ktoś mógł okraść 100* milionów *ludzi? Ale to nie jest tylko kradzież..."*.[5]

W tym samym roku dyrektor FBI Robert S. Mueller wygłosił przemówienie na konferencji RSA Cyber Security Conference (San Francisco, Kalifornia), w którym stwierdził między innymi*: "Jestem przekonany, że istnieją tylko dwa rodzaje firm: te, które już zostały zhakowane, i te, które dopiero zostaną zhakowane. A nawet te dwie grupy bardzo szybko łączą się w jedną kategorię: firmy, których systemy zostały zhakowane i firmy, które zostaną zhakowane ponownie*". [6]

Obecnie mamy do czynienia z coraz większym i masowym połączeniem różnych systemów komputerowych w cyberprzestrzeni, co de facto generuje bezpośrednią proporcjonalność polegającą na następującym stwierdzeniu "*im więcej połączonych urządzeń, tym większa ich podatność na ataki i tym większa liczba ataków".* Graficzne przedstawienie trwających ataków można znaleźć na stronach: http://map.norsecorp.com/#/; https://cybermap.kaspersky.com/; https://map.lookingglasscyber.com/ itd.

Uważam, że nie ma wątpliwości co do tego, że cyberprzestępczość rośnie i jest problemem globalnym. Różne statystyki podają częściowo różne szkody spowodowane przez cyberprzestępczość, ale nie zmienia to faktu, że wszystkie one obejmują szkody pierwotne (np. nieprawidłowe działanie systemu komputerowego, jego części, oferowanych usług, awarię infrastruktury itp.) oraz szkody wtórne (np. odzyskiwanie systemów, ratowanie danych, ponowne podłączenie użytkowników końcowych itp. Europol w swoim raporcie z 2014 r.[7] podaje, że cyberprzestępczość kosztuje światową gospodarkę około 300 miliardów dolarów rocznie. Od czasu masowego rozpowszechnienia Internetu społeczność atakujących znacznie się zmieniła. Przede wszystkim nie są to już osoby, które popełniały nielegalne czyny dla zabawy lub pokonania przeszkód. Obecnie są to zazwyczaj profesjonaliści, którzy wykonują swoją pracę dla zysku i często działają w zorganizowanych grupach.

Zmiana ta jest zrozumiała i nieodłącznie związana z trzema aspektami:

1) **Zależność społeczeństwa od Internetu** (lub usług, technologii itp.),

2) **Cyberprzestępczość stała się lukratywnym globalnym biznesem** [już pierwsze ataki **cybernetyczne** pokazały możliwość osiągnięcia korzyści finansowych, zarówno bezpośrednich (poprzez wyłudzanie środków finansowych), jak i pośrednich (np. poprzez płacenie za uszkodzenie usługi innej osoby)].

3) **Minimalne umiejętności czytania** i **pisania użytkowników** korzystających z technologii informacyjno-komunikacyjnych (użytkownik jest typowym przykładem najsłabszego ogniwa w łańcuchu).

Wraz z rozwojem wszelkiego rodzaju usług opartych na zasadzie as-a-service[8] , w środowisku cyberprzestępczym pojawiło się wiele platform (zazwyczaj podziemnych, darknetowych forów), na których oferowane są usługi, które można określić jako **Crime-as-a-service** (cyberprzestępczość jako usługa). Powstaje zatem *"złośliwe oprogramowanie* lub szara *strefa", w której* niemal każdy użytkownik może popełnić cyberprzestępstwo. Domyślnie oferowane są następujące usługi, określane zbiorczo jako "przestępczość jako usługa" (crime-as-a-service):

- *Badania jako usługa (Research-as-a-service),*[9]
- *Crimeware-as-a-service,*[10]
- *Infrastruktura jako usługa (Infrastructure-as-a-service),*[11]
- *Hakowanie jako usługa,*[12]
- *Dane jako usługa (Data-as-a-service),*[13]
- *Spam jako usługa,*[14]
- *Ransomware-as-a-service* i.

Lista poszczególnych usług nie jest wyczerpująca i można stwierdzić, że w ramach przestępczości jako usługi można zamówić każdą możliwą usługę lub towar, który można wykorzystać lub uzyskać w cyberprzestrzeni. Wzrost tych negatywnych działań jest również bezpośrednio związany ze zjawiskiem Internetu Rzeczy (IoT), który łączy urządzenia (systemy komputerowe) z Internetem, a tym samym stanowi kolejne istotne zagrożenie, polegające przede wszystkim na nieprzestrzeganiu jednej z podstawowych zasad bezpieczeństwa.

Wielu producentów i dystrybutorów systemów komputerowych, które można zaklasyfikować jako IoT, nie zajmuje się kwestią bezpieczeństwa (ich celem jest wprowadzenie na rynek i sprzedaż jak największej liczby urządzeń, które można zaklasyfikować jako system komputerowy), co wykorzystują atakujący.

Koszty związane z rozwojem bezpieczeństwa są zwykle najdroższą częścią rozwoju, ale jest to obszar, którym należy się zająć nawet w obliczu znanych zagrożeń. Przykłady to: niezabezpieczony kanał komunikacyjny rozrusznika serca[15] ; samochód lub samolot, którym można zdalnie sterować[16] ; inteligentny dom lub jego elementy (lodówka, bojler, system bezpieczeństwa, telewizor itp.), którymi można zdalnie sterować[17] itp.

*"Zastanawiam się, jak potoczą się losy świata, w którym już w **tym roku będziemy** korzystać z 6,4 mld urządzeń IoT. W ciągu najbliższych czterech lat liczba ta powinna wynieść 20,8 mld urządzeń. Co więcej, wiele z tych urządzeń będzie miało znacznie dłuższą żywotność w porównaniu z normalnym cyklem życia telefonów komórkowych, tabletów czy laptopów. W jaki sposób producenci samochodów będą w stanie zapewnić bezpieczeństwo modelu z 2020 roku dziesięć lat później? A może lodówka, która wytrzyma w Twoim domu dobre piętnaście lat? Ile czasu zajęło firmie Microsoft nauczenie się, jak aktualizować swój własny system operacyjny?".*[18]

Schneier twierdzi, że atakujący mogą zrobić z danymi zasadniczo trzy podstawowe rzeczy: ukraść je (naruszając zasadę **poufności**), zmienić (naruszając zasadę **integralności**) lub uniemożliwić właścicielom dostęp do nich (naruszając zasadę **dostępności**). Schneier twierdzi, że wraz z pojawieniem się IoT to właśnie te dwa ostatnie rodzaje ataków staną się niezwykle skuteczne.[19]

W dalszej części artykułu przedstawię niektóre ataki występujące w cyberprzestrzeni. Nie jest możliwe zdefiniowanie wszystkich ataków, zarówno ze względu na zakres niniejszej publikacji, jak i na brak możliwości opisania wszystkich możliwych alternatywnych zachowań, które można by objąć terminem cyberprzestępczość. Tam, gdzie jest to możliwe, wskazana zostanie ewentualna kwalifikacja karna takiego zachowania w odniesieniu do konkretnego przejawu cyberprzestępczości.

---

[1] *Sędzia, 69-latek, który ściągał dziecięce porno, narażony na "katastrofalne upokorzenie".* [online]. [cyt. 2009-09-01]. Dostępny pod adresem: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

[2] HILL, Kaszmir. *Ci dwaj gracze Diablo III ukradli wirtualną zbroję i złoto - i zostali oskarżeni w IRL* [online]. [cyt. 2015-08-10]. Dostępne od:

http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/

[3] Więcej szczegółów w: SCHNEIER, Bruce. *Przestępczość: The Internet's Next Big Thing* . [online]. [cyt. 6.11.2007]. Dostępne na stronie https://www.schneier.com/crypto-gram/archives/2002/1215.html

[4] JIROVSKÝ, Václav. *Cyberprzestępczość to nie tylko hakerstwo, cracking, wirusy i trojany bez tajemnic.* Praga: Grada, 2007, s. 30.

[5] Więcej szczegółów w: GOODMAN, Marc. *Wizja przestępczości w przyszłości* [online]. [cyt. 13.11.2014]. Dostępny pod adresem: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071

[6] MUELLER, Robert. [online]. [cit.3.4.2013]. Dostępne od:

https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

[7] Zob. *The Internet Organised Crime Threat Assessment (iOCTA) 2014* [online]. [cyt. 10.8.2015]. Dostępny pod adresem: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

[8]Jest to świadczenie usług typowo związanych z rozwiązaniem chmurowym. Przykłady to: infrastruktura jako usługa, platforma jako usługa, usługa jako usługa, bezpieczeństwo jako usługa itp.

[9] Dzięki tej usłudze można sobie wyobrazić działania polegające na wykrywaniu różnych, nieznanych wcześniej luk w zabezpieczeniach docelowego systemu komputerowego lub oprogramowania (luki te są znane jako luki typu zero-day).

Sama działalność Research-as-a-Service nie musi być przestępcza ani nielegalna. Wykrywaniem podatności i błędów zajmuje się wielu specjalistów ds. bezpieczeństwa IT (np. testy penetracyjne itp.). Zazwyczaj usługi te są świadczone na podstawie warunków umowy między podmiotem testującym a testerem lub z wykorzystaniem jakichś okoliczności wykluczających nielegalność.

[10] Usługa "crimeware-as-a-service" oferuje szereg działań, począwszy od zwykłej sprzedaży złośliwego oprogramowania, poprzez "dostosowywanie" go do potrzeb użytkownika, aż po dostarczanie exploitów (luk w zabezpieczeniach) itp.

[11] Infrastruktura jako usługa to oferta fizycznych lub wirtualnych systemów komputerowych (botnety, usługi hostingowe, wynajem sieci itp.).

[12] Usługa ta może polegać na zwykłym złamaniu danych dostępowych do poczty elektronicznej, konta w sieci społecznościowej itp. do profesjonalnych i wyrafinowanych ataków na wybraną ofiarę. Obszar ten może również obejmować np. przeprowadzanie ataków DoS i DDoS.

[13] Data-as-a-service oferuje towar, na który jest największy popyt, czyli dane. W szczególności są to: dane dostępowe (nazwa użytkownika i hasło) do różnych kont, karty kredytowe, konta bankowe, skradzione karty kredytowe, a także informacje o osobach (miejsce zamieszkania, daty urodzenia, numery telefonów, wiadomości e-mail itp.)

[14] Nazwa wskazuje na możliwość subskrypcji i opłacenia kampanii spamowej.

[15] Por. TAYLOR, Harriet. W *jaki sposób "Internet rzeczy" może okazać się zgubny.* [online]. [cyt. 17.6.2016]. Dostępny pod adresem: http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html

[16] Więcej szczegółów w: GREENBERG, Andy. *Hakerzy zdalnie przechwycili Jeepa na autostradzie - ze mną w środku.* [online]. [cyt. 2016 maj 4]. Dostępny pod adresem: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Wersja w języku czeskim jest dostępna m.in. na stronie: http://auto.idnes.cz/hackeri-unesli-jeep-dalkove-ovladani-auta-f1l-/automoto.aspx?c=A150723_135910_automoto_fdv.

Więcej informacji na ten temat można znaleźć w publikacji ZETTER, Kim. *Czy pasażerowie mogą włamać się do samolotów komunikacyjnych?* [online]. [cyt. 2016 maj 5]. Dostępny pod adresem: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/

[17] Możliwe jest na przykład ominięcie zabezpieczeń domowych, podniesienie temperatury za pomocą zdalnie sterowanego termostatu i wyrządzenie krzywdy innym osobom, zamawianie nieuzasadnionych ilości jedzenia za pomocą "inteligentnej" lodówki itp.

[18] DOČEKAL, Daniel. Bruce Schneier: *Internet rzeczy przyniesie ataki, których nie jesteśmy w stanie sobie wyobrazić.* [online]. [cyt. 10.8.2016]. Dostępny pod adresem: http://www.lupa.cz/clanky/bruce-schneier-internet-veci-prinese-utoky-ktere-si-neumime-predstavit/

[19] SCHNEIER, Bruce. *Internet rzeczy zmieni wielkie włamania w prawdziwe katastrofy.* [online]. [cyt. 10.8.2016]. Dostępny pod adresem: https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster

4.1. Inżynieria społeczna (socjotechnika)

Inżynierii społecznej nie można w każdych okolicznościach uznać za bezpośredni atak cybernetyczny, ale jest ona warunkiem koniecznym powodzenia wielu ataków cybernetycznych.

Gdybyśmy chcieli zdefiniować pojęcie inżynierii społecznej, moglibyśmy powiedzieć, że jest to wywieranie wpływu na ludzi, przekonywanie ich lub manipulowanie nimi w celu skłonienia ich do wykonania określonego działania lub uzyskania od nich informacji, których w przeciwnym razie by nie przekazali. Ma to na celu wywołanie u ofiary wrażenia, że sytuacja, w której się znajduje, jest inna niż w rzeczywistości. W bardziej uproszczonym ujęciu można powiedzieć, że jest to "sztuka oszustwa", a Mitnick wyróżnia dwie specjalizacje w zawodzie manipulatora. *"Ten, kto wyłudza pieniądze od ludzi, jest zwykłym oszustem, natomiast ten, kto stosuje manipulację i perswazję wobec firm - zwykle z zamiarem zdobycia informacji - jest socjotechnikiem".* [1]

Jestem przekonany, że to stwierdzenie Mitnicka z 2003 r. nie utrzymałoby się w obecnym cyfrowym świecie, ponieważ wielu atakujących wykorzystuje techniki inżynierii społecznej do pozyskiwania informacji lub danych, a następnie wykorzystuje je, na przykład w ramach usługi "przestępstwo jako usługa" (crime-as-a-service). Co więcej, techniki te są wykorzystywane nie tylko przeciwko firmom, ale także przeciwko osobom prywatnym. Faktyczny atak może nie przybrać przede wszystkim formy oszustwa, ale informacje mogą zostać sprzedane lub wykorzystane do poważniejszego ataku.

Główną ideą socjotechniki nie jest stosowanie różnych czysto technicznych metod lub narzędzi do złamania hasła, gdy na przykład o wiele łatwiej jest wprowadzić ofiarę w błąd, aby dobrowolnie podała hasło. Najsłabszym ogniwem w systemie bezpieczeństwa jest i zawsze będzie człowiek (użytkownik). Ponieważ nie ma na świecie systemu komputerowego, który przynajmniej na jakimś etapie (czy to przy uruchamianiu, konfigurowaniu, czy konserwacji systemu komputerowego) nie byłby zależny od człowieka, najłatwiejszym sposobem uzyskania niezbędnych informacji jest właśnie człowiek.

To właśnie prostota ataku ukierunkowanego na najsłabsze ogniwo systemu sprawia, że jest to zazwyczaj najskuteczniejsza forma ataku. Inżynieria społeczna wysunęła się na pierwszy plan wraz ze sprawą Mitnicka[2] , który przez wielu uważany jest za hakera, ale sam uważa się raczej za socjotechnika. Mitnick pokazuje w swoich książkach[3] , jak łatwo jest uzyskać informacje, które są wrażliwe i stanowią zagrożenie dla bezpieczeństwa osób i organizacji. Podczas przesłuchania przed Komisją Senatu USA ds. Rządowych[4] , gdzie Mitnick zeznawał na temat sposobu, w jaki zdobył hasła i poufne informacje do systemów komputerowych spenetrowanych przez siebie firm, Mitnick stwierdził między innymi: *"Przedstawiłem się jako ktoś inny i po prostu poprosiłem o nie".*

W przypadku inżynierii społecznej jednym z kluczowych czynników jest zdobycie jak największej ilości informacji o celu ataku (niezależnie od tego, czy jest to system komputerowy, podmiot prawny czy osoba fizyczna). Często przed właściwym atakiem następuje długotrwałe oddziaływanie na kluczową osobę i budowanie "zaufania" między atakującym a ofiarą, przy czym atakujący zazwyczaj wykorzystuje ludzką nieostrożność, łatwowierność, chęć niesienia pomocy innym, lenistwo, słabość, strach (np. aby nie wpaść w kłopoty), nieodpowiedzialność, głupotę itp.

Powyższe cechy ludzkie bardzo pomagają napastnikowi w przeprowadzeniu ataku. Zadaj sobie pytanie, na ile weryfikujesz drugą stronę, np. w rozmowie telefonicznej lub komunikacji za pośrednictwem ICT? W jakim stopniu sprawdzasz nośniki pamięci (dyski USB, karty pamięci itp.), które otrzymałeś w prezencie podczas prezentacji?

Szczególnie w dziedzinie ICT można zaobserwować coraz bardziej wyrafinowane i rozbudowane ataki [np. dobrze przygotowane oszukańcze e-maile, prawdziwe instytucje (wykorzystywane jako rzekomy nadawca), przekierowania na oszukańcze strony lub instalacja złośliwego oprogramowania w załączniku do dokumentu lub na nośniku pamięci itp.]

Ataki socjotechniczne są zwykle przeprowadzane na trzy sposoby, które są ze sobą połączone:

1. **Gromadzenie swobodnie** (publicznie) **dostępnych danych** o celu ataku

2. **Atak fizyczny** (np. napastnik podszywa się pod pracownika agencji usługowej - np. serwisanta drukarek, konserwatora itp.), w którym napastnik stara się uzyskać jak najwięcej informacji z "wnętrza" firmy lub poufnych informacji o poszczególnych pracownikach (w tym np. przeszukuje śmieci itp.)

3. **Atak psychologiczny**

Do najczęstszych metod ataków socjotechnicznych należą:

1. **Oszukańcza wiadomość e-mail** lub **fałszywa strona internetowa**

2. **Rozmowa telefoniczna**

3. **Atak twarzą w twarz**

4. **Dumpster diving** ("nurkowanie po śmietnikach", a także "nurkowanie z danymi"**)**

5. **Przeszukiwanie sieci, portali społecznościowych itp.**(jest to łatwo dostępne**,** otwarte źródło danych dla osób zajmujących się inżynierią społeczną, które pomaga w zdobyciu lub zweryfikowaniu informacji o potencjalnym celu ataku). **Informacje publiczne dostępne w** Internecie (np. życiorysy, prace dyplomowe, propozycje itp. zamieszczone w Internecie). **Raporty roczne i inne publicznie dostępne informacje o firmie.**

6. **Dostarczanie reklam lub innych materiałów na płytach CD, DVD lub innych nośnikach pamięci**

7. **Pozostawienie nośnika danych** (USB itp.) w **obszarze zainteresowania (np. w** firmie, w domu pracownika itp. nośnik ten zwykle zawiera złośliwe oprogramowanie**)**

8. **Zaproponuj wypróbowanie usługi online** (np. oferta przechowywania danych w chmurze lub interesujących bezpłatnych usług itp.)

9. **Dostawa lub znalezienie sprzętu** (systemu komputerowego)

10. Fałszywy serwisant

11. Inne

Jeśli chodzi o cele ataków socjotechnicznych w organizacji, to mogą nimi być:

- stanowiska kierownicze,
- dział IT,
- pracownicy działu pomocy technicznej,
- recepcjonistki (sekretariaty),
- pracownicy ochrony,
- zarządzanie budynkiem,
- czyszczenie itp.

Socjotechnik jest w stanie manipulować ludźmi dzięki swoim umiejętnościom, jednak w niektórych przypadkach zwykła manipulacja nie wystarcza i konieczne jest połączenie tych informacji z wiedzą techniczną z zakresu technologii informacyjno-komunikacyjnych.

Rozdział ten kończę przykładem, w którym Mitnick pokazuje, w jaki sposób można połączyć techniki społeczne z wiedzą z zakresu technologii informacyjno-komunikacyjnych:[5]

Młody haker, którego będę nazywał Ivan Peters, wyruszył, aby zdobyć kod źródłowy nowej gry. Nie miał problemów z dostaniem się do sieci WAN firmy, ponieważ jego kolega haker zdołał już włamać się do jednego z serwerów internetowych. Po odkryciu słabego punktu w oprogramowaniu aż dziw, że nie spadł z krzesła. Okazało się, że system korzystał z *"podwójnego naprowadzania", co oznacza, że* miał dostęp do sieci wewnętrznej również z tego miejsca.

Jednak po wstąpieniu Ivan stanął przed problemem podobnym do tego, z jakim spotyka się turysta w Luwrze, który chce znaleźć portret Mony Lisy. Bez przewodnika może tam być tygodniami. Była to globalna korporacja z setkami biur i tysiącami serwerów, która nie publikowała w swojej sieci indeksów deweloperskich ani innych usług przewodników po swoich danych. Zamiast korzystać z metod technologicznych, aby znaleźć serwer, do którego chciał się dostać, użył metody socjotechnicznej. Przeprowadził kilka rozmów telefonicznych w oparciu o procedury opisane wcześniej w tej książce. Po pierwsze, zadzwonił do działu pomocy technicznej działu IT, przedstawił się jako pracownik firmy i powiedział, że chce omówić konkretny problem związany z interfejsem produktu, nad którym pracuje jego grupa. Poprosił o numer telefonu kierownika projektu w grupie programistów, którzy pracowali nad grami. Następnie zadzwonił pod wskazany numer i podał się za pracownika działu IT. "*Późnym wieczorem*" - powiedział - *"będziemy zmieniać router i chcemy mieć pewność, że osoby z Twojej grupy nie stracą połączenia z serwerem. Jakiego serwera używasz?"* Sieć była stale unowocześniana, a podanie nazwy serwera nie zaszkodzi, prawda? W końcu jest on chroniony hasłem, a sama znajomość nazwy nikomu nie pomoże. Kierownik projektu podał więc nazwę serwera. Nie próbował nawet oddzwonić i zweryfikować tej historii, a przynajmniej zapisać nazwiska i numeru telefonu rozmówcy. Podał jedynie nazwy serwerów: ATM5 i ATM6.

Teraz Ivan powrócił do metod technologicznych, aby uzyskać informacje o uwierzytelnianiu. W większości przypadków pierwszym krokiem jest zidentyfikowanie konta za pomocą łatwego hasła, które pozwoli uzyskać dostęp do systemu. Jeśli atakujący próbuje zdalnie zidentyfikować hasła za pomocą narzędzi hakerskich, wymaga to wielogodzinnego połączenia z siecią firmową.

Wiąże się z tym pewne niebezpieczeństwo: im dłużej jest on podłączony do sieci, tym większe ryzyko jego wykrycia i schwytania. Po pierwsze, Ivan użył wyliczania, aby ujawnić szczegóły systemu. Jak zwykle, odpowiednie narzędzia można znaleźć w Internecie (http://mtslenth.0catch.com). Ivan znalazł w sieci kilka ogólnodostępnych narzędzi hakerskich, które pozwoliły mu zautomatyzować proces i uniknąć ręcznej pracy, która wydłużałaby czas operacji, a tym samym zwiększała ryzyko złapania. Wiedząc, że firma używa głównie serwerów opartych na systemie Windows, pobrał program o nazwie NTBEnum, narzędzie do wyliczania[6] NetBIOS (podstawowy system wejścia/wyjścia). Wprowadził adres IP serwera ATM5 i uruchomił program. Narzędzie zidentyfikowało kilka kont istniejących na serwerze.

Po zidentyfikowaniu istniejących kont ten sam program umożliwił przeprowadzenie ataku słownikowego. Atak słownikowy jest dobrze znany osobom zajmującym się bezpieczeństwem komputerowym i, oczywiście, hakerom. Inni ludzie są zszokowani, że coś takiego jest w ogóle możliwe. Celem tego ataku jest poznanie haseł użytkowników przy użyciu powszechnie używanych słów. Wszyscy jesteśmy leniwi w niektórych sprawach, ale nigdy nie przestaje mnie zadziwiać, że ludzka kreatywność i wyobraźnia biorą urlop, gdy przychodzi do wyboru hasła. Większość z nas chce mieć hasło, które będzie nas chronić, ale jednocześnie będzie łatwe do zapamiętania. Zazwyczaj oznacza to użycie słowa, które jest nam bliskie. Mogą to być na przykład nasze inicjały, drugie imię, przezwisko, imię współmałżonka, nazwa ulubionej piosenki, filmu lub marki piwa. Następnie nazwę ulicy lub miasta, w którym mieszkamy, markę samochodu, którym jeździmy, ulubione miejsce na wakacje lub nazwę strumienia, w którym pstrągi najlepiej biorą. Czy widzimy regułę? W większości przypadków są to nazwy lub wyrażenia, które można znaleźć w słowniku. Atak słownikowy polega na próbach użycia jako hasła haseł słownikowych jednego lub kilku użytkowników.

Iwan przeprowadził atak słownikowy w trzech fazach. W pierwszej fazie - lista 800 najczęściej używanych haseł. Na liście znajdują się takie hasła*, jak sekret, praca* czy *hasło.* Ponadto program tworzył permutacje tych wyrażeń z dodanymi cyframi lub numerem bieżącego miesiąca. Program wypróbował każde hasło na wszystkich kontach znalezionych w systemie. Brak wyników. W drugiej fazie otwarto stronę wyszukiwarki Google i wpisano hasło "*wordlists dictionaries*", po czym znaleziono tysiące stron zawierających wordlists oraz słowniki angielskie i inne. Pobrał cały elektroniczny słownik języka angielskiego. Uzupełnił ją o kilka list terminów, które wyszukiwarka znalazła. Ivan wybrał adres www.outpost9.com/files/Wordlists.html. Z tej strony mógł pobrać (całkowicie za darmo) zestaw plików zawierających nazwiska, nietypowe imiona, nazwy i terminy związane z polityką, nazwiska aktorów oraz słowa i imiona z Biblii. Inna strona z listami wyrażeń jest dostępna na Uniwersytecie Oksfordzkim pod adresem ftp://ftp.ox.ac.uk/pub/wordlists. Pod innymi adresami można znaleźć listy imion postaci z filmów animowanych, cytaty z Szekspira, Odysei, Tolkiena i Gwiezdnych wojen oraz słowa związane z nauką, religią itp. (Jedna z firm internetowych sprzedaje listę 4,4 mln słów i imion już za 20 dolarów). Program atakujący można również skonfigurować tak, aby tworzył anagramy na podstawie terminów słownikowych - jest to kolejna ulubiona metoda użytkowników zwiększająca ich bezpieczeństwo.

Gdy Ivan wybrał listę, której będzie używał, i uruchomił program, przełączył go w tryb automatyczny, aby mógł zająć się czymś innym. Można by pomyśleć, że taki atak dałby atakującemu czas na dłuższą drzemkę, a nawet, że po przebudzeniu postępy byłyby niewielkie. W rzeczywistości, w zależności od rodzaju zaatakowanego systemu, konfiguracji systemów bezpieczeństwa i szybkości połączenia, cały zasób słownictwa angielskiego można przetestować w ciągu 30 minut! W trakcie ataku Ivan włączył drugi komputer i przeprowadził podobny atak na drugi serwer wykorzystywany przez grupę programistyczną ATM6. Dwadzieścia minut później udało się dokonać czegoś, co większość ludzi uznałaby za niemożliwe: złamać hasło i odkryć, że jeden z użytkowników wybrał hasło *"Frodo"*, imię jednego z hobbitów, bohatera Władcy Pierścieni. Mając hasło w ręku, Ivan połączył się z serwerem ATM6. Czekały na niego dobre i złe wieści. Dobra wiadomość była taka, że konto, na które się włamał, miało uprawnienia administratora. A zła wiadomość była taka, że nigdzie nie mógł znaleźć kodu źródłowego gry. Najwyraźniej znajdował się on na drugim serwerze, ATM5, który oparł się atakowi słownikowemu. Ale Ivan nie poddawał się - miał jeszcze w zanadrzu kilka sztuczek. W niektórych systemach operacyjnych Windows i UNIX zaszyfrowane hasła są dostępne dla każdego, kto ma dostęp do komputera, na którym się znajdują. Dzieje się tak dlatego, że zaszyfrowanych haseł nie można odszyfrować, a zatem nie ma powodu, aby je chronić. Ta teoria jest błędna. Używając innego narzędzia dostępnego w sieci, *pwdump3,* pobrał zaszyfrowane hasła z serwera ATM6. Typowy plik z zaszyfrowanym hasłem wygląda tak:

Administrator: 500:95E4321A38AD8D6AB75E0C8D76954A50:

2E48927AQB04F3BFB341E266D6L

akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357F157873D72D

digger:1111:5D15COD58D0216C525AD3B83FA6627C7:17AD564144308B42B8403D01AE256

555

ellgan:1112:2017DA45D8O1383EFF17365FAF1FFE89:07AEC950C22CBB9C2C734EB89j1

tafeeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A728447212FC05E1D208203

35

vkantar;1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD12258946FCC7BD153F1

CD6

vwallwick:1119:25904EC665BA30F44494F42E1054F192:15B2B7953FB632907455D2706A432

mmcdonald: 1121:

A4AED098D29A3217AAD3B435B51404EE:40670F936B79C2ED522F5ECA939c

kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DEC8E827A121273EF084CDBF5F

D192

Mając plik na swoim komputerze, Ivan użył innego narzędzia do przeprowadzenia *ataku*, który nazwał *atakiem brute force.*[7] Testuje wszystkie kombinacje znaków alfanumerycznych i większości znaków specjalnych.

Ivan użył narzędzia *L0phtcrack3* (czytaj loft-crack; dostępne pod adresem www.atstake.com; inne źródło doskonałych narzędzi do zgadywania haseł to *www.elcomsoft.com*). Administratorzy używają L0phtcrack3 do znajdowania *"słabych"* haseł, a hakerzy do ich łamania. Program L0phtcrack3 umożliwia wypróbowywanie haseł zawierających kombinacje liter, cyfr i większości symboli, w tym @#$%^&. Systematycznie testuje wszystkie możliwe kombinacje większości znaków. (Jeśli jednak w haśle użyto niewidocznych znaków, L0phtcrack3 nie będzie w stanie wykryć takiego hasła). Program ten działa z niewiarygodną szybkością, która na komputerze z procesorem 1 GHz może osiągnąć 2,8 miliona prób na sekundę. Nawet przy takiej szybkości, jeżeli administrator dobrze skonfigurował system Windows (tzn. wyłączył korzystanie z funkcji haszowania LANMAN), złamanie hasła może zająć dużo czasu. Z tego powodu atakujący często pobiera pliki z hasłami na swój komputer i przeprowadza atak na własnym komputerze, aby nie ryzykować wykrycia podczas długotrwałego połączenia. Ivan nie musiał długo czekać.

Kilka godzin później program odnalazł hasła wszystkich członków grupy programistów. Były to jednak hasła użytkowników korzystających z ATM6, gdzie nie było kodu źródłowego. Co teraz? Nadal nie udało się uzyskać haseł dostępu do serwera ATM5. Będąc hakerem, znał złe nawyki większości użytkowników i doszedł do wniosku, że jeden z członków zespołu mógł wybrać to samo hasło na obu serwerach. I tak właśnie się stało. Jeden z programistów miał hasło *gracza* zarówno w ATM5, jak i ATM6. Drzwi otworzyły się dla Ivana, który mógł poszukać kodu źródłowego.

Gdy je znalazł i pobrał całe drzewo, zrobił jeszcze jedną typową dla hakerów rzecz. Zmienił hasło na nieaktywnym koncie z uprawnieniami administratora, na wszelki wypadek, gdyby chciał później wrócić i pobrać nową wersję programu.

Aby zmniejszyć ryzyko związane z socjotechniką, należy podnosić świadomość potencjalnych zagrożeń nie tylko wewnątrz organizacji, ale w całym społeczeństwie. Jak już wspomniałem, socjotechnika pomaga w przeprowadzeniu ataku, a określenie celu zależy wyłącznie od osoby atakującej. O wiele łatwiej jest atakować masy niewyrobionych i nieświadomych ludzi niż względnie dobrze chronione społeczeństwo.

---

[1] MITNICK, Kevin D. i William L. SIMON. *Sztuka podstępu*. Gliwice: Helion, 2003, ISBN 83-7361-210-6. s. 6

[2] *Sprawa Kevina Mitnicka: 1999* [online] . [cyt. 2.11.2011]. Dostępny pod adresem: http://www.encyclopedia.com/doc/1G2-3498200381.html

[3] Więcej informacji można znaleźć na stronie:

MITNICK, Kevin D. i William L., SIMON. *Sztuka podstępu*. Gliwice: Helion, 2003, ISBN 83-7361-210-6.

MITNICK, Kevin D. *Sztuka włamywania się: prawdziwe historie kryjące się za wyczynami hakerów, intruzów i oszustów*. Indianapolis: Wiley, c2006. ISBN 0-471-78266-1.

MITNICK, Kevin D. i William L., SIMON. *Duch w przewodach: moje przygody jako najbardziej poszukiwanego hakera na świecie*. New York: Little, Brown & Co, 2012. ISBN 9780316037723.

[4] *Świadectwo byłego hakera.* [online]. [cyt. 26.9.2008]. Dostępny pod adresem: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html

[5] Przykład przytoczony dosłownie z: MITNICK, Kevin D. i William L. SIMON. *Sztuka podstępu*. Gliwice: Helion, 2003, ISBN 83-7361-210-6, s. 127-130.

[6] **Enumeracja -** proces wykrywania usług dostępnych na danym serwerze, jego systemu operacyjnego oraz nazw kont użytkowników mających dostęp do systemu.

[7] **Brute force attack** - strategia łamania haseł polegająca na testowaniu wszystkich możliwych kombinacji znaków alfanumerycznych i specjalnych.

4.2. Botnet

Botnet można zdefiniować po prostu jako sieć połączonych programowo botów[1] , które wykonują działania na polecenie "właściciela" (lub administratora) tej sieci. Tak skonstruowana sieć może być wykorzystywana do działalności legalnej (np. przetwarzanie rozproszone) lub do działalności nielegalnej (patrz niżej).

To właśnie przetwarzanie rozproszone, de facto nieumyślnie, podsunęło przestępcom pomysł na tworzenie botnetów w formie, w jakiej widzimy je dzisiaj. Z przyczepy do obliczeń rozproszonych wynika, że *"**większość komputerów na świecie wykorzystuje swój pełny potencjał obliczeniowy tylko przez bardzo niewielki ułamek czasu pracy,** a ich zużycie energii elektrycznej jest tylko nieznacznie mniejsze niż gdyby były w pełni obciążone". **Wielka szkoda nie skorzystać z tego leniwego komputera, a mało kto zdaje sobie sprawę, ile takiej niewykorzystanej mocy jest na świecie**... W informatyce rozproszonej przysłowie **"Nie musi padać deszcz, wystarczy, że będzie kapać" ma** zastosowanie jak ulał, **a tu miliony zwykłych komputerów na świecie ociekają mocą, która kilkakrotnie przewyższa moc nawet największych superkomputerów na świecie...** Zaangażowanie w jakikolwiek projekt dotyczący przetwarzania rozproszonego polega jedynie na zainstalowaniu klienta, który zazwyczaj potrafi już wykonać wszystkie niezbędne czynności i zająć się określonymi aplikacjami... Większość projektów działa w ten sposób, że całość pracy jest dzielona na wiele części, które są następnie rozdzielane do poszczególnych komputerów, które o nie poproszą. Po przetworzeniu każdego fragmentu poszczególne komputery przesyłają uzyskane dane z powrotem do centrum projektowego, gdzie wyniki są łączone w jedną całość".*[2]

Sama idea dystrybucji zasobów lub wykorzystania niewielkiej mocy obliczeniowej innych systemów komputerowych do np. obliczania skomplikowanych algorytmów matematycznych itp. z pewnością nie jest zła i jest o wiele bardziej efektywna niż używanie i budowanie "superkomputerów". Jednak jako ludzie jesteśmy dość zaradni, więc było naturalne, że pomysł ten zostanie wykorzystany w celach innych niż altruistyczne czy dobroczynne. Możliwość rozdzielenia różnych zadań między różne komputery znajdujące się w różnych miejscach geograficznych była i jest atrakcyjna dla atakujących.

Obecny system komputerowy, np. w postaci serwera pocztowego, nie ma problemu z wysyłaniem dziesiątek milionów czy miliardów wiadomości e-mail dziennie. Jeśli użytkownik zdecyduje się użyć tego systemu do np. rozsyłania spamu, ten system komputerowy (identyfikowalny za pomocą identyfikatorów takich jak adres IP) będzie wykonywał tę czynność tylko przez bardzo krótki okres czasu, ponieważ bardzo szybko zostanie zablokowany przez dostawcę usług internetowych (np. z powodu nielegalnego lub nadmiernego ruchu w sieci, który można zaklasyfikować jako spam), jego adres pojawi się na "czarnych listach", a ruch (np. poczta wychodząca) zostanie zablokowany na podstawie tej informacji. Jeśli jednak atakujący wykorzystuje moc rozproszoną w postaci botnetu, będzie miał od tysięcy do setek tysięcy komputerów, z których każdy wysyła część wiadomości (np. 1000-2000 wiadomości dziennie). Taki ruch nie będzie wtedy uważany za problematyczny i nie będzie zatrzymywany.

Typowe dla **botnetu** jest to, że **jeżeli docelowy system komputerowy zostanie skutecznie zainfekowany, system ten,** nazywany "zombie" lub "bot" (zniewolony system komputerowy), **łączy się z centralnym serwerem kontroli** [zwanym serwerem dowodzenia i kontroli (C&C)]. **Kontrola nad całym tym systemem** (zawierającym zombie i C&C) **spoczywa na atakującym** (zwanym botmasterem lub botherderem), który **kontroluje boty za pośrednictwem serwera C&C**. [3]

Następujące elementy są charakterystyczne (niezbędne) dla botnetu:

1. **Infrastruktura dowodzenia i kontroli (C&C)**

Jest to infrastruktura, która składa się z elementu (lub elementów) kontrolnego oraz botów (sterowanych systemów komputerowych).

2. **Instalacja i obsługa buta**

Najczęściej jest to złośliwe oprogramowanie rozprzestrzeniane za pośrednictwem botnetu lub w inny sposób. Głównym celem takiego złośliwego oprogramowania jest podłączanie innych systemów komputerowych do botnetu. Złośliwe oprogramowanie wykorzystuje różne luki w zabezpieczeniach systemów komputerowych.

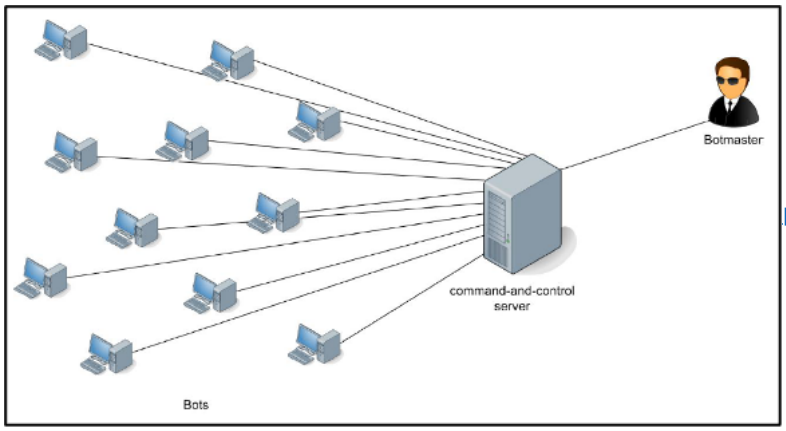
3. **Kontrolowanie botów za pomocą infrastruktury C&C**

Bot to oprogramowanie działające w ukryciu i wykorzystujące popularne kanały komunikacyjne (IRC, IM, RFC 1459 itp.) do komunikacji z serwerem C&C. Nowe boty starają się uzyskać jak najwięcej informacji z otoczenia i promować się wśród innych systemów komputerowych.

W oparciu o architekturę, istnieją botnety z:

1. **Architekturą scentralizowaną**

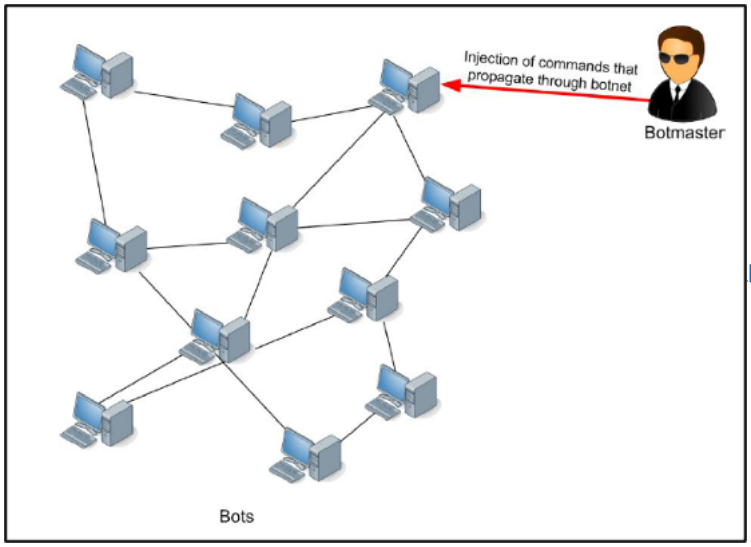
Architektura ta jest zwykle oparta na zasadzie komunikacji klient-serwer. Systemy komputerowe punktów końcowych (zombie/boty) komunikują się bezpośrednio z serwerem C&C (centralnym elementem sterującym) i wykonują instrukcje oraz korzystają z zasobów pochodzących z tego serwera.



[4]

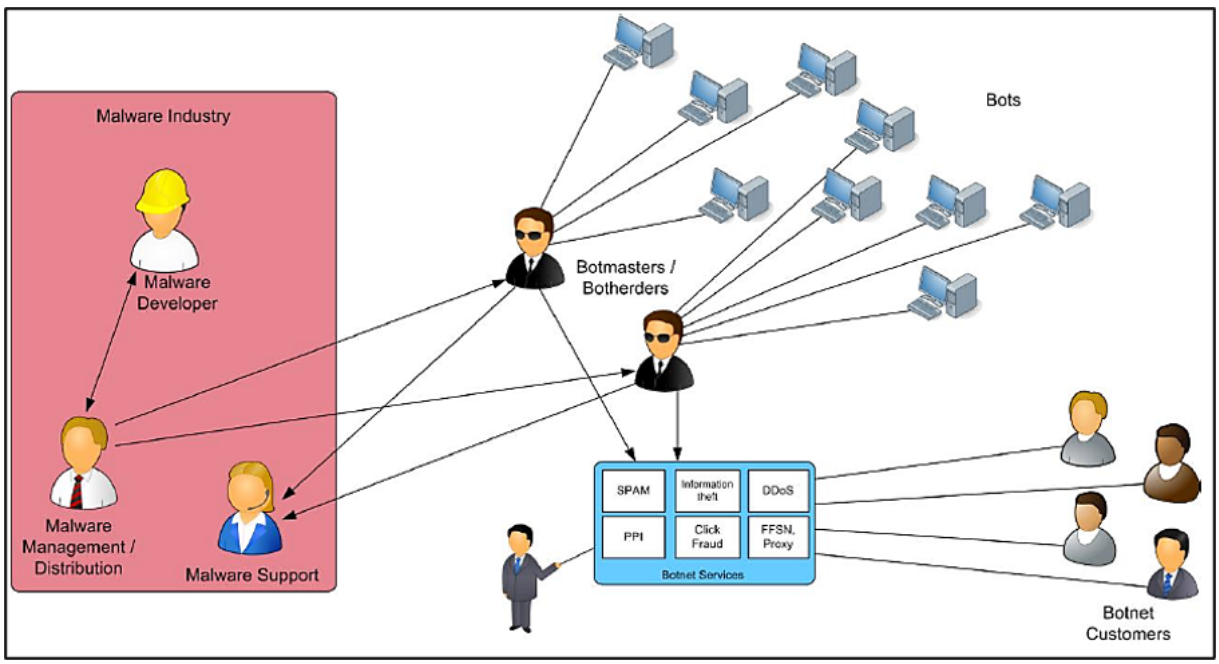
2. **Architekturą zdecentralizowaną**

Zazwyczaj jest on zbudowany w architekturze peer-to-peer (P2P). Architektura ta umożliwia współdzielenie zasobów i poleceń w ramach sieci P2P. Brakuje w nim centralnego elementu sterującego w "tradycyjnej" formie, co sprawia, że system jest bardziej odporny na próby sterowania za pomocą tego elementu.



[5]

Botnety mogą być wykorzystywane do wielu działań, ale główny nacisk kładzie się na zysk finansowy, który polega zarówno na generowaniu własnych ataków (np. ransomware, phishing, spam, kradzież informacji, DDoS itp.), jak i na wynajmowaniu klientom swoich usług lub całego botnetu. Dzięki powyższemu botnet można zaliczyć do struktury **przestępczości jako** usługę (gdzie oferowana jest usługa: **botnet-as-a-service**) lub do gospodarki złośliwego oprogramowania[6] , gdzie stanowi podstawową platformę techniczną niezbędną do przeprowadzenia szeregu cyberataków.



Gospodarka złośliwego oprogramowania

System komputerowy, który staje się częścią botnetu, jest następnie zazwyczaj wykorzystywany do jednego z działań opisanych w poniższej tabeli. Należy zauważyć, że ataki te są zwykle łączone lub rozprowadzane w obrębie botnetu, z uwzględnieniem jego obciążenia pracą, zapotrzebowania "klientów" itp.

Wysyłanie	Kradzież tożsamości	Ataki DoS	Oszustwo przez kliknięcie
- spam - phishing - złośliwe oprogramowanie - adware - oprogramowanie szpiegujące	Uzyskanie i przesłanie (z powrotem do atakującego) osobistych i poufnych danych oraz informacji - Dane dostępu do kont - Dane dostępu do poczty elektronicznej, sieci społecznościowych itp. - Inne dane lub informacje, które mogą zostać wykorzystane lub sprzedane przez atakującego	Przeprowadzenie ataku DoS na cel (system komputerowy) określony przez botmastera.	System komputerowy wyświetla (lub klika) linki reklamowe w witrynie bez wiedzy użytkownika. Stwarza to wrażenie, że witryna zyskuje na ruchu, a reklamodawcy tracą pieniądze.[7]

Poniższa tabela zawiera listę niektórych znanych botnetów[8] :

Data utworzenia	Data rozwiązania umowy	Nazwa	Szacunkowa liczba botów	Liczba wiadomości spamowych w miliardach na dzień	Alias (znany również jako)	Dodatkowe informacje
2002						
	2011	Coreflood	2,300,000			Backdoor. Gromadzenie danych osobowych i informacji wrażliwych.
2004						
		Bagle	230,000[16]	5.7	Beagle, Mitglieder, Lodeight	Masowe spamowanie. Przeznaczona dla systemów komputerowych z systemem operacyjnym Windows.
		Botnet Marina	6,215,000[16]	92	Damon Briant, BOB.dc, Cotmonger, Hacktool.Spammer, Kraken	
		Torpig	180,000[17]		Sinowal, Anserin	Wysyłanie złośliwego oprogramowania oraz gromadzenie danych wrażliwych i osobistych. Przeznaczona dla systemów komputerowych z systemem Windows.
		Burza	160,000[18]	3	Nuwar, Peacomm, Zhelatin	Spamowanie. Przeznaczona dla systemów komputerowych z systemem Windows.
2006						
	marzec 2011 r.	Rustock	150,000[19]	30	RKRustok, Kostrat	Spamowanie. Możliwość wysyłania do 25 000 wiadomości spamowych na godzinę z jednego komputera. Aktywny w systemie operacyjnym Windows.

		Donbot	125,000[20]	0.8	Buzus, Bachsoy	Wysyłanie głównie spamu farmaceutycznego.
2007						
		Cutwail	1,500,000[21]	74	Pandex, Mutant (związany z: Wigon, Pushdo)	Spamowanie. Domyślnie do infekowania systemu komputerowego wykorzystuje konia trojańskiego Pushdo. Aktywny w systemie operacyjnym Windows.
		Akbot	1,300,000[22]			Backdoor umożliwiający przejęcie kontroli nad zainfekowanym komputerem. Po zainstalowaniu zbierał dane, zatrzymywał procesy lub przeprowadzał ataki DDoS.
marzec 2007 r.	Listopad 2008 r.	Srizbi	450,000[23]	60	Cbeplay, Wymiennik	Przede wszystkim spamowanie. Trojan Srizbi został wykorzystany do zainfekowania systemów komputerowych.
		Lethic	260,000[16]	2	brak	Wysyłanie głównie spamu farmaceutycznego.
Wrzesień 2007 r.		dBot	10 000+ (Europa)		dentaoBot, d-net, SDBOT	
		Xarvester	10,000[16]	0.15	Rlsloup, Pixoliz	Spamowanie.
2008						
		Sality	1,000,000[24]		Sektor, kucharz	Grupa złośliwego oprogramowania. Systemy komputerowe zainfekowane wirusem Sality komunikują się za pośrednictwem sieci P2P. Działania obejmują: wysyłanie spamu, zbieranie poufnych danych, infekowanie serwerów WWW, wykonywanie obliczeń rozproszonych (np. łamanie haseł itp.). Aktywny w systemie operacyjnym Windows.
Kwiecień 2008		Kraken	495,000[33]	9	Kracken	Wysyłanie złośliwego oprogramowania. Podłączanie innych komputerów do botnetu.
	Grudzień 2009 r.	Mariposa	12,000,000[25]			Botnet zajmujący się głównie oszustwami i atakami DDoS. **Był to jeden z największych botnetów w historii.**

Listopad 2008 r.		Conficker	10,500,000+[26]	10	DownUp, DownAndUp, DownAdUp, Kido	Robak atakujący systemy komputerowe z systemem Windows. Dziury w tym systemie operacyjnym zostały wykorzystane do dalszej ekspansji botnetu.
Listopad 2008 r.	marzec 2010 r.	Waledac	80,000[27]	1.5	Waled, Waledpak	Wysyłanie spamu i rozprzestrzenianie złośliwego oprogramowania. Zakończone w wyniku działania firmy Microsoft.
		Maazben	50,000[16]	0.5	Brak	Wysyłanie spamu, złośliwego oprogramowania, oszustw, phishingu.
		OnewordSub	40,000[28]	1.8		
		Gheg	30,000[16]	0.24	Tofsee, Mondera	
		Nucrypt	20,000[28]	5	Loosky, Locksky	
		Wopla	20,000[28]	0.6	Poker, Slogger, Kryptowaluty	
		Asprox	15,000[29]		Danmec, Hydraflux	Ataki phishingowe, wstrzykiwanie kodu SQL, rozprzestrzenianie się złośliwego oprogramowania.
		Spamthru	12,000[28]	0.35	Spam-DComServ, Covesmer, Xmiler	Korzystanie z P2P
	19.7.2012	Grum	560,000[31]	39.9	Tedroo	Wysyłanie głównie spamu farmaceutycznego.
		Gumblar				
2009						
maj 2009 r.	Listopad 2010 r.	BredoLab	30,000,000[30]	3.6	Oficla	Spamowanie. Zakończona dzięki wspólnym działaniom policji holenderskiej, Govcert NL, Europolu. Kasperky Lab itp. **Prawdopodobnie największy znany botnet.**
	Listopad 2009 r.	Mega-D	509,000[32]	10	Ornament	Spamowanie.
sierpień 2009 r.		Festi	250,000[34]	2.25	Spam	Wysyłanie spamu i przeprowadzanie ataków DDoS.
2010						
styczeń 2010 r.		LowSec	11,000+[16]	0.5	LowSecurity, FreeMoney, Ring0.Tools	
		TDL4	4,500,000[35]		TDSS, Alureon	

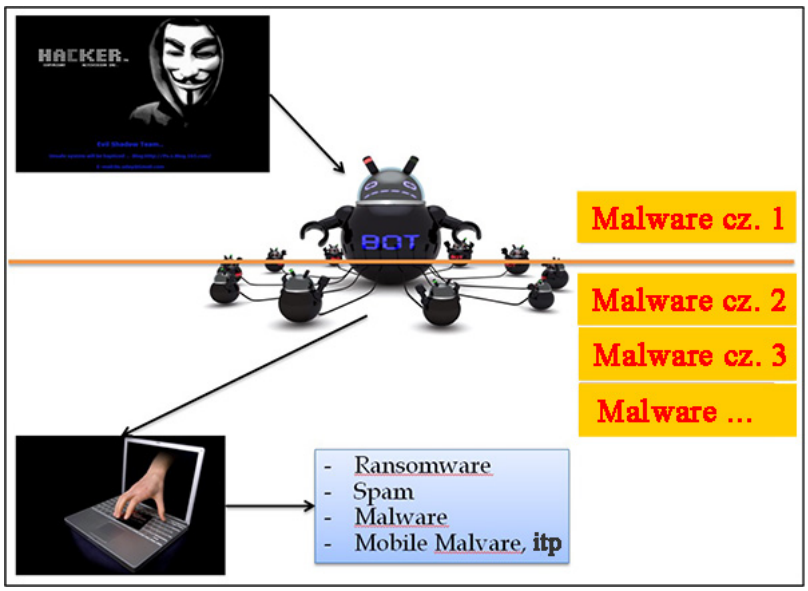
		Zeus	3 600 000 (tylko USA)[36]		Zbot, PRG, Wsnpoem, Gorhax, Kneber	Skupił się na działaniach związanych z kradzieżą informacji o kontach bankowych. Zainstalował również oprogramowanie Cryptolocker Ransomware itp. Aktywny w systemie operacyjnym Windows.
	(kilka: 2011, 2012)	Kelihos	300,000+	4	Hlux	Zajmuje się głównie kradzieżą Bitcoinów i rozsyłaniem spamu.
2011						
	2015-02	Ramnit	3,000,000[37]			Robak atakujący systemy komputerowe z systemem Windows. Zlikwidowany w wyniku wspólnego działania Europolu i firmy Symantec.
		Dostęp zerowy	2,000,000		Max++ Sirefef	Botnet wykorzystywany głównie do wydobywania bitcoinów i oszustw kliknięć. Aktywny w systemie operacyjnym Windows.
2012						
		Kameleon	120,000		Brak	Oszustwo przez kliknięcie
		Nitol				Botnet zajmujący się rozprzestrzenianiem złośliwego oprogramowania i atakami DDoS. Większość zombie (do 85%) znajduje się w Chinach. Klient botnetu został znaleziony w systemach komputerowych dostarczonych bezpośrednio z fabryki.
2013						
		Boatnet	500+ komputerów serwerowych	0.01	YOLOBotnet	
		Zer0n3t	200+ komputerów serwerowych	4	FiberOptck, OptckFiber, Fib3rl0g1c	
2014						
		Semalt	300,000+		Soundfrost	Spamowanie.
		Necurs	6,000,000			
2016						
		Mirai	380,000			DDoS.Wysyłanie spamu.

		Methbot	6 000 domen i 250 267 różnych adresów URL			
2018						
		3ve	1,7 mln komputerów i duża liczba serwerów			Kradzież pieniędzy.

De facto każdy system komputerowy może zostać podłączony do botnetu. Dotyczy to między innymi systemów, które spełniają warunki IoT (Internet of Things). W 2014 r. zgłoszono przypadek, w którym lodówka była częścią botnetu, który rozesłał ponad 750 000 wiadomości spamowych. [9]

Z badania Nigama wynika[10] , że istnieją dziesiątki botnetów stworzonych bezpośrednio i ukierunkowanych przede wszystkim na systemy komputerowe, które można określić jako urządzenia mobilne (np. smartfon, tablet itp.). Instalowanie aplikacji z nieznanych źródeł oraz znaczny brak produktów antywirusowych na urządzeniach mobilnych użytkowników znacznie ułatwia również instalowanie na nich złośliwego oprogramowania, a tym samym przejmowanie nad nimi kontroli. Urządzenia te są obecnie w stanie w pełni sprostać wymaganiom botmastera w zakresie prowadzenia botnetu lub zadań stawianych "zombie".

Nie tylko w przypadku botnetów złośliwe oprogramowanie służy do uzyskiwania dostępu, kontrolowania i dalszego rozprzestrzeniania złośliwego oprogramowania lub wykonywania innych zadań zgodnie z instrukcjami atakującego, jednak jeśli system komputerowy użytkownika jest obecnie zainfekowany złośliwym oprogramowaniem, istnieje duże prawdopodobieństwo, że stał się on również częścią botnetu. Atakujący (botmaster) instaluje na systemie komputerowym (zombie) złośliwe oprogramowanie, które pozwala mu na zdalne manipulowanie systemem komputerowym (Malware #1 - przy czym to złośliwe oprogramowanie pozostawia kontrolę botmasterowi nawet wtedy, gdy np. część lub całość botnetu jest wynajęta). Dopiero potem instalowane jest kolejne złośliwe oprogramowanie (od Malware **2** do Malware ∞), które wykonuje inne zadania (np. spamowanie, zbieranie danych, oprogramowanie ransomware itd.) Całą tę strukturę można przedstawić w następujący sposób:



Złośliwe oprogramowanie zainstalowane na systemie komputerowym podłączonym do botnetu

Z prawnego punktu widzenia botnety to całe sieci zainfekowanych systemów komputerowych, nad którymi osoba trzecia przejęła do pewnego stopnia nieuprawnioną kontrolę bez wiedzy uprawnionych użytkowników. Takie zainfekowane systemy najczęściej służą atakującemu jako baza do anonimowego łączenia się z Internetem, wysyłania złośliwych programów, przeprowadzania ataków na inne cele, przeprowadzania ataków DoS, rozsyłania spamu, kradzieży tożsamości lub przeprowadzania innych ataków cybernetycznych.

Możliwości stosowania sankcji karnych w Republice Czeskiej

Jeśli chodzi o faktyczne działanie osoby atakującej, polegające na zainstalowaniu złośliwego oprogramowania w celu późniejszego przejęcia kontroli nad systemem komputerowym, można je oceniać na podstawie **paragrafu 230** Kodeksu karnego (Nieuprawniony dostęp do systemu komputerowego i nośnika informacji). Jeśli atakujący wprowadzi złośliwe oprogramowanie do systemu komputerowego z zamiarem wyrządzenia szkody lub innej krzywdy innej osobie lub uzyskania nieuzasadnionej korzyści dla siebie lub innej osoby, jego zachowanie można zakwalifikować z paragrafu 230(2)(d) kodeksu karnego.

Można argumentować, że stanowi to również nieuprawnione korzystanie z cudzej własności (ponieważ system komputerowy, o którym mowa w tych przypadkach, jest cudzą własnością) zgodnie z **art. 207 ust. 1 pkt 1** kodeksu karnego. Zastosowanie paragrafu 207(1) lub (2) kodeksu karnego[11] może być bardzo problematyczne, ponieważ decydujące znaczenie ma intensywność ingerencji i sposób wykorzystania systemu komputerowego. Na podstawie takiego poziomu intensywności możliwe byłoby ilościowe określenie poniesionej szkody jako wyrazu amortyzacji w okresie użytkowania. Niestety, stosując takie wyliczenie, można stwierdzić, że wyrządzone szkody są na ogół niemałe.

Rzeczywista ochrona przed połączeniem i korzystaniem z komputerów w ramach botnetu może być dwojaka. Na pierwszym poziomie ochrona praw własności mogłaby zostać zwiększona poprzez dodanie do paragrafu 207 kodeksu karnego faktu podstawowego o następującym brzmieniu: "***Kto korzysta z systemu komputerowego bez zgody osoby uprawnionej".***

Przepis ten definiowałby również okoliczność, która polega na naruszeniu prawa własności innej osoby. W przypadku nieuprawnionego korzystania z cudzej własności w odniesieniu do systemu komputerowego rozwiązaniem nie jest zmniejszenie szkody z niewielkiej do nieznacznej (zob. § 207 ust. 1 pkt 1 kodeksu karnego), ponieważ cena wielu systemów komputerowych jest obecnie niższa niż nawet wartość nieznaczna (tj. co najmniej 5 000 CZK), a mimo to te systemy komputerowe są w stanie w pełni wykonywać przypisane im działania w ramach botnetu.

Drugi poziom, opisujący powagę zachowania napastnika, polega na wprowadzeniu nowej okoliczności kwalifikującej do paragrafu 230(3) Kodeksu karnego, która może mieć następujące brzmienie:

"umyślnie podłącza system komputerowy do sieci komputerowej z zamiarem popełnienia przestępstwa lub używa go w tej sieci z takim samym zamiarem,"

Możliwości ścigania karnego w Polsce

Nielegalny dostęp do systemu (hacking) - art. 267 § 1 i 2 Kodeksu karnego. Przestępstwo to jest ścigane na wniosek pokrzywdzonego. Jest zagrożone karą grzywny, ograniczenia wolności lub pozbawienia wolności do 2 lat.

Artykuł 267. Bezprawne uzyskanie informacji

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonych, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając jej elektroniczne, magnetyczne, komputerowe lub inne specjalne zabezpieczenia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega każdy, kto bez upoważnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do których nie jest uprawniony, zakłada lub wykorzystuje urządzenie podsłuchowe, wizualne lub inne urządzenie albo oprogramowanie.

§ 4. Tej samej karze podlega, kto ujawnia innej osobie informacje uzyskane w sposób określony w § 1 do 3.

§ 5 Ściganie przestępstwa określonego w § 1-4 odbywa się na wniosek pokrzywdzonego.

---

[1] **Bot** (skrót od robot). Jest to program, który może wykonywać polecenia wydane przez napastnika z innego systemu komputerowego. Najczęściej jest to infekcja komputera przez wirusy, takie jak robak, koń trojański itp. System komputerowy, który jest w ten sposób zdalnie kontrolowany, jest określany mianem **zombie.** W niektórych źródłach zainfekowany system komputerowy określa się jednak również mianem bota.

Bot może zbierać dane, przetwarzać żądania, wysyłać wiadomości, komunikować się z kontrolerem itp.

[2] Więcej informacji można znaleźć w rozdziale *Obliczenia rozproszone.* [online]. [cyt. 2.11.2013]. Dostępny pod adresem: http://dc.czechnationalteam.cz/

[3] Więcej szczegółów w PLOHMANN, Daniel, Elmar GERHARDS-PADILLA i Felix LEDER. *Botnety: wykrywanie, pomiar, dezynfekcja i obrona.* ENISA, 2011 [online]. [cytowany 17 maja 2015], s. 14. Dostępny w: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence.

Dalsze definicje botnetów i informacje na ich temat można znaleźć np. na stronie:

Co to jest botnet i jak się rozprzestrzenia? [online]. [cit.15.7.2016]. Dostępny pod adresem:

Botnety: nowe zagrożenie w Internecie. [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://www.lupa.cz/clanky/botnety-internetova-hrozba/

Wojny botnetów - jak działają botnety. [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://tmp.testnet-8.net/docs/h9_botnet.pdf

Botnety. [online]. [cyt. 2016-07-15]. Dostępny pod adresem: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6

[4] Obraz scentralizowanego botnetu. Więcej szczegółów w PLOHMANN, Daniel, Elmar GERHARDS-PADILLA i Felix LEDER. *Botnety: wykrywanie, pomiar, dezynfekcja i obrona.* ENISA, 2011 [online]. [cytowany 17 maja 2015], s. 16. Dostępny w: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence.

[5] Obraz zdecentralizowanego botnetu. Tamże, s. 18.

[6] Gospodarka złośliwego oprogramowania. Więcej szczegółów w PLOHMANN, Daniel, Elmar GERHARDS-PADILLA i Felix LEDER. *Botnety: wykrywanie, pomiar, dezynfekcja i obrona.* ENISA, 2011 [online]. [cytowany 17 maja 2015], s. 21. Dostępny w: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence.

[7] *Boty i botnety - rosnące zagrożenie.* [online]. [cyt. 11.8.2016]. Dostępny pod adresem: https://us.norton.com/botnet/

[8] Tabela została opracowana na podstawie informacji pochodzących z następujących źródeł:

Botnet. [online]. [cyt. 2016-07-15]. Dostępne od: https://en.wikipedia.org/wiki/Botnet

Botnet - historyczna lista botnetów. [online]. [cyt. 2016-08-15]. Dostępny pod adresem: http://www.liquisearch.com/botnet/historical_list_of_botnets

Botnet. [cyt. 8.7.2016]. Dostępny pod adresem: http://research.omicsgroup.org/index.php/Botnet

Historyczna lista botnetów. [online]. [cyt. 2016-08-15]. Dostępny pod adresem: http://jpdias.me/botnet-lab//history/historical-list-of-botnets.html

[9] *Lodówka przyłapana na wysyłaniu spamu w ramach ataku botnetowego.* [online]. [cyt. 2016 maj 17]. Dostępny pod adresem: http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

[10] Więcej informacji na ten temat można znaleźć w publikacji NIGAM, Ruchna. *Oś czasu botnetów mobilnych.* [online]. [cyt. 12.7.2016]. Dostępny pod adresem: https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf ;

[11] Przepis ten przewiduje wyrządzenie szkody w mieniu innych osób, przy czym szkoda nie może być mała (tj. co najmniej 25 000 CZK, patrz paragraf 138 ust. 1 kodeksu karnego).

4.3. Złośliwe oprogramowanie

Złośliwe oprogramowanie (połączenie angielskich słów malicious software) to dowolne oprogramowanie używane do zakłócania standardowego działania systemu komputerowego, zdobywania informacji (danych) lub uzyskiwania dostępu do systemu komputerowego. Złośliwe oprogramowanie może przybierać różne formy, a wiele jego typów jest nazywanych zgodnie z wykonywanymi przez nie czynnościami.

Jedno złośliwe oprogramowanie jest w stanie wykonywać kilka funkcji (wykonywać kilka czynności) jednocześnie. Na przykład, może rozprzestrzeniać się za pośrednictwem poczty elektronicznej (jako załącznik) lub jako dane w sieciach P2P, jednocześnie pozyskując np. adresy e-mail ze skompromitowanego systemu komputerowego.

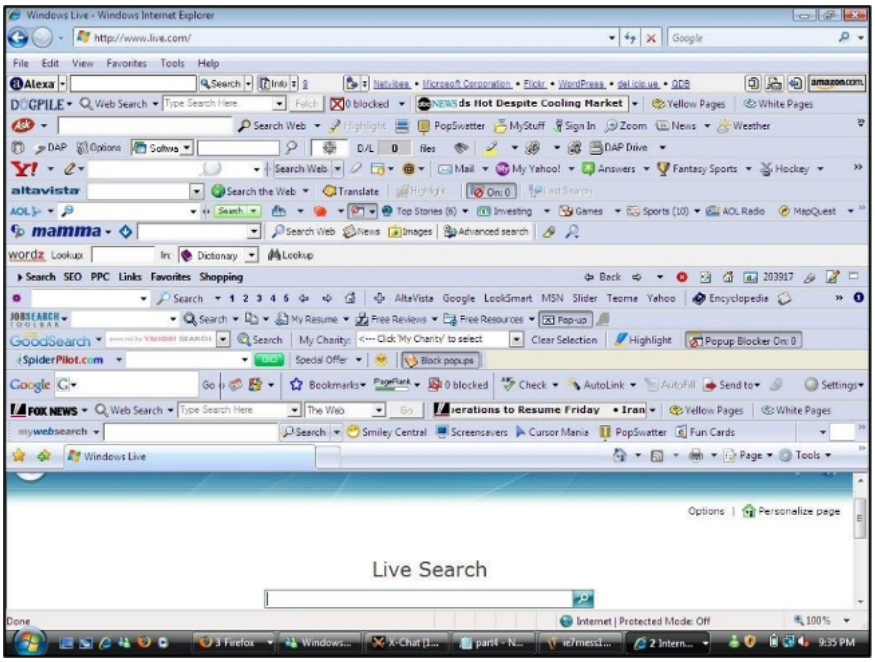
W przeszłości istniało wiele różnych terminów określających oprogramowanie, które obecnie określa się wspólnym mianem złośliwego oprogramowania. Nazwy konkretnych złośliwych programów były zazwyczaj oparte na czynnościach, które wykonywał dany program. Pomimo stwierdzenia, że złośliwe oprogramowanie jest podstawowym terminem używanym obecnie, nadal można spotkać się z historycznie starszymi określeniami złośliwego oprogramowania. Są to następujące grupy:

1. **Adware**
2. **Oprogramowanie szpiegujące**
3. **Wirusy**
4. **Robaki (Worms)**
5. **Konie trojańskie**
6. **Backdoor**
7. **Rootkity**
8. **Keylogger**
9. **Również oprogramowanie typu ransomware.**[1]

Ad 1) Adware

Termin adware jest skrótem od angielskiego wyrażenia "advertising *supported software*", które można luźno przetłumaczyć na język czeski jako oprogramowanie wspierające *reklamy. Jest to* najmniej niebezpieczna, ale zyskowna forma złośliwego oprogramowania.[2] Adware wyświetla reklamy w systemie komputerowym użytkownika (np. okna pop-up w systemie operacyjnym[3] lub na stronach internetowych, reklamy wyświetlane razem z oprogramowaniem itp.) Chociaż w większości przypadków są to produkty, które jedynie denerwują użytkownika ciągłymi komunikatami reklamowymi wyskakującymi na ekranie, oprogramowanie adware może być również powiązane z oprogramowaniem szpiegującym, którego celem jest śledzenie aktywności użytkownika i wykradanie ważnych informacji.

Adware



Przykładowe programy typu adware i inne dodatki instalowane w przeglądarce internetowej [4]

Ad 2) Oprogramowanie szpiegujące

Termin "spyware" jest złożeniem angielskich słów "*spy*" i "*software*". Oprogramowanie szpiegowskie służy do pozyskiwania danych statystycznych[5] o działaniu systemu komputerowego i wysyłania ich do skrzynki pocztowej napastnika bez wiedzy i zgody użytkownika. Dane te mogą obejmować dane osobowe lub informacje o osobowości użytkownika, informacje o odwiedzonych witrynach internetowych, uruchomionych aplikacjach itp.

Oprogramowanie szpiegujące może być instalowane jako samodzielne złośliwe oprogramowanie, ale często jest też częścią innych, swobodnie dystrybuowanych i całkowicie bezpiecznych programów. W takim przypadku instalacja i inne działania oprogramowania szpiegującego są zazwyczaj objęte umową EULA, a użytkownik zazwyczaj nieświadomie dobrowolnie zgadza się na monitorowanie swoich działań. Dołączanie programów szpiegujących do innych programów (np. programów klienckich sieci P2P, różnych programów typu shareware itp.) jest często motywowane chęcią poznania zainteresowań lub potrzeb użytkownika przez producenta programu i wykorzystania tych informacji, np. do reklamy ukierunkowanej.[6] Cechą charakterystyczną programów szpiegujących, które są częścią "programu dołączonego", jest również to, że zazwyczaj pozostają one zainstalowane na komputerze nawet po odinstalowaniu głównego programu, co w większości przypadków jest ukryte przed użytkownikiem.

Oprogramowanie szpiegowskie stanowi zagrożenie zarówno dlatego, że przesyła różne informacje z systemu komputerowego użytkownika do "atakującego" (przy czym informacje te są dalej przetwarzane i korelowane z danymi i informacjami uzyskanymi z innych źródeł), jak i dlatego, że oprogramowanie szpiegowskie może zawierać inne narzędzia, które wpływają na działania samego użytkownika.[7] .

Ad 3) Wirusy

Jest to program lub złośliwy kod, który dołącza się do innego istniejącego pliku wykonywalnego (np. oprogramowania itp.) lub dokumentu. Wirus rozmnaża się w momencie uruchomienia programu lub otwarcia zainfekowanego dokumentu. Wirusy rozprzestrzeniają się najczęściej poprzez współdzielenie oprogramowania między systemami komputerowymi; do ich rozprzestrzeniania się nie jest potrzebna interakcja ze strony użytkownika. Wirusy stanowiły dominującą formę szkodliwego oprogramowania, zwłaszcza w latach 80. i 90. ubiegłego wieku. [8]

Istnieje wiele wirusów, których celem jest niszczenie, podczas gdy inne są zaprojektowane tak, aby "zadomowić się" w jak największej liczbie systemów komputerowych, a następnie wykorzystać je do przeprowadzenia ukierunkowanego ataku. Typową cechą tych programów jest zdolność do rozprzestrzeniania się między systemami bez konieczności interwencji użytkownika systemu komputerowego. Objawy działania wirusów mogą być różne - od niegroźnej melodyjki, przez przeciążenie systemu, zmianę lub zniszczenie danych, aż po całkowite zniszczenie zainfekowanego systemu. Wirusy komputerowe można klasyfikować według wielu różnych kryteriów, np. według gospodarza (czyli rodzaju programów, które przenoszą wirusy komputerowe), według sposobu, w jaki manifestują się w systemie, według ich lokalizacji w pamięci itd.[9] Wirusy, w zależności od infekowanych przez nie plików, można podzielić na:

- wirusy rozruchowe (infekują tylko obszary systemowe)
- wirusy plikowe (infekują tylko pliki)
- wirusy wieloczęściowe (infekują pliki i obszary systemowe)
- makrowirusy (atakują aplikacje wykorzystujące makra)

Ad 4) Robaki

Robaki **komputerowe** są również znane jako wirusy. Powodem bliższego skojarzenia z wirusami jest to, że robaki nie potrzebują żadnego gospodarza, czyli pliku wykonywalnego (podobnie jak wirusy). Zazwyczaj rozprzestrzeniają się samodzielnie, w przeciwieństwie do wirusów, które są zwykle dołączane jako część innego programu. Zainfekowany system jest następnie wykorzystywany przez robaka do wysyłania swoich kopii do innych użytkowników za pośrednictwem komunikacji sieciowej.[10] W ten sposób bardzo szybko się rozprzestrzenia, co może doprowadzić do przeciążenia sieci komputerowej, a tym samym całej infrastruktury. W przeciwieństwie do wirusów, programy te są w stanie analizować słabe punkty zabezpieczeń w zaatakowanym systemie informatycznym,[11] . Dlatego też są one również wykorzystywane do wyszukiwania luk w zabezpieczeniach systemów lub programów pocztowych. [12]

Ad 5, 6) Konie trojańskie i backdoory

Konie trojańskie są ogólnie definiowane jako programy komputerowe zawierające ukryte funkcje, których użytkownik nie zgadza się używać lub których nie jest świadomy, a które są potencjalnie niebezpieczne dla dalszego funkcjonowania systemu. Podobnie jak w przypadku wirusów, programy te mogą być dołączone do innego, bezpiecznego programu lub aplikacji albo mogą sprawiać wrażenie nieszkodliwych programów komputerowych. Trojany, w przeciwieństwie do tradycyjnych wirusów, nie są w stanie replikować się ani rozprzestrzeniać bez "pomocy" użytkownika. Jeśli trojan zostanie aktywowany, może zostać użyty do usuwania, blokowania, modyfikowania, kopiowania danych lub na przykład zakłócania działania systemu komputerowego lub sieci komputerowych.

Niektóre konie trojańskie po aktywacji otwierają porty komunikacyjne komputera bez wiedzy użytkownika, co znacznie ułatwia dalsze infekcje zainfekowanego systemu przez inne złośliwe programy lub ułatwia bezpośrednie zdalne sterowanie zainfekowanym komputerem. Takie trojany są określane mianem backdoorów.[13] Nowoczesne programy typu backdoor mają ulepszoną komunikację i zazwyczaj wykorzystują protokoły niektórych narzędzi komunikacyjnych, np. programu ICQ.[14]

Wykorzystanie koni trojańskich jest często związane z używaniem różnych **programów skanujących** (lub *skanerów portów*)[15] , czyli programów służących głównie do określania, które porty sieci komunikacyjnej komputera są otwarte, jakie usługi są na nich uruchomione i czy możliwe jest przeprowadzenie za ich pośrednictwem ataku na taki system. Dane te są ponownie przesyłane do osoby atakującej i potencjalnie wykorzystywane do dalszych ataków cybernetycznych.

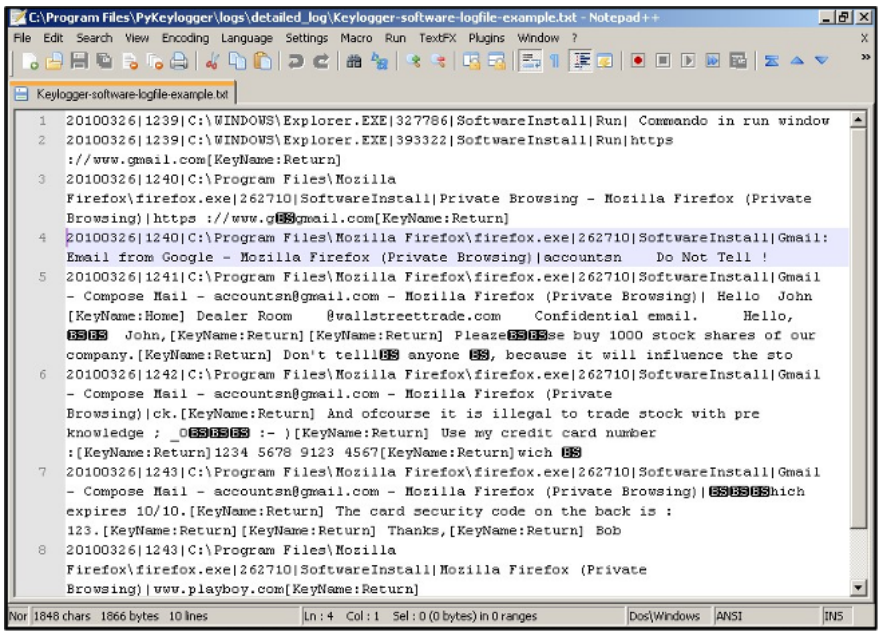
Ad 7) Rootkity

Termin ten odnosi się nie tylko do programów komputerowych, ale także do całej technologii wykorzystywanej do ukrywania obecności złośliwego oprogramowania (np. wirusów komputerowych, koni trojańskich, robaków itp.) w zainfekowanym systemie. Najczęściej mają one postać niezbyt rozbudowanych programów komputerowych. Rootkity same w sobie nie są złośliwe, ale są wykorzystywane przez twórców złośliwych programów, takich jak wirusy, oprogramowanie szpiegujące itp.[16] Program typu rootkit zmienia zachowanie całego systemu operacyjnego, jego części lub aplikacji nadrzędnych w taki sposób, że użytkownik nie jest świadomy istnienia niebezpiecznych programów w swoim systemie komputerowym. Ogólnie rzecz biorąc, programy typu rootkit można podzielić na programy **systemowe** (modyfikujące jądro systemu) oraz **programy użytkowe** (modyfikujące konfigurację **aplikacji).**[17]

Wśród aplikacji rootkity atakują głównie programy specjalistyczne służące do wyszukiwania i usuwania niebezpiecznych programów z systemu, np. programy antywirusowe itp.[18] Programy antywirusowe nie są w stanie usunąć złośliwego programu z zainfekowanego systemu, gdy używany jest program typu rootkit. W ten sposób obecność szkodliwego programu w zainfekowanym systemie jest przedłużana. Z tego punktu widzenia można stwierdzić, że programy typu rootkit mogą być bardzo łatwo wykorzystywane do popełniania przestępstw związanych z używaniem lub niewłaściwym używaniem technologii informatycznych.[19] W niektórych publikacjach narzędzia te określane są jako podzbiór trojanów typu backdoor.[20]

Ad 8) Keylogger (Keystroke Logger**)**

Keylogger to oprogramowanie, które rejestruje poszczególne naciśnięcia klawiszy w zaatakowanym systemie komputerowym. Najczęściej keylogger jest używany do rejestrowania danych logowania (nazwa użytkownika i hasło) do kont, do których dostęp jest uzyskiwany z systemu komputerowego. Uzyskane informacje są następnie zazwyczaj przesyłane do osoby atakującej.



Demonstracja keyloggera[21]

Ad 9) Ransomware

Oprogramowanie ransomware zostanie opisane bardziej szczegółowo w osobnym rozdziale.

Dystrybucja złośliwego oprogramowania

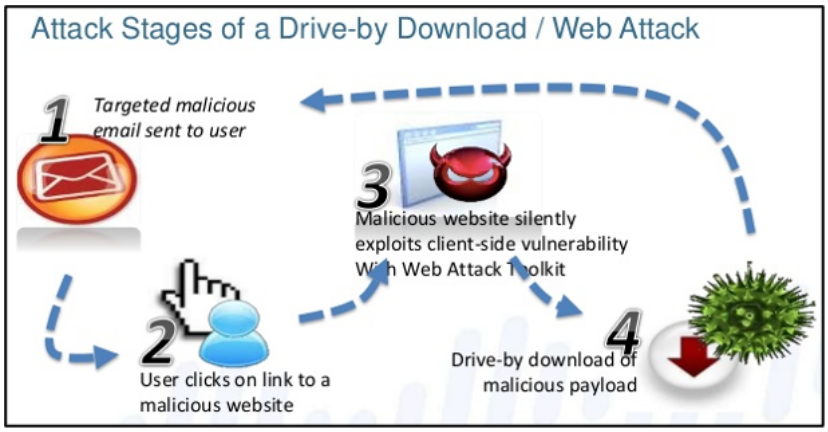
Złośliwe oprogramowanie może zostać dostarczone do docelowego systemu komputerowego na wiele sposobów. W tym miejscu wymienię pokrótce niektóre z metod dystrybucji złośliwego oprogramowania. Złośliwe oprogramowanie może być rozpowszechniane za pośrednictwem:

- **Przenośne nośniki pamięci**

Na przykład przy użyciu płyty CD, DVD, USB, dysku zewnętrznego itp. Jest to najstarszy, ale nadal skuteczny sposób rozprzestrzeniania złośliwego oprogramowania, w którym użytkownicy przesyłają sobie nawzajem zainfekowane pliki **lub do sieci komputerowych** zawierających **zainfekowane** pliki (udostępnianie takich plików w sieciach komputerowych, zazwyczaj sieciach P2P).

- **Drive-by-download**

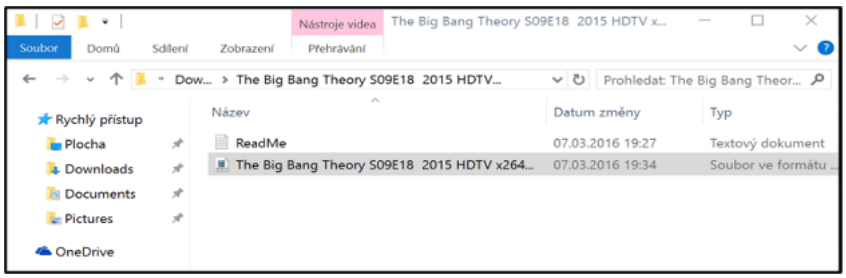
Jednym z najczęstszych sposobów infekowania złośliwym oprogramowaniem jest pobieranie go z Internetu, a następnie uruchamianie pliku, zwykle z rozszerzeniem . exe (plik wykonywalny), pochodzącego z nieznanego źródła. Mogą to być fałszywe lub podrobione programy (np. podróbki Flapp Bird, fałszywe kodeki multimedialne itd.), programy używane do obchodzenia praw autorskich (cracki, keygeny itd.), prawdziwie zainfekowane programy itd.

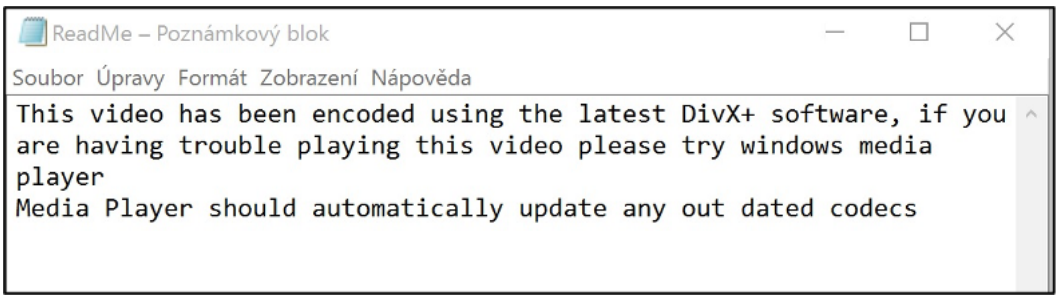


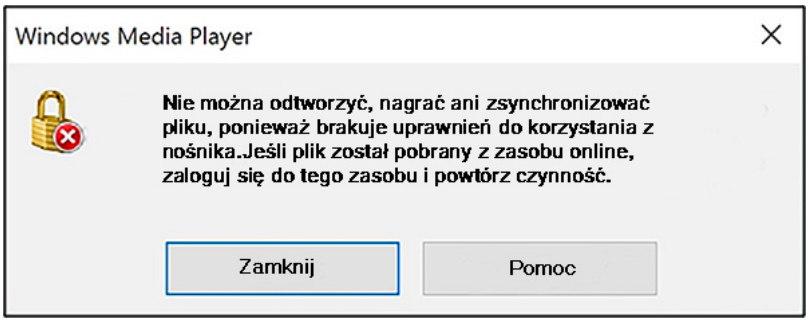
Przedstawienie jednej z możliwych zasad działania napędu przez pobieranie.[22]

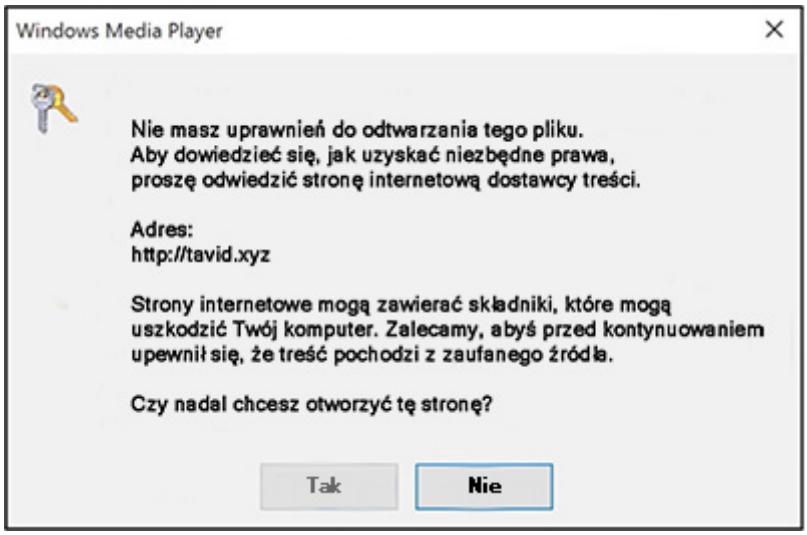
Poniższy przykład przedstawia złośliwe oprogramowanie pobrane przez użytkownika za pośrednictwem sieci P2P (w szczególności plik zawierający odcinek serialu *The Big Bang Theory - sezon 9, odcinek 18*). To złośliwe oprogramowanie nakłaniało użytkownika do pobrania nowego kodeka za pośrednictwem programu Media Player w celu odtworzenia filmu. Odtwarzacz multimedialny nawiązywał połączenie ze stroną atakującego, a następnie fikcyjnie instalował kodek, jednak w rzeczywistości na komputerze instalowane było złośliwe oprogramowanie (w tym przypadku kombinacja złośliwych programów: backdoor, keylogger, bot), które umożliwiało atakującemu przejęcie całkowitej kontroli nad systemem komputerowym użytkownika.

W tym przypadku uderzający był również fakt, że odcinek serialu *The Big Bang Theory* nie został jeszcze wyemitowany w Stanach Zjednoczonych, gdzie miał swoją premierę, a mimo to odnotował dziesiątki tysięcy pobrań.









- **"Dokumenty biurowe"**

Bardzo często złośliwe oprogramowanie jest rozprzestrzeniane w postaci plików, takich jak np: .doc, . xls, . avi itd. W ten sposób mogą być rozpowszechniane tylko makrowirusy. Użytkownik zakłada, że otwiera dokument Worda, ale jednocześnie wykonuje plik wykonywalny, który podszywa się pod ten dokument.

- e-mail

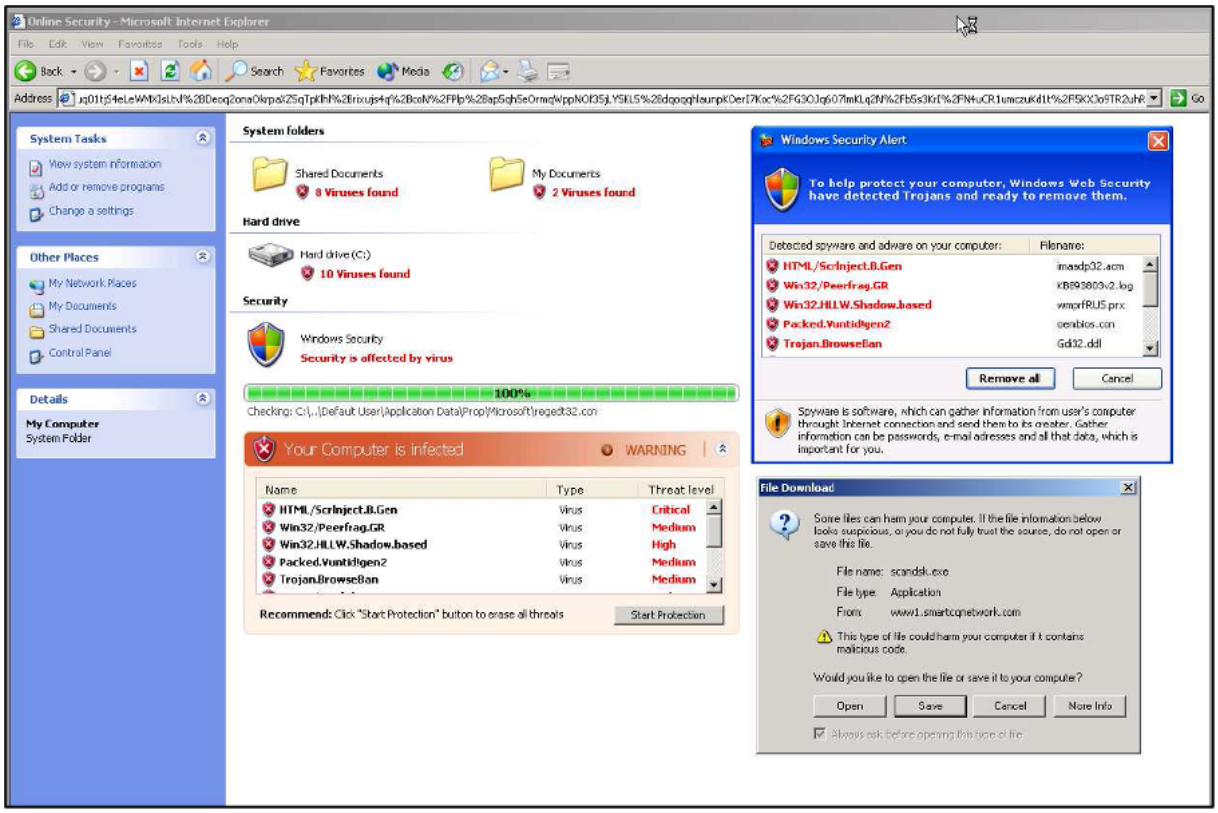
Złośliwe oprogramowanie może być przechowywane w załączniku do wiadomości lub w postaci skryptów w treści wiadomości e-mail w formacie HTML[23] . Jest to obecnie jeden z najczęstszych sposobów rozprzestrzeniania złośliwego oprogramowania. Przykłady obejmują aktualne kampanie phishingowe, hakerskie, spam itp.

- HTML

Złośliwe oprogramowanie może być umieszczane bezpośrednio na stronie internetowej lub w poszczególnych skryptach.

- **Fałszywy antywirus**

Użytkownikowi zwykle oferuje się darmowy program antywirusowy, podobny do oprogramowania typu adware. Ten program antywirusowy "testuje komputer" i wykrywa poważne luki w zabezpieczeniach oraz złośliwe oprogramowanie, które nie zostało wykryte przez program antywirusowy użytkownika. Fałszywy program antywirusowy łączy w sobie atak socjotechniczny (wzbudzający strach przed złośliwym oprogramowaniem) z instalacją złośliwego oprogramowania zawartego w fałszywym programie antywirusowym.



Fałszywy antywirus

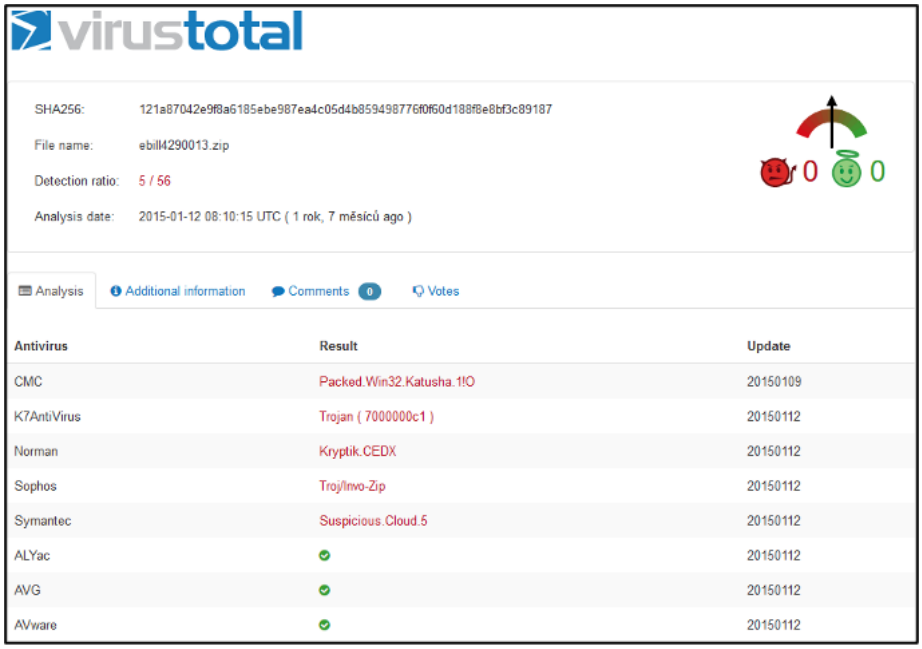
Fałszywy antywirus[24]

Jeśli użytkownik nie jest pewien, czy dany plik lub witryna zawiera złośliwe oprogramowanie, może skorzysta z wielu narzędzi pomocnych w sprawdzeniu, czy nie zawiera ono złośliwego oprogramowania.

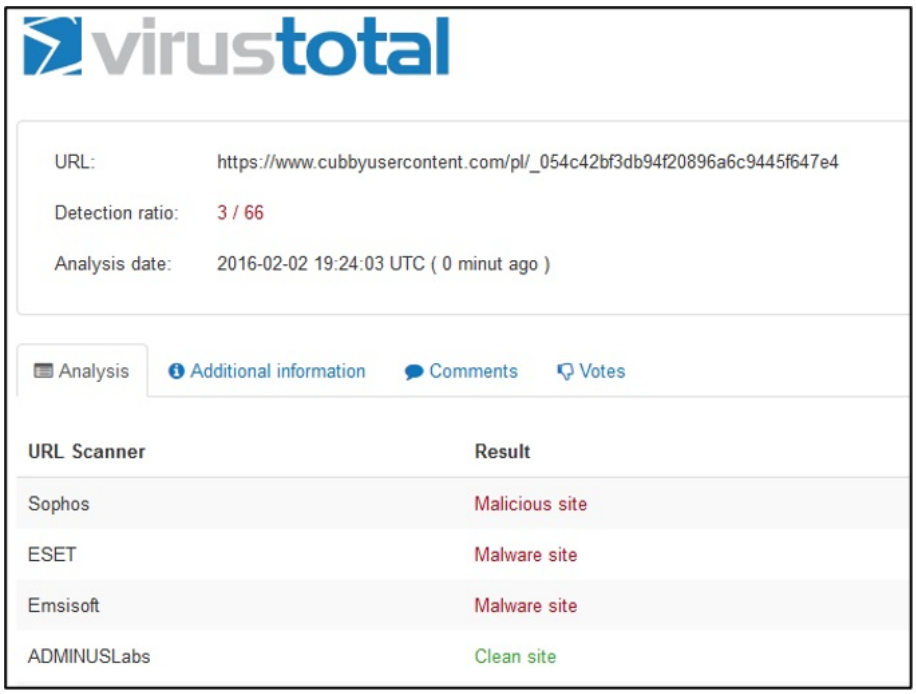
Jedną ze sprawdzonych usług jest **https://www.virustotal.com/** . Na tej stronie użytkownik może przeskanować plik o rozmiarze do 128 MB lub stronę internetową, do której ma zamiar wejść (zaleca się przeprowadzenie takiego skanowania podczas odwiedzania np. stron bankowości internetowej lub stron z płatnościami). Virustotal łączy firmy zajmujące się cyberbezpieczeństwem, tworzeniem programów antywirusowych itp., a zapytanie użytkownika jest skanowane przez narzędzia wszystkich tych firm, co zwiększa prawdopodobieństwo wykrycia złośliwego oprogramowania.

Poniższy ekran wydruku przedstawia wynik skanowania nowo dostarczonego pliku w ramach kampanii phishingowej. Dzień po rozpoczęciu kampanii tylko 5 firm zidentyfikowało złośliwe oprogramowanie w załączonym pliku, a w ciągu tygodnia wszystkie pozostałe firmy były w stanie je zidentyfikować. Jednak to właśnie czas między dostarczeniem aktualizacji do programów antywirusowych użytkowników w ich systemach komputerowych a

rozpoczęciem ataku ma decydujące znaczenie dla ostatecznego sukcesu atakującego.



Wynik badania pliku



Wynik badania strony internetowej

Złośliwe oprogramowanie można zainstalować na prawie każdym systemie komputerowym. Przykłady specyficznych instalacji obejmują przypadki **instalacji oprogramowania mikroprogramowego.** Jest to złośliwy kod, który jest rozpowszechniany na stosunkowo niewielkiej liczbie systemów komputerowych. Kod ten wykazuje nietypowe zachowanie, a programy zabezpieczające często nie reagują na niego. Najbardziej znanym przypadkiem micromalware jest **robak STUXNET**.[25] , czyli instalacja klienta botnetu we wspomnianej wcześniej lodówce.

Mobilne złośliwe oprogramowanie jest przedmiotem osobnego rozdziału. Pierwsze złośliwe oprogramowanie przeznaczone do atakowania telefonów komórkowych zostało odkryte około 2004 roku. Obecnie firma Kaspersky Lab, która poinformowała o tym odkryciu, podaje, że istnieje ponad **340 000 szkodliwych programów.**[26]

Jeżeli skupimy się na najbardziej zagrożonym systemie operacyjnym w urządzeniach mobilnych, to większość zagrożeń jest skierowana na system operacyjny Android. Wynika to głównie z różnorodności używanych wersji systemów operacyjnych i ich przestarzałości. **Większość urządzeń z systemem Android nie pozwala na aktualizację systemu operacyjnego do najnowszej wersji, która zazwyczaj jest zmodyfikowana w taki sposób, aby była odporna na znane luki w zabezpieczeniach i zawierała już poprawki do luk z poprzednich wersji systemu.** [27] **Szacuje się jednak, że 77% zagrożeń atakujących system operacyjny Android można wyeliminować, używając najnowszej wersji systemu operacyjnego.**

W przypadku urządzeń mobilnych napastnicy wykorzystują głównie:

- **Nieaktualna wersja systemu operacyjnego urządzenia mobilnego** (znane luki w zabezpieczeniach każdego systemu);
- **Minimalne zabezpieczenie urządzenia mobilnego** za pomocą agenta antywirusowego;

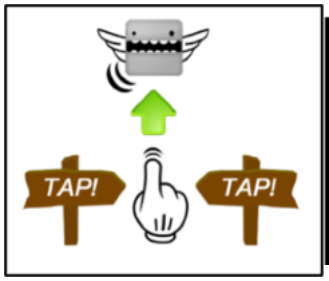
- **Niewiedza użytkownika** (wielu użytkowników bezmyślnie instaluje aplikacje "z nieznanego źródła" lub takie, które wymagają nadmiernego dostępu i uprawnień w urządzeniu).

- **Inżynieria społeczna i "fale zainteresowania" aplikacjami określonego typu.**

Jednym z powodów, dla których Android jest atakowany jako podstawowy system operacyjny, jest fakt, że kanał dystrybucji (Google Play) nie weryfikuje bezpieczeństwa aplikacji (ani tego, czy dana aplikacja zawiera np. złośliwe oprogramowanie), jak ma to miejsce w przypadku systemu operacyjnego iOS i jego kanału dystrybucji (App Store)**.**

Przykładem tego jest aplikacja **Flappy Bird** i jej "klony". Ta aplikacja została stworzona przez Nguyễn Hà Đông i została wydana dla systemu iOS 24 maja 2013 r. Dla systemu operacyjnego Android aplikacja ta została udostępniona w 2014 roku i stała się najczęściej pobieraną darmową grą w styczniu 2014 roku. Twórca usunął grę z rynku 10 lutego 2014 r. Gra została pobrana ponad 50 milionów razy.

Kiedy na rynku pojawił się oryginalny Flappy Bird, zaczęły pojawiać się różne klony tej gry na Androida, z których wiele tylko skapitalizowało sukces oryginału. Szacuje się, że nawet 79% klonów gry zostało zainfekowanych złośliwym oprogramowaniem.[28] Przykładami zakażonych klonów są:



Zainfekowanie telefonu komórkowego może być jednym z głównych celów atakującego, ponieważ urządzenia te są obecnie zazwyczaj wykorzystywane do uwierzytelniania dwuskładnikowego w bankowości internetowej lub podczas zakupów. Atakujący próbują wykorzystać uzyskane informacje, na przykład w celu wyprowadzenia środków finansowych poprzez bezpośredni dostęp do konta bankowego użytkownika za pośrednictwem bankowości internetowej lub w celu uzyskania poufnych informacji.

Możliwości stosowania sankcji karnych w Republice Czeskiej

W Republice Czeskiej atak za pomocą złośliwego oprogramowania można karać na podstawie paragrafu **230** (Nieuprawniony dostęp do systemu komputerowego i nośnika informacji) kodeksu karnego. **Posiadanie złośliwego oprogramowania, z zamiarem popełnienia przestępstwa z Artykułu** 182 (Naruszenie tajemnicy przesyłanych wiadomości) lub przestępstwa z **Artykułu** 230 Kodeksu karnego, **jest karalne na mocy Artykułu 231** (Posiadanie i dysponowanie urządzeniem dostępowym i hasłem do systemu komputerowego i innych tego typu danych) Kodeksu karnego. Jeżeli **celem wirusa** było na przykład uzyskanie informacji niejawnych lub wsparcie grupy terrorystycznej, atakujący mógł na przykład popełnić przestępstwa z **§ 311** (Atak terrorystyczny), **§ 316 (**Szpiegostwo) lub **§ 317** (Narażenie na niebezpieczeństwo informacji niejawnych) **na etapie przygotowywania** TZK.

Możliwości ścigania karnego w Polsce

Naruszenie integralności danych (wirusy, trojany), 268 Kodeksu karnego, art. 268a Kodeksu karnego Przestępstwo to dotyczy m.in. kradzieży danych osobowych, udostępniania ich osobom trzecim bez zgody właściciela, a także wykorzystywania ich w sposób nieuprawniony. Za popełnienie tych czynów grożą sankcje finansowe (do 100 000 PLN).

Artykuł 268. Utrudnianie osobie upoważnionej dostępu do informacji

§ 1. Kto, nie będąc do tego upoważnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnych informacji albo w inny sposób uniemożliwia lub znacznie utrudnia osobie upoważnionej zapoznanie się z nimi, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn, o którym mowa w § 1, dotyczy zapisu na informatycznym nośniku danych, sprawca jest obowiązany
podlega karze pozbawienia wolności na czas nie dłuższy niż 3 lata.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Artykuł 268a. Niszczenie, uszkadzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych komputerowych

§ 1. Kto bez upoważnienia niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych komputerowych albo w istotny sposób zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych,
podlega karze pozbawienia wolności na okres do 3 lat.

§ 2. Kto, popełniając czyn, o którym mowa w § 1, wyrządza znaczną szkodę majątkową,
podlega karze pozbawienia wolności od 3 miesięcy do 5 lat.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

---

[1] Nie jest to pełna lista różnych typów złośliwego oprogramowania. Jest to raczej definicja podstawowych typów złośliwego oprogramowania, wraz z wyjaśnieniem sposobu ich działania.

[2] Istnieją firmy specjalizujące się w usługach *pay per install* (*PPI*). "*PPI" objawia się następnie w powodzi działań prowadzących do instalacji dodatków lub innego niechcianego oprogramowania, które (w najmniej szkodliwym przypadku) zastępuje reklamy na stronach internetowych bez wiedzy użytkowników lub wstawia je tam, gdzie nie ma żadnych reklam.... **Cały model PPI jest zbudowany na tym, że ci, którzy oferują te usługi, nie zwracają uwagi na to, czy użytkownik chce coś zainstalować. Otrzymują do 1,50 USD za każdą instalację**, więc jest więcej niż pewne, że oszukańcze i zautomatyzowane instalacje są istotnym elementem ich "modelu biznesowego".*

Więcej informacji można znaleźć w artykule DOČEKAL, Daniel. *Google: Oprogramowanie typu adware infekuje miliony urządzeń i szkodzi reklamodawcom, witrynom internetowym i użytkownikom.* [online]. [cyt. 10.8.2016]. Dostępny pod adresem: http://www.lupa.cz/clanky/google-adware-napada-miliony-zarizeni-a-poskozuje-inzerenty-weby-i-uzivatele/

[3] Obraz tych wyskakujących okienek. Więcej informacji na *ten* temat można znaleźć w części *Adware.* [online]. [cyt. 10.8.2016]. Dostępny pod adresem: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking

[4] [online]. [cyt. 10.8.2016]. Dostępny pod adresem: https://i.ytimg.com/vi/GcvlB-EpMwA/maxresdefault.jpg

[5] Na przykład przegląd odwiedzanych stron internetowych, ich adresów IP, listy zainstalowanych i używanych programów, zapisy pobierania plików z Internetu, dane dotyczące struktury i zawartości katalogów przechowywanych na dysku twardym itp.

[6] [cyt. 8.1.2008]. Dostępny pod adresem: http://www.spyware.cz/go.php?p=spyware&t=clanek&id=9

[7] Może to być na przykład: **Browser Helper Object** (biblioteka DLL umożliwiająca programistom modyfikowanie i monitorowanie przeglądarki Internet Explorer); **Hijacker** (oprogramowanie zmieniające stronę główną przeglądarki internetowej); **Dialery** [przekierowujące linie telefoniczne na drogie plany telefoniczne (obecnie głównie ataki na telefony komórkowe i centrale VoIP)]; **Keystroke Logger/Keylogger** (monitorowanie uderzeń klawiszy); **Remote Administration** (umożliwienie zdalnemu użytkownikowi zdalnego sterowania systemem komputerowym użytkownika); **Tracer** (program **śledzący** ruch systemu komputerowego - zazwyczaj urządzenia mobilnego) itp.

[8] Więcej informacji naten temat można znaleźć w Muzeum złośliwego oprogramowania. *The Malware Museum @ Internet Archive*. [online]. [cyt. 17.5.2016]. Dostępny pod adresem: https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/

[9] Na przykład POŽÁR, Josef. *Bezpieczeństwo informacji*. Pilzno: Aleš Čeněk, 2005, s. 216 i nast.

[10] Patrz na przykład LI, Tao, GUAN, Zhihong, WU, Xianyong. Modelowanie i analiza rozprzestrzeniania się aktywnych robaków w oparciu o systemy P2P. *Computers & Security*, 2007, vol. 26, nr 3, s. 213-218.

[11] Por. RAK, Roman i Radek KUMMER. Zagrożenia informacyjne w latach 2007 - 2017. *Magazyn Bezpieczeństwa*, 2007, t. 14, nr 1, s. 4.

[12] Por. JIROVSKÝ, Václav i Oldřich KRULÍK. Podstawowe definicje związane z tematem. *Magazyn Bezpieczeństwa*, 2007, t. 14, nr 2, s. 47.

[13] Przegląd najczęściej spotykanych trojanów wraz z listą ich funkcji i portów komunikacyjnych można znaleźć na różnych stronach internetowych. Więcej informacji można znaleźć np. na stronie http://www.test.bezpecnosti.cz/full.php.

[14] Por. JIROVSKÝ, Václav. *Cyberprzestępczość. Nie tylko o hakowaniu, łamaniu* zabezpieczeń*, wirusach i trojanach bez tajemnic.* Praga: Grada, 2007, s. 63.

[15] Programy te są czasami nazywane również programami skanującymi, skanującymi, skanerami lub programami do skanowania.

[16] Por. np. BALIGA, Arati, Liviu IFTODE i Xiaoxin CHEN. Zautomatyzowane powstrzymywanie ataków typu Rootkits. *Computers & Security*, 2008, vol. 27, nr 7-8, s. 323-334.

BAUDIŠ, Pavel. Programy typu rootkit. Kolejne zagrożenie dla systemu Windows. *CHIP*, 2005, nr 7, s. 14.

[17] Por. RAK, Roman i Radek KUMMER. Zagrożenia informacyjne w latach 2007 - 2017. *Magazyn Bezpieczeństwa*, 2007, t. 14, nr 1, s. 5.

[18] Na przykład, trojan DNS-Changer atakuje najpierw programy zabezpieczające, z których usuwa się z listy złośliwych programów, uniemożliwiając tym samym ich wykrycie. Bliżej. PLETZER, Valentin. Oprogramowanie szpiegowskie zdemaskowane. *CHIP*, 2007, nr 10, s. 116-120.

[19] Więcej szczegółów na ten temat można znaleźć np. w pracy PŘIBYL, Tomáš. Poznaj rootkity. *PC World*, 2007, nr 9, s. 108-110.

[20] JIROVSKÝ, Václav. *Cyberprzestępczość. Nie tylko o hakowaniu, łamaniu* zabezpieczeń*, wirusach i trojanach bez tajemnic.* Praga: Grada, 2007, s. 65.

[21] Przechwytywanie naciśnięć klawiszy i informacji o uruchomionych plikach. [online]. [cyt. 10.8.2016]. Dostępny pod adresem: http://img.zerosecurity.org/files/2013/10/Keylogger-software-logfile-example.jpg

[22] [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://image.slidesharecdn.com/delljointevent2014november-onur-141105074412-conversion-gate02/95/end-to-end-security-with-palo-alto-networks-onur-kasap-engineer-palo-alto-networks-23-638.jpg?cb=1415174438

[23] Hyper Text Markup Language - jest to nazwa języka znaczników używanego do tworzenia stron internetowych.

[24] Dwie wersje fałszywego programu antywirusowego. [online]. [cyt. 10.8.2016]. Dostępny pod adresem: http://www.cctslo.com/images/fake-personal-antivirus.jpg

[25] Więcej szczegółów można znaleźć np. w artykule *Stuxnet.* [online]. [cyt. 23.7.2016]. Dostępny pod adresem: https://cs.wikipedia.org/wiki/Stuxnet

[26] Więcej informacji na *ten* temat można znaleźć w części *Pierwsze mobilne szkodliwe oprogramowanie: jak Kaspersky Lab odkrył Cabir.* [online]. [cyt. 29.6.2015]. Dostępny pod adresem: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir

Zob. też np:

Złośliwy kod jest kierowany na *telefony komórkowe i rozprzestrzenia się jak lawina.* [online]. [cyt. 17.5.2016]. Dostępny pod adresem: https://www.novinky.cz/internet-a-pc/bezpecnost/401956-skodlivy-kod-cili-na-mobily-siri-se-jako-lavina.html

Ostrzeżenie! Ponad 900 milionów telefonów z systemem Android jest podatnych na nowy atak "QuadRooter". [online]. [cyt. 2016-08-10]. Dostępny pod adresem: https://thehackernews.com/2016/08/hack-android-phone.html

[27] Według danych statystycznych odsetek wszystkich urządzeń z systemem operacyjnym Android jest następujący: Marshmallow 6.0 - 7,5%; Lollipop 5.1 - 19,4%; Lollipop 5.0 - 16,2%; KitKat 4.4 - 32,5%; Jelly Bean 4.1,2,3 - 20,1%; starsze wersje - 4,3%.

Zob. np. *rozkład udziału wersji systemu Android w rynku wśród posiadaczy smartfonów według stanu na maj 2016 r.* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

[28] Patrz np.: *Flappy Bird Clones Help Mobile Malware Rates Soar.* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx

Do tej grupy złośliwego oprogramowania zalicza się również tzw. ransomware, dla którego utrwaliła się nazwa *ransomware*[1] . Ransomware to złośliwe oprogramowanie, które uniemożliwia lub ogranicza użytkownikowi prawidłowe korzystanie z systemu komputerowego do czasu zapłacenia "okupu" przez atakującego. Oprogramowanie ransomware najczęściej dostaje się do komputera za pośrednictwem złośliwego oprogramowania (konia trojańskiego lub robaka), które jest umieszczane na stronie internetowej lub dołączane do wiadomości e-mail. Gdy to złośliwe oprogramowanie zostanie bezpiecznie "osadzone" w systemie komputerowym, pobierane jest właściwe oprogramowanie ransomware.

Ogólnie rzecz biorąc, można wyróżnić dwa typy oprogramowania ransomware w zależności od stopnia, w jakim zakłócają one rzeczywiste działanie systemu komputerowego. **Pierwszy typ to oprogramowanie ransomware, które ogranicza funkcjonalność całego systemu komputerowego** i uniemożliwia użytkownikowi korzystanie z systemu (np. poprzez uniemożliwienie uruchomienia systemu operacyjnego lub zablokowanie ekranu systemowego). Typowym przykładem tego typu oprogramowania jest *"Police ransomware*" - patrz poniżej). **Drugi typ to oprogramowanie ransomware, które pozostawia system komputerowy włączony, ale blokuje i uniemożliwia dostęp do danych użytkownika.**

Obecnie częściej wykorzystywany jest drugi rodzaj oprogramowania ransomware, znany jako **crypto-ransomware.** Celem tego złośliwego oprogramowania jest zaszyfrowanie dysku twardego lub wybranych typów plików w systemie komputerowym, przy czym głównym celem jest zaszyfrowanie prywatnych plików użytkownika, takich jak obrazy, dokumenty tekstowe lub arkusze kalkulacyjne, filmy itp. Po zakończeniu szyfrowania użytkownik zazwyczaj otrzymuje komunikat, że jego pliki są zaszyfrowane i jeśli chce je odzyskać (odszyfrować), musi przesłać pewną sumę pieniędzy na konto atakującego. Z reguły do transakcji wykorzystywane są waluty wirtualne, takie jak Bitcoin lub różne usługi subskrypcyjne. W większości przypadków obowiązuje termin płatności. Po upływie tego czasu klucz umożliwiający otwarcie zaszyfrowanych plików jest usuwany.

Ewolucja oprogramowania ransomware

Ransomware, podobnie jak inne złośliwe oprogramowanie, ewoluuje - pierwsze złośliwe oprogramowanie, które można określić mianem ransomware, pojawiło się około 2005 roku. Był to zasadniczo **fałszywy program antywirusowy (screware), który wykorzystywał** socjotechnikę do przekonania użytkowników do zapłacenia pewnej sumy pieniędzy za oczyszczenie zainfekowanego systemu komputerowego. To oprogramowanie ransomware zazwyczaj pozwalało użytkownikowi na korzystanie z systemu komputerowego (bez blokowania go lub szyfrowania danych), ale denerwowało go wyskakującymi okienkami i alertami o nieistniejących wirusach na komputerze. To oprogramowanie ransomware było bardzo łatwe do usunięcia.

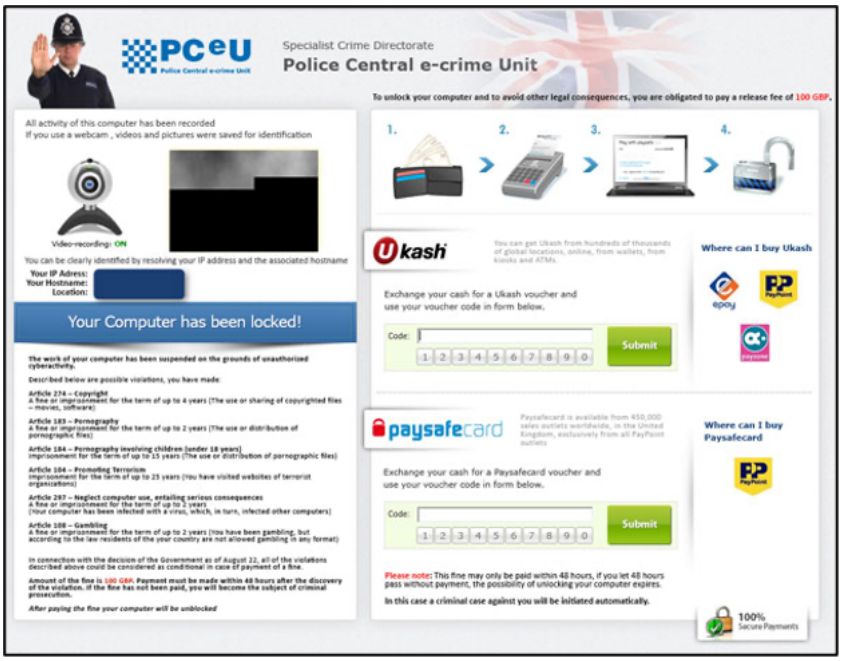
Masowe pojawienie się oprogramowania ransomware można datować na około 2011 rok, kiedy to atak ransomware zaczął rozprzestrzeniać się globalnie, blokując dostęp do konta Windows użytkownika i powiadamiając go, że jego komputer został zablokowany przez policję danego kraju.

Faktyczny atak polegał na zainfekowaniu użytkownika złośliwym oprogramowaniem (zazwyczaj podczas odwiedzania pewnych stron internetowych[2] pobierany był "klient botnetu"), a następnie staniu się częścią botnetu, za pośrednictwem którego rozprowadzane było rzeczywiste "**policyjne oprogramowanie ransomware".** To policyjne oprogramowanie ransomware blokowało następnie dostęp do konta użytkownika[3] w systemie operacyjnym Windows, informując go, że na jego komputerze znaleziono materiały naruszające prawo danego kraju (np. naruszenie praw autorskich, pornografia dziecięca itp.) W tym samym czasie użytkownik był proszony przez "policję" o wpłacenie żądanej kwoty pieniędzy, po czym komputer miał zostać odblokowany, a sprawa "rozwiązana". W tym przypadku atakujący wykorzystali techniki inżynierii społecznej, a mianowicie strach i łatwowierność użytkownika, i próbowali uzyskać od niego środki finansowe, powołując się na oficjalne władze.

W całej sprawie uderzający był fakt, że znaczna liczba użytkowników chętnie płaciła wymaganą kwotę (w Czechach kwota ta stale wahała się między 2000 a 4000 koron czeskich), nie sprawdzając, czy policja jest upoważniona do blokowania komputerów w ten sposób ani do "załatwiania" ewentualnych wykroczeń użytkownika.

Na poniższych print screenach przedstawiono "policyjne oprogramowanie ransomware" w różnych krajach, a następnie pokazano wersje stosowane w Republice Czeskiej.

Oprogramowanie ransomware dla policji[4]



Brytyjska wersja policyjnego oprogramowania ransomware[5]

W Europie stopniowo pojawiały się różne wersje (tzn. wygląd stron) policyjnego oprogramowania ransomware. Pierwsza wersja została nagrana pod koniec 2011 roku i wyświetlała adres IP połączenia, dostawcę usług internetowych połączenia oraz lokalizację [gdzie wymieniony był adres IP konkretnego dostawcy usług internetowych (ISP) połączenia]; jeśli użytkownik miał włączoną kamerę internetową, robione było zdjęcie, które również było wyświetlane.

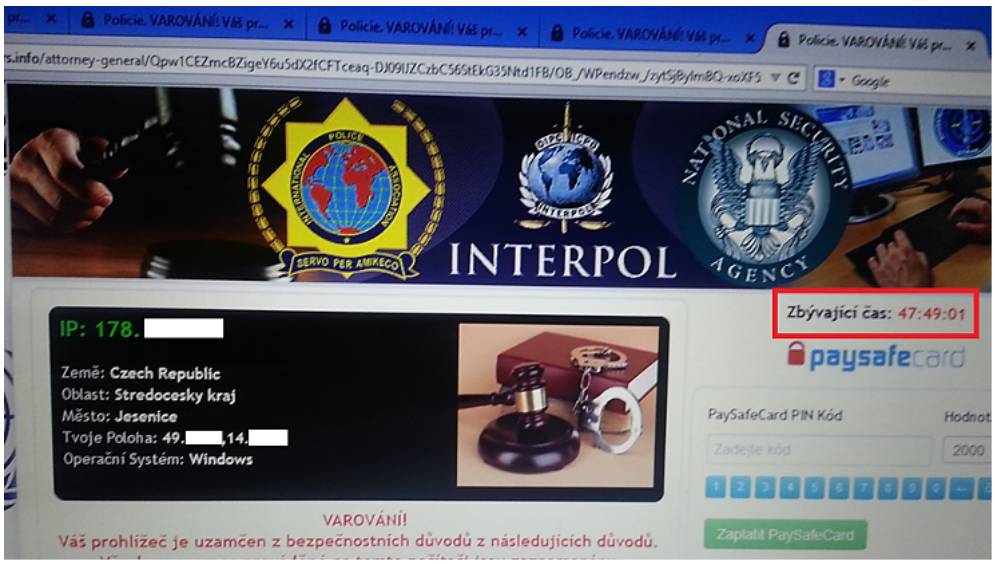
Pierwsza wersja policyjnego oprogramowania ransomware w Republice Czeskiej

Nowsze wersje, oprócz różnic graficznych, wyświetlały także wersję systemu operacyjnego i nazwę użytkownika. Poprawiono także język angielski używany na zablokowanej stronie.

Policyjne oprogramowanie ransomware Republika Czeska - kolejna wersja

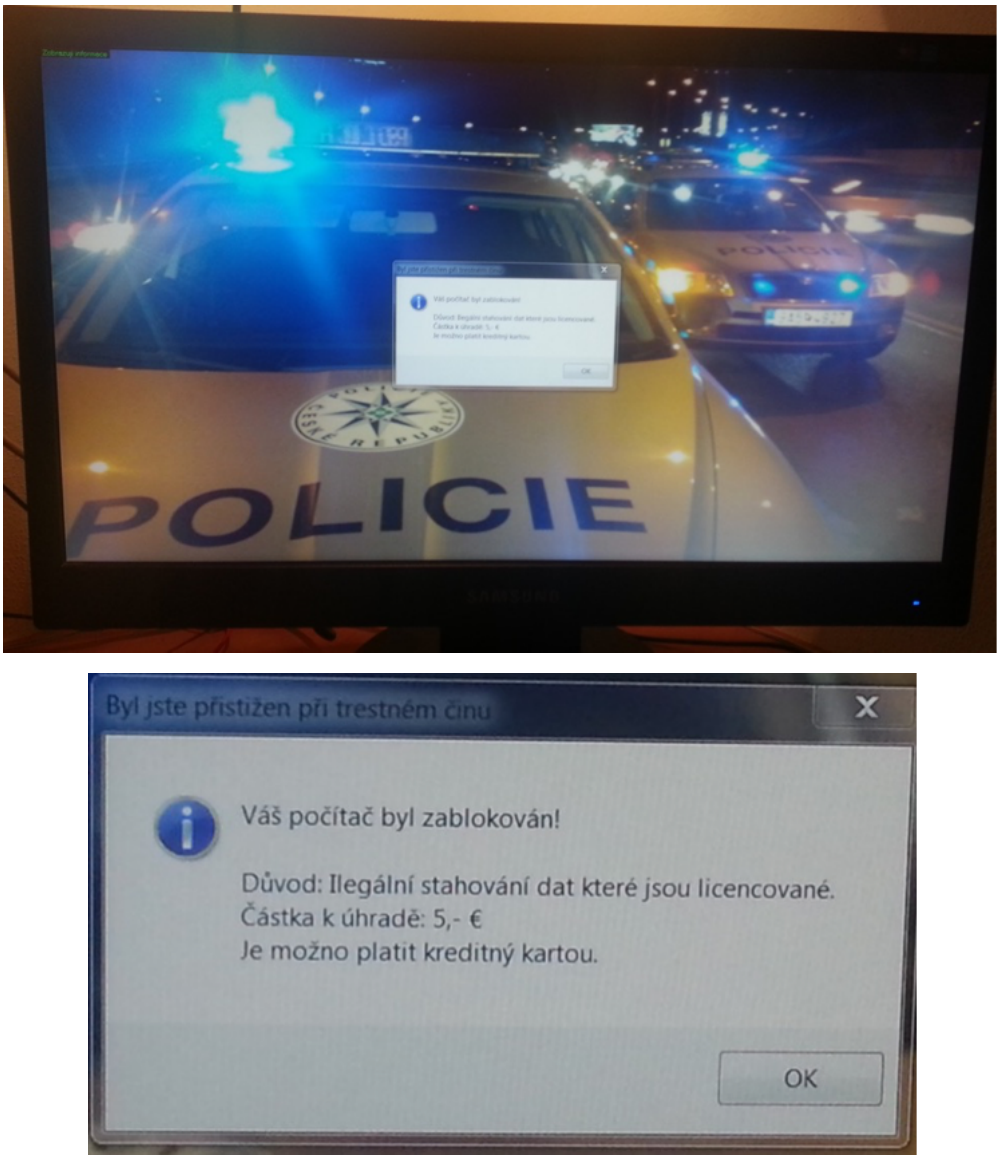
Opisane powyżej "policyjne oprogramowanie ransomware" przeżywało swój największy rozkwit w latach 2011-2013, jednak od tego czasu pojawiły się inne warianty tego szkodliwego oprogramowania w różnych odmianach. Na poniższych print screenach pokazano modyfikacje oprogramowania "police ransomware". Oba przypadki zostały wykryte w 2015 r. Pierwszy printscreen pokazuje, że ransomware blokuje główną przeglądarkę internetową używaną na zagrożonym komputerze (podczas gdy inne przeglądarki nie zostały zainfekowane). Użytkownik był w stanie korzystać ze wszystkich funkcji systemu komputerowego z wyjątkiem zainfekowanej przeglądarki.

Oprócz wcześniej wymienionych informacji wyświetlana jest pozycja GPS oraz czas pozostały do zapłaty.



Policyjne oprogramowanie ransomware w Republice Czeskiej (2015)

Drugi printscreen pokazuje "zablokowany" komputer z oprogramowaniem ransomware ukrytym w cracku nielegalnie pobranej i zainstalowanej gry (w tym przypadku Far Cry 4 pobranej z czeskich torrentów).

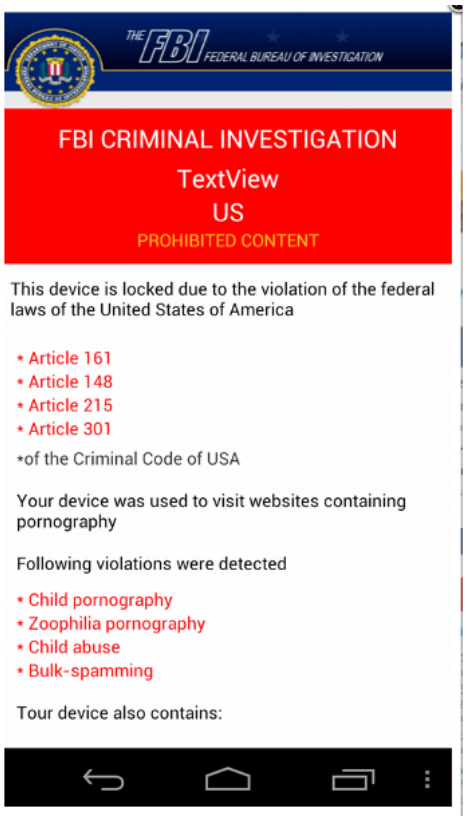


Policyjne oprogramowanie ransomware w Republice Czeskiej (2015)

Od 2013 r. nastąpiła znaczna zmiana w oprogramowaniu ransomware. Atakujący ograniczyli ataki polegające na ograniczaniu funkcjonalności całego systemu komputerowego i skupili się przede wszystkim na blokowaniu danych użytkowników. Dane na dyskach lokalnych, dyskach podłączonych w sieci komputerowej oraz wszystkich podłączonych urządzeniach peryferyjnych (np. zewnętrzne dyski USB, HDD itp.) są zablokowane. Dane stają się "zakładnikiem", a złamanie szyfrowania jest prawie niemożliwe. Jednym z pierwszych ransomware tego typu był CryptoLocker (potem CryptoWall itd.).

Cryptolocker (r. 2013)

Petya (2017)



Mobilne oprogramowanie ransomware (r. 2018)

W ramach działalności przestępczej od 2016 r. oferowana jest **usługa Ransomware-as-a-service.** Użytkownik (tj. atakujący) ma możliwość zdefiniowania własnego oprogramowania Ransomware zgodnie z własnymi życzeniami. Jednocześnie zapewnia się mu wsparcie techniczne w postaci serwerów C&C, portfela bitcoin, pomocy technicznej online 24/7 itp. Przykładem oprogramowania typu Ransomware-as-a-service jest oprogramowanie **Ransom32.**

Ransomware (klient)

Inne zmiany można zaobserwować w działaniach samych napastników. Zainstalowane oprogramowanie ransomware może mieć na celu na przykład zaszyfrowanie zapisanych pozycji w grach lub "zablokowanie" telewizorów korzystających z systemu operacyjnego Android.[6]

Zapobieganie i reagowanie na oprogramowanie ransomware można podsumować w następujących punktach:

1. **Natychmiast:**

- Unikać wzajemnego łączenia systemów, chyba że jest to konieczne
- Unikanie łączenia się z Internetem, chyba że jest to konieczne
- Zmiana haseł do kont uprzywilejowanych

2. **Za kilka dni:**

- Przenieś kopie zapasowe do trybu offline, sprawdź funkcjonalność kopii zapasowych
- Przegląd planów ciągłości działania i przeniesienie ich poza systemy
- Nie usuwaj danych dotyczących incydentów związanych z bezpieczeństwem cybernetycznym
- Zbadanie wskaźników kompromitacji
- Ostrzegaj pracowników o ryzyku phishingu

3. **Za tydzień:**

- Sprawdź, czy kopie zapasowe są rozdzielone tak, aby nawet uprzywilejowany administrator nie mógł ich usunąć
- Jeśli to możliwe, wyłącz użycie makr bez znaku
- Sprawdź segmentację sieci i zarządzanie międzysegmentowe
- Zaostrzenie zasad bezpieczeństwa punktów końcowych (zakaz używania niezatwierdzonych aplikacji, niepodpisanego PowerShella itp.)
- Jeśli nie wprowadzono zarządzania ciągłością działania - opracuj plany ciągłości działania dla co najmniej kluczowych systemów
- Wdrożenie programów antywirusowych na wszystkich odpowiednich urządzeniach.
- Rozważ aktualizację, aby przetestować i wdrożyć ją

4. **Długoterminowe zalecenia dotyczące radzenia sobie z atakami typu ransomware**

- Regularne szkolenia pracowników
- Wyraźniejsza segmentacja sieci
- Ograniczenie do minimum korzystania z kont administratorów
- Twórz kopie zapasowe, regularnie testuj kopie zapasowe, przechowuj kopie zapasowe w trybie offline
- Zasada 3 - 2 - 1 = co najmniej 3 kopie na 2 różnych urządzeniach, z których 1 znajduje się poza organizacją.
- posiadanie planów ciągłości działania (BCM) i ich testowanie
- Regularnie przeglądać aplikacje dostępne z Internetu i oceniać, czy nadal są one

Możliwości stosowania sankcji karnych w Republice Czeskiej

W Republice Czeskiej atak za pomocą złośliwego oprogramowania, którym jest również ransomware, można karać na podstawie paragrafu **230** (Nieuprawniony dostęp do systemu komputerowego i nośnika informacji) kodeksu karnego. **Posiadanie złośliwego oprogramowania, z zamiarem popełnienia przestępstwa z Artykułu** 182 (Naruszenie tajemnicy przesyłanych wiadomości) lub przestępstwa z **Artykułu** 230 Kodeksu karnego, **jest karalne z Artykułu 231** (Posiadanie i dysponowanie urządzeniem dostępowym i hasłem do systemu komputerowego i innych tego typu danych) Kodeksu karnego**.**

W przypadku oprogramowania ransomware można również zastosować przepisy **sekcji 230(3)** kodeksu karnego, gdy osoba atakująca popełnia to przestępstwo z zamiarem uzyskania nieuzasadnionej korzyści dla siebie lub innej osoby. Można też rozważyć zastosowanie paragrafu 175 (Wymuszenie) Kodeksu Karnego, gdy osoba jest zmuszana do zapłacenia sumy pieniędzy pod groźbą innej poważnej szkody (np. złożenia skargi karnej[7]).

Możliwości ścigania karnego w Polsce

W Polsce obowiązują następujące przepisy:

Artykuł 267. Bezprawne uzyskanie informacji

Artykuł 269a. Zakłócanie działania systemu informatycznego, systemu IT lub sieci IT

---

[1] Na przykład Reventon, CryptoLocker, CryptoWall, Loky, Petya, Cerber, SamSam, Jig Saw i inne. Więcej informacji na ten temat można znaleźć np:

Ransomware. [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://www.trendmicro.com/vinfo/us/security/definition/ransomware

Security Insights: Ransomware sześć razy inne. [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://www.root.cz/clanky/postrehy-z-bezpecnosti-ransomware-sestkrat-jinak/

[2] Bardzo często były to strony z pornografią lub innymi materiałami o charakterze seksualnym. Użytkownik mógł nawet zostać przekierowany na te strony z innej witryny, na której znajdowała się "przynęta".

[3] Aplikacja została ustawiona jako "zawsze na wierzchu" (StayOnTop). Użytkownik nie widzi innych aplikacji ukrytych pod tym "oknem dialogowym okupu" i nie może wywołać menedżera zadań. Rzeczywiste oprogramowanie ransomware zapisywało się w rejestrach Run i RunOnce i wykonywało skanowanie co 500 ms, ukrywając menedżera zadań w tym samym przedziale czasu. Jedyna inna uruchomiona aplikacja komunikowała się z serwerem C&C (zamaskowanym w procesie przeglądarki).

[4] *Policyjne oprogramowanie ransomware.* [online]. [cyt. 14.8.2016]. Dostupné z: https://www.f-secure.com/documents/996508/1018028/multiple_ransomware_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000

[5] [online]. [cyt. 14.8.2016]. Dostępny pod adresem: https://sophosnews.files.wordpress.com/2012/11/cool_ransom_uk_full.png

[6] Por. np. *New Ransomware Encrypts Your Game Files (Nowe oprogramowanie okupowe szyfruje pliki gier).* [online]. [cit.14.8.2016]. Dostępny pod adresem: https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/

Android Ransomware atakuje także Twój Smart TV! [online]. [cyt. 14.8.2016]. Dostępny pod adresem: https://thehackernews.com/2016/06/smart-tv-ransomware.html

Mobilne oprogramowanie ransomware FLocker przenosi się na telewizory Smart TV. [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/

[7] Na temat pojęcia innej poważnej szkody zob. ŠÁMAL, Pavel et al. *Kodeks karny II, §§ 140-421. Komentarz.* 2. 2. edycja. Praga: C. H. Beck, 2012, s. 1752-1753.

W szczególności *"groźba wyrządzenia innej poważnej krzywdy może polegać na groźbie spowodowania szkód majątkowych, poważnego uszczerbku na honorze lub reputacji itp. Inna poważna szkoda może polegać na wszczęciu postępowania karnego w wyniku zgłoszenia przestępstwa, w którym sprawca grozi ofierze, zmuszając ją w ten sposób do zrobienia, zaniechania lub doznania czegoś. Nie ma znaczenia, czy ofiara popełniła przestępstwo, którego dotyczy groźba, czy też nie (por. R 27/1982)".*

4.5. Spam

Z perspektywy technologii informacyjnych i komunikacyjnych treść pojęcia spamu można zasadniczo rozumieć na dwóch poziomach. W **węższym znaczeniu odnosi się** do masowego rozpowszechniania niezamówionych komunikatów, najczęściej o charakterze reklamowym, za pośrednictwem Internetu, najczęściej drogą elektroniczną. W **szerszym znaczeniu odnosi się** do wszystkich otrzymywanych niezamówionych wiadomości, w tym np. wiadomości zawierających wirusy, konie trojańskie itp. [1]

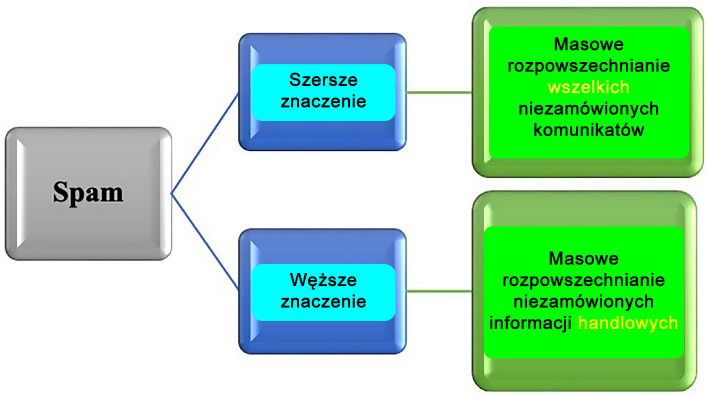


Diagram - Dystrybucja spamu

Spam charakteryzuje się **wiadomościami przesyłanymi drogą elektroniczną, masowo, a w szczególności niezamówionymi.**

Spam wykorzystuje różne kanały komunikacyjne do wysyłania niechcianych wiadomości:

- e-mail;
- inny komunikator (ICQ, Skype itp.);
- SMS, MMS;
- fora dyskusyjne, blogi, sieci społecznościowe itp;
- platformy do gier itp.

Spam może zawierać informacje:

- **biznesowe lub reklamowe;**
- na temat **zdrowia i medycyny** (w tej kategorii znajduje się spam oferujący produkty do odchudzania, kosmetyki, medycynę nietradycyjną, leki niedostępne w regionie itp;)
- **finansowe** (w szczególności oferty różnych kredytów, możliwości zarobkowania itp;)
- **pornograficzne** (Ten spam oferuje różne, nawet farmaceutyczne produkty zwiększające potencję seksualną lub zawiera łącza do stron z treściami pornograficznymi);
- **edukacyjne** (oferty różnych kursów, szkoleń itp.);
- **hoax** (łańcuszek);
- **polityczne;**
- **religijne;**
- **przestępcze** (do tej kategorii należą wiadomości zawierające np. złośliwe oprogramowanie lub odsyłające do stron ze złośliwym kodem itp.)

Obecnie istnieje wiele statystyk pokazujących różne liczby wiadomości spamowych. Na przykład Jirovsky twierdzi, że w poczcie elektronicznej można się spodziewać ponad 90% spamu. W 2006 r. wysyłano średnio 14,5 miliarda wiadomości spamowych dziennie.[2] Doprowadziło to również do powstania wielu organizacji zajmujących się spamem i dostarczających narzędzia do ochrony przed nim. Jedną z tych firm była TrustedSource[3] , z której pochodzi poniższy wykres przedstawiający zawartość spamu w poczcie elektronicznej w latach 2005-2010. Niebieska linia pokazuje liczbę wiadomości e-mail, a czerwona ramka odzwierciedla liczbę wiadomości spamowych w poczcie elektronicznej (obie wartości w miliardach).

Niezależnie od dokładnych danych procentowych, tego typu niechciane wiadomości stanowią obecnie większość wszystkich otrzymywanych wiadomości e-mail.[4] Jednak dzięki szeregowi środków technicznych stosowanych przez poszczególnych dostawców usług internetowych do użytkownika dociera minimalna liczba wiadomości spamowych.

Ewolucja spamu w latach 2005-2010

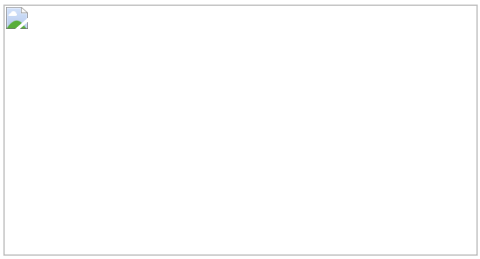
Znaczny spadek ilości spamu pod koniec 2009 r. wynika z zamknięcia firmy **McColo**, która rozsyłała niechciane wiadomości w Internecie. [5]

Ewolucja spamu po zamknięciu McColo w listopadzie 2008 r.

Spam zakłóca komunikację elektroniczną, często całkowicie ją uniemożliwiając (przytłacza strukturę informacji), a tym samym zmniejsza zaufanie społeczeństwa do technologii informacyjnych. Jeśli jednak spam jest ograniczany, prawo do wolności wypowiedzi jest de facto ograniczane na rzecz prawa do ochrony nietykalności osobistej.

Również z opisanego powyżej powodu karanie spamerów jest bardzo skomplikowane i obecnie korzysta się z instytucji prawa cywilnego i administracyjnego, ponieważ prawo karne nie pozwala na ukaranie spamera.

Spam zawierający treści przestępcze lub inne oszukańcze treści jest określany mianem *scamu.* Oszustwa stanowią obecnie znaczną część spamu, a ich celem jest zdobycie zaufania użytkownika, zazwyczaj poprzez wykorzystanie socjotechniki, oraz skłonienie go do wykonania pożądanych działań (np. otwarcia załącznika do wiadomości e-mail, odwiedzenia wyświetlonego adresu URL itp.) Oszustwa mogą obejmować *phishing, złośliwe oprogramowanie, 419, oszustwa, oszukańcze loterie i oferty, oszustwa związane z darowiznami, oszustwa typu "cold call", oszustwa typu "Facebook like scam" itp.*



Schemat podziału oszustw

W tym miejscu zwrócę szczególną uwagę na trzy rodzaje oszustw: oszustwo **419**, oszustwo hakerskie i fałszywe **oferty.**

1.1.1. Oszustwo 419

Scam 419 to oznaczenie wiadomości e-mail, które są bardziej znane jako **listy nigeryjskie.** Oszustwa te są przykładem przeniesienia zwykłego przestępstwa (oszustwa) ze świata rzeczywistego do świata wirtualnego.

Dla ciekawości załączamy trzy bardzo różne wiadomości o charakterze oszustwa 419.

Raport nr 1 - "Odziedziczyłeś ogromną sumę pieniędzy".

Witaj, kochanie,

Jestem adw. Victoria Joseph, mam dla Pana wiadomość w sprawie mojego zmarłego klienta, który nosi takie samo nazwisko jak Pan. Wiem, że nie jestem z nim spokrewniona, ale jest on obywatelem Pana kraju, który wraz z najbliższą rodziną stracił życie w wypadku samochodowym w Togo.

Odszedł za sumę 2,7 mln dolarów, tymczasem jego bank chce przekazać świadczenia na rzecz któregoś z członków jego dalszej rodziny, ponieważ prezentację można przeprowadzić za pośrednictwem mojego biura. Szczerze mówiąc, te pieniądze należą do mojego zmarłego klienta, który nosi to samo nazwisko i obywatelstwo co Ty, mieszkał i pracował w Togo przez ponad 20 lat jako wykonawca, ale zginął w śmiertelnym wypadku samochodowym wraz z członkami swojej rodziny w 2009 r. Niedawno bank, w którym zdeponował te pieniądze, upoważnił mnie do przekazania ich jakiemuś członkowi jego rodziny, w przeciwnym razie zostaną one przekazane na konto skarbu państwa jako pieniądze porzucone.

Nie chcę, żeby tak się stało, ale problem polega na tym, że jego domniemana najbliższa rodzina zginęła w tym samym wypadku samochodowym, a wszystkie moje starania, żeby odnaleźć członków jego rodziny od czasu jego śmierci, spełzły na niczym, ponieważ za życia nigdy mi ich nie przedstawił.

Przyjacielu, właśnie dlatego podjąłem się tej misji, aby znaleźć kogoś, kto ramię w ramię ze mną upomni się o ten fundusz, aby pomóc naszym rodzinom i potrzebującym, zamiast pozwolić tym skorumpowanym urzędnikom państwowym przejąć te ciężko zarobione pieniądze i roztrwonić je, pozostawiając biedne masy na pastwę losu. To, że mogę się czepiać ciebie spośród milionów ludzi na Facebooku, oznacza po prostu, że to Bóg uczynił naszą drogę złą, więc pracujmy razem w jednym duchu, dzieląc się pieniędzmi tak, jak się o to prosi.
Proszę zaznaczyć swoje zainteresowanie tym roszczeniem, abym mógł przekazać Ci informacje dotyczące pracy i wytycznych.

Adwokat Victoria Joseph Esq.

Komunikat 2 - "Jestem zakochany"

Cześć, kochanie.

Nazywam się Joe Anita jestem kobietą, dowiedziałem się jego tożsamość na boku i chcę się dowiedzieć, że wiemy więcej o sobie i dzielić życie społeczne z kulturą i nie mam nic do powiedzenia, więc proszę mi odpowiedzieć, więc ja też wysłać moje dane do Ciebie i powiedzieć więcej o sobie w swoich zdjęciach. Bardzo dziękuję.

Z przyjemnością Anita

Raport nr 3 - "Seks intymny"

Raport nr 4 - Nigeryjski astronauta został zapomniany w kosmosie i musi wrócić do domu

Wieść o tym zaczęła się rozchodzić w 2004 r., kiedy to "pierwszy afrykański astronauta" przebywał w kosmosie bez przerwy przez 14 lat. Należy zauważyć, że długość pobytu przewyższała wszystkie czasy pobytu astronautów (być może nawet w ogóle). Najnowszą wersję tego scamu 419 otrzymałem w 2016 r. Chociaż bardzo współczuję temu wyimaginowanemu astronaucie (26 lat w kosmosie i samotnie), z pewnością nie zamierzam przyczyniać się do pomocy oszustom. Niestety, pomimo całkowicie bezsensownej treści i bezpodstawnych informacji zawartych w tym e-mailu, istnieje znaczna liczba osób, które chcą pomóc osobie w potrzebie (ze względu na tę pomoc, oszustwo to można również zakwalifikować jako *oszustwo związane z darowiznami*).

Ze względu na charakter oszustwa, Scam 419 można w niektórych przypadkach zakwalifikować również jako phishing.

1.1.2. Hoax

Oszustwo to inna forma spamu lub wyłudzenia informacji. Oszustwo to termin oznaczający łańcuszki (łańcuszki wiadomości, takie jak *"przekaż dalej"*, *"jeśli nie wyślesz tego do 20 innych osób, to stanie się..."* itp.), które przedstawiają zniekształcone, fałszywe, wprowadzające w błąd lub w inny sposób nieprawdziwe informacje. Hoaxes często zawierają ostrzeżenia przed atakami, opisy niebezpieczeństwa, prośby o pomoc, apele, petycje, poparcie celebrytów, łańcuszki szczęścia, wiadomości żartobliwe, zdjęcia i filmy w prezentacjach, odgrywanie kotów i innych zwierząt itp.

1.1.3. Nieuczciwe oferty

Bardzo skuteczną formą oszustwa są różne oszukańcze oferty, które mogą być wysyłane masowo lub celowo. Obecnie takie oferty wysyłane są nie tylko pocztą elektroniczną, ale także za pośrednictwem wszelkich komunikatorów, portali społecznościowych, portali aukcyjnych itp.

Jeśli chodzi o **masowe rozsyłanie** oszukańczych ofert, można wymienić cały szereg działań opartych na zasadzie "piramidy" lub "samolotu", oferty dochodowej pracy w domu[6] , "gwarantowane" metody pomnażania pieniędzy (o najwyższym oprocentowaniu), oferty pożyczek (o najniższym oprocentowaniu), "świetne" oferty pracy itp.

Ukierunkowane wysyłanie oszukańczych ofert powinno również obejmować działania, które nie są zwykłym spamem, ale na przykład stanowią połączenie składania ofert na określony rodzaj towarów na portalach aukcyjnych i późniejszej komunikacji z użytkownikami, którzy przyjęli ofertę. Jest to tak zwane "oszustwo aukcyjne".

Nieodparta oferta pracy w domu (masowe umieszczanie na Facebooku)

W dzisiejszych czasach zdecydowanie nie jest już regułą, że oferty są wysyłane masowo lub celowo pisane podejrzanym lub łamanym językiem czeskim (albo po angielsku lub rosyjsku); wręcz przeciwnie, celem atakującego jest przekonanie ofiary o całkowitej poprawności, powadze i "uczciwości" swoich działań. Na portalach aukcyjnych bardzo często w nieuczciwy sposób oferowane są różnego rodzaju urządzenia elektroniczne, zwłaszcza telefony komórkowe i komputery. Faktyczne oszustwo może polegać na przykład na zmianie istotnych informacji [np. kraju pochodzenia telefonu komórkowego; informacji, że telefon jest kopią (podróbką)] lub na niedostarczeniu towaru jako takiego (atakujący bardzo często prosi o zapłatę całości lub depozytu).

W środowisku internetowym pomysłowość napastników jest znaczna, dlatego warto zachować paranoję i nie ufać nieznanym osobom w przypadku jakichkolwiek ofert, reklam, a zwłaszcza wysyłania zaliczek lub płatności.

W przypadku oszukańczych ofert, gdy osoba atakująca próbuje uzyskać różne zaliczki lub inne płatności z góry, takie postępowanie może być karalne na podstawie **paragrafu 209** (Oszustwo) Kodeksu karnego.

Możliwości stosowania sankcji karnych w Republice Czeskiej

Jeśli chodzi o sankcje karne wobec spamerów i spamerów, to w Republice **Czeskiej nie są one obecnie w pełni (rozwiązane).** Brak jest zarówno krajowej, jak i międzynarodowej ochrony prawnej przed tym niepożądanym zachowaniem. Nawet Konwencja o cyberprzestępczości nie definiuje spamu jako przestępstwa.

Na przykład w **USA w przeszłości** skazywano spamerów z portalu[7] za rozsyłanie wiadomości-śmieci. Na przykład **Jeremy Jaynes** został skazany w 2007 r. przez sąd w Wirginii na 9 lat więzienia. Został skazany w 2003 r., a jako dowód posłużyło mu 53 000 wiadomości spamowych wysłanych w ciągu trzech dni. Prokurator powiedział jednak, że jego zdaniem Jaynes był odpowiedzialny za wysyłanie ponad 10 000 000 wiadomości spamowych dziennie, co miało mu przynosić miesięcznie około 750 000 USD.

Ponieważ spamu nie można zaklasyfikować jako jednej z form szkodliwego zachowania, bardzo trudno jest karać spam per se za pomocą prawa karnego. Można to zrobić tylko w przypadku poszczególnych rodzajów spamu. W niektórych przypadkach może istnieć możliwość sankcjonowania gromadzenia adresów e-mail, jeśli takie gromadzenie wypełnia znamiona przestępstwa nieuprawnionego posługiwania się danymi osobowymi na podstawie paragrafu **180** (Nieuprawnione posługiwanie się danymi osobowymi) Kodeksu karnego. Jeśli spam zawiera złośliwe oprogramowanie lub ma na celu dokonanie oszustwa, działalność spamera może zostać ukarana na mocy przepisów dotyczących złośliwego oprogramowania lub phishingu.

Możliwości ścigania karnego w Polsce

W Polsce przesyłanie niezamówionych informacji handlowych za pomocą środków komunikacji elektronicznej jest uznawane za wykroczenie i podlega karze grzywny. Reguluje to ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r. Nr 144, poz. 1204):

Kto wysyła niezamówione informacje handlowe za pomocą środków komunikacji elektronicznej, podlega karze grzywny.

(2) Ściganie przestępstwa, o którym mowa w ustępie 1, odbywa się na wniosek pokrzywdzonego.

Art. 25 Orzekanie w sprawach o wykroczenia, o których mowa w art. 23 i 24, odbywa się w trybie przepisów o postępowaniu w sprawach o wykroczenia.

[1] Na temat klasyfikacji spamu por. np. GONZÁLES-TALAVÁN, Guillermo. Prosty, konfigurowalny filtr antyspamowy SMTP. *Computers & Security*, 2006, vol. 25, nr 3, s. 229-236.

[2] Por. np. *statystyki spamu*. [online]. [cit.14.8.2016]. Dostępny pod adresem: https://www.spamcop.net/spamstats.shtml

Statystyki i fakty dotyczące spamu [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://www.spamlaws.com/spam-stats.html

[3] Oryginalne źródło internetowe: http://www.trustedsource.org/TS?do=home [cytowany 12 lutego 2010].

[4] Nie da się dokładnie określić, jaki procent wszystkich wiadomości e-mail stanowi spam. Różne dostępne źródła podają różne, czasem bardzo zróżnicowane liczby. Na przykład jeden z dostawców rozwiązań antyspamowych, firma POSTINI, podała w marcu 2005 r., że w ciągu 24 godzin 10 na 12 wiadomości e-mail było spamem. Na temat częstotliwości występowania spamu por. np. *Phishing bez tajemnic*. Praga: Grada, 2007, s. 22, SCHRYEN, Guido. Wpływ umieszczania adresów e-mail w Internecie na otrzymywanie spamu: analiza empiryczna. *Computers & Security*, 2007, vol. 26, nr 5, s. 361-372.

[5] *Złośliwe oprogramowanie, chaos i zatrzymanie McColo.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/

[6] Oferty te mogą zawierać prośbę typu: *"prześlij nam 10 dolarów na swoje konto, a my wyślemy Ci instrukcje, jak zarobić 8847 dolarów miesięcznie"*. Po drugie, te oferty pracy nie wymagają żadnych opłat z góry, wymagają jedynie rejestracji użytkownika. Po faktycznym zarejestrowaniu się atakujący otrzymuje dane osobowe użytkownika. Następnie na adres e-mail użytkownika może zostać wysłana wiadomość z firmy, zawierająca np. złośliwe oprogramowanie itp.

[7] *Skazany spamer kwestionuje prawo obowiązujące w Va.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm

Czołowy spamer skazany na prawie cztery lata. [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://www.pcworld.com/article/148780/spam.html

Spamer Buffalo idzie do więzienia na 7 lat za spamowanie. [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality

4.6. Spam

Z perspektywy technologii informacyjnych i komunikacyjnych treść pojęcia spamu można zasadniczo rozumieć na dwóch poziomach. W **węższym znaczeniu odnosi się** do masowego rozpowszechniania niezamówionych komunikatów, najczęściej o charakterze reklamowym, za pośrednictwem Internetu, najczęściej drogą elektroniczną. W **szerszym znaczeniu odnosi się** do wszystkich otrzymywanych niezamówionych wiadomości, w tym np. wiadomości zawierających wirusy, konie trojańskie itp. [1]

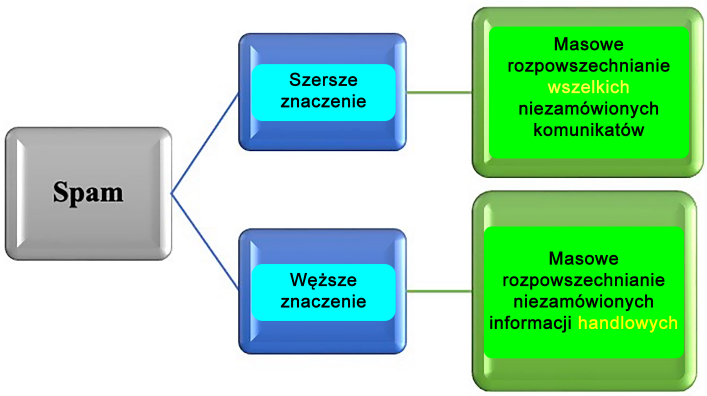


Diagram - Dystrybucja spamu

Spam charakteryzuje się **wiadomościami przesyłanymi drogą elektroniczną, masowo, a w szczególności niezamówionymi.**

Spam wykorzystuje różne kanały komunikacyjne do wysyłania niechcianych wiadomości:

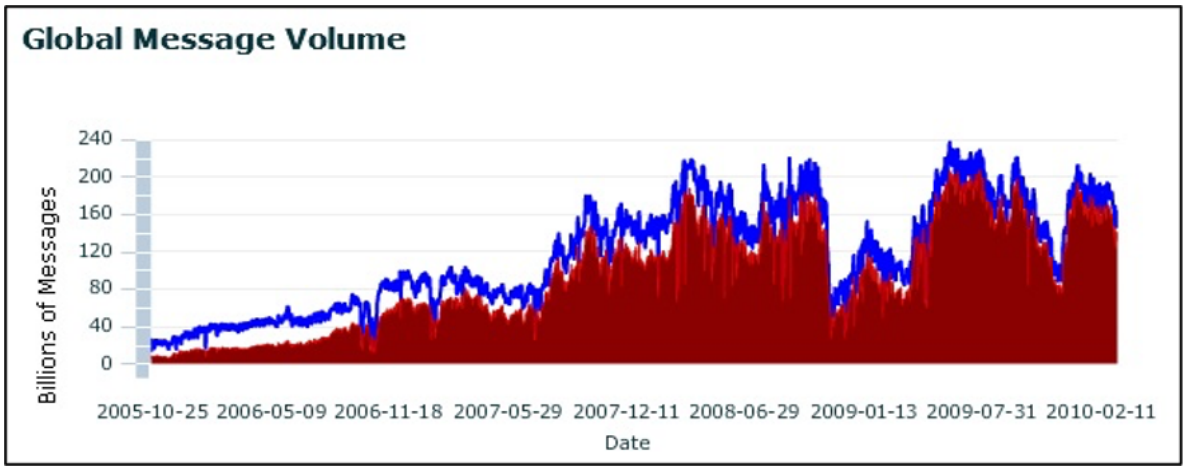
- e-mail;
- inny komunikator (ICQ, Skype itp.);
- SMS, MMS;
- fora dyskusyjne, blogi, sieci społecznościowe itp;
- platformy do gier itp.

Spam może zawierać informacje:

- **biznesowe lub reklamowe;**
- na temat **zdrowia i medycyny** (w tej kategorii znajduje się spam oferujący produkty do odchudzania, kosmetyki, medycynę nietradycyjną, leki niedostępne w regionie itp;)
- **finansowe** (w szczególności oferty różnych kredytów, możliwości zarobkowania itp;)
- **pornograficzne** (Ten spam oferuje różne, nawet farmaceutyczne produkty zwiększające potencję seksualną lub zawiera łącza do stron z treściami pornograficznymi);
- **edukacyjne** (oferty różnych kursów, szkoleń itp.);
- **hoax** (łańcuszek);
- **polityczne;**
- **religijne;**
- **przestępcze** (do tej kategorii należą wiadomości zawierające np. złośliwe oprogramowanie lub odsyłające do stron ze złośliwym kodem itp.)

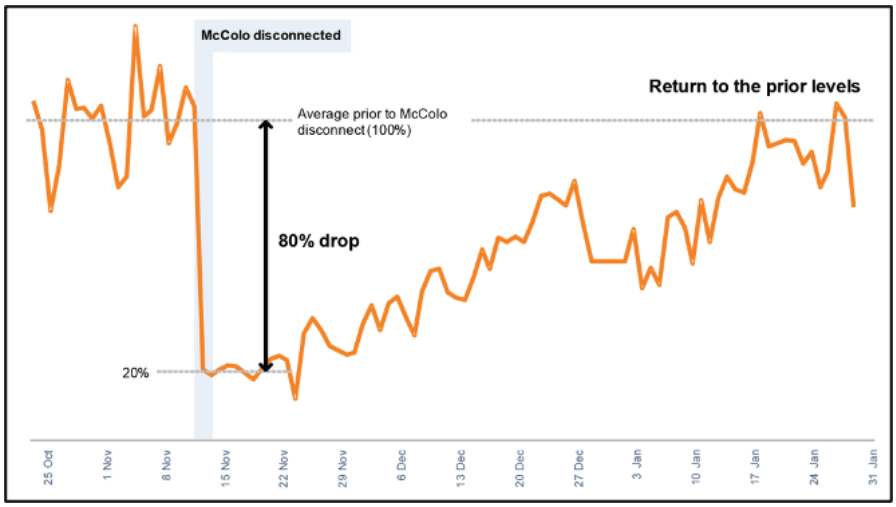
Obecnie istnieje wiele statystyk pokazujących różne liczby wiadomości spamowych. Na przykład Jirovsky twierdzi, że w poczcie elektronicznej można się spodziewać ponad 90% spamu. W 2006 r. wysyłano średnio 14,5 miliarda wiadomości spamowych dziennie.[2] Doprowadziło to również do powstania wielu organizacji zajmujących się spamem i dostarczających narzędzia do ochrony przed nim. Jedną z tych firm była TrustedSource[3] , z której pochodzi poniższy wykres przedstawiający zawartość spamu w poczcie elektronicznej w latach 2005-2010. Niebieska linia pokazuje liczbę wiadomości e-mail, a czerwona ramka odzwierciedla liczbę wiadomości spamowych w poczcie elektronicznej (obie wartości w miliardach).

Niezależnie od dokładnych danych procentowych, tego typu niechciane wiadomości stanowią obecnie większość wszystkich otrzymywanych wiadomości e-mail.[4] Jednak dzięki szeregowi środków technicznych stosowanych przez poszczególnych dostawców usług internetowych do użytkownika dociera minimalna liczba wiadomości spamowych.



Ewolucja spamu w latach 2005-2010

Znaczny spadek ilości spamu pod koniec 2009 r. wynika z zamknięcia firmy **McColo**, która rozsyłała niechciane wiadomości w Internecie. [5]

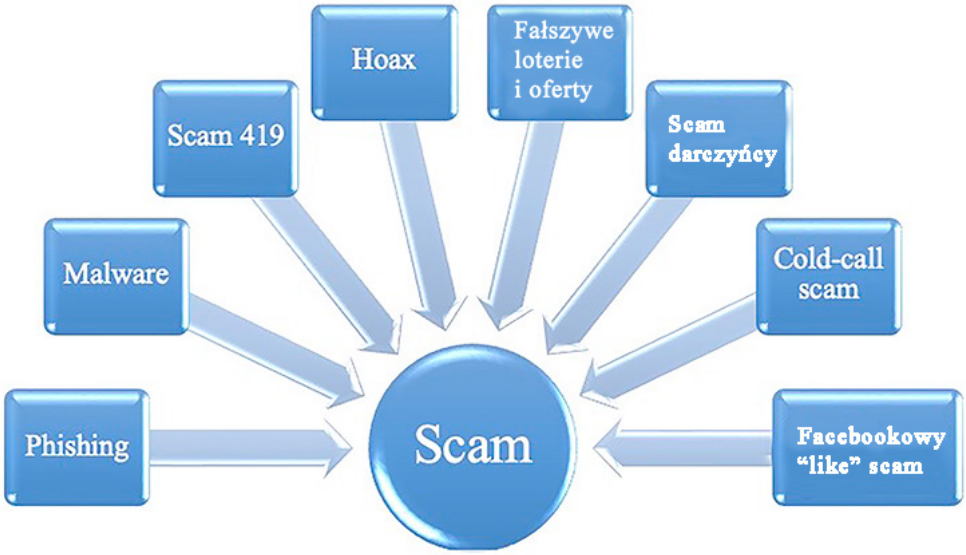


Ewolucja spamu po zamknięciu McColo w listopadzie 2008 r.

Spam zakłóca komunikację elektroniczną, często całkowicie ją uniemożliwiając (przytłacza strukturę informacji), a tym samym zmniejsza zaufanie społeczeństwa do technologii informacyjnych. Jeśli jednak spam jest ograniczany, prawo do wolności wypowiedzi jest de facto ograniczane na rzecz prawa do ochrony nietykalności osobistej.

Również z opisanego powyżej powodu karanie spamerów jest bardzo skomplikowane i obecnie korzysta się z instytucji prawa cywilnego i administracyjnego, ponieważ prawo karne nie pozwala na ukaranie spamera.

Spam zawierający treści przestępcze lub inne oszukańcze treści jest określany mianem *scamu*. Oszustwa stanowią obecnie znaczną część spamu, a ich celem jest zdobycie zaufania użytkownika, zazwyczaj poprzez wykorzystanie socjotechniki, oraz skłonienie go do wykonania pożądanych działań (np. otwarcia załącznika do wiadomości e-mail, odwiedzenia wyświetlonego adresu URL itp.) Oszustwa mogą obejmować *phishing, złośliwe oprogramowanie, 419, oszustwa, oszukańcze loterie i oferty, oszustwa związane z darowiznami, oszustwa typu "cold call", oszustwa typu "Facebook like scam" itp.*



Schemat podziału oszustw

W tym miejscu zwrócę szczególną uwagę na trzy rodzaje oszustw: oszustwo **419**, oszustwo hakerskie i fałszywe **oferty.**

4.4.1. Oszustwo 419

Scam 419 to oznaczenie wiadomości e-mail, które są bardziej znane jako **listy nigeryjskie.** Oszustwa te są przykładem przeniesienia zwykłego przestępstwa (oszustwa) ze świata rzeczywistego do świata wirtualnego.

Dla ciekawości załączamy trzy bardzo różne wiadomości o charakterze oszustwa 419.

Wiadomość nr 1 - "Odziedziczyłeś ogromną sumę pieniędzy"**.**

Witaj, kochanie,

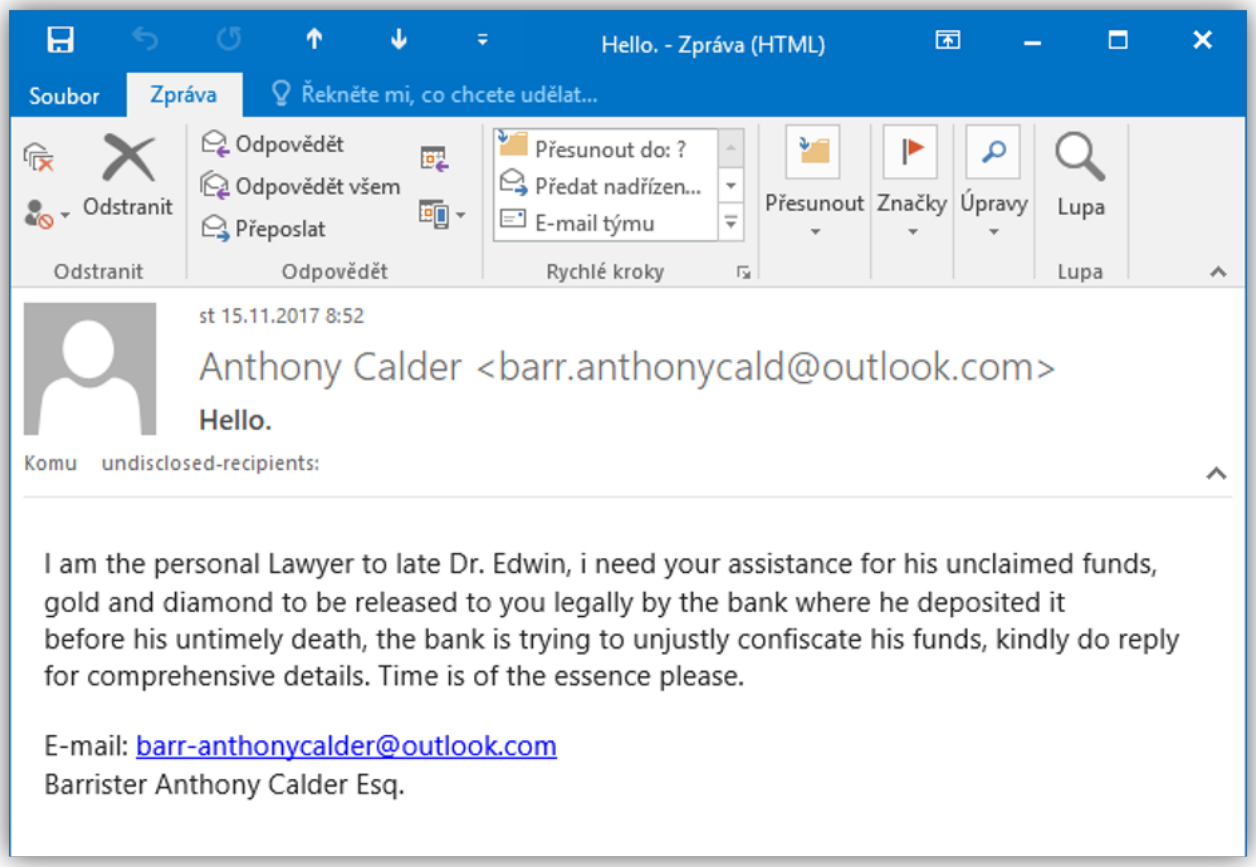
Jestem adw. Victoria Joseph, mam dla Pana wiadomość w sprawie mojego zmarłego klienta, który nosi takie samo nazwisko jak Pan. Wiem, że nie jestem z nim spokrewniona, ale jest on obywatelem Pana kraju, który wraz z najbliższą rodziną stracił życie w wypadku samochodowym w Togo.

Odszedł z sumą 2,7 mln dolarów, tymczasem jego bank chce przekazać świadczenia na rzecz któregoś z członków jego dalszej rodziny, ponieważ prezentację można przeprowadzić za pośrednictwem mojego biura. Szczerze mówiąc, te pieniądze należą do mojego zmarłego klienta, który nosi to samo nazwisko i obywatelstwo co Ty, mieszkał i pracował w Togo przez ponad 20 lat jako wykonawca, ale zginął w śmiertelnym wypadku samochodowym wraz z członkami swojej rodziny w 2009 r. Niedawno bank, w którym zdeponował te pieniądze, upoważnił mnie do przekazania ich jakiemuś członkowi jego rodziny, w przeciwnym razie zostaną one przekazane na konto skarbu państwa jako pieniądze porzucone.

Nie chcę, żeby tak się stało, ale problem polega na tym, że jego domniemana najbliższa rodzina zginęła w tym samym wypadku samochodowym, a wszystkie moje starania, żeby odnaleźć członków jego rodziny od czasu jego śmierci, spełzły na niczym, ponieważ za życia nigdy mi ich nie przedstawił.

Przyjacielu, właśnie dlatego podjąłem się tej misji, aby znaleźć kogoś, kto ramię w ramię ze mną upomni się o ten fundusz, aby pomóc naszym rodzinom i potrzebującym, zamiast pozwolić tym skorumpowanym urzędnikom państwowym przejąć te ciężko zarobione pieniądze i roztrwonić je, pozostawiając biedne masy na pastwę losu. To, że mogę się czepiać ciebie spośród milionów ludzi na Facebooku, oznacza po prostu, że to Bóg uczynił naszą drogę złą, więc pracujmy razem w jednym duchu, dzieląc się pieniędzmi tak, jak się o to prosi.
Proszę zaznaczyć swoje zainteresowanie tym roszczeniem, abym mógł przekazać Ci informacje dotyczące pracy i wytycznych.

Adwokat Victoria Joseph Esq.

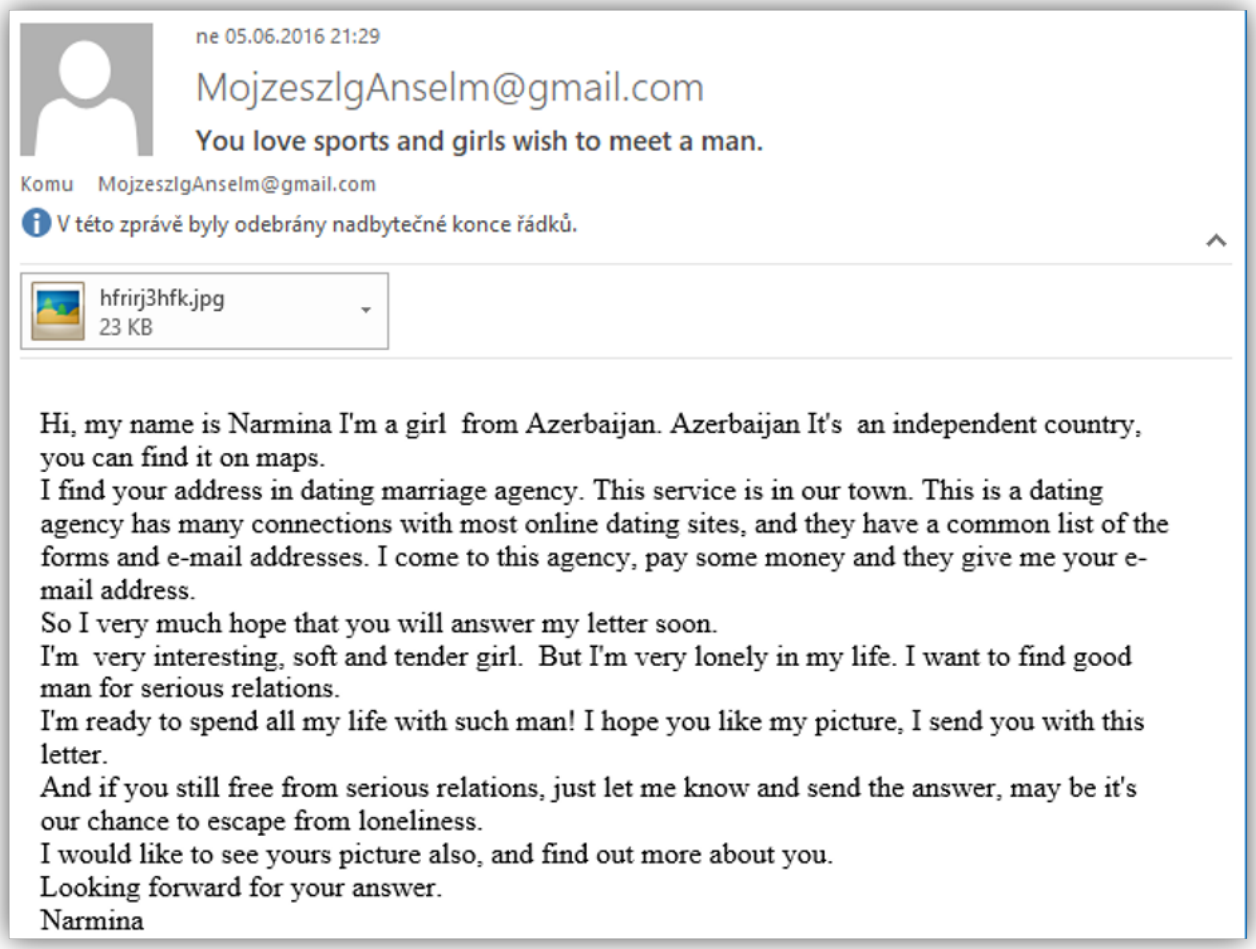


Wiadomość 2: "Jestem zakochana"

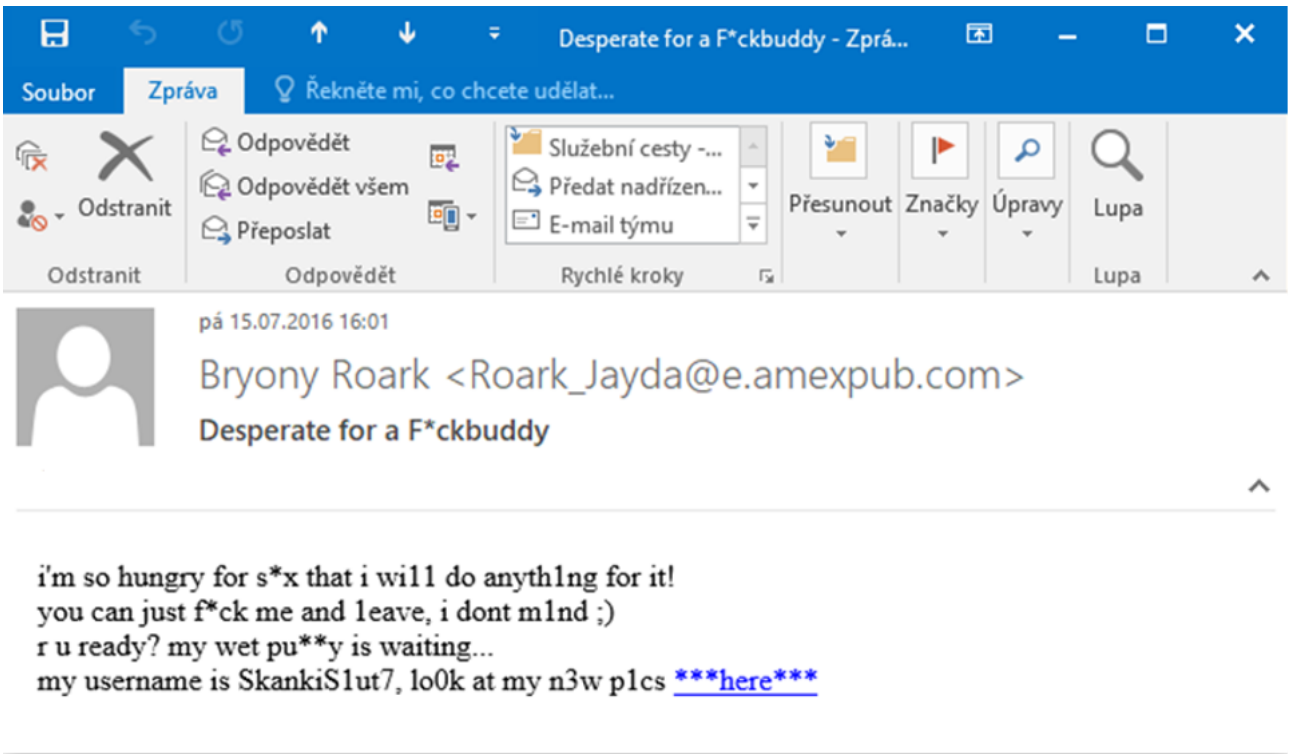
Cześć, kochanie.

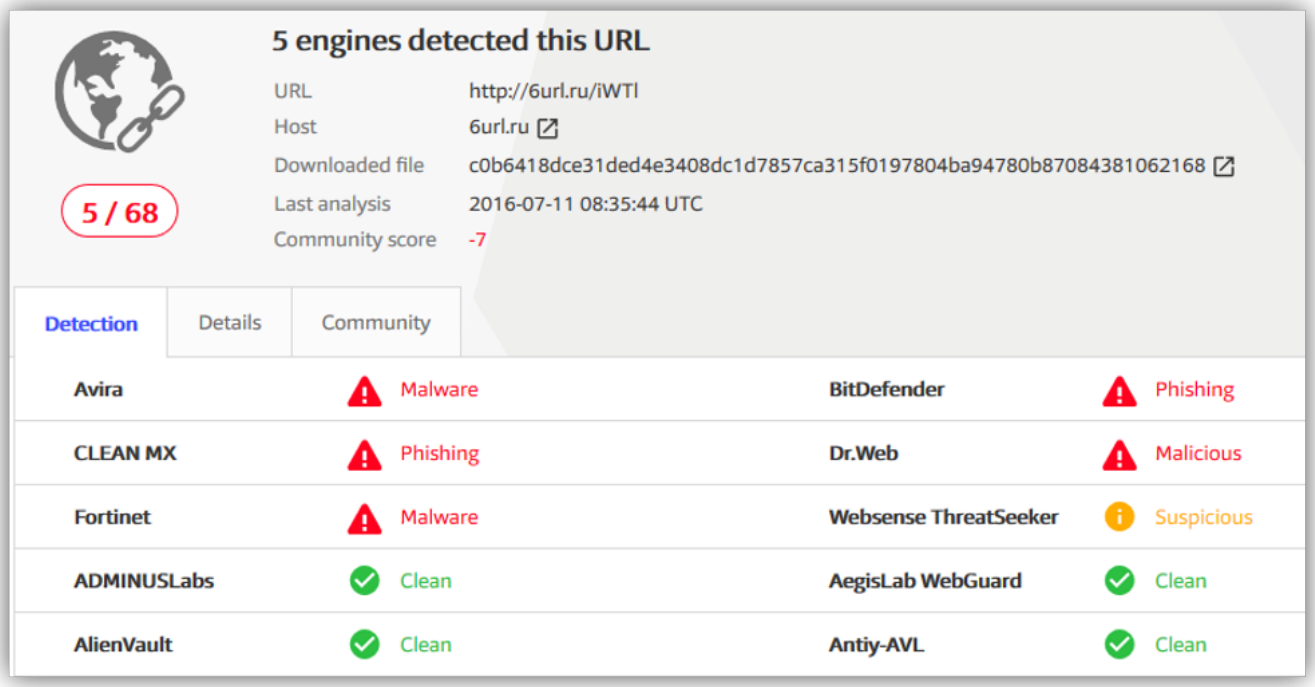
Nazywam się Joe Anita jestem kobietą, znam twoją tożsamość i chcę się dowiedzieć, że wiemy więcej o sobie i dzielić życie społeczne z kulturą i nie mam nic do powiedzenia, więc proszę mi odpowiedzieć, więc ja też wysłać moje dane do Ciebie i powiedzieć więcej o sobie w swoich zdjęciach. Bardzo dziękuję.

Z radością Anita



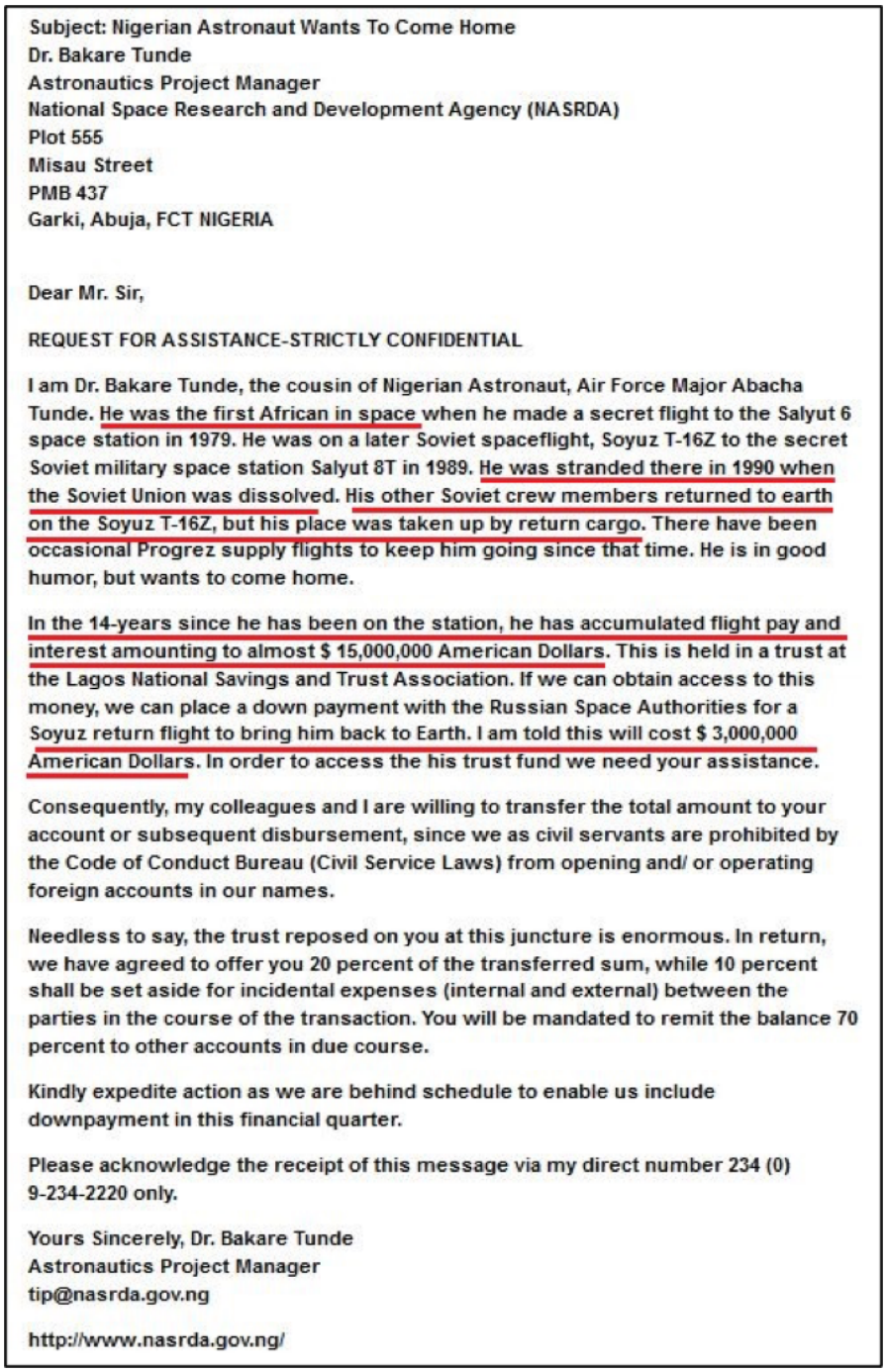
Wiadomość 3: "Szybki seks"





Raport nr 4 - Nigeryjski astronauta został zapomniany w kosmosie i musi wrócić do domu

Wieść o tym zaczęła się rozchodzić w 2004 r., kiedy to "pierwszy afrykański astronauta" przebywał w kosmosie bez przerwy przez 14 lat. Należy zauważyć, że długość pobytu przewyższała wszystkie czasy pobytu astronautów (być może nawet w ogóle). Najnowszą wersję tego scamu 419 otrzymałem w 2016 r. Chociaż bardzo współczuję temu wyimaginowanemu astronaucie (26 lat w kosmosie i samotnie), z pewnością nie zamierzam przyczyniać się do pomocy oszustom. Niestety, pomimo całkowicie bezsensownej treści i bezpodstawnych informacji zawartych w tym e-mailu, istnieje znaczna liczba osób, które chcą pomóc osobie w potrzebie (ze względu na tę pomoc, oszustwo to można również zakwalifikować jako *oszustwo związane z darowiznami*).



Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost $ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number 234 (0) 9-234-2220 only.

Yours Sincerely, Dr. Bakare Tunde
Astronautics Project Manager
tip@nasrda.gov.ng

http://www.nasrda.gov.ng/

Ze względu na charakter oszustwa, Scam 419 można w niektórych przypadkach zakwalifikować również jako phishing.

4.4.2. Hoax

Oszustwo to inna forma spamu lub wyłudzenia informacji. Oszustwo to termin oznaczający łańcuszki (łańcuszki wiadomości, takie jak *"przekaż dalej"*, *"jeśli nie wyślesz tego do 20 innych osób, to stanie się..."* itp.), które przedstawiają zniekształcone, fałszywe, wprowadzające w błąd lub w inny sposób nieprawdziwe informacje. Hoaxes często zawierają ostrzeżenia przed atakami, opisy niebezpieczeństwa, prośby o pomoc, apele, petycje, poparcie celebrytów, łańcuszki szczęścia, wiadomości żartobliwe, zdjęcia i filmy w prezentacjach, odgrywanie kotów i innych zwierząt itp.

4.4.3. Nieuczciwe oferty

Bardzo skuteczną formą oszustwa są różne oszukańcze oferty, które mogą być wysyłane masowo lub celowo. Obecnie takie oferty wysyłane są nie tylko pocztą elektroniczną, ale także za pośrednictwem wszelkich komunikatorów, portali społecznościowych, portali aukcyjnych itp.

Jeśli chodzi o **masowe rozsyłanie** oszukańczych ofert, można wymienić cały szereg działań opartych na zasadzie "piramidy" lub "samolotu", oferty dochodowej pracy w domu[6] , "gwarantowane" metody pomnażania pieniędzy (o najwyższym oprocentowaniu), oferty pożyczek (o najniższym oprocentowaniu), "świetne" oferty pracy itp.

Ukierunkowane wysyłanie oszukańczych ofert powinno również obejmować działania, które nie są zwykłym spamem, ale na przykład stanowią połączenie składania ofert na określony rodzaj towarów na portalach aukcyjnych i późniejszej komunikacji z użytkownikami, którzy przyjęli ofertę. Jest to tak zwane "oszustwo aukcyjne".

Oferta pracy w domu (masowe umieszczanie na Facebooku)

W dzisiejszych czasach zdecydowanie nie jest już regułą, że oferty są wysyłane masowo lub celowo pisane podejrzanym lub łamanym językiem czeskim (albo po angielsku lub rosyjsku); wręcz przeciwnie, celem atakującego jest przekonanie ofiary o całkowitej poprawności, powadze i "uczciwości" swoich działań. Na portalach aukcyjnych bardzo często w nieuczciwy sposób oferowane są różnego rodzaju urządzenia elektroniczne, zwłaszcza telefony komórkowe i komputery. Faktyczne oszustwo może polegać na przykład na zmianie istotnych informacji [np. kraju pochodzenia telefonu komórkowego; informacji, że telefon jest kopią (podróbką)] lub na niedostarczeniu towaru jako takiego (atakujący bardzo często prosi o zapłatę całości lub depozytu).

W środowisku internetowym pomysłowość napastników jest znaczna, dlatego warto zachować paranoję i nie ufać nieznanym osobom w przypadku jakichkolwiek ofert, reklam, a zwłaszcza wysyłania zaliczek lub płatności.

W przypadku oszukańczych ofert, gdy osoba atakująca próbuje uzyskać różne zaliczki lub inne płatności z góry, takie postępowanie może być karalne na podstawie **paragrafu 209** (Oszustwo) Kodeksu karnego.

Możliwości stosowania sankcji karnych w Republice Czeskiej

Jeśli chodzi o sankcje karne wobec spamerów i spamerów, to w Republice **Czeskiej nie są one obecnie w pełni (rozwiązane).** Brak jest zarówno krajowej, jak i międzynarodowej ochrony prawnej przed tym niepożądanym zachowaniem. Nawet Konwencja o cyberprzestępczości nie definiuje spamu jako przestępstwa.

Na przykład w **USA w przeszłości** skazywano spamerów z portalu[7] za rozsyłanie wiadomości-śmieci. Na przykład **Jeremy Jaynes** został skazany w 2007 r. przez sąd w Wirginii na 9 lat więzienia. Został skazany w 2003 r., a jako dowód posłużyło mu 53 000 wiadomości spamowych wysłanych w ciągu trzech dni. Prokurator powiedział jednak, że jego zdaniem Jaynes był odpowiedzialny za wysyłanie ponad 10 000 000 wiadomości spamowych dziennie, co miało mu przynosić miesięcznie około 750 000 USD.

Ponieważ spamu nie można zaklasyfikować jako jednej z form szkodliwego zachowania, bardzo trudno jest karać spam per se za pomocą prawa karnego. Można to zrobić tylko w przypadku poszczególnych rodzajów spamu. W niektórych przypadkach może istnieć możliwość sankcjonowania gromadzenia adresów e-mail, jeśli takie gromadzenie wypełnia znamiona przestępstwa nieuprawnionego posługiwania się danymi osobowymi na podstawie paragrafu **180** (Nieuprawnione posługiwanie się danymi osobowymi) Kodeksu karnego. Jeśli spam zawiera złośliwe oprogramowanie lub ma na celu dokonanie oszustwa, działalność spamera może zostać ukarana na mocy przepisów dotyczących złośliwego oprogramowania lub phishingu.

Możliwości ścigania karnego w Polsce

W Polsce przesyłanie niezamówionych informacji handlowych za pomocą środków komunikacji elektronicznej jest uznawane za wykroczenie i podlega karze grzywny. Reguluje to ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r. Nr 144, poz. 1204):

Kto wysyła niezamówione informacje handlowe za pomocą środków komunikacji elektronicznej, podlega karze grzywny.

(2) Ściganie przestępstwa, o którym mowa w ustępie 1, odbywa się na wniosek pokrzywdzonego.

Art. 25 Orzekanie w sprawach o wykroczenia, o których mowa w art. 23 i 24, odbywa się w trybie przepisów o postępowaniu w sprawach o wykroczenia.

---

[1] Na temat klasyfikacji spamu por. np. GONZÁLES-TALAVÁN, Guillermo. Prosty, konfigurowalny filtr antyspamowy SMTP. *Computers & Security*, 2006, vol. 25, nr 3, s. 229-236.

[2] Por. np. *statystyki spamu*. [online]. [cit.14.8.2016]. Dostępny pod adresem: https://www.spamcop.net/spamstats.shtml

Statystyki i fakty dotyczące spamu [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://www.spamlaws.com/spam-stats.html

[3] Oryginalne źródło internetowe: http://www.trustedsource.org/TS?do=home [cytowany 12 lutego 2010].

[4] Nie da się dokładnie określić, jaki procent wszystkich wiadomości e-mail stanowi spam. Różne dostępne źródła podają różne, czasem bardzo zróżnicowane liczby. Na przykład jeden z dostawców rozwiązań antyspamowych, firma POSTINI, podała w marcu 2005 r., że w ciągu 24 godzin 10 na 12 wiadomości e-mail było spamem. Na temat częstotliwości występowania spamu por. np. *Phishing bez tajemnic*. Praga: Grada, 2007, s. 22, SCHRYEN, Guido. Wpływ umieszczania adresów e-mail w Internecie na otrzymywanie spamu: analiza empiryczna. *Computers & Security*, 2007, vol. 26, nr 5, s. 361-372.

[5] *Złośliwe oprogramowanie, chaos i zatrzymanie McColo.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/

[6] Oferty te mogą zawierać prośbę typu: *"prześlij nam 10 dolarów na swoje konto, a my wyślemy Ci instrukcje, jak zarobić 8847 dolarów miesięcznie".* Po drugie, te oferty pracy nie wymagają żadnych opłat z góry, wymagają jedynie rejestracji użytkownika. Po faktycznym zarejestrowaniu się atakujący otrzymuje dane osobowe użytkownika. Następnie na adres e-mail użytkownika może zostać wysłana wiadomość z firmy, zawierająca np. złośliwe oprogramowanie itp.

[7] *Skazany spamer kwestionuje prawo obowiązujące w Va.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm

Czołowy spamer skazany na prawie cztery lata. [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://www.pcworld.com/article/148780/spam.html

Spamer Buffalo idzie do więzienia na 7 lat za spamowanie. [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality

4.7. Phishing, Pharming, Spear Phishing, Vishing, Smishing

Termin phishing jest najczęściej używany w odniesieniu do oszukańczych lub podstępnych działań mających na celu uzyskanie informacji o użytkowniku, takich jak nazwa użytkownika, hasło, numer karty kredytowej, PIN itp.

W **węższym znaczeniu tego słowa,** phishing to działanie, które wymaga od użytkownika odwiedzenia oszukańczej strony internetowej (np. wyświetlającej stronę bankowości internetowej, sklepu internetowego itp.

W **szerszym znaczeniu** phishing można zdefiniować jako każde oszukańcze działanie mające na celu wzbudzenie zaufania u użytkownika, obniżenie jego czujności lub zmuszenie go w inny sposób do zaakceptowania scenariusza przygotowanego wcześniej przez atakującego. W tym szerszym znaczeniu użytkownik nie musi już wypełniać danych, ale otrzymuje wiadomość (lub jest przekierowywany na stronę) zawierającą zazwyczaj złośliwe oprogramowanie, które samo zbiera dane. Do tego szerszego pojęcia można zaliczyć również oszustwa związane z darowiznami itp.

W obu przypadkach użytkownik, który jest celem ataku phishingowego, zostaje oszukany, różnica polega przede wszystkim na poziomie interakcji wymaganym od użytkownika.

Istotą phishingu jest wykorzystanie socjotechniki. Phishing może być również przeprowadzany w świecie rzeczywistym (zob. oszustwa itp.), ale świat wirtualny pozwala atakującemu na wysyłanie fałszywych wiadomości do ogromnej liczby potencjalnych ofiar przy minimalnym wysiłku. Phishing można, ze sporą dozą przesady, porównać do *"bombardowania dywanowego"*. Podobnie jak w przypadku bombardowania dywanowego, phishing jest ukierunkowany na stosunkowo nieokreśloną liczbę ofiar, aby dać atakującemu szansę na sukces. Na przykład firma Google podała w 2014 r., że oszustwo o charakterze naprawdę dobrego phishingu jest w 45% skuteczne w przechwytywaniu danych użytkownika.[1]

Phishing nie koncentruje się wyłącznie na wiadomościach e-mail. Z phishingiem można spotkać się w wiadomościach błyskawicznych (Skype, ICQ, Jabber itp.), sieciach społecznościowych, wiadomościach SMS i MMS, czatach, oszustwach (fałszywe oferty pracy, towarów itp.), fałszywych aplikacjach przeglądarek[2] itp.

Phishing w ścisłym tego słowa znaczeniu

Zasada działania *"klasycznego"* ataku phishingowego polega najczęściej na wysłaniu do ofiary wiadomości phishingowej, która na pierwszy rzut oka nie wzbudza żadnych podejrzeń, że jest to oszukańcza wiadomość. W takiej wiadomości e-mail zwykle znajduje się łącze, które użytkownik powinien kliknąć.

Po kliknięciu załączonego łącza użytkownik jest przenoszony na fałszywą stronę internetową, która wyglądem i działaniem prawie nie różni się od oryginalnej, poprawnej skrzynki pocztowej. Jeżeli jest to imitacja strony internetowej, która może być wykorzystywana do dokonywania płatności, uzyskiwania dostępu do zabezpieczonych kont, zarządzania nimi itp. to dane wprowadzone przez użytkownika są automatycznie przesyłane do osoby atakującej.[3] W ten sposób atakujący może uzyskać dane identyfikacyjne użytkowników internetowych usług bankowych, dostęp do indywidualnych kont bankowych użytkowników zagrożonych systemów, uzyskać numery identyfikacyjne i inne dane na kartach płatniczych, które następnie mogą być wykorzystane do dokonywania płatności w środowisku internetowym itp.

Właściwy atak phishingowy przebiega w kilku etapach.[4]

1. **Planowanie ataku phishingowego**

W tej fazie ataku phishingowego wybierany jest cel (grupa użytkowników) oraz metoda, która zostanie użyta do ataku. Ocenia się, w jaki sposób cel jest zabezpieczony technicznie, jakie jest ryzyko ujawnienia tożsamości atakującego itp.

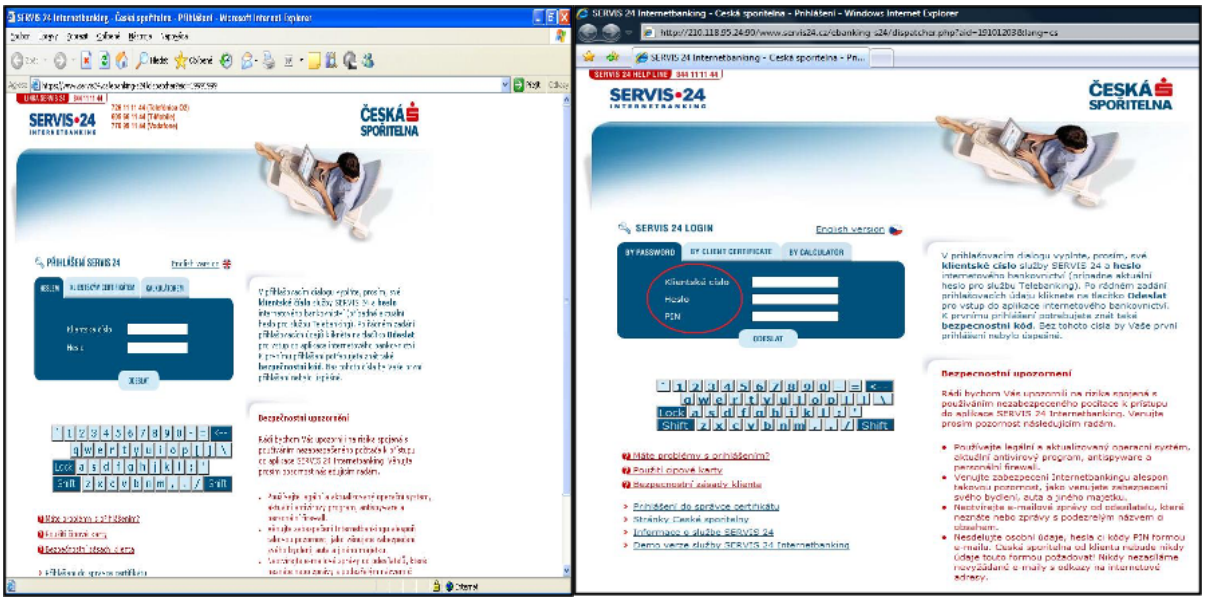
2. **Tworzenie warunków do przeprowadzenia ataku phishingowego**

Na tym etapie wdrażane jest techniczne rozwiązanie ataku phishingowego. Atakujący uzyskuje listę adresów e-mail użytkowników, do których ma zostać wysłana wiadomość phishingowa, tworzona jest skrzynka pocztowa z danymi, do której system wysyła uzyskane dane użytkowników, tworzona jest zaufana wiadomość, która następnie jest rozsyłana do użytkowników.

3. **Niestandardowy atak phishingowy**

Wiadomość phishingowa jest dostarczana do poszczególnych użytkowników i w zależności od jakości przetwarzania tej wiadomości oraz innych czynników (doświadczenie użytkownika, świadomość użytkownika na temat phishingu, oprogramowanie antyphishingowe celu itp. Na tym etapie ataku phishingowego użytkownik po raz pierwszy styka się z wiadomością phishingową.

Pretekstem jest często informacja o błędzie w systemie bezpieczeństwa firmy lub inne ostrzeżenie, które ma dać użytkownikowi poczucie, że wiadomość jest autentyczna. Po uruchomieniu interaktywnego łącza osoba zostaje przekierowana na stronę stworzoną przez atakującego, która wiernie naśladuje stronę internetową oryginalnej instytucji finansowej. Użytkownik jest proszony o podanie danych do logowania, zwykle obejmujących numer karty i kod PIN. Wypełnione dane są przesyłane na adres phishera, który następnie wypłaca część lub całość środków z konta, wyrządzając szkodę klientowi (patrz ilustracja poniżej).



Miejsce oryginalne (po lewej) i miejsce podrobione (po prawej)

4. **Gromadzenie danych**

Napastnik pobiera dane wprowadzone przez poszczególnych użytkowników zagrożonego systemu na fałszywej stronie internetowej.

5. **Wypłata środków lub innych korzyści z ataku phishingowego**

Napastnik wykorzystuje uzyskane dane do wejścia na rzeczywiste konta bankowe poszczególnych użytkowników i wypłaty środków. Przelewając środki na inne rachunki, zwłaszcza zagraniczne, rozcieńczając je i stosując inne techniki, zrabowane środki stają się praktycznie niemożliwe do wyśledzenia.

Bardzo trudno jest określić, ile ataków phishingowych przeprowadzanych jest każdego dnia na całym świecie. Podobnie, trudno jest określić, ilu klientów zagrożonych firm odpowiada na wiadomości phishingowe. Szacuje się, że stopa zwrotu wynosi około 0,01 i 0,1%.[5]

Prognozy z 2007 roku przewidywały, że liczba "klasycznych" oszustw lub kampanii phishingowych wzrośnie w przyszłości.[6] Prognozy te częściowo się sprawdziły, ponieważ liczba "klasycznych" kampanii phishingowych maleje, ale phishing w szerszym znaczeniu wzrasta[7] , w szczególności pojawiają się nowe modyfikacje phishingu lub powiązania między phishingiem a innymi rodzajami ataków (złośliwym oprogramowaniem, botnetami itp.).

Phishing w szerszym znaczeniu

Aby przedstawić phishing w szerszym ujęciu, wspomnę o czterech kampaniach, które miały miejsce w Czechach i zakończyły się mniejszym lub większym sukcesem. Ataki te nie są oczywiście jedynymi atakami phishingowymi w szerszym znaczeniu, które miały miejsce w Republice Czeskiej. Powodem wyboru tych czterech konkretnych ataków jest chęć zwrócenia szczególnej uwagi na nowatorskie podejście atakującego oraz odpowiednie połączenie ataku technicznego z socjotechniką. W szczególności są to następujące ataki:

1. **Zadłużenie/Bank/Ekzekucja**
2. **Poczta czeska**
3. **Święta i prezenty**
4. **Seznam.cz - hasło jednorazowe**

4.6.1.1. Zadłużenie/Bank/Ekzekucja [8]

Kampania phishingowa, znana pod fachową nazwą DBE, uderzyła na masową skalę w Czechach w 2014 roku (a pogłosy tej kampanii trwały co najmniej do końca 2015 roku).[9] Sam atak był bardzo precyzyjnie przygotowany i obejmował zarówno sam phishing, jak i dystrybucję złośliwego oprogramowania (na komputer i urządzenie mobilne). Cały atak można podzielić na następujące etapy:

1. **Kampania phishingowa**
2. **Instalowanie złośliwego oprogramowania na komputerze**
3. **Dostęp do bankowości internetowej**
4. **Instalowanie złośliwego oprogramowania na urządzeniu mobilnym**
5. **Przelew i wypłata środków**

Ad 1) **Kampania phishingowa**

Pierwszym warunkiem skutecznego pozyskania środków przez atakujących była duża kampania phishingowa, na którą odpowiedziałaby wystarczająca liczba osób. Faktyczne wysyłanie oszukańczych e-maili zostało rozłożone na trzy kolejne fale wiadomości phishingowych:

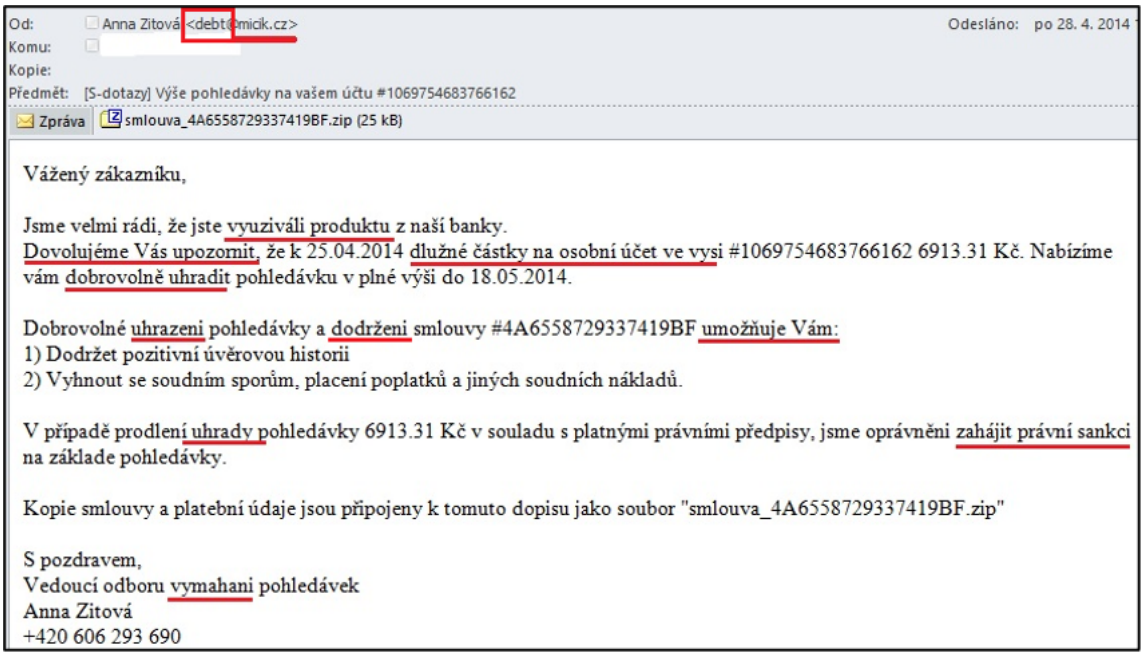
I. **Zadłużenie** (zadłużenie@....); marzec-kwiecień **2014 r.**

II. **Bank** (bank@....); maj - czerwiec **2014 r.**

III. **Egzekucje** (emisja@...); lipiec - wrzesień 2014 r.

Poszczególne kampanie miały na celu podniesienie "jakości" własnych wiadomości e-mail, a w szczególności lepsze wykorzystanie socjotechniki w stosunku do zamierzonych ofiar w regionie docelowym, tj. w Czechach. Wszystkie wspomniane kampanie phishingowe miały jednak co najmniej dwie cechy wspólne. Po pierwsze, załącznik do wysyłanej wiadomości zawsze zawierał plik udający dokument tekstowy, ale był to plik wykonywalny, czyli złośliwe oprogramowanie: Trojan.[10] Drugą wspólną cechą było to, że inżynieria społeczna wykorzystywała obawy osób, z którymi nawiązano kontakt, przed ewentualnymi sporami sądowymi, w ostatnim przypadku przed wykluczeniem.

Pierwsza fala ataków phishingowych wykorzystywała bardzo słaby język czeski i była wysyłana z różnych domen, które nie są w pełni godne zaufania, jeśli chodzi o windykację należności zarejestrowanych w Czechach (np. micik.cz lub dhome.cz itp.). Wykorzystano różne nazwiska osób i istniejące numery telefonów, które można znaleźć w Internecie (osoba, która była właścicielem numeru, nie miała nic wspólnego z samym atakiem).


Od: Anna Zitová <debt@micik.cz> Odesláno: po 28. 4. 2014
Komu:
Kopie:
Předmět: [S-dotazy] Výše pohledávky na vašem účtu #1069754683766162
Zpráva smlouva_4A6558729337419BF.zip (25 kB)

Vážený zákazníku,

Jsme velmi rádi, že jste vyuziváli produktu z naší banky.
Dovolujéme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve vysi #1069754683766162 6913.31 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 18.05.2014.

Dobrovolné uhrazeni pohledávky a dodrženi smlouvy #4A6558729337419BF umožňuje Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

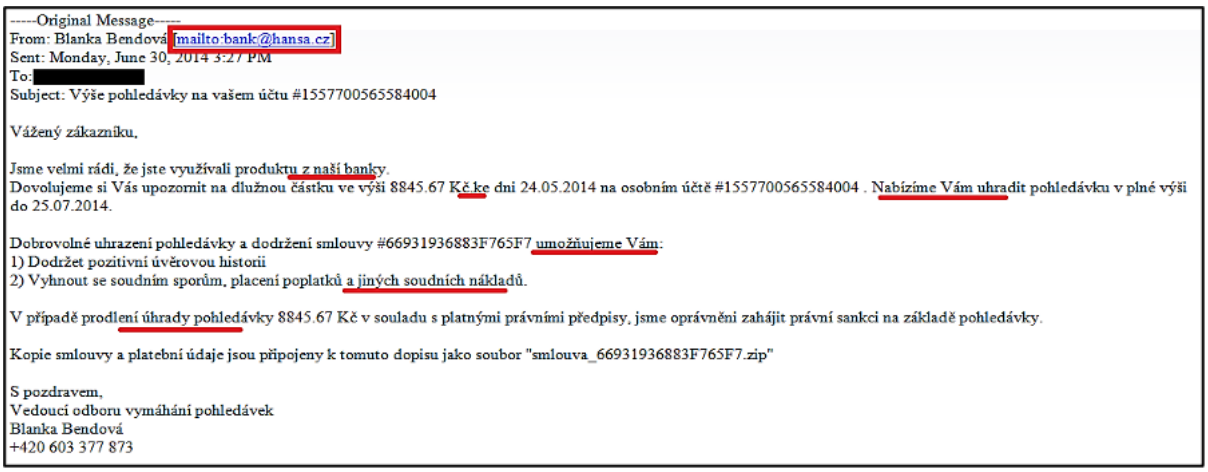
V případě prodlení uhrady pohledávky 6913.31 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základe pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_4A6558729337419BF.zip"

S pozdravem,
Vedoucí odboru vymahani pohledávek
Anna Zitová
+420 606 293 690

Oszukańcze wiadomości e-mail wysyłane w ramach akcji "Fala zadłużenia

W drugiej edycji nastąpiła poprawa w zakresie używania języka czeskiego.


-----Original Message-----
From: Blanka Bendová [mailto:bank@hansa.cz]
Sent: Monday, June 30, 2014 3:27 PM
To: [redacted]
Subject: Výše pohledávky na vašem účtu #1557700565584004

Vážený zákazníku,

Jsme velmi rádi, že jste využívali produktu z naší banky.
Dovolujeme si Vás upozornit na dlužnou částku ve výši 8845.67 Kč ke dni 24.05.2014 na osobním účtě #1557700565584004 . Nabízíme Vám uhradit pohledávku v plné výši do 25.07.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #66931936883F765F7 umožňujeme Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení úhrady pohledávky 8845.67 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základě pohledávky.

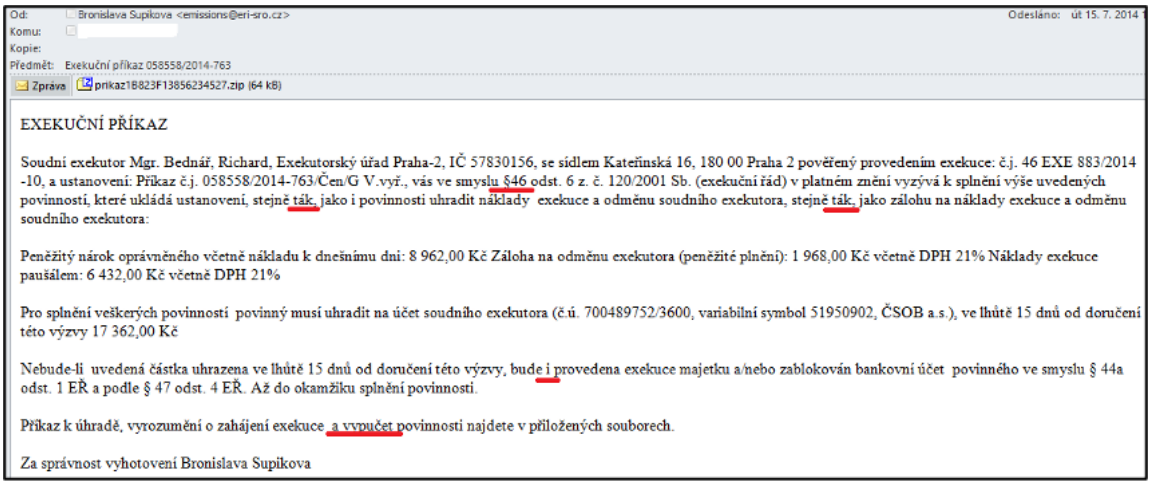
Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_66931936883F765F7.zip"

S pozdravem,
Vedoucí odboru vymáhání pohledávek
Blanka Bendová
+420 603 377 873

Oszukańcze wiadomości e-mail wysyłane w ramach fali bankowej

W czasie, gdy zaczęły pojawiać się ataki phishingowe, różne organizacje zajmujące się bezpieczeństwem i zespoły CSIRT[11] , a także środki masowego przekazu, publikowały ostrzeżenia, w tym instrukcje, jak podchodzić do takich wiadomości. [12]

Obie kampanie okazały się stosunkowo udane, ale najbardziej skuteczny okazał się atak, w którym oszukańcza wiadomość e-mail była ostrzeżeniem (zaproszeniem) od komornika.


Od: Bronislava Supikova <emissions@eri-sro.cz> Odesláno: út 15. 7. 2014
Komu:
Kopie:
Předmět: Exekuční příkaz 058558/2014-763
Zpráva prikaz1B823F13856234527.zip (64 kB)

EXEKUČNÍ PŘÍKAZ

Soudní exekutor Mgr. Bednář, Richard, Exekutorský úřad Praha-2, IČ 57830156, se sídlem Kateřinská 16, 180 00 Praha 2 pověřený provedením exekuce: č.j. 46 EXE 883/2014 -10, a ustanovení: Příkaz č.j. 058558/2014-763/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění výše uvedených povinností, které ukládá ustanovení, stejně tak, jako i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, stejně tak, jako zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 8 962,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 968,00 Kč včetně DPH 21% Náklady exekuce paušálem: 6 432,00 Kč včetně DPH 21%

Pro splnění veškerých povinností povinný musí uhradit na účet soudního exekutora (č.ú. 700489752/3600, variabilní symbol 51950902, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 17 362,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

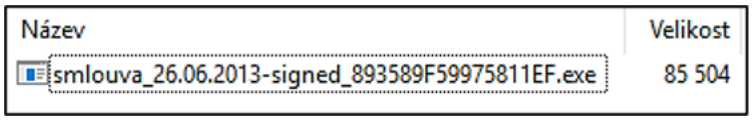
Za správnost vyhotovení Bronislava Supikova

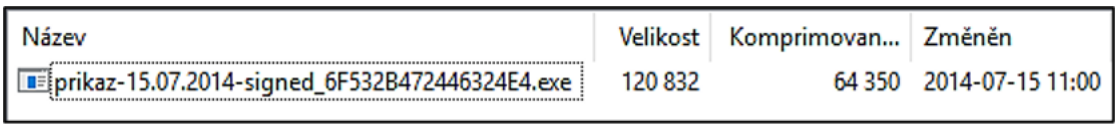
Oszukańcze wiadomości e-mail wysyłane w ramach Fali egzekucyjnej

Język czeski użyty w "zleceniu wykonania" zawierał głównie błędy w znakach diakrytycznych lub niektóre zdania były sformułowane w nieco bardziej zawiły sposób (najbardziej zauważalne błędy są podkreślone). Użyto jednak nazwisk prawdziwych komorników, których można znaleźć w Internecie (wspomniany komornik nie miał nic wspólnego z rzeczywistym atakiem), a także realnie wyglądających numerów egzekucyjnych.

Ad 2) Instalowanie złośliwego oprogramowania na komputerze

Jak wspomniano wcześniej, wszystkie kampanie phishingowe zawierały w załączniku do wysłanej wiadomości złośliwe oprogramowanie: TrojanDownloader (tj. złośliwe oprogramowanie przeznaczone do pobierania kolejnych złośliwych programów). To złośliwe oprogramowanie zostało zaprojektowane głównie z myślą o systemie operacyjnym Windows XP, dla którego wsparcie zakończyło się w marcu 2014 roku.





Plik wykonywalny (złośliwe oprogramowanie) zawarty w załączniku oszukańczej wiadomości e-mail

Po uruchomieniu załącznika złośliwe oprogramowanie (trojan bankowy) *"Tinba"* było instalowane i pobierane z Internetu w tle, podczas gdy użytkownikowi pokazywano umowę lub polecenie wykonania w edytorze tekstu.[13]

Złośliwe oprogramowanie zapisało się w katalogu: **Users/particular** *user/AppData/Roaming/brothel*. W tym katalogu można było znaleźć plik ate.exe, który został utworzony po otwarciu pliku wykonywalnego w wiadomości phishingowej. Jednocześnie w rejestrze został utworzony odpowiedni klucz w gałęzi **HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun**. W ten sposób można było sprawdzić, czy złośliwe oprogramowanie pochodzi z tego ataku.

Ad 3) Dostęp do bankowości internetowej

Następnym krokiem napastnika było czekanie, aż ofiara zaloguje się do bankowości internetowej. Szkodliwe oprogramowanie na komputerze jest w stanie rejestrować komunikację między użytkownikiem a bankowością internetową, a osoba atakująca może monitorować tę komunikację. Użytkownik miał minimalne szanse na wykrycie rzeczywistego ataku, ponieważ adres URL w przeglądarce należał do banku, a komunikacja była bezpieczna (HTTPS).

*"Kradzież poufnych danych odbywa się poprzez umieszczenie złośliwego kodu na oficjalnych stronach internetowych banków. Skrypty konfiguracyjne są pobierane z serwerów C&C (maszyn należących do atakujących, wykorzystywanych do kontrolowania botnetu) i odszyfrowywane w wyżej opisany sposób. Interesującą cechą jest ponowne wykorzystanie tego samego formatu pliku konfiguracyjnego, co w przypadku znanych trojanów bankowych Carberp i Spyeye. Dla każdego botoidu (unikalnej wartości identyfikującej środowisko użytkownika) na serwerze C&C przechowywana jest lista nazw użytkowników i haseł. W zależności od użytego banku pobierane są dodatkowe skrypty**: **hXXps://andry-shop.com/gate/get_html.js; hXXps://andry-shop.com/csob/gate/get_html.js;** *lub* **hXXps://yourfashionstore.net/panel/a5kGcvBqtV**, **które są** *pobierane, gdy ofiara odwiedza strony internetowe odpowiednio Česká spořitelna, ČSOB lub Fia."***[14]**

Ad 4) Instalowanie złośliwego oprogramowania na urządzeniu mobilnym

Kolejnym krokiem napastnika było przekonanie użytkowników o konieczności zwiększenia bezpieczeństwa podczas korzystania z bankowości internetowej. Powodem ostrzeżenia wydanego przez rzekomy bank (który w rzeczywistości był stroną kontrolowaną przez atakującego) było "zwiększenie" bezpieczeństwa połączenia. Ofiara otrzymywała stronę z możliwością wyboru systemu operacyjnego urządzenia mobilnego (Android OS, Windows Phone, Blackberry i iPhone), ale tylko wersja dla Androida pozwalała na pobranie złośliwego oprogramowania na telefon. Atakujący wybrali różne sposoby dystrybucji złośliwego oprogramowania na telefon - od zwykłego wysłania wiadomości SMS z odsyłaczem, z którego użytkownik miał pobrać program, po wysłanie wiadomości SMS z kodem QR.[15]

Vlastní znění zprávy: *Niestandardowy tekst raportu:*

CS-S24

Stáhněte si zabezpečení z *Pobierz zabezpieczenia z*

Bit.ly/Tp9JjU

Szkodliwe oprogramowanie pobrane i zainstalowane na urządzeniu mobilnym zostało wykryte przez Avast! jako Android: *Perkele-T*. Szkodliwe oprogramowanie zostało zaprojektowane w celu uzyskania dostępu i pełnej kontroli nad drugim sposobem uwierzytelniania (uwierzytelnianie dwuskładnikowe), którym w większości przypadków jest telefon komórkowy. Jeśli użytkownik korzystał z systemu operacyjnego innego niż Android, pojawiał się komunikat "Proszę *spróbować ponownie później*".

Ad 5) Przekazywanie i wycofywanie środków

Kolejnym krokiem napastnika było wypłacenie środków z konta zaatakowanej osoby na konto białych koni, które następnie miały wypłacić lub przelać gotówkę na inne konta. Mając pełną kontrolę (za pośrednictwem złośliwego oprogramowania) zarówno nad poświadczeniami dostępu do bankowości internetowej (zob. skompromitowany komputer), jak i nad drugorzędnymi środkami uwierzytelniania (zob. skompromitowany telefon komórkowy - gdzie wiadomości uwierzytelniające były przekazywane napastnikowi bez wyświetlania ich ofierze), napastnik był w stanie wprowadzić "legalne" polecenie przelewu pieniędzy.

Według raportu firmy Avast! za tym atakiem stali rosyjskojęzyczni napastnicy. Wiadomości SMS z zainfekowanego telefonu są przekazywane na numer 79023501934, który jest zarejestrowany w Astrachaniu w Rosji.[16]

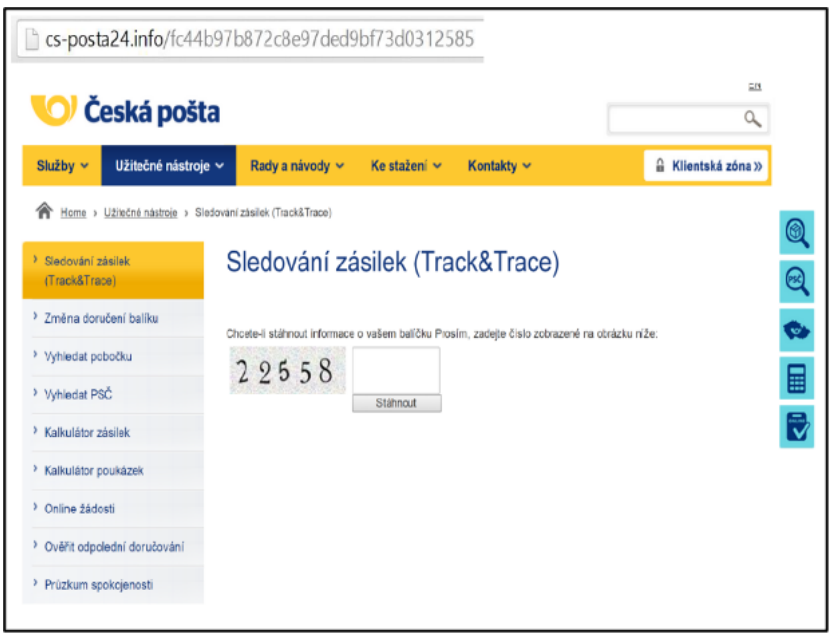
4.6.1.2. Poczta czeska

Drugi duży atak phishingowy rozpoczął się w listopadzie 2014 r. i trwał do grudnia 2014 r. Początkiem ataku była wiadomość phishingowa z powiadomieniem od "Poczty Czeskiej", że nie udało się skontaktować z Tobą jako odbiorcą przesyłki i że powinieneś pobrać informacje o przesyłce. Język czeski użyty w tej wiadomości phishingowej jest jednym z najgorszych, jakie można spotkać w phishingu. Najwyraźniej do wygenerowania tej wiadomości e-mail użyto jednego z automatycznych translatorów internetowych.

Oszukańcze e-maile zostały wysłane z adresów, które nie należą do Poczty Czeskiej. Były to na przykład następujące adresy: upport@cs-post.net, tracktrace@cs-post.net, cpost@cs-post.net, post@cs-post.net, zasilka@cs-post.net , które dzięki domenie ***en-post*** mogły wywołać u użytkownika przekonanie, że są to strony internetowe Poczty Czeskiej. Należy jednak zauważyć, że domena ***cs-post*** została zarejestrowana w domenie ***.net,*** podczas gdy rzeczywista strona internetowa Poczty Czeskiej jest zarejestrowana w domenie ***.cz*** (zob. https://www.ceskaposta.cz).

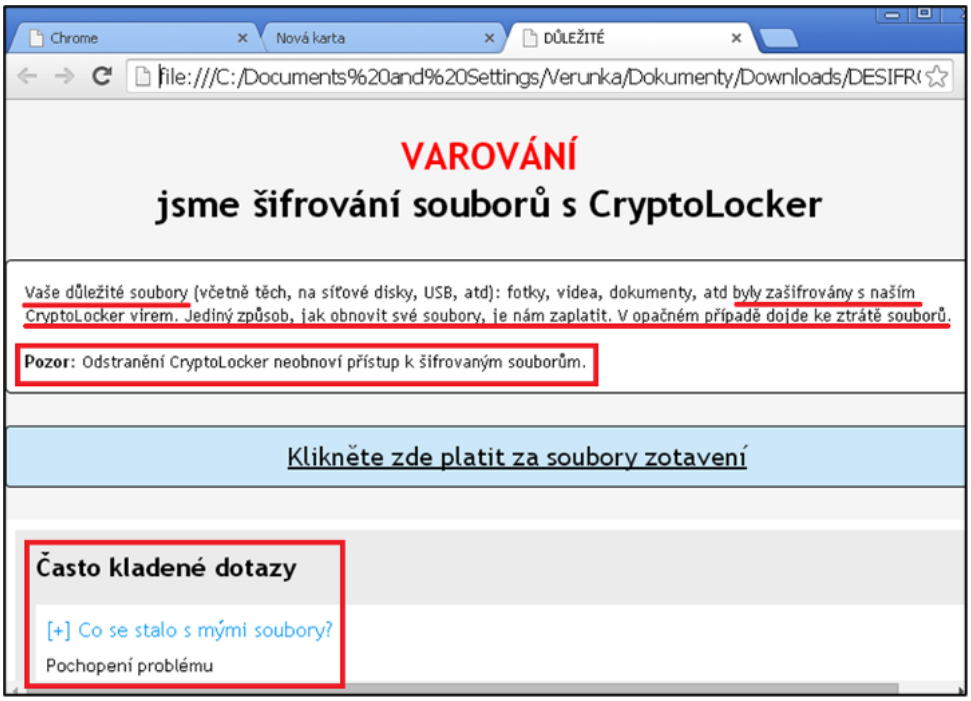
Obraz 64 - Oszukańcza wiadomość e-mail od "Poczty Czeskiej"

Jeśli użytkownik kliknął na pole: *pobierz informacje o przesyłce*, był przekierowywany na stronę, która przypominała rzeczywistą stronę internetową Poczty Czeskiej. W tym przypadku użytkownik został poproszony o wprowadzenie kodu zabezpieczającego (Captcha), a następnie mógł pobrać plik .zip zawierający "informacje o śledzonej przesyłce". Podobnie jak w poprzedniej kampanii phishingowej, załącznik zawierał plik wykonywalny (ransomware), jednak jego celem było zaszyfrowanie danych użytkownika.



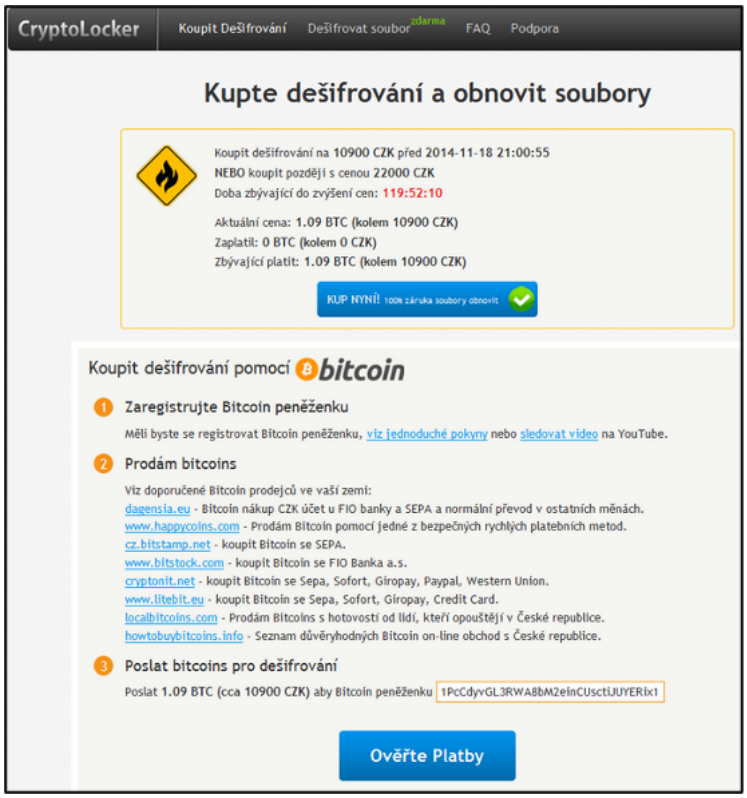
Fałszywa strona internetowa "Poczty Czeskiej"

Po zaszyfrowaniu danych użytkownik był proszony o zapłacenie pewnej sumy pieniędzy za dostarczenie klucza umożliwiającego odszyfrowanie zaszyfrowanych plików. Sama zachęta była już napisana w znacznie lepszej wersji języka czeskiego. Użytkownik mógł również poznać odpowiedzi na pytania, które go nurtowały.



Informacje wyświetlane użytkownikowi po zaszyfrowaniu jego danych

W tym czasie przywrócenie danych kosztowało 1,09 BTC, a użytkownik otrzymywał szczegółowe instrukcje, jak założyć portfel bitcoinów, gdzie i jak kupić bitcoiny oraz gdzie je wysłać, a także jak przeliczyć je na korony czeskie.



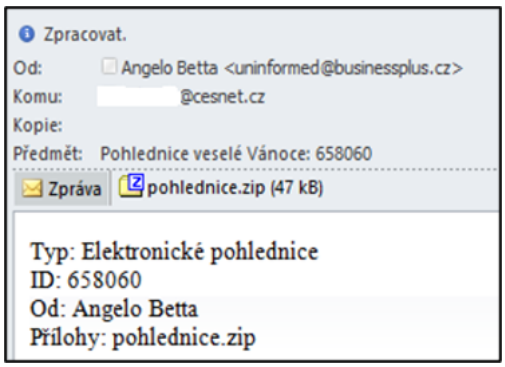
Instrukcje dotyczące odszyfrowywania plików[17]

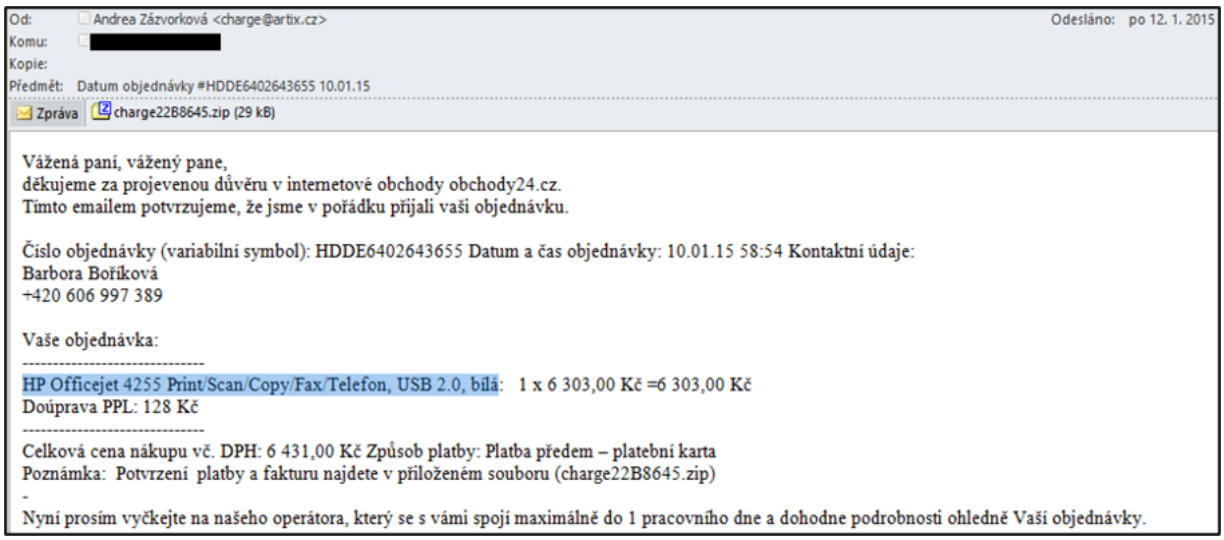
Sam atak jest o tyle specyficzny, że z jednej strony do kampanii phishingowej dołączono oprogramowanie ransomware, które natychmiast zaczęło szyfrować dane użytkownika, a z drugiej strony wykorzystano okres przedświąteczny, w którym wiele osób czeka na dostarczenie paczek, do przeprowadzenia własnego ataku. Te dwa czynniki sprawiły, że faktyczny atak był bardzo udany.

4.6.1.3. Święta i prezenty

Kolejny duży atak phishingowy rozpoczął się w grudniu 2014 r. (szczególnie w okresie świąt Bożego Narodzenia) i trwał do stycznia 2015 r. Atak został podzielony na dwie fazy. W pierwszej fazie do użytkowników wysyłane były wiadomości e-mail z życzeniami Wesołych Świąt za pośrednictwem e-kartki. W drugiej fazie w styczniu wysłano wiadomości z elektronicznym potwierdzeniem zamówienia. Komunikat informował użytkownika o dokonaniu zakupu towarów (np. drukarki, dysku twardego, aparatu fotograficznego itp.), za które zapłacił z góry kartą kredytową, powołując się na załączoną fakturę.

Oba ataki mają wspólny element, którym jest złośliwe oprogramowanie zawarte w załączniku do wiadomości e-mail. Konkretnie, był to koń trojański (*Kryptik*), który był przedstawiany jako wygaszacz ekranu. To złośliwe oprogramowanie było, podobnie jak w przypadku ataku opisanego w rozdz. 4.6.1.1 Dluh/Banka/Exekuce został skompresowany w pliku .zip. Po rozpakowaniu pliku .zip wielu użytkowników nie uznało pliku *.scr*[18] za program wykonywalny i w ten sposób zainfekowało swój komputer.





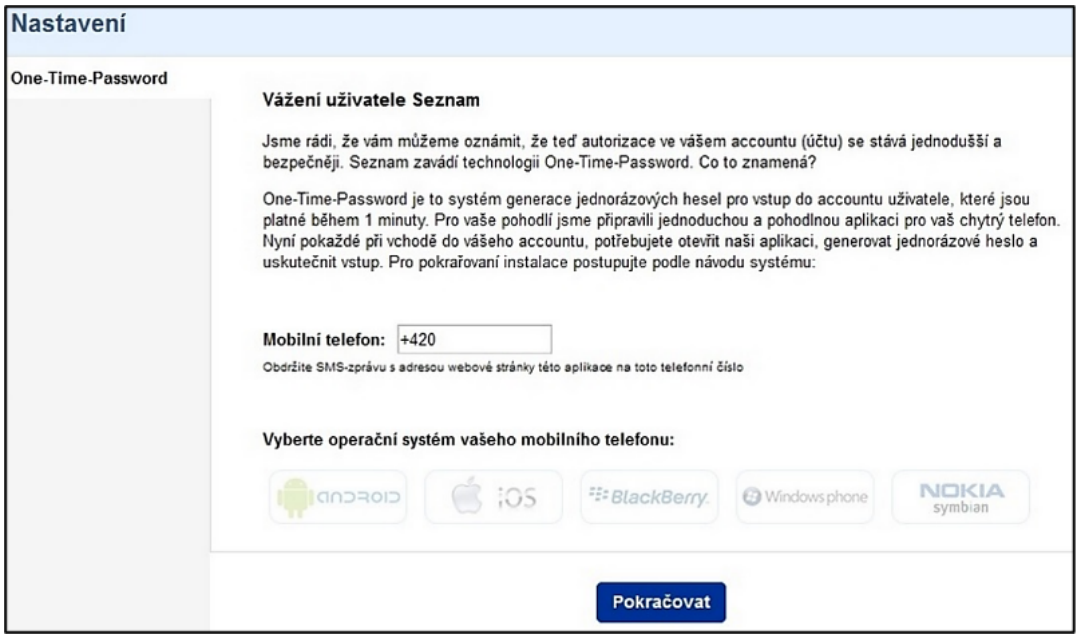
Przykładowe wiadomości phishingowe

Sam atak jest specyficzny, ponieważ wykorzystano w nim typ pliku, którego wielu użytkowników nie uważa za niebezpieczny, a także czas, w którym został przeprowadzony. Dzięki rozmaitym łańcuszkom użytkownicy przyzwyczaili się do otwierania kartek elektronicznych lub załączników, które wyglądają tak samo, bez dokładniejszego sprawdzenia ich zawartości. Drugi atak miał na celu sprawdzenie, czy użytkownik rzeczywiście zamówił jakieś towary, które nie zostały dostarczone ze względu na święta Bożego Narodzenia.

4.6.1.4. Seznam.cz - hasło jednorazowe

Najnowszy atak phishingowy świadczy o znaczącej zmianie taktyki atakujących. Napastnik nadal wykorzystuje fakt, że komputer został zainfekowany złośliwym oprogramowaniem. Napastnik może sam kontrolować komputer lub może go wynająć, np. jako część botnetu. Do faktycznej infekcji mogło dojść na przykład za pośrednictwem innej skrzynki pocztowej, podczas odwiedzania zainfekowanych witryn internetowych lub w inny sposób. W przypadku List - One Time Password[19] celem atakującego było przejęcie kontroli nad telefonem komórkowym użytkownika.

Złośliwe oprogramowanie, które zostało zainstalowane na komputerze, nakłaniało użytkowników do zainstalowania w telefonie komórkowym narzędzia, które ułatwiało pracę ze skrzynką pocztową i zwiększało bezpieczeństwo podczas logowania się na konto e-mail Seznam.cz. Następnie użytkownik jest prowadzony krok po kroku przez instalację aplikacji SeznamOTP z niezaufanego źródła. Po zakończeniu instalacji użytkownik otrzymuje swój "unikalny klucz licencyjny". W rzeczywistości jednak użytkownik zainstalował na swoim telefonie komórkowym złośliwe oprogramowanie.



Ekran główny instalacji SeznamOTP[20]

Ryzyko związane z tym ostatnim atakiem phishingowym **polega na tym, że "wiadomość phishingowa" nie została dostarczona za pośrednictwem** poczty elektronicznej **ani innych środków komunikacji, ale została wyświetlona użytkownikowi tylko w określonej sytuacji** (w tym przypadku po zalogowaniu się na skrzynkę pocztową seznam.cz)**, a inicjatorem tej wiadomości było złośliwe oprogramowanie zlokalizowane na już zainfekowanym komputerze. Drugim czynnikiem ryzyka jest fakt, że prośba o wprowadzenie ustawień bezpieczeństwa nie jest w żaden sposób powiązana z rachunkiem bankowym. Dlatego użytkownik może nie zdawać sobie sprawy z niebezpieczeństwa związanego z instalacją tej aplikacji.**

W Republice Czeskiej postępowanie mające charakter "klasycznego phishingu" może być karane na podstawie **paragrafu 209** (Oszustwo) Kodeksu karnego. Oszustwo dopełnia się poprzez wzbogacenie się. Stworzenie repliki strony internetowej i uzyskanie loginów i haseł mogłoby zostać zakwalifikowane jako przygotowanie lub próba popełnienia przestępstwa z paragrafu 209 Kodeksu karnego. Samo pozyskanie danych dostępowych, w tym numerów kont, numerów kart kredytowych i kodów PIN bez ich dalszego wykorzystania nie byłoby karalne.

Możliwości stosowania sankcji karnych w Republice Czeskiej

W przypadku połączonych form ataków phishingowych, w których do zainfekowania komputera wykorzystywane jest złośliwe oprogramowanie, zachowanie sprawcy musi być również karane na podstawie paragrafu **230** (Nieuprawniony dostęp do systemu komputerowego i nośnika informacji) Kodeksu karnego. Jeśli celem ataku phishingowego jest uzyskanie nieuzasadnionej korzyści dla siebie lub innej osoby, można również zastosować postanowienia **paragrafu 230(3)** kodeksu karnego.

W szczególnych przypadkach można również skorzystać z przepisów paragrafu **234** (Nieuprawnione użycie, fałszowanie i przerabianie środków płatniczych) kodeksu karnego.

Możliwości ścigania karnego w Polsce

Naruszenie tajemnicy komunikowania się (węszenie) - art. 267 § 3 Kodeksu karnego. Ten rodzaj przestępstw polega na pozyskiwaniu informacji zastrzeżonych, np. za pomocą snifferów, czyli programów przechwytujących dane (hasła i identyfikatory użytkowników). Czyn taki jest zagrożony karą do 2 lat pozbawienia wolności.

Artykuł 267. Bezprawne uzyskanie informacji

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając jej elektroniczne, magnetyczne, informatyczne lub inne szczególne zabezpieczenia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez upoważnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do których nie jest uprawniony, zakłada lub wykorzystuje urządzenie podsłuchowe, wizualne lub inne urządzenie albo oprogramowanie.

§ 4. Kto ujawnia informacje uzyskane w sposób określony w § 1-3 innej osobie, podlega takiej samej karze.

§ 5. Ściganie przestępstwa, o którym mowa w § 1-4, odbywa się na wniosek pokrzywdzonego.

4.6.2. Pharming

Pharming[21] stanowi bardziej wyrafinowaną i niebezpieczną formę phishingu. Jest to atak na serwer Systemu Nazw Domen (DNS), który rozwiązuje nazwę domeny na adres IP. Atak następuje po wpisaniu przez użytkownika w przeglądarce internetowej adresu serwera WWW, do którego chce uzyskać dostęp. Połączenie nie jest jednak nawiązywane z odpowiednim adresem IP oryginalnego serwera WWW, ale z innym, sfałszowanym adresem IP. Z

reguły strona internetowa pod fałszywym adresem bardzo dokładnie imituje oryginalną stronę i jest od niej de facto nieodróżnialna. Następnie użytkownik wprowadza dane uwierzytelniające do logowania, które zostały uzyskane przez atakującego. Atak ten jest zwykle przeprowadzany podczas uzyskiwania przez użytkownika dostępu do witryny bankowości internetowej.

"Fałszywe strony internetowe mogą być wykorzystywane do instalowania wirusów lub koni trojańskich na komputerach użytkowników, a także do pozyskiwania informacji osobistych lub finansowych, które mogą być następnie wykorzystane do kradzieży tożsamości. Pharming jest szczególnie niebezpieczną formą cyberprzestępczości, ponieważ w przypadku zainfekowania serwera DNS użytkownik może stać się ofiarą nawet wtedy, gdy na jego komputerze nie jest zainstalowane żadne złośliwe oprogramowanie. Nawet jeśli użytkownik podejmie środki ostrożności, takie jak ręczne wpisywanie adresów internetowych lub korzystanie tylko z zaufanych zakładek, nie jest chroniony przed tego typu atakiem, ponieważ niepożądane przekierowanie następuje po wysłaniu przez komputer żądania połączenia."[22]

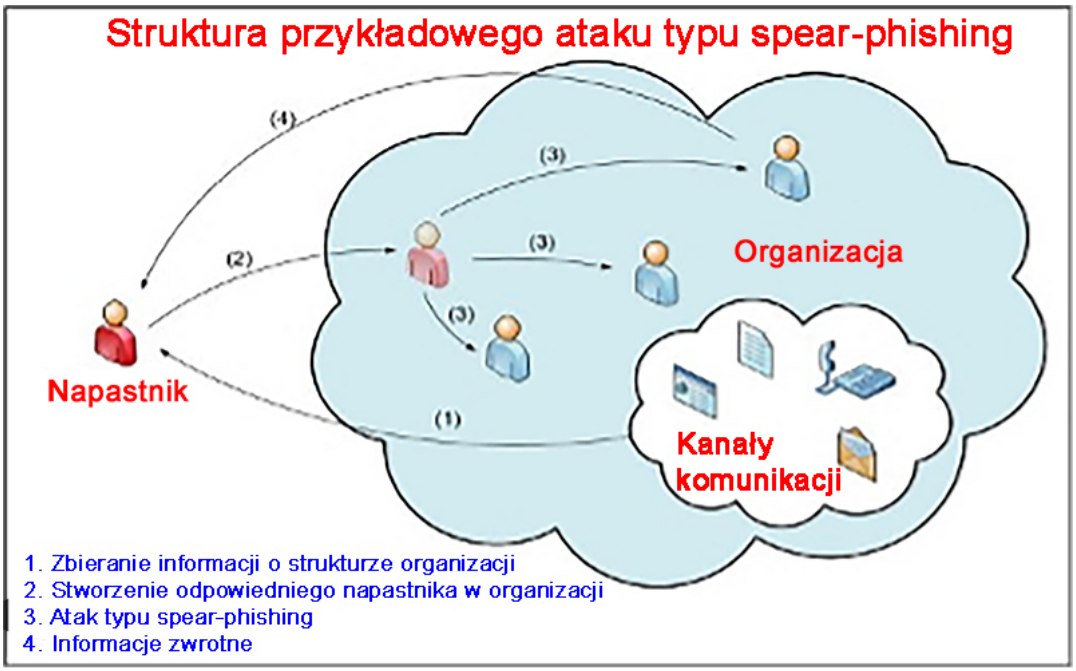
Druga typowa metoda pharmingu polega na zainfekowaniu komputera użytkownika końcowego złośliwym oprogramowaniem, co pozwala na obniżenie poziomu bezpieczeństwa. To złośliwe oprogramowanie modyfikuje plik hosts w celu przekierowania ruchu z miejsca docelowego i przekierowania użytkownika do fałszywej witryny.

Sankcje karne są podobne jak w przypadku phishingu.

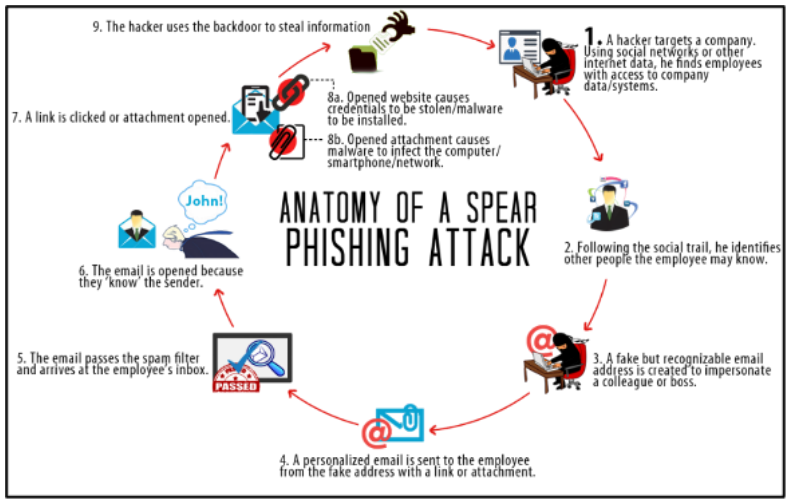
4.6.3. Spear Phishing

Spear phishing jest formą ataku phishingowego, z tą jednak różnicą, że spear phishing jest atakiem precyzyjnie ukierunkowanym, w przeciwieństwie do phishingu, który jest raczej atakiem ogólnym (losowym). Celem ataku jest zazwyczaj określona grupa, organizacja lub osoba, a konkretnie informacje i dane znajdujące się w posiadaniu tej organizacji (np. własność intelektualna, dane osobowe i finansowe, strategie biznesowe, informacje niejawne itp.)

Różnica między spear phishingiem a tradycyjnym phishingiem polega na tym, kto wysyła wiadomości. Na początku ataku to sam atakujący korzysta z otwartych źródeł w celu zdobycia jak największej ilości informacji o atakowanej organizacji, jej strukturze itp. Następnie tworzy wysokiej jakości wiadomość e-mail lub inną wiadomość i zaczyna komunikować się z osobą z wewnątrz organizacji jako współpracownikiem. Osoba ta jest następnie wykorzystywana przez atakującego do rozprzestrzeniania innych wiadomości (np. zainfekowanych złośliwym oprogramowaniem) w obrębie organizacji. Ponieważ jest to osoba "znana" ofierze, nie ma ona problemu z komunikowaniem się z nią i mniej, jeśli w ogóle, kontroluje jej wiadomości.[23]



Struktura ataku Spear-Phishing[24]



Przebieg ataku typu spear phishing[25]

Możliwości stosowania sankcji karnych w Republice Czeskiej

Kara dla spear phisherów jest podobna do kary za phishing. Atak typu spear phishing może być również przeprowadzony np. przez organizację terrorystyczną. W tym przypadku nie jest wykluczona odpowiedzialność za przestępstwo z paragrafu **311** (Atak terrorystyczny) Kodeksu Karnego.

Możliwości ścigania karnego w Polsce

Obowiązują te same przepisy, co w przypadku phishingu

4.6.4. Vishing

Termin vishing[26] odnosi się do phishingu telefonicznego, w którym atakujący wykorzystuje techniki socjotechniczne w celu wyłudzenia od użytkownika poufnych informacji (np. numerów kont, danych do logowania - nazwy i hasła, numerów kart kredytowych itp. Atakujący celowo próbuje sfałszować swoją tożsamość. Atakujący często podają się za przedstawicieli prawdziwych banków lub innych instytucji, aby w jak najmniejszym stopniu wzbudzać podejrzenia użytkowników. Vishing jest wykorzystywany w telefonii VoIP (Voice over Internet Protocol).

4.6.5. Smishing

Smishing[27] działa na podobnej zasadzie jak vishing lub phishing, ale do rozsyłania wiadomości wykorzystuje wiadomości SMS. Smishing to przede wszystkim próba nakłonienia użytkowników do wpłacenia pewnej sumy pieniędzy (np. zadzwonienia pod bezpłatny numer, wysłania SMS-a z darowizną itp.) lub kliknięcia podejrzanych linków URL. Jeżeli użytkownik odwiedzi ten adres URL, zostanie przekierowany na stronę, która wykorzystuje lukę w zabezpieczeniach systemu komputerowego, lub zostanie poproszony o wprowadzenie poufnych danych lub zainstalowanie złośliwego oprogramowania. [28]

Przykład smishingu:

"Ostrzeżenie - jest to automatycznie wygenerowana wiadomość z (nazwa lokalnego banku), Twoja karta kredytowa została zablokowana. Aby ponownie aktywować, zadzwoń pod numer 866#### ###".

Możliwości stosowania sankcji karnych w Republice Czeskiej

Sankcje karne za vishing i smishing są podobne do tych za phishing.

Możliwości ścigania karnego w Polsce

Obowiązują te same przepisy, co w przypadku phishingu

---

[1] *Google twierdzi, że najlepsze oszustwa phishingowe mają 45-procentowy wskaźnik skuteczności.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/

Phishing w liczbach: statystyki dotyczące phishingu, które trzeba znać w 2016 r. [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://blog.barkly.com/phishing-statistics-2016

[2] Zob. np. *Beware of Fake Android Prisma Apps Running Phishing, Malware Scam* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: https://www.hackread.com/fake-android-prisma-app-phishing-malware/

[3] LANCE, James. *Phishing bez tajemnic*. Praga: Grada Publishing, 2007. s. 45.

[4] **WILSON Tracy, V.** *Jak działa phishing.* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://computer.howstuffworks.com/phishing.htm

[5] LANCE, James. *Phishing bez tajemnic*. Praga: Grada, 2007, s. 35.

Na temat phishingu zob. *Cyfrowy świat Digi Dooma*, 2008, ISSN 1802-047X. [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://**www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html**

[6] Na temat tendencji rozwojowych phishingu zob. np. DODGE, Ronald. C., Curtis CARVE i Aaron J. FERGUSON. Phishing dla zwiększenia świadomości bezpieczeństwa użytkowników. *Computers & Security*, 2007, vol. 26, nr 1, s. 73-80.

[7] **Według poniższego badania, w ciągu ostatnich 6 miesięcy phishing wzrósł o 250%.** Zobacz *Raport dotyczący działań phishingowych.* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

[8] Zwane dalej w skrócie **DBE**.

[9] *Spłać swoje długi, to jest tytuł egzekucyjny. Izba ostrzega przed kolejną falą oszukańczych e-maili* [online]. [cyt. 15.8.2016]. Dostępny pod adresem: http://zpravy.aktualne.cz/finance/falesne-exekuce-jsou-zpet-komora-varuje-pred-dalsi-vlnou-pod/r~cbdac6de765111e599c80025900fea04/

[10] Więcej szczegółów można znaleźć w wynikach badania Virustotal. [online]. [cyt. 2016-08-15]. Dostępne od:

https://www.virustotal.com/cs/file/62170532b1f656c6917fa66d0ed98462e106f3aa139273c9f2c3a370a67d265f/analysis/1471330723/

[11] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego. Więcej informacji na ten temat można znaleźć na stronie https://www.csirt.cz/.

[12] *Uważaj na zgłoszenie o rzekomym niezapłaconym roszczeniu - to oszustwo* . [online]. [cyt. 15.8.2016]. Dostępny pod adresem: https://www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/
Znów pojawiły się fałszywe doniesienia. [online]. [cyt. 15.8.2016]. Dostępny pod adresem: https://www.csirt.cz/news/security/?page=97

Oszukańcze e-maile grożą egzekucją, nie płać nic i nie otwieraj! [online]. [cyt. 15.8.2016]. Dostępne od:

http://tn.nova.cz/clanek/zpravy/cernakronika/podvodne-emaily-hrozi-exekuci-nic-jim-neplatte-a-neotvirejte.html

Należy wystrzegać się zawiadomienia o żądaniu przejęcia przed przejęciem - jest to oszustwo. [online]. [cyt. 15.8.2016]. Dostępny pod adresem: https://www.csirt.cz/news/security/?page=87

Co kryje się w załącznikach oszukańczych wiadomości e-mail? [online]. [cyt. 15.8.2016]. Dostępny pod adresem: https://blog.nic.cz/2014/07/23/co-se-skryva-v-prilohe-podvodnych-e-mailov-2/

[13] Więcej szczegółów można znaleźć w analizie funkcjonalności złośliwego oprogramowania Tinba: *W32. Tinba (Tinybanker)*. [online]. [cyt. 2016-08-15]. Dostępny pod adresem: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf

[14] HOŘEJŠÍ, Jaromír. *Fałszywy nakaz egzekucji zagraża użytkownikom czeskich banków* [online]. [cit.15.8.2016]. Dostępny pod adresem: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

[15] Ibid - obrazek z kodem captcha.

[16] HOŘEJŠÍ, Jaromír. *Fałszywy nakaz egzekucji zagraża użytkownikom czeskich banków* [online]. [cit.15.8.2016]. Dostępny pod adresem: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

[17] *Śledzenie przesyłek Poczty Czeskiej lub nowy szkodnik.* [online]. [cit.14.8.2016]. Dostępny pod adresem: http://www.viry.cz/sledovani-zasilky-ceske-posty-aneb-nova-havet/

[18] Pliki SCR są *plikami*wykonywalnymi.

Są one przede wszystkim przypisane do programu Unknown Apple II File (znajdującego się na płycie CD Rom z Apple II firmy Golden Orchard). Przypisano im także Windows Screen Saver, Image Pro Plus Ver. 1.x - 4.5.1.x Macro (Media Cybernetics Inc.), TrialDirector Script File (inData Corporation), Screen Dump, Screen Font, Statistica Scrollsheet, Procomm Plus Screen Snapshot File, Movie Master Screenplay, Mastercam Dialog Script File (CNC Software Inc.).), Sun Raster Graphic, LocoScript Screen Font File (oprogramowanie LocoScript), Faxview Fax, DOS DEBUG Input File, Script i FileViewPro.

Co to jest rozszerzenie pliku SCR [online]. [cit.14.8.2016]. Dostępny pod adresem: http://www.solvusoft.com/cs/file-extensions/file-extension-scr/

[19] Zwany dalej **SeznamOTP**

[20] Więcej informacji na temat tego złośliwego oprogramowania i ataku można znaleźć np. pod adresem *Scammers Change Tactics. Znaleźli nowy sposób na wyczyszczenie kont ludzi.* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: https://www.novinky.cz/internet-a-pc/bezpecnost/364094-podvodnici-meni-taktiku-nasli-novou-cestu-jak-vybilit-lidem-ucty.html

[21] Jest to połączenie słów "**farming"** i "**phreaking".**

[22] Więcej informacji można znaleźć w części *Co to jest pharming?* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://www.kaspersky.com/cz/internet-security-center/definitions/pharming

[23] *"Atakujący wyszukuje organizację, która przetwarza cenne informacje, analizuje jej stronę internetową w celu uzyskania informacji o strukturze kadrowej, pracownikach i procedurach (atakujący może wykorzystać prywatne strony i fora dyskusyjne, aby uzyskać bardziej szczegółowe informacje o pracownikach), a w kolejnym kroku tworzy wiadomość, której treść, forma i wygląd naśladują komunikację wewnętrzną organizacji. W wiadomości proszono pracowników o podanie poufnych informacji w celu uzyskania dostępu do sieci komputerowej."*

Teoria ewolucji przedstawiona za pomocą spear phishingu. [online]. [cyt. 15.2.2010]. Dostępny pod adresem: http://connect.zive.cz/content/evolucni-teorie-v-podani-spear-phishingu

[24] Ibid

[25] *Porada miesiąca lipiec 2016 - Unikaj phishingu*. [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/

[26] Jest to połączenie słów voice i phishing.

[27] Jest to połączenie słów SMS i phishing.

[28] Np. **Xshqi** - *robak Android w chińskie walentynki.* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/

Selfmite - *Android SMS robak Selfmite powraca, bardziej agresywny niż kiedykolwiek.* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html

4.8. Prześladowanie użytkowników poczty elektronicznej (BEC)

Business Email Compromise[1] to rodzaj oszustwa, w którym osoba atakująca podszywa się pod członka zarządu (zazwyczaj dyrektora generalnego) i próbuje nakłonić pracownika, klienta lub sprzedawcę do przekazania pieniędzy lub poufnych informacji osobie atakującej.

Oszustwo BEC może być powiązane z innymi formami oszustw, takimi jak oszustwa dotyczące romansów, loterii, zatrudnienia i wynajmu.

Zgodnie z definicją FBI, BEC to *wyrafinowane oszustwo, którego celem są firmy współpracujące z zagranicznymi dostawcami i/lub firmy regularnie dokonujące płatności przelewem. Oszustwo polega na naruszeniu legalnych biznesowych kont e-mail za pomocą technik inżynierii społecznej lub włamań komputerowych w celu przeprowadzenia nieuprawnionych transferów środków.**[2]*

W przeciwieństwie do tradycyjnego ataku phishingowego, atak BEC jest wymierzony w konkretną osobę lub organizację. W przypadku ataku BEC atakujący bardzo dokładnie przygotowuje się do ataku i stara się uzyskać jak najwięcej informacji o ofierze przed jego przeprowadzeniem. Zazwyczaj wykorzystują strony internetowe, raporty roczne, informacje o pracownikach organizacji pochodzące z sieci społecznościowych, ze skompromitowanych kont e-mail itp.

Tak wysoki poziom ukierunkowania pomaga tym oszustwom e-mailowym prześlizgnąć się przez filtry antyspamowe i ominąć kampanie białej rejestracji wiadomości e-mail. Może to również znacznie utrudnić pracownikom rozpoznanie, że wiadomość e-mail nie jest prawdziwa.[3]

Ofiarami oszustw BEC padają zarówno małe firmy, jak i duże korporacje. Oszustwo BEC jest powiązane z innymi formami oszustw, w tym między innymi z oszustwami dotyczącymi romansów, loterii, zatrudnienia i wynajmu.

FBI ostrzegło, że oszustwa BEC będą *"nadal rosły, ewoluowały i stawały się celem firm różnej wielkości"*. FBI wspomniało również, że od stycznia 2015 r. zaobserwowało 1300% wzrost liczby ataków na kompromitujące wiadomości e-mail w przedsiębiorstwach.[4]

Napastnicy BEC wykorzystują taktykę inżynierii społecznej, aby oszukać niczego niepodejrzewających pracowników i kadrę kierowniczą. Niektóre z przykładowych wiadomości e-mail mają tematy zawierające między innymi takie słowa**, jak *prośba, płatność*, *przelew* i *pilne.***

Oszustwo BEC przybiera zwykle jedną z następujących form:

1. **Oszustwo na Prezesa Zarządu**

Atakujący podszywają się pod dyrektora generalnego firmy lub innego członka zarządu i wysyłają spreparowaną wiadomość e-mail do pracowników z możliwością wysyłania przelewów bankowych oraz instruują ich, aby wysyłali środki do atakujących.

2. **Fałszywe faktury** [5]

Firma, która często utrzymuje długotrwałe relacje z dostawcą, otrzymuje prośbę o przelanie środków na zapłatę za fakturę na inne, fałszywe konto. Napastnik zazwyczaj kontaktuje się z ofiarą za pośrednictwem poczty elektronicznej lub telefonu. Atak za pośrednictwem poczty elektronicznej zazwyczaj zawiera sfałszowany kod źródłowy (nagłówek) i temat żądania, dzięki czemu wygląda ono bardzo podobnie do prawdziwego żądania.

3. **Włamanie na konto**

Ten atak jest podobny do ataku Fałszywe faktury. Atakujący wykorzystuje konto e-mail pracownika (zhakowane lub sfałszowane), a następnie wysyła wiadomość e-mail do klientów, informując ich, że wystąpił problem z ich płatnością i muszą ponownie przesłać ją na inne konto.

4. **Wcielanie się w członków zarządu i adwokatów**

Z ofiarami kontaktują się napastnicy, którzy podają się za prawników lub przedstawicieli firm prawniczych. Atakujący prosi o duży przelew środków, aby pomóc w rozwiązaniu sporu prawnego lub zapłaceniu zaległego rachunku. Atakujący stara się przekonać ofiary, że przelew jest poufny i ma duże znaczenie czasowe, więc jest mniej prawdopodobne, że pracownik będzie próbował potwierdzić, czy powinien przelać środki.

5. **Kradzież danych**

Rodzaj BEC, którego celem nie jest bezpośredni transfer pieniędzy. Typowymi ofiarami takiego ataku są pracownicy działów finansowych lub kadrowych. Atakujący prosi ich o przesłanie na swoje konto danych o wysokim stopniu poufności. Wykorzystywana jest socjotechnika, a atak polegający na kradzieży danych może stanowić punkt wyjścia do wspomnianych wyżej ataków BEC ukierunkowanych na transfery finansowe.

Od 2017 r. w Republice Czeskiej odnotowano gwałtowny wzrost liczby ataków oszukańczych mających charakter BEC. Również w tym przypadku większość ataków BEC wykorzystuje podobny modus operandi:

1. **Wybieranie ofiary i zdobywanie informacji na jej temat** (najczęstszym celem są średnie i małe organizacje)

2. **Przygotowanie fałszywej wiadomości e-mail** (do stworzenia fałszywej wiadomości e-mail bardzo często wykorzystywane są ogólnodostępne darmowe serwisy, np. www.5ymail.com. Usługa ta umożliwia atakującemu stworzenie i wysłanie dowolnej fałszywej wiadomości e-mail, która odpowiada istniejącej wiadomości e-mail. Usługa ta nie umożliwia jednak otrzymywania odpowiedzi, dlatego konieczne jest przekierowanie komunikacji e-mailowej na inny istniejący adres e-mail, zarejestrowany np. w serwisie freemail. Prawdziwą tożsamość można znaleźć w kodzie źródłowym komunikatu).

3. **Wysyłanie spreparowanej wiadomości e-mail do pracownika ofiary** (najczęstsze ataki BEC to Oszustwo dyrektora generalnego i Fałszywe faktury). Kwoty wymagane w ten sposób wynoszą zazwyczaj od kilkuset euro do 4000 euro).

4. **Żądanie natychmiastowego lub "pilnego" przelania pieniędzy na konto** osoby **atakującej lub mułów pieniężnych** [zatwierdzenie płatności, jak również osoby, która wydaje polecenie dokonania płatności, jest kluczowym momentem, w którym można zapobiec realizacji czynu przestępczego. Jeśli organizacja ma odpowiednio skonfigurowane protokoły bezpieczeństwa, takie przekazywanie danych zwykle nie ma miejsca. Z punktu widzenia

identyfikacji napastnika, konto napastnika lub konto mułów pieniężnych jest narzędziem, które pozwala w praktyce stwierdzić, czy mamy do czynienia z kontynuacją czynu zabronionego (tj. z punktu widzenia prawa karnego materialnego z jednym czynem zabronionym), czy też ze zbiegiem czynów zabronionych. Jednocześnie jest to de facto najbardziej znaczący ślad cyfrowy, który umożliwia identyfikację napastnika].

5. **Przelew pieniędzy na konto osoby atakującej lub "słupa".**

---

[1] Oszustwa BEC znane są również pod nazwą "oszustwa CEO" lub "oszustwa typu Man-in-the-Email".

[2] *Przejęcie służbowej poczty elektronicznej: oszustwo* warte *3,1 miliarda dolarów.* [online]. [quote12.6.2018]. Dostępny pod adresem: https://www.ic3.gov/media/2016/160614.aspx
[3] *Co to jest atak typu BEC (Business Email Compromise)? I jak temu zapobiec?* [online]. [quote12.6.2018]. Dostępny na stronie: https://blog.barkly.com/what-is-a-business-email-compromise-bec-attack-and-how-can-i-stop-it

[4] *Przejęcie służbowej poczty elektronicznej: oszustwo* warte *3,1 miliarda dolarów.* [online]. [quote12.6.2018]. Dostępny pod adresem: https://www.ic3.gov/media/2016/160614.aspx

[5] Atak ten nazywany jest również: "schematem fałszywej faktury" (Bogus Invoice Scheme). "Oszustwo dostawcy" oraz "Schemat modyfikacji faktur".

4.9. Nieuczciwe strony internetowe (firmy)

W Internecie można natknąć się na różne działania lub strony[1] prezentujące niesamowite nagrody lub oferujące różne towary po bardzo niskich cenach. Atakujący stosują socjotechnikę i bazują przede wszystkim na ludzkiej naiwności i nieostrożności. Rzeczywiste działania atakującego mogą przybierać dwie formy.

W pierwszym przypadku atakujący próbuje wyłudzić poufne dane (np. imię, nazwisko, adres dostawy, adres e-mail, numer telefonu i hasło), zazwyczaj w celu rejestracji, dostarczenia towarów, nagród itp. Wszystkie te dane użytkownik wprowadza samodzielnie i dobrowolnie. W ten sposób atakujący uzyskuje dostęp do danych, które - podobnie jak w przypadku phishingu - mogą zostać wykorzystane do różnych działań. Na przykład na podstawie wprowadzonego hasła i innych danych użytkownika atakujący może próbować uzyskać dostęp do innych usług, z których korzysta użytkownik.[2]

W drugim, znacznie częstszym przypadku, działanie polega na wyłudzeniu środków od użytkownika. Samochody, motocykle, traktory, inne maszyny rolnicze, a przede wszystkim wszelkiego rodzaju sprzęt elektroniczny są powszechnie oferowane w Internecie po bardzo przystępnych cenach.

W kontekście oszukańczych ofert w Internecie, Europejskie Centrum Konsumenckie[3] wydało zalecenie dla użytkowników, które ma im pomóc w rozpoznawaniu oszukańczych zachowań:

- ***Wpisz dane swojej firmy (np. nazwę firmy, adres strony internetowej, adres e-mail) do wyszukiwarki internetowej***.
- ***Zastanów się, jak prezentuje się inwestor.*** *Czy wygląd i sposób działania witryny, na której zamierzasz dokonać zakupu, są profesjonalne? Adresy e-mail na bezpłatnych i anonimowych serwerach, takich jak yahoo.com, hotmail.com, gmail.com, live.com, seznam.cz itp. z pewnością nie będą sprawiać wrażenia godnych zaufania. Podobnie, jeśli witryna jest umieszczona na darmowym serwerze hostingowym, nie jest to oznaką profesjonalizmu.*
- ***Płać z góry tylko wtedy, gdy masz do czynienia z naprawdę godnym zaufania handlowcem.*** *Z pewnością nie daje się pieniędzy na ulicy nieznajomemu z obietnicą, że w przyszłości dostarczy nam jakiś przedmiot. Wielu użytkowników robi to jednak w Internecie. Płatności z góry dokonuj tylko wtedy, gdy masz pewność, że masz do czynienia z godnym zaufania dostawcą. Przede wszystkim należy chronić dane kart kredytowych.*
- ***Szczególnie podejrzany jest wymóg dokonywania płatności za pośrednictwem Western Union.*** *W przypadku przelewów bankowych nigdy nie należy wysyłać pieniędzy na konto osoby prywatnej, chyba że jest to konto firmy/spółki sprzedającej.*
- ***Do typowych oznak oszustwa należą: niewyparzony język, żądanie zapłaty z góry w gotówce lub przelewem bankowym, inne żądania zapłaty pod fałszywym pretekstem*** *(cło, ubezpieczenie, pakowanie wielu sztuk produktu)* ***itp. Pamiętaj, że jeśli oferta wydaje się zbyt korzystna, aby była prawdziwa, to prawdopodobnie nie jest!***
- ***Sprawdź w krajowym rejestrze handlowym,*** *czy firma jest tam zarejestrowana (zdarza się też, że ktoś nadużywa nazwy istniejącej firmy i zakłada stronę internetową o podobnej nazwie).*
- ***Sprawdź domenę witryny.*** *Zdarza się, że adres strony internetowej jest taki sam jak adres faktycznie istniejącej i zarejestrowanej firmy. Jest jednak jedna różnica - domena, tj. końcówka adresu internetowego, jest inna (np. nie ".co.uk" dla Wielkiej Brytanii, ale być może ".co.cc" dla Wysp Kokosowych).*
- ***Znajdź siedzibę firmy na stronie internetowej, która oferuje fotografie ulic miast,*** *pod adresem podanym w ogłoszeniach i na stronie internetowej firmy.*
- ***Szanuj swoje dane osobowe.*** *Nie udostępniaj informacji o sobie na niezaufanych lub nieznanych witrynach. Podawaj tylko te informacje, które są naprawdę niezbędne.*
- ***Nie należy odpowiadać na niechcianą pocztę (spam).*** *Nie odpowiadaj na wiadomości-śmieci i w żadnym wypadku nie wysyłaj pocztą elektroniczną danych konta bankowego, numeru karty kredytowej ani danych logowania do bankowości internetowej. Usuwaj niechciane wiadomości e-mail i nigdy nie otwieraj nieznanych załączników.*[4]

Wszystkie powyższe oznaki należy traktować jako zwykłe wskazówki, które mogą doprowadzić do wykrycia oszustwa. Atakujący może modyfikować swoje działania w zależności od powodzenia własnego ataku. **Oprócz powyższych wskazówek zaleca się również korzystanie z ostrzeżeń publikowanych na innych stronach internetowych, takich jak** www.podvodnefirmy.cz **itp.**

Możliwości stosowania sankcji karnych w Republice Czeskiej

W Republice Czeskiej opisane powyżej postępowanie może być karane na podstawie paragrafu **209** (Oszustwo) Kodeksu karnego. Dopełnieniem oszustwa jest wzbogacenie się. Stworzenie repliki strony internetowej oraz uzyskanie loginów i haseł może być uznane za przygotowanie lub próbę popełnienia przestępstwa z paragrafu 209 Kodeksu karnego. Jeżeli osoba atakująca próbuje (§ 21 TZK) uzyskać nieuprawniony dostęp do konta innego użytkownika na podstawie uzyskanych danych dostępowych, czyn taki można również zakwalifikować jako **§ 230** (Nieuprawniony dostęp do systemu komputerowego i nośnika informacji) TZK**.**

Możliwości ścigania karnego w Polsce

W Polsce jest to regulowane przez art. 286 (oszustwo), który mówi, że:

§ 1 Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do przywłaszczenia sobie lub innej osobie mienia własnego lub cudzego za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

[1] Najczęściej są to strony internetowe, portale ogłoszeniowe, ale mogą to być również konta w mediach społecznościowych itp.

[2] Bardzo często zdarza się, że użytkownicy wprowadzają te same lub podobne hasła do różnych usług internetowych. Umożliwia to atakującemu wykorzystanie np. techniki ataku słownikowego do złamania danych uwierzytelniających innych usług. W ten sposób atakujący może również popełnić inne nielegalne czyny (np. zob. rozdz. 4.15 Identity theft, 4.8 Hacking itp.).

Więcej informacji na ten temat można znaleźć np. w *Ataku słownikowym.* [online]. [cyt. 30.8.2016]. Dostępny pod adresem: https://managementmania.com/cs/slovnikovy-utok

[3] Więcej informacji można znaleźć na stronie http://www.evropskyspotrebitel.cz/.

[4] Więcej informacji na ten temat można znaleźć w *poradach ESC dotyczących wykrywania oszustw internetowych.* [online]. [cyt. 30.8.2016]. Dostępny pod adresem: http://www.evropskyspotrebitel.cz/nakupy-online/esc-radi-jak-poznat-podvod-na-internetu-27250

4.10. Hacking

Termin hacking jest obecnie postrzegany pejoratywnie przez opinię publiczną jako wszelkie działania osoby mające na celu uzyskanie nielegalnego dostępu do cudzego systemu lub komputera osobistego.[1] Zwłaszcza w mediach termin ten jest powszechnie używany w odniesieniu do wszystkich napastników, których działania są skierowane przeciwko technologiom informatycznym lub których działalność opiera się na wykorzystaniu tych technologii.[2] W tym kontekście istnieje jednak zasadnicza różnica między postrzeganiem przez opinię publiczną treści terminu "hakerstwo" a postrzeganiem tych, którzy określają się jako hakerzy lub są określani jako hakerzy przez własną społeczność.

Termin **"haker"**[3] i "**hacking**" pochodzą z USA z lat 50. XX wieku i **odnoszą się do osób uzdolnionych technicznie** (i ich działań), które **potrafią znajdować nowe, często niekonwencjonalne rozwiązania problemów.**

Aby zrozumieć, jak napastnicy, których zwykliśmy uważać za hakerów, postrzegają społeczeństwo i jego zasady, warto poznać ich punkt widzenia. W 1984 r. Levy określił następujące zasady etyki hakerów:

1. Dostęp do komputerów i wszystkiego innego, co może nauczyć nas czegoś o funkcjonowaniu świata, powinien być nieograniczony i absolutny. Zawsze przestrzegaj zasady osobistego doświadczenia.
2. Wszystkie informacje powinny być bezpłatne.
3. Nie ufaj władzy, popieraj decentralizację.
4. Hakerów powinno się oceniać na podstawie ich działań, a nie na podstawie błędnych kryteriów, takich jak wiek, rasa czy status.
5. Możesz tworzyć "piękno" na komputerze.
6. Komputery mogą zmienić Twoje życie na lepsze.[4]

Choć zasady te nie zawsze są respektowane lub uznawane, stanowią one podstawowe ramy postrzegania świata wirtualnego przez napastników, których nazywamy hakerami.

Innym ważnym spojrzeniem na postrzeganie świata oczami hakera jest film dokumentalny Manifest hakera:

Poniższy tekst został napisany krótko po moim aresztowaniu...

Sumienie hakera

Dzisiaj złapali kolejnego. Gazety są pełne informacji na ten temat. "Młody człowiek skazany za skandaliczne przestępstwo komputerowe", "Haker aresztowany za włamanie do banku"...

Pieprzone dzieci. Wszystkie są takie same.

Ale czy kiedykolwiek próbowałeś spojrzeć oczami hakera, mając do dyspozycji potrójną psychologię i technobrain z lat 50. Czy kiedykolwiek zadałeś sobie pytanie, jaka siła go ukształtowała, co ukształtowało jego osobowość?

Jestem Haker. Wejdź do mojego świata...

Moje życie zaczyna się od szkoły... Jestem mądrzejszy niż większość innych dzieci, a te bzdury, które nam opowiadają, nudzą mnie...

Pieprzony obibok. Wszystkie są takie same.

Jestem w gimnazjum lub liceum. Już po raz piętnasty nauczyciel wyjaśnia, jak skrócić ułamek. Rozumiem. "Nie, panno Smith, to nie ja napisałem procedurę. Zrobiłem to z głowy...".

Pieprzony dzieciak. Prawdopodobnie gdzieś go skopiował. Wszystkie są takie same.

Dokonałem dziś pewnego odkrycia. Odkryłem komputer. Chwileczkę, to świetnie. Robi to, co chcę. A jeśli popełni błąd, to dlatego, że ja coś spieprzyłem. I to nie tylko dlatego, że mnie nie lubi...

...albo czuje się zagrożony przeze mnie...

...albo uważa mnie za wkurzonego drania...

...albo że nie lubię uczyć i nie powinienem tu być...

Pieprzony dzieciak. On zawsze gra w gry. Wszystkie są takie same.

I wtedy to się stało... drzwi do świata otworzyły się... sygnał elektroniczny popędził przez linię telefoniczną jak heroina przez żyły uzależnionego, znajdując schronienie przed uciążliwą codziennością... znajduje tablicę.

"To jest to miejsce... tu jest moje miejsce...".

Znam tu wszystkich. Mimo że nigdy w życiu ich nie widziałem, nie rozmawiałem z nimi i być może nigdy więcej się nie odezwą... Znam was wszystkich...

Cholerne dzieci. Zawsze pilnują linii. Wszystkie są takie same...

Założysz się, że wszyscy jesteśmy tacy sami!

W szkole karmiono nas łyżeczką, a my chcieliśmy stek... kawałki mięsa, które nam podsuwano, były wstępnie przeżute i bez smaku. Byliśmy zdominowani przez sadystów i ignorowani przez tępaków. Było kilku takich, którzy powinni byli nas uczyć i znaleźć w nas chętnych uczniów, ale byli jak krople wody na pustyni.

*"**To jest teraz nasz świat...** Świat elektronów i przełączników, piękno przyjemności. **Korzystamy z istniejących usług, nie płacąc za nie, mogłyby one być prawie darmowe, gdyby nie należały do szumowin, a wy nazywacie nas przestępcami. Odkrywamy... a wy nazywacie nas przestępcami. Jesteśmy spragnieni wiedzy... a wy nazywacie nas przestępcami. Istniejemy bez koloru skóry, bez narodowości, bez uprzedzeń religijnych, a wy nazywacie nas przestępcami. Budujecie bomby atomowe, prowadzicie wojny, mordujecie i oszukujecie, okłamujecie nas i chcecie, żebyśmy uwierzyli, że to dla naszego dobra, a przecież jesteśmy przestępcami.***

Tak, jestem przestępcą. Moją zbrodnią jest ciekawość. Moją zbrodnią jest ocenianie ludzi na podstawie tego, co mówią i myślą, a nie tego, jak wyglądają. Moją zbrodnią jest bycie mądrzejszym od ciebie, czego nigdy mi nie wybaczysz. Jestem Hakerem i to jest mój manifest. Można powstrzymać pojedyncze osoby, ale nie można powstrzymać nas wszystkich... w końcu wszyscy jesteśmy tacy sami.

Mentor

Manifest hakera[5]

8 stycznia 1986 r.

Obecnie sami hakerzy używają terminu haker w odniesieniu do osób, które doskonale znają działanie systemów teleinformatycznych, systemów komputerowych, ich systemów operacyjnych i innych programów, zasady działania i mechanizmy sieciowe, a jednocześnie są doskonałymi programistami potrafiącymi w bardzo krótkim czasie stworzyć własne oprogramowanie. Filozofią wielu osób jest chęć zrozumienia, jak działają technologie informacyjne, aplikacje i zasoby techniczne, oraz udostępnienia tych informacji innym użytkownikom. Zdolność hakera do uzyskiwania dostępu do systemów komputerowych poza normalnymi sposobami dostępu za pomocą samodzielnie zaprojektowanych i napisanych programów komputerowych (co nie oznacza, że uzyskanie takiego dostępu musi być motywowane chęcią wyrządzenia krzywdy lub innej szkody użytkownikowi lub wzbogacenia się w inny sposób poprzez przeniknięcie do systemu) jest jedną, ale nie jedyną umiejętnością.

Oddział hakerów

To właśnie motywacja do uzyskania niestandardowego (niekoniecznie nielegalnego) dostępu, sposób penetracji, motywacja i ostateczne postępowanie z uzyskanymi danymi są kluczowymi czynnikami pozwalającymi podzielić te osoby na trzy podstawowe grupy:[6]

Białe kapelusze - są to hakerzy, którzy przenikają do systemu, wykorzystując jego słabe punkty, właśnie po to, aby ujawnić te luki w zabezpieczeniach i stworzyć mechanizmy i bariery, które powinny uniemożliwić takie ataki. Często są oni pracownikami lub współpracownikami zewnętrznymi renomowanych firm informatycznych. Nie powodują one żadnych szkód ani nie wyrządzają innych krzywd użytkownikom poprzez penetrację systemu, ale w wielu przypadkach ostrzegają administratora zagrożonego systemu o lukach w zabezpieczeniach. Ich działalność ma zasadniczo charakter nieniszczący.

Czarne kapelusze - zasadniczo przeciwieństwo hakerów zaklasyfikowanych jako białe kapelusze. Ich motywacją jest chęć wyrządzenia szkody lub innego uszczerbku użytkownikowi zagrożonego systemu albo zdobycie własności lub innych korzyści. Oprócz samej realizacji włamania do zagrożonego systemu, w ich działaniach jest jeszcze jeden, przestępczy element.

Szare kapelusze - to szara strefa hakerów, czyli osoby, które nie sprofilowały się w kierunku dwóch wyżej wymienionych grup. Niekiedy naruszają prawa lub zasady moralne innych osób, ale ich działania nie są powodowane chęcią wyrządzenia krzywdy, jak w przypadku Czarnych Kapeluszy.

Oprócz powyższego, czyli najczęściej stosowanego podziału, hakerów można podzielić na inne grupy ze względu na motywy ich działania. Są to: Script Kiddies, haktywiści, hakerzy sponsorowani przez państwo, hakerzy szpiedzy, cyberterroryści, początkujący hakerzy (n00b), hakerzy Blue Hat itd.[7]

Kluczowym czynnikiem w ocenie hakerstwa jako potencjalnego zagrożenia bezpieczeństwa jest określenie przyczyny działań hakera (zob. klasyfikacja hakerów). W niektórych przypadkach hakerstwo może stanowić rzeczywiste zagrożenie dla bezpieczeństwa, ponieważ jest to naruszenie bezpieczeństwa systemu komputerowego, złamanie zabezpieczeń lub wykorzystanie słabości systemu. Z drugiej strony, w innych przypadkach może to być użyteczne uzupełnienie, wykorzystywane do zwiększenia bezpieczeństwa systemu jako całości lub do znalezienia słabych punktów i podatności na ataki.

Ogólnie rzecz biorąc, hakerstwo można zdefiniować jako nieuprawnioną penetrację systemu komputerowego z zewnątrz, najczęściej za pośrednictwem Internetu. Jednak nie każdy atak hakerski musi stanowić przestępstwo.

Niebezpieczeństwo działań hakerów polega m.in. na tym, że oprócz uzyskania nieautoryzowanego dostępu do atakowanego systemu (niezależnie od motywacji hakera), osoby te tworzą i wykorzystują do przeprowadzania ataków bardzo skuteczne narzędzia programowe, których kody źródłowe są często następnie publikowane przez samych hakerów, np. na giełdach Darknet. Może to prowadzić do dalszego masowego nadużywania tych programów przez użytkowników, którzy sami nie posiadają umiejętności programistycznych do tworzenia takich programów, ale dzięki istnieniu udostępnionych w ten sposób narzędzi mogą potencjalnie wyrządzić dość znaczne szkody użytkownikom zagrożonych systemów. Dlatego często można nabyć przez Internet całe zestawy oprogramowania hakerskiego zawierające podstawowe oprogramowanie i informacje niezbędne do jego używania, de facto nie posiadając żadnej dogłębnej wiedzy na temat działania tych programów.

Formy hakowania

Rzeczywista działalność hakerów składa się z szeregu czynności. Typowe działania stosowane przez hakerów obejmują:

1. Inżynieria społeczna
2. Łamanie haseł[8]
3. Skanowanie portów[9]

4. Używanie złośliwego oprogramowania do infiltracji systemu komputerowego

5. Phishing

6. Cros Site Script[10]

7. Przechwytywanie komunikatów[11]

Znane grupy hakerów i hakerzy

Prawdopodobnie najbardziej znaną obecnie grupą hakerów jest Anonymous, ale istnieją lub istniały także inne grupy:[12]

- Oddział Jaszczurów
- Śruba poziomu siódmego
- Klub Komputerowy Chaos
- Lulzsec
- Syryjska Armia Elektroniczna
- Globalhell
- Program do łamania zabezpieczeń sieciowych Grupa Hakerów
- Ruch antysocjalistyczny
- Legion zagłady (1984-2000)
- Mistrzowie podstępu (1989-1993)
- Milw0rm i.

Do **najsłynniejszych hakerów** należą Johnatan James, Vladimir Levin, Gary McKinnon, John McAfee, Astra, Stephen Wozniak, James Kosta, Kevin Mitnick, Adrian Lamo, David L. Smith.[13]

Nie ma wątpliwości, że **nie wszystkie działania hakerów są legalne**. W związku z ingerencją w system komputerowy z pewnością dojdzie do naruszenia gwarantowanych podstawowych praw i wolności człowieka.

Możliwości stosowania sankcji karnych w Republice Czeskiej

Jak wspomniano powyżej, istnieje wiele działań lub ataków, które można określić mianem hakerstwa (od łamania haseł po wyrafinowane ataki phishingowe połączone z socjotechniką i wykorzystaniem złośliwego oprogramowania).

Działania hakera, polegające wyłącznie na wykorzystaniu swoich umiejętności w celu pokonania zabezpieczeń i uzyskania dostępu do systemu komputerowego lub jego części, mogą być karane na podstawie paragrafu **230(1)** (Nieuprawniony dostęp do systemu komputerowego i nośnika informacji) Kodeksu karnego.

W przypadku połączonych form ataków, gdy np. złośliwe oprogramowanie jest wykorzystywane do zainfekowania komputera, takie zachowanie sprawcy musi być również karane na podstawie **paragrafu 230(2)** (Nieuprawniony dostęp do systemu komputerowego i nośnika informacji) Kodeksu karnego. Jeśli celem ataku jest uzyskanie nieuzasadnionej korzyści dla siebie lub innej osoby albo bezprawne ograniczenie funkcjonalności systemu komputerowego lub innego urządzenia technicznego do przetwarzania danych, można również zastosować postanowienia **paragrafu 230(3)** Kodeksu karnego.

Możliwości ścigania karnego w Polsce

Przestępstwo hakerstwa jest uregulowane w art. 267§1 Kodeksu karnego.

Kto bez upoważnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonych, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając jej elektroniczne, magnetyczne, informatyczne lub inne szczególne zabezpieczenia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Przełamanie zabezpieczenia elektronicznego jest jednym z ustawowych znamion przestępstwa z art. 267 (1) Kodeksu karnego. "Zabezpieczenie konta hasłem (kodem) stanowi przeszkodę w uzyskaniu dostępu do informacji przez osobę nieuprawnioną. Pokonanie tej przeszkody poprzez użycie przez sprawcę kodu dostępu wbrew woli osoby uprawnionej powinno być traktowane jako naruszenie bezpieczeństwa elektronicznego. Użycie takiego kodu (hasła) przez osobę nieuprawnioną wbrew woli właściciela rachunku przełamuje elektroniczną przeszkodę chroniącą dostęp czy to do rachunku bankowego, czy do konta użytkownika na portalu internetowym" (wyrok Sądu Okręgowego w Świdnicy z 10 kwietnia 2019 r., sygn. akt: IV Ka112/19). Do znamion tego przestępstwa należy, oprócz łamania, "obchodzenie zabezpieczeń elektronicznych, magnetycznych, informatycznych, polegające na usuwaniu specjalnych struktur, osłon", które służą do uniemożliwienia dostępu do informacji przechowywanych w systemie; przepis obejmuje również łamanie konkretnych zabezpieczeń informacji innych niż elektroniczne, magnetyczne czy informatyczne, co oznacza, że chodzi o takie zabezpieczenia,

których usunięcie wymaga od sprawcy specjalistycznej wiedzy lub posiadania specjalistycznych narzędzi. W każdym razie złamanie zabezpieczenia powinno sprawiać pewne trudności - wtedy można założyć, że takie zabezpieczenie ma charakter "specjalny". Przełamanie zabezpieczeń to bezpośrednia ingerencja w system bezpieczeństwa, zwykle jego zniszczenie, oraz obejście zabezpieczeń bez dokonywania w nie żadnej ingerencji. W celu realizacji założeń art. 267 § 1 konieczne jest złamanie takiego zabezpieczenia, którego główną funkcją jest ochrona informacji przed nieuprawnionym dostępem do nich. Zgodnie z wyrokiem Sądu Okręgowego w Świdnicy z dnia 10 kwietnia 2019 r., sygn. akt: IV Ka112/19, "istota przestępstwa z art. 267 § 1 kk polega na tym, że sprawca nie zna sposobu zabezpieczenia (np. kodów dostępu do określonych informacji lub treści haseł) po zastosowaniu, podjęciu określonych czynności (w tym np.Nie jest przestępstwem z art. 267 ust. 1 kodeksu karnego "uzyskanie informacji, co do których nie podjęto żadnych środków zabezpieczających, chyba że polega na podłączeniu do sieci telekomunikacyjnej".

Podsumowując poniższe rozważania, wynika z nich, że zgodnie z wyrokiem Sądu Administracyjnego w Szczecinie z dnia 14 października 2008 r., sygn. akt: II AKa 120/08, "nie popełnia przestępstwa z art. 267 § 1 k.k. ten, kto uzyskał nieuprawniony dostęp do informacji bez przełamania lub obejścia zabezpieczenia, nawet jeśli uczynił to podstępnie". Zgodnie z wyrokiem Sądu Okręgowego w Świdnicy z dnia 10 kwietnia 2019 r., sygnatura akt: IV Ka112/19, z powyższego wynika, że "uzyskanie dostępu, bez upoważnienia, do informacji, o których mowa w art. 267 § 1 Kodeksu karnego, poprzez np. posłużenie się hasłem przekazanym lub wcześniej udostępnionym przez pokrzywdzonego, lub e.g. zapamiętanie hasła przez przeglądarkę internetową lub pozostawienie komputera z wpisanym hasłem do danego konta i po zalogowaniu się do systemu nie może być uznane za złamanie hasła, a więc powyższe nie wyczerpuje znamion przestępstwa z art. 267 § 1 k.k.". Przestępstwo hakerstwa jest ścigane na wniosek pokrzywdzonego.

---

[1] Por. np. GRIFFITHS, Marek. Przestępczość komputerowa i hakerstwo: poważny problem dla policji? The *Police Journal,* 2000, vol. 73, nr 1, s. 18-24.

YAR, Majid. Hakerstwo komputerowe: kolejny przypadek przestępczości nieletnich? *The Howard Journal*, 2005, t. 44, nr 4, s. 387-399.

[2] Por. np. artykuły w prasie codziennej:

Największy atak hakerski potwierdzony. Zagrożone setki milionów użytkowników [online]. [cyt. 16.8.2015]. Dostępny pod adresem: https://www.novinky.cz/internet-a-pc/bezpecnost/405260-nejvetsi-hackersky-utok-potvrzen-v-ohrozeni-jsou-stovky-milionu-uzivatelu.html

*Hakerzy podszywają się pod Anonymous i grożą atakami na czeskie firmy [*online]. [cyt. 16.8.2015]. Dostępny pod adresem: http://www.lupa.cz/clanky/hackeri-vydavajici-se-za-anonymous-hrozi-utokem-na-ceske-firmy-chteji-zaplatit/

Yahoo bada, czy haker rzeczywiście posiada dane 200 milionów kont. [online]. [cyt. 16 sierpnia 2015]. Dostępny pod adresem: http://www.lupa.cz/clanky/yahoo-resi-jestli-hacker-opravdu-ma-udaje-o-200-milionech-tamnich-uctu/

Hakerzy zaatakowali użytkowników Facebooka. [online]. [cyt. 16.8.2015]. Dostępny pod adresem: http://tech.ihned.cz/c1-37133210-hackeri-zautocili-na-uzivatele-facebooku-chteli-jejich-hesla

Hakerzy wykradli Amerykanom dane dotyczące nowego typu myśliwca. [online]. [cyt. 16.8.2015]. Dostępne od:

http://digiweb.ihned.cz/c1-36816420-hackeri-ukradli-americanum-data-o-novem-typu-bojovych-stihacek

Już wkrótce hakerzy będą wykradać dane bezpośrednio z Twojej klawiatury. [online]. [cyt. 16.8.2015]. Dostępne od:

http://digiweb.ihned.cz/c1-29295240-hackeri-vam-brzy-ukradnou-data-primo-z-klavesnice

[3] Termin ten można tłumaczyć na wiele sposobów i musi on wynikać z kontekstu. W żargonie amerykańskim oznaczało to pierwotnie jazdę konno bez celu. Hack oznaczał również proste rozwiązanie problemu. W związku z tym oznaczało to popełnienie jakiegoś wykroczenia przez studentów uniwersytetu.

[4] LEVY, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly edia, s. 32-41. ISBN 978-1449388393.

Dostępne również w Internecie:

https://e11c1b148f6c7c56754c9184e0d1c52ac4d888f9-www.googledrive.com/host/0ByAMXZI2-PZ0WjBPYmhaWVVRN0E

[5] Tłumaczenie z języka czeskiego pochodzi z: *1986 - Manifest Hakerów.* [online]. [cit.16.8.2015]. Dostępny pod adresem: http://blisty.cz/art/14662.html

Oryginalną wersję można znaleźć na stronie Phrack.org [online]. [cyt. 2015-08-16]. Dostępny pod adresem: http://phrack.org/issues/7/3.html

[6] Oznaczenie tych grup, choć dziwaczne, jest faktycznie stosowane w sferze informacyjnej i nie jest tłumaczone na język czeski.

[7] Więcej szczegółów można znaleźć np. w: SHNEIER, Bruce. *Siedem typów hakerów.* [online]. [cyt. 16.8.2015]. Dostępny pod adresem: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html

7 typów motywacji hakerów [online]. [cyt. 2015-08-16]. Dostępny pod adresem: https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

7 typów hakerów, których powinieneś znać. [online]. [cyt. 2015-08-16]. Dostępny pod adresem: https://www.cybrary.it/0p3n/types-of-hackers/

[8] Jest to proces uzyskiwania hasła do systemu komputerowego. Jest on powszechnie używany do łamania haseł:

- Odgadywanie haseł metodą brute force (testowanie haseł. Wystarczająco silne hasło jest środkiem zapobiegawczym);
- Odgadywanie hasła na podstawie pewnej wiedzy o użytkowniku (np. uzyskanej z sieci społecznościowych itp.);
- Korzystanie ze słownika powszechnie używanych haseł (atak słownikowy);
- Żądanie hasła od administratora systemu poprzez podszywanie się pod uprawnionego użytkownika (napastnik udaje, że zapomniał hasła i próbuje je odzyskać).

- Eliminowanie haseł z niezaszyfrowanej lub niewystarczająco zaszyfrowanej komunikacji sieciowej między systemem komputerowym a użytkownikiem
- Wyszukiwanie haseł w plikach danych przechowywanych przez system

[9] Jest to metoda służąca do wykrywania otwartych portów sieciowych w systemie komputerowym podłączonym do sieci komputerowej. Na podstawie tego odkrycia można określić, jakie usługi są uruchomione w systemie komputerowym (np. serwer WWW, serwer ftp itp.). Właściwy atak jest następnie kierowany na wykryte usługi w oparciu o ich luki.

[10] Jest to atak polegający na włamaniu się na stronę internetową. W tym typie ataku wykorzystywane są aktywne elementy (skrypty) na stronie WWW, do których wstawiany jest złośliwy kod, a następnie oferowany ofierze.

Jednym z mniej popularnych, ale jeszcze bardziej niebezpiecznych działań jest wykorzystanie luki w aplikacji sieciowej do uruchomienia złośliwego oprogramowania w przeglądarce ofiary. Ofiara nie jest wtedy w stanie wykryć takiego zachowania. Złośliwy kod jest wykonywany tak samo jak reszta strony, a atakujący może przejąć uprawnienia przeglądarki w systemie.

Więcej szczegółów można znaleźć np. w *OWASP, XSS* [online]. [cyt. 15.7.2016]. Dostępne pod adresem: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

[11] Zob. rozdz. 4.11 Sniffing.

[12] Zob. np. *10 Most Notorious Hacking Groups* [online]. [cit.15.7.2016]. Dostępny pod adresem: https://www.hackread.com/10-most-notorious-hacking-groups/

Obraz zaczerpnięty z [online]. [cyt. 2016-07-15]. Dostępne od:

http://img02.deviantart.net/a2fd/i/2012/330/7/5/we_are_anonymous_by_mrj_5412-d5mb6xc.jpg

[13] Więcej informacji na ten temat można znaleźć np. w artykule *10 najbardziej znanych hakerów wszech czasów.* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: https://hacked.com/hackers/

Najsłynniejsi hakerzy komputerowi i ich ataki. [online]. [cyt. 2016-07-15]. Dostępny pod adresem: https://www.stream.cz/top-5/10004402-nejznamejsi-pocitacovi-hackeri-a-jejich-utoky

4.11. Cracking

Termin **cracking** jest utożsamiany z terminem hacking, a czasami terminy te są nawet błędnie mylone przez opinię publiczną lub media. Termin ten można przetłumaczyć na język czeski jako pęknięcie lub rozerwanie. W kontekście treści, cracking oznacza łamanie lub obchodzenie zabezpieczeń systemu komputerowego, programu lub aplikacji w celu ich późniejszego nieuprawnionego użycia.

Hakerzy czarnych kapeluszy są często określani mianem crackerów, czyli osób, które włamują się do systemów, próbując wyrządzić szkodę użytkownikowi, zdobyć informacje lub wzbogacić siebie lub innych. Co więcej, cracking jest głównie związany z naruszaniem praw autorskich i praw pokrewnych. W tym sensie cracking definiuje się jako działanie polegające na obchodzeniu zabezpieczeń, które uniemożliwiają tworzenie kopii lub nielegalne korzystanie z programów komputerowych oraz produktów muzycznych lub filmowych (płyt CD, DVD itp.). Zabezpieczenia te są stosowane jako środek ochrony praw autorskich w rozumieniu art. 43 ust. 1 ustawy o prawie autorskim z późniejszymi zmianami.

Jedną z form łamania **haseł** jest **"łamanie haseł"**, które służy do poznania hasła dostępu do systemu komputerowego, systemu licencjonowanego lub programu. W przypadku naruszenia praw autorskich cracker zazwyczaj tworzy keygen lub crack[1] , który umożliwia dalsze korzystanie z programu. Takie zmodyfikowane programy są następnie zazwyczaj udostępniane na forach warezowych lub w sieciach P2P.

Możliwości stosowania sankcji karnych w Republice Czeskiej

Działanie sprawcy, polegające na naruszeniu ochrony systemu lub programu komputerowego z zamiarem zdobycia informacji i ich późniejszego nieuprawnionego wykorzystania, wypełnia znamiona przestępstwa z paragrafu **230 (1) lub (2)** (Nieuprawniony dostęp do systemu komputerowego i nośnika informacji) Kodeksu Karnego. Jeśli celem kradzieży jest uzyskanie nieuzasadnionej korzyści dla siebie lub innej osoby, można również zastosować przepisy **paragrafu 230(3)** Kodeksu karnego.

Nie wyklucza się odpowiedzialności karnej na podstawie paragrafu **231** (Posiadanie i przechowywanie urządzenia dostępowego i hasła do systemu komputerowego oraz innych tego typu danych) Kodeksu karnego. Rozpowszechnianie utworu chronionego prawem autorskim powoduje naruszenie **paragrafu 270** (Naruszenie praw autorskich, praw pokrewnych i praw do baz danych) Kodeksu karnego.

Możliwości ścigania karnego w Polsce

Obowiązują te same przepisy, co w przypadku hakowania.

---

[1] **Keygen** - Generator kluczy. Program, który generuje numery seryjne lub inne dane. **Crack** - program służący do usuwania lub ograniczania funkcjonalności cech ochronnych innego programu.

4.12. Piractwo internetowe (komputerowe)

Każdy autor ma prawo do decydowania o tym, jak jego dzieło może być traktowane.

Jeśli nie zgadzam się z warunkami korzystania z utworu,

Nie rozumiem ich lub ich nie znam,

Mam prawo nie korzystać z utworu.

Jan Kolouch

Termin piractwo internetowe jest terminem ogólnym, obejmującym przestępstwa naruszające prawa własności intelektualnej (bardzo często zawężane do praw autorskich). Dopiero wraz z upowszechnieniem się systemów komputerowych, a w szczególności Internetu, możemy mówić o masowym piractwie jako jednej z najbardziej rozpowszechnionych form cyberprzestępczości.

Naruszenie praw własności intelektualnej, w szczególności praw autorskich i praw pokrewnych, jest obecnie jednym z najbardziej palących problemów w środowisku technologii informacyjnych.

4.11.1. Prawo własności intelektualnej

W odniesieniu do piractwa internetowego należy najpierw zdefiniować zagadnienie własności intelektualnej, w szczególności prawa autorskiego. Definicja ta jest niezbędna do zrozumienia różnicy między legalnym a nielegalnym postępowaniem osób działających w Internecie.

Prawo własności intelektualnej dotyczy dóbr o charakterze niematerialnym, tzw. dóbr niematerialnych, które są **wynikiem działalności twórczej człowieka.** Prawo to jest **niezależne od substratu materialnego** (może być zatem wykorzystywane w dowolnym czasie i w dowolnym miejscu na świecie), pod warunkiem, że jest **niepowtarzalne, nie powtarzalne i wystarczająco oryginalne.**

Prawo własności intelektualnej można podzielić na dwa obszary:

1) Prawo **autorskie** (chroni m.in. oryginalne utwory literackie i artystyczne, kompozycje muzyczne, audycje telewizyjne, programy komputerowe, bazy danych, reklamy, multimedia itp.)

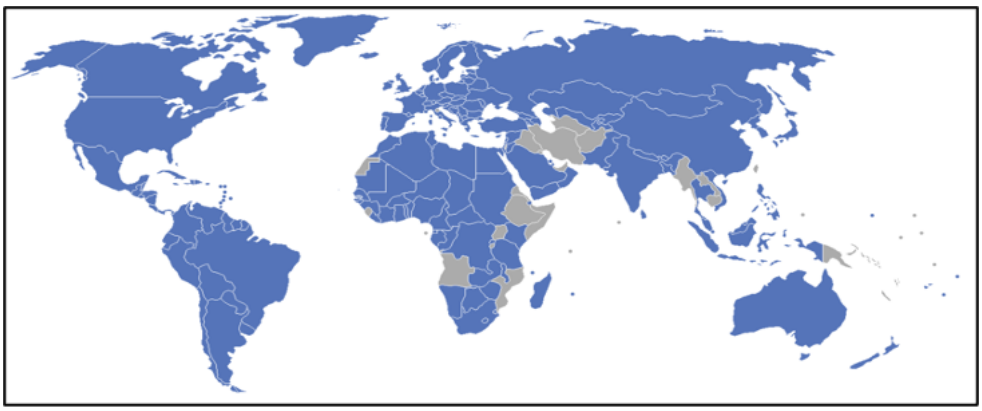
2) **Prawa przemysłowe** (chroniące np. patenty na wynalazki, wzory, modele przemysłowe, znaki towarowe, pochodzenie geograficzne itp.)

Z punktu widzenia tematyki niniejszej monografii zajmę się przede wszystkim prawem autorskim i ingerencją w to prawo.

4.11.2. Ramy legislacyjne

Ochrona praw autorskich zaczęła być po raz pierwszy poruszana na arenie międzynarodowej w XIX wieku, a do najważniejszych dokumentów prawnych dotyczących tej kwestii należą:

- **Konwencja berneńska o ochronie dzieł literackich i artystycznych**[1] (1886), która była następnie uzupełniana i zmieniana [1908 (Berlin), 1928 (Rzym), 1948 (Bruksela), 1967 (Sztokholm), 1971 (Paryż)]. Od 1967 r. jest ona administrowana przez **WIPO** *(Światową Organizację Własności Intelektualnej)*.



Obraz 73 - Lista krajów. Państwa, które przyjęły Konwencję Berneńską, zaznaczono kolorem niebieskim.**[2]**

- Porozumienie w sprawie handlowych aspektów praw własności intelektualnej, które jest jednym z załączników do Porozumienia ustanawiającego Światową Organizację Handlu (WTO) - zob. komunikat nr 191/1995 Coll., (**TRIPS - Trade Related Aspects of Intellectual Property Rights**)[3]
- Międzynarodowa konwencja o ochronie wykonawców, producentów fonogramów oraz organizacji nadawczych z 26 października 1961 r. (dekret nr 192/1964 Dz. U., zmieniony poprawką nr 157/1965 Dz. U.) - **Konwencja rzymska**[4]
- Traktat Światowej Organizacji Własności Intelektualnej o prawie autorskim Genewa 1996 z 20 grudnia 1996 r. (zob. komunikat nr 33/2002 Dz.U.), (**WCT - WIPO Copyright Treaty**)[5]
- Traktat Światowej Organizacji Własności Intelektualnej o artystycznych wykonaniach i fonogramach Genewa 1996 z 20 grudnia 1996 r. (zob. komunikat nr 48/2002 Dz.U.), (**WPPT - Traktat WIPO o artystycznych wykonaniach i fonogramach**).[6]

- Konwencja o ochronie producentów fonogramów przed nieuprawnionym zwielokrotnianiem ich fonogramów z dnia 29 października 1971 r. (zob. dekret 32/1985 Dz.U.) - **Konwencja genewska**[7]
- Powszechna konwencja o prawie autorskim, zrewidowana w Paryżu 24 lipca 1971 r. (zob. dekret nr 134/1980 Dz.U.) [8]
- Dyrektywa Rady 91/250/EWG z dnia 14 maja 1991 r. w sprawie ochrony prawnej programów komputerowych,
- Dyrektywa Rady 92/100/EWG z dnia 19 listopada 1992 r. w sprawie prawa najmu i użyczenia oraz niektórych praw w zakresie własności intelektualnej związanych z prawem autorskim, z późniejszymi zmianami,
- Dyrektywa Rady 93/83/EWG z dnia 27 września 1993 r. w sprawie koordynacji niektórych przepisów dotyczących prawa autorskiego oraz praw pokrewnych prawu autorskiemu w odniesieniu do przekazu satelitarnego oraz przekazu kablowego,
- Dyrektywa Rady 93/98/EWG z dnia 29 października 1993 r. w sprawie harmonizacji czasu ochrony prawa autorskiego i niektórych praw pokrewnych, z późniejszymi zmianami,
- Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych,
- Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym,
- Dyrektywa 2001/84/WE Parlamentu Europejskiego i Rady z dnia 27 września 2001 r. w sprawie prawa autora do wynagrodzenia z tytułu odsprzedaży oryginalnego egzemplarza dzieła sztuki,
- Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej.
- Konwencja Rady Europy nr 185 o cyberprzestępczości.

4.11.3. Ataki niestandardowe

Na określenie zjawiska naruszeń praw autorskich i praw pokrewnych w środowisku internetowym powstało kilka terminów. Najczęściej używane terminy to **piractwo oprogramowania** (w przypadku naruszania praw autorskich w odniesieniu do programów komputerowych) i **piractwo audiowizualne** (w przypadku naruszania praw autorskich do utworów audiowizualnych - muzyki i filmu). **Jednak podstawą piractwa zarówno w** przypadku **oprogramowania, jak i materiałów audiowizualnych jest zawsze naruszenie praw autorskich lub praw pokrewnych.**[9] Ogólnym terminem obejmującym piractwo oprogramowania i audiowizualne jest piractwo internetowe (czasem także komputerowe).

Wraz z masowym pojawieniem się Internetu przestępstwa przeciwko własności intelektualnej znacznie się nasiliły. Do najczęstszych przypadków naruszenia praw autorskich w cyberprzestrzeni należą:

- *rozpowszechnianie utworu za pomocą poczty elektronicznej*, która jest najprostszym sposobem rozpowszechniania małych plików (w szczególności autorskich utworów literackich lub graficznych),

- *publikacja utworu na stronie internetowej* bez zgody autora. Jest to kolejny bardzo prosty sposób na naruszenie praw autorskich. Publikowane są mniejsze pliki (pod względem rozmiaru danych), a to nielegalne zachowanie jest zwykle szybko wykrywane.

- *rozpowszechnianie utworu poprzez umieszczenie go na wyspecjalizowanym serwerze, z* którego można go swobodnie pobrać (np. Megaupload, Rapidshare),

- *rozpowszechnianie pracy za pomocą sieci peer-to-peer (P2P)*. [10] Sieci te są w stanie przesyłać/współdzielić ogromne ilości danych (rzędu od kilku GB do kilkudziesięciu TB). To właśnie w tych sieciach dochodzi do najpoważniejszych naruszeń praw autorskich.

- *manipulowanie programami komputerowymi w celu pokonania środków technicznych podjętych przez właściciela praw autorskich w celu uniemożliwienia tworzenia kopii takich chronionych programów* (crack),

- *rozpowszechnianie utworu za pośrednictwem nośników danych bezpośrednio wśród użytkowników* (wypożyczanie i kopiowanie danych z płyt DVD, dysków twardych itp., sprzedaż nośników danych itp,)

- *wykonanie nagrania bezpośrednio w trakcie produkcji i jego późniejsze rozszerzenie* (np. wykonanie zapisu wideo pracy filmowej bezpośrednio z ekranu) - tzw. camcording,

- *niedozwolona projekcja utworów audiowizualnych*,

- *faktyczne zamówienie pracy przy komputerze*. Program komputerowy korzysta ze szczególnej ochrony i nie jest możliwe sporządzanie kopii takiego utworu, nawet na własny użytek, bez zgody właścicieli praw autorskich w rozumieniu ustawy o prawie autorskim,

- *korzystanie z programu komputerowego z naruszeniem licencji*,

- i innych.

Do najczęstszych przejawów piractwa audiowizualnego należą w szczególności: nieuprawnione rozpowszechnianie utworów audiowizualnych za pośrednictwem sieci komputerowych, uzyskiwanie nagrań utworów filmowych bezpośrednio podczas seansów kinowych, a następnie "umieszczanie" ich do pobrania w cyberprzestrzeni, rozpowszechnianie oryginalnych nośników z utworami filmowymi lub muzycznymi z naruszeniem umowy licencyjnej, produkcja i rozpowszechnianie podrobionych oryginalnych utworów filmowych lub muzycznych oraz publiczne pokazy utworów filmowych z naruszeniem umowy licencyjnej. Ponadto czyny polegające na rozpowszechnianiu produktów oprogramowania, ingerencji w produkty oprogramowania, nielegalnej produkcji produktów oprogramowania oraz korzystaniu z produktów oprogramowania niezgodnie z umową licencyjną. Faktyczne nieuprawnione nabycie oprogramowania bez jego dalszego wykorzystania stanowi naruszenie praw autorskich.

Umieszczenie utworu (audiowizualnego lub oprogramowania) **w** cyberprzestrzeni (**upload**) spełnia znamiona rozpowszechniania utworu w rozumieniu ustawy o prawie autorskim i (o ile nie zezwolił na to twórca lub inna osoba uprawniona) może być karalne na gruncie prawa karnego. **Nieuprawnione korzystanie z utworu obejmuje również publikację linku do miejsca w cyberprzestrzeni, z którego można uzyskać utwór**.

Jeśli chodzi o porównanie z ustawodawstwem zagranicznym, warto wspomnieć o francuskiej ustawie HADOPI,[11] , która miała na celu ochronę przed piractwem internetowym. Na mocy tej ustawy utworzono specjalne biuro zajmujące się wykrywaniem nielegalnego pobierania materiałów chronionych prawem autorskim. Użytkownicy, którzy ściągali z Internetu muzykę i filmy bez płacenia za nie (z wyjątkiem utworów rozpowszechnianych bezpłatnie),

otrzymywali trzykrotne ostrzeżenie, a jeśli nie zastosowali się do tych ostrzeżeń, dany urząd miał prawo odłączyć ich od Internetu na okres do jednego roku.[12] Jednak nawet tak surowe prawo nie ograniczyło liczby nielegalnych pobrań utworów chronionych prawem autorskim. Jednocześnie zrodziło to szereg pytań dotyczących dopuszczalności ingerencji w podstawowe prawa i wolności człowieka bez decyzji sądu.[13] Ustawa o HADOPI została uchylona 10 lipca 2013 r.

Termin "Warez" jest również często używany w odniesieniu do piractwa internetowego. **Warez to po** prostu **forma piractwa komputerowego,** w której technologia informatyczna jest jedynie środkiem przyspieszającym rozpowszechnianie nielegalnych kopii utworów chronionych prawem autorskim za pośrednictwem Internetu. Fora warezowe są obecnie wykorzystywane głównie do pobierania cracków i keygenów, ale także kompletnych, zmodyfikowanych programów, filmów i muzyki. Końcowy produkt sceny warezowej nazywany jest **wydaniem.** Aby chronić swoją prywatność, klienci forów warezowych korzystają z serwerów proxy i bouncerów, które maskują ich adres IP, zapobiegając w ten sposób ewentualnemu śledzeniu. Faktyczna komunikacja i składanie ofert na uwolnienia odbywa się w utworzonych w tym celu prywatnych pokojach w Internecie, do których dostęp mają tylko członkowie grupy.

Możliwości stosowania sankcji karnych w Republice Czeskiej

Udostępnianie plików, czy to w ramach magazynu, czy sieci P2P, może być karane na podstawie paragrafu **270** (Naruszenie praw autorskich, praw pokrewnych i praw do baz danych) lub **paragrafu 231** (Posiadanie i przechowywanie urządzenia dostępowego i hasła do systemu komputerowego oraz innych tego typu danych) Kodeksu karnego.

Możliwości ścigania karnego w Polsce

Kwestie własności intelektualnej w Polsce zostały uregulowane w dwóch podstawowych aktach prawnych: ustawie o prawie autorskim i prawach pokrewnych oraz ustawie Prawo własności przemysłowej.

Kodeks karny zawiera dwa artykuły dotyczące naruszania lub kradzieży własności intelektualnej:

Art. 115: 1. Kto przywłaszcza sobie autorstwo albo wprowadza w błąd co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Oraz art. 278 (kradzież)

*§ 1. Kto zabiera cudzą rzecz ruchomą w celu przywłaszczenia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § **2**. Tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej.*

---

[1] Dostępne w Internecie. [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=34669&nr=133~2F1980&rpp=100#local-content; http://www.zakonyprolidi.cz/cs/1985-19

[2] *Konwencja berneńska o ochronie dzieł literackich i artystycznych.* [online]. [cyt. 15.7.2016]. Dostępny pod adresem: https://cs.wikipedia.org/wiki/Bernsk%C3%A1_%C3%BAmluva_o_ochran%C4%9B_liter%C3%A1rn%C3%ADch_a_um%C4%9Bleck%C3%BDch_d%C4%9Bl. Prezentowana mapa ma charakter poglądowy i nie przedstawia rzeczywistego podziału geopolitycznego świata. Pełną listę krajów, które ratyfikowały Traktat WIPO, można znaleźć pod adresem: http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15.

[3] Dostępne w Internecie. [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://www.mkcr.cz/assets/autorske-pravo/sb51-95.pdf

[4] Dostępne w Internecie. [online]. [cyt. 2016-07-15]. Dostępne na stronach: http://www.zakonyprolidi.cz/cs/1964-192; http://www.zakonyprolidi.cz/cs/1965-157

[5] Dostępne w Internecie. [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://www.mkcr.cz/assets/autorske-pravo/sb015-02m.pdf

[6] Dostępne w Internecie. [online]. [cyt. 2016-07-15]. Dostępny pod adresem: https://www.mkcr.cz/assets/autorske-pravo/sb021-02m.pdf

[7] Dostępne w Internecie. [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://www.zakonyprolidi.cz/cs/1985-32

[8] Dostępne w Internecie. [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://www.zakonyprolidi.cz/cs/1980-134

[9] Więcej na ten temat zob. VOLEVECKÝ, Petr. Cyberprzestępstwa w kodeksie karnym. *Trestní právo*, 2010, t. 14, nr 7-8, s. 34 i nast.

[10] Przystępując do P2P, użytkownik domyślnie zaczyna automatycznie udostępniać swoje treści innym (zwykle nieznanym sobie) użytkownikom. Zazwyczaj podczas pobierania automatycznie konfigurowane jest przesyłanie pobranych materiałów.

[11] **HADOPI** (Wysoki Urząd ds. Ochrony Praw Autorskich i Rozpowszechniania Utworów w Internecie), Fr: ***Loi favorisant la diffusion et la protection de la création sur Internet.***

[12] Do podjęcia tej decyzji Urząd nie potrzebował orzeczenia sądu. Zgodnie z opinią Trybunału Konstytucyjnego Fr. z 22 listopada 2009 r., do odłączenia od sieci wymagana jest zgoda sądu.

[13] Na przykład *Francja chce zakazać piractwa internetowego.* [online]. [cyt. 15.7.2016]. Dostępny pod adresem: http://www.blisty.cz/2009/5/13/art46807.html

Surowe prawo przeciwko piratom muzycznym i filmowym nie pomogło Francji. [online]. [cyt. 15.7.2016]. Dostępny pod adresem: http://technet.idnes.cz/prisny-zakon-proti-hudebnim-a-filmovym-piratum-francii-nepomohl-phi-/sw_internet.asp?c=A100330_095705_sw_internet_vse

Francja rezygnuje z kontrowersyjnego prawa Hadopi po wydaniu milionów [online]. [cyt. 2016-07-15]. Dostępny pod adresem: https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy i.

4.13. Sniffing (wąchanie)

Sniffing to metoda nielegalnego przechwytywania danych przechodzących przez sieć komputerową podczas komunikacji pomiędzy świadczoną usługą a systemem komputerowym za pomocą tzw. **sniffera.** [1]

Technicznie rzecz biorąc, sniffing oznacza przechwytywanie i odczytywanie pakietów TCP. Z punktu widzenia bezpieczeństwa sniffing może być również określany mianem monitorowania sieci lub monitorowania ruchu sieciowego i jest jednym ze standardowych sposobów diagnostyki sieci, czyli diagnozowania anomalii w ruchu sieciowym. Monitorowanie sieci może wtedy wykazać np. niestandardową komunikację systemu komputerowego zainfekowanego złośliwym oprogramowaniem itp. Faktyczna działalność administratorów sieci w przypadku monitorowania sieci nie jest nielegalna (chyba że dopuszczają się oni innych czynów, które mogą spowodować odpowiedzialność prawną - np. instalują keyloggera lub inne złośliwe oprogramowanie w systemie komputerowym bez wiedzy użytkownika), ponieważ umożliwia im to utrzymanie sieci komputerowej i zarządzanie nią.

Do monitorowania ruchu sieciowego wykorzystuje się wiele narzędzi (np. Wireshark[2] , NetWorx, PRTG Network monitor itp.)

Aby sniffing można było uznać za jeden z przejawów cyberprzestępczości, osoba wykonująca takie działanie musi działać nielegalnie, zazwyczaj bez zgody lub wiedzy użytkownika. Na podstawie danych przechwyconych podczas sniffingu atakujący może wydobyć i skompilować poufne informacje o użytkowniku, np. dane logowania (nazwa użytkownika i hasło), wiadomości e-mail lub komunikację VOIP, informacje o używanych usługach itp. Do sniffowania można również wykorzystać złośliwe oprogramowanie, np. trojany, keyloggery lub programy szpiegujące.

Password Sniffer Spy. Nazwy i hasła są zamazane.[3]

Możliwości stosowania sankcji karnych w Republice Czeskiej

De facto takie działania można określić jako **nielegalne przechwytywanie i rejestrowanie ruchu telekomunikacyjnego**. Opisane powyżej postępowanie z pewnością narusza podstawowe prawa i wolności człowieka, w szczególności **art. 13** Karty, i **jest całkowicie obojętne, czy nielegalnego sniffingu dokonuje napastnik z zewnątrz czy administrator sieci.** Zgodnie z normami prawa karnego taki czyn mógłby być objęty **paragrafem 182(1)** (Naruszenie tajemnicy przekazywanych wiadomości) Kodeksu karnego, a w przypadku niewłaściwego wykorzystania uzyskanych w ten sposób informacji mógłby stanowić przestępstwo z paragrafu **182(2)** Kodeksu karnego. Jeśli wspomniane nielegalne działanie zostanie wykonane przez pracownika poczty, operatora usług telekomunikacyjnych lub systemu komputerowego albo inną osobę wykonującą czynności związane z komunikacją, może ono wypełniać znamiona przestępstwa z **artykułu 185(5)** Kodeksu karnego.

Możliwości ścigania karnego w Polsce

W Polsce wąchanie jest przestępstwem karanym zgodnie z przepisami:

Naruszenie tajemnicy komunikacji (sniffing) - art. 267 § 3 Kodeksu karnego.

---

[1] **Sniffing** to angielskie słowo oznaczające - **wąchać, wąchać**.

[2] Więcej informacji na temat korzystania z oprogramowania Wireshark można znaleźć w części *Jak używać* programu *Wireshark do przechwytywania, filtrowania i sprawdzania pakietów.* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

MINAŘÍK, Pavel. *Wireshark - analiza pakietów dla wszystkich.* [online]. [cit.18.8.2016]. Dostępny pod adresem: https://www.systemonline.cz/it-security/wireshark-paketova-analyza-pro-vsechny.htm

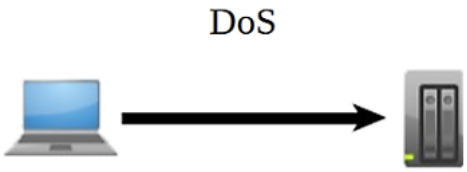
[3] *Password Sniffer Spy.* [online]. [cyt. 2016-08-18]. Dostępny pod adresem: http://securityxploded.com/password-sniffer-spy.php

4.14. Ataki DoS, DDoS, DRDoS

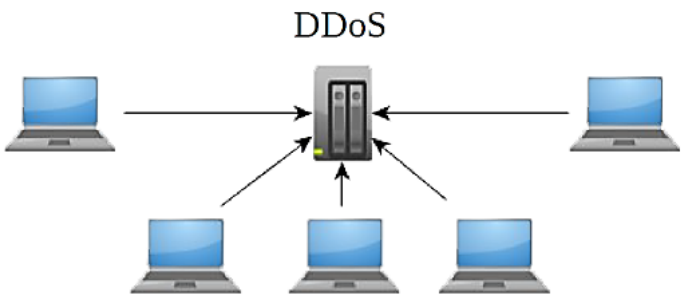
Termin **DoS** jest skrótem od angielskiego słowa "***denial of service***" *(odmowa **usługi)***, które na język polski można przetłumaczyć jako "odmowa świadczenia usługi". Jest to jedna z form ataków na usługi (internetowe), której celem jest wyłączenie lub zmniejszenie wydajności atakowanego urządzenia technicznego.[1] Atak ten jest realizowany przez przytłoczenie atakowanego systemu komputerowego (lub elementu sieci) powtarzającymi się żądaniami wykonania czynności przez system komputerowy. Atak ten może być również przeprowadzony poprzez przeciążenie kanałów informacyjnych między serwerem a komputerem użytkownika lub poprzez przeciążenie wolnych zasobów systemowych. System zaatakowany przez atak DoS objawia się w szczególności niezwykłym spowolnieniem działania usługi, całkowitą lub chwilową niedostępnością usługi (np. strony WWW) itp.

Różnica między atakami DoS, DDoS i DRDoS polega przede wszystkim na sposobie przeprowadzenia ataku. W celach ilustracyjnych do każdego typu ataku dołączono obrazy przedstawiające sposób jego przeprowadzenia.

W przypadku **odmowy usługi (Denial of Service, DoS)** istnieje tylko jedno źródło ataku. Ten rodzaj ataku jest stosunkowo łatwy do odparcia, ponieważ możliwe jest zablokowanie ruchu ze źródła ataku.

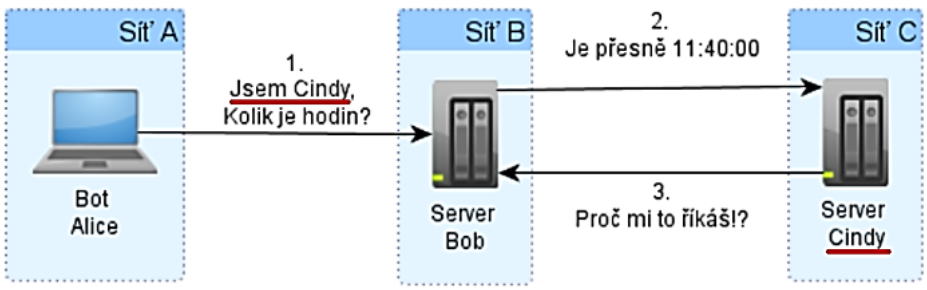


W przypadku **DDoS** (**Distributed Denial of Service**) docelowy system komputerowy zostaje przytłoczony **pakietami wysyłanymi z wielu systemów komputerowych, które są rozmieszczone geograficznie, co utrudnia obronę i identyfikację atakującego.** Takie ataki były stosowane na przykład przeciwko Yahoo! Inc., serwisy e-commerce itp.[2] Bardzo często do tego typu ataków wykorzystywane są botnety lub działania użytkowników wspierających określoną kampanię internetową (patrz poniżej - Anonymous i LOIC).



W przypadku **DRDoS** (**Distributed Reflected Denial of Service**) jest to atak typu spoofed distributed DoS wykorzystujący mechanizm zwany odbiciem. Atak polega na wysyłaniu spreparowanych żądań połączenia do dużej liczby systemów komputerowych, które następnie odpowiadają na te żądania, ale nie do inicjatora połączenia, lecz do ofiary. Dzieje się tak dlatego, że w spreparowanych żądaniach połączenia jako adres źródłowy podawany jest adres ofiary, która jest następnie zalewana odpowiedziami na te żądania. Wiele systemów komputerowych staje się w ten sposób mimowolnymi uczestnikami ataku, odpowiadając poprawnie na żądanie połączenia.

Ataki DoS, DDoS, DRDoS bardzo często wykorzystują luki w systemie operacyjnym, działających programach lub protokołach sieciowych - UDP, TCP, IP, http itp.



Istnieje kilka podstawowych metod ataku DoS lub DDoS, z których najbardziej znane to:[3]

- Ping-Flood

Dzięki protokołowi Internet Control Message Protocol i narzędziu Ping (Packet Internet Groper) możliwe jest użycie polecenia "ping" do określenia "żywotności" systemu komputerowego o danym adresie IP oraz do określenia czasu odpowiedzi takiego systemu. W ataku Ping-Flood ofiara jest zalewana dużą liczbą tzw. pakietów ICMP Echo Request, na które ofiara zaczyna odpowiadać, wysyłając tzw. pakiety ICMP Echo Replay. Atakujący ma nadzieję, że w ten sposób przeciąży przepustowość łącza ofiary (zarówno dla odbierania, jak i wysyłania danych). Sam atak można dodatkowo wzmocnić, ustawiając pakiet ping emitujący pakiety ICMP na flood. Wówczas pakiety te zaczną być wysyłane bez oczekiwania na odpowiedź. Jeśli docelowy system komputerowy nie dysponuje wystarczającą mocą obliczeniową, można go w ten sposób uczynić niedostępnym.

- Przepełnienie wolnych zasobów systemowych (*SYN-Flood*)

SYN-Flood to rodzaj ataku, w którym atakujący próbuje przytłoczyć swoją ofiarę dużą liczbą żądań połączenia. Atakujący wysyła sekwencję pakietów poleceń SYN (zwanych pakietami SYN) do docelowego systemu komputerowego (ofiary), a docelowy system odpowiada na każdy pakiet SYN wysyłając pakiet SYN-ACK, ale atakujący nie odpowiada dalej. Docelowy system komputerowy czeka na ostateczne potwierdzenie, zwane pakietem ACK, od inicjatora połączenia (atakującego) i posiada zasoby przydzielone dla tego połączenia, ale ma ich ograniczoną ilość. Może to spowodować wyczerpanie zasobów systemowych celu ataku.[4]

- Spofing adresu źródłowego (*spoofing IP*)

Spoofing IP to działania polegające na spoofingu (fałszowaniu) adresu źródłowego wysyłanych pakietów, kiedy to atakujący inicjujący połączenie z maszyny A o adresie IP **a.b.c.d** jako adresie źródłowym wstawia np. **adres IP d.c.b.a do** wysyłanych pakietów i wysyła je do celu B. Miejsce docelowe B odpowiada na ten adres źródłowy, tzn. nie kieruje odpowiedzi na adres IP a.b.c.d, ale na adres IP **d.c.b.a.** Tę metodę można wykorzystać do nasilenia (wzmocnienia) ataków DoS, DDoS. Atakujący stosuje tę technikę, gdy nie potrzebuje odpowiedzi od miejsca docelowego na swoje żądanie nawiązania połączenia, ale chce je tylko zaangażować. Jeśli atakujący umieści adres IP celu ataku (np. a.a.a.a) jako źródłowy adres IP w wysyłanych przez siebie pakietach i wyśle te pakiety do wielu innych systemów komputerowych (adresów IP), to odpowiadają one systemowi komputerowemu a.a.a.a. W ten sposób realizowany jest atak DRDoS.

- Atak **smerfów**

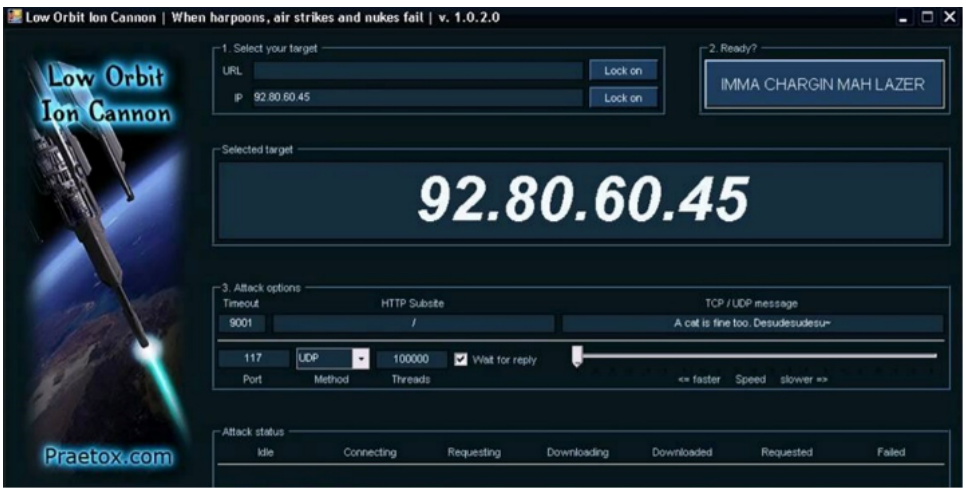
Atak ten jest realizowany poprzez błędną konfigurację systemu, która umożliwia wysyłanie pakietów do wszystkich komputerów podłączonych do sieci komputerowej za pośrednictwem adresu rozgłoszeniowego.

Celem ataków DoS/DDoS zazwyczaj **nie** jest **zainfekowanie komputera** lub systemu komputerowego **ani pokonanie zabezpieczeń, np.** chroniącego go **hasła,** ale **obezwładnienie go lub czasowe wyłączenie** poprzez serię powtarzających się żądań. Zazwyczaj powoduje to ograniczenie lub zablokowanie dostępu do usług.

Aby móc prawnie ukarać "atakującego" za ataki DoS lub DDoS, należy ustalić, czy jego **działania były nielegalne, a** jeśli tak, to jak poważne. Chodzi o to, że charakter ataku DDoS może mieć np. całkowicie prawidłowe działanie internautów, którzy w jednym momencie (w krótkim czasie) próbują połączyć się z serwerem internetowym firmy oferującej zniżki na bilety lotnicze i np. ogłosić, że od godz. 12.00 nastąpi powszechna obniżka cen biletów lotniczych o 75%. Duża liczba użytkowników może też korzystać z serwisu internetowego popularnego dziennika medialnego, który informuje o ważnym lub interesującym dla mediów wydarzeniu, takim jak objęcie urzędu przez nowego prezydenta, śmierć ważnej osobistości itp. Jeśli docelowy system komputerowy (serwer WWW) jest niewymiarowy lub źle skonfigurowany (nie jest w stanie obsłużyć wymaganej liczby dostępów), ulegnie awarii w podobny sposób, jak w przypadku ukierunkowanego ataku DDoS. Powstaje zatem pytanie, czy użytkownicy, którzy próbowali zalogować się na stronie w danym czasie i w ten sposób de facto spowodowali zamknięcie danego serwisu, powinni zostać ukarani.

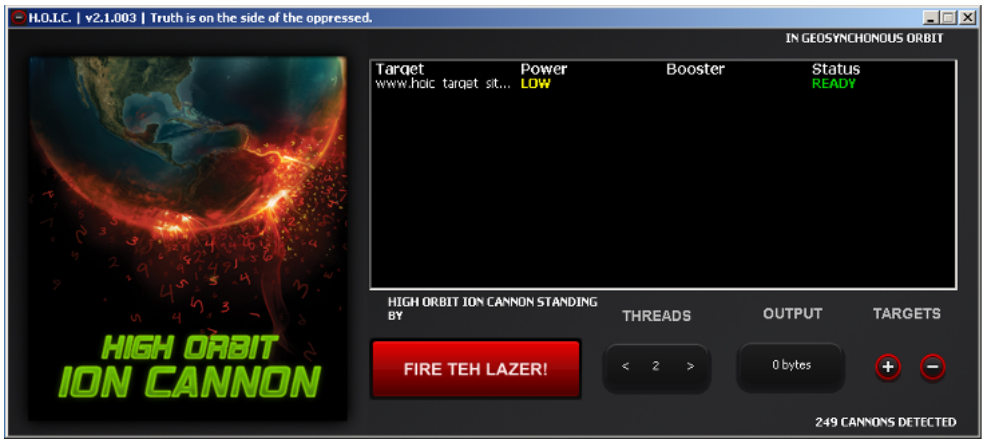
Uważam, że w opisanych powyżej przypadkach, mimo że użytkownicy spowodowali zmasowany atak DDoS na usługi dostawcy, nie jest realistyczne, ani nawet możliwe, aby ukarać tych "pseudo-atakujących" za pomocą jakichkolwiek środków prawnych, ponieważ ich działania od początku nie były nielegalne.

Innym przypadkiem byłaby jednak sytuacja, w której atakujący, na przykład, zbierają się za pośrednictwem Internetu i w określonym czasie, dzięki ponownemu zalogowaniu się do udostępnionej usługi, przejmują nad nią kontrolę.[5] Takie przypadki miały miejsce np. w kontekście protestów przeciwko ACTA (Anti-Counterfeiting Trade Agreement) w 2012 r., kiedy jedną z możliwości przeprowadzenia tych ataków było użycie urządzenia rozpowszechnianego przez zwolenników Anonymous, LOIC (Low Orbit Ion Cannon).



LOIC (Low Orbit Ion Cannon)[6]

Wyimaginowanym następcą LOIC było oprogramowanie HOIC (High Orbit Ion Cannon), które zostało opracowane jako zamiennik LOIC.



HOIC (Wysokoorbitalne Działo Jonowe)[7]

Działania napastników w tym przypadku są z pewnością bezprawne, ponieważ napastnicy mieli świadomość lub przynajmniej rozumieli, że ich działania naruszają prawa innych osób. W takim przypadku można zastosować środki prawne z zakresu prawa karnego, administracyjnego i cywilnego.

Dzięki przyjęciu Konwencji o cyberprzestępczości, nie tylko w krajach Unii Europejskiej, powinna nastąpić harmonizacja prawa karnego, a w szczególności przyjęcie takich norm prawnych, które umożliwią karanie ataków DoS lub DDoS na podstawie prawa karnego danego kraju. Rozdział II - Środki, które należy podjąć na szczeblu krajowym, Sekcja 1 - Przestępstwa przeciwko poufności, integralności i użyteczności danych i systemów komputerowych, Artykuł 4 - Ingerencja w dane, Konwencji wzywa do ochrony przed takimi atakami oraz do wdrożenia środków prawnych:

1. *Each Party shall take such legislative and other measures as may be necessary to make it a criminal offence under its national law to intentionally damage, erase, degrade, alter* ***or suppress computer data.***

2. *Strona może zastrzec sobie prawo do uznania zachowania opisanego w ust. 1 za przestępstwo tylko wtedy, gdy powoduje ono poważną szkodę.*

Możliwości stosowania sankcji karnych w Republice Czeskiej

Z brzmienia **paragrafu 230(2)** (Nieuprawniony dostęp do systemu komputerowego i nośnika informacji) TZK wynika, że:

Kto uzyskuje dostęp do systemu komputerowego *lub nośnika informacji oraz*

(a) w sposób nieuprawniony wykorzystuje dane przechowywane w systemie komputerowym lub na nośniku informacji,
(b) w sposób nieuprawniony usuwa ***dane*** *przechowywane w systemie komputerowym lub na nośniku informacji lub w inny sposób niszczy, uszkadza, zmienia,* ***tłumi****, obniża ich jakość lub czyni je bezużytecznymi...*

Z powyższego przepisu wynika, że napastnik dopuszczający się ataku DoS lub DDoS, aby zostać pociągniętym do odpowiedzialności karnej, musi **nielegalnie uzyskać dostęp do systemu komputerowego, a następnie wyprzeć znajdujące się w nim dane.** [8]

W tym przypadku dwa odrębne artykuły (rozdział II, sekcja 1, **art. 2 - Bezprawny dostęp** i **art. 4 - Ingerencja w dane**) konwencji o cyberprzestępczości zostały de facto połączone w jedno postanowienie.

Tym samym ustawodawca de facto uniemożliwił karanie sprawców ataków DoS lub DDoS na drodze karnej, gdyż wymagane jest, aby sprawca **uzyskał nieuprawniony dostęp do systemu komputerowego**. Tak więc taka interpretacja prawna wymagająca nieuprawnionego dostępu do systemu komputerowego pozwala na ukaranie sprawcy jedynie za zachowania wymienione w Konwencji o cyberprzestępczości w **Artykule 2 - Nieuprawniony dostęp: "***Każda ze Stron podejmie takie środki ustawodawcze i inne, jakie mogą być konieczne do uznania za przestępstwo karne, zgodnie z jej prawem krajowym, umyślnego* ***uzyskania nieuprawnionego dostępu do całości lub części systemu komputerowego"****.*

Z technicznego punktu widzenia ataki DoS lub DDoS **nie powodują uzyskania dostępu do** systemu komputerowego lub jego części, a przynajmniej nie jest to ich głównym celem.[9]

Z powyższych względów jestem przekonany o konieczności wprowadzenia do czeskiego ustawodawstwa odrębnego przestępstwa, które chroniłoby systemy komputerowe przed DoS, DDoS, DRDoS itp. i które w szczególności przestrzegałyby postanowień Konwencji o cyberprzestępczości. Na przykład, można użyć następującego sformułowania:

"Kto utrudnia korzystanie z systemu komputerowego bez upoważnienia.... "

Obecnie teoretycznie możliwe jest karanie sprawców ataków DoS i DDoS za przestępstwo z paragrafu **228** (uszkodzenie mienia) kodeksu karnego.[10] Jednak warunkiem skorzystania z instytucji szkody majątkowej musiałby być fakt, że mienie to (w tym system komputerowy) zostało zniszczone, uszkodzone lub stało się bezużyteczne. Warunek ten dotyczy jednak zasadniczo tylko tego typu ataków, jeśli chodzi o pewną czasową bezużyteczność.

W tym kontekście pojawia się jednak pytanie, w jaki sposób i w jaki sposób zostanie określona rzeczywista szkoda w przypadku uszkodzenia mienia oraz przeciwko komu będzie można ją odzyskać.[11]

Inne przestępstwa, które atakujący przeprowadzający atak DoS lub DDoS może popełnić w pewnych okolicznościach, obejmują paragraf 272 (Ogólne zagrożenie), paragraf 273 (Ogólne zagrożenie przez zaniedbanie) kodeksu karnego.

Z punktu widzenia ewentualnego ścigania karnego sprawcy ataków DoS lub DDoS istotne jest również ustalenie (identyfikacja) sprawcy tego konkretnego przestępstwa. Pozostaje pytanie, **kto powinien być pociągnięty do odpowiedzialności karnej jako sprawca, który np.** spowodował niedostępność określonej usługi (np. aplikacji internetowej).

W tym przypadku zastosowanie ma art. 268 Kodeksu karnego, który stanowi, że:

§ 1. Kto, nie będąc do tego upoważnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnych informacji albo w inny sposób uniemożliwia lub znacznie utrudnia osobie upoważnionej zapoznanie się z nimi, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

---

[1] Por. np. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO i Pedro GARCÍA-TEODORO. Ocena ataku DoS o małej szybkości przeciwko serwerom aplikacji. *Computers & Security*, 2008, vol. 27, nr 7-8, s. 335-354.

CARL, Glenn, Richard BROOKS i Rai SURESH. Wykrywanie odmowy usługi na podstawie falek. *Computers & Security*, 2006, vol. 25, nr 8, s. 600-615.

RAK, Roman i Radek KUMMER. Zagrożenia informacyjne w latach 2007 - 2017. *Magazyn Bezpieczeństwa*, 2007, t. 14, nr 1, s. 3.

[2] Ponadto, na przykład, ataki DoS na strony internetowe urzędu prezydenckiego, parlamentu, ministerstw, mediów i dwóch estońskich banków - Estonia (2007). *Estonia odzyskuje siły po potężnym ataku DDoS.* [online]. [cytowany 4 marca 2010] Dostępny w: http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

[3] Por. JIROVSKÝ, Václav. *Cyberprzestępczość. Nie tylko o hakowaniu, łamaniu* zabezpieczeń*, wirusach i trojanach bez tajemnic.* Praga: Grada, 2007, s. 66.

[4] W tym miejscu warto wspomnieć o **Handshake -** procesie, którego zadaniem jest ustalenie parametrów kanału komunikacyjnego między dwoma podmiotami przed rozpoczęciem właściwej komunikacji. Handshake jest wykorzystywany na przykład w Internecie do otwierania połączenia TCP (tzw. **trójstronny handshake, czyli** wymiana trzech datagramów), a dopiero potem następuje właściwa transmisja danych. Nawiązanie połączenia TCP wymaga wykonania trzech osobnych kroków:

1. **Strona inicjująca połączenie (klient) wysyła segment TCP z ustawioną flagą SYN.**
2. **Strona odbierająca połączenie (serwer) odpowiada segmentem TCP z ustawionymi flagami SYN+ACK.**
3. **Klient odpowiada segmentem TCP z ustawioną flagą ACK**

Inne segmenty TCP mają ustawioną tylko flagę ACK.

Więcej szczegółów można znaleźć np. w dokumencie *TCP handshake krok po kroku.* [online]. [cyt. 18.8.2016]. Dostępny pod adresem: http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000

Istnieją inne sposoby ataku DoS, np. "TearDrop", "Nuke", "Peer-to-Peer attack" itp. Por. [online]. [cyt. 25.9.2010]. Dostępny pod adresem: http://cs.wikipedia.org/wiki/Denial_of_Service

[5] Może się również zdarzyć, że atakujący rozsyła fałszywe informacje, np. *"6 czerwca 2016 r. od 12 do 13 bilety Lufthansy będą darmowe! Kliknij tutaj, aby uzyskać więcej informacji."*

[6] *LOIC* [online]. [cyt. 18.8.2016]. Dostępny pod adresem: https://i.ytimg.com/vi/QAbXGy0HbrY/maxresdefault.jpg

[7] *HOIC* [online]. [cyt. 18.8.2016]. Dostupné z: https://npercoco.typepad.com/.a/6a0133f264aa62970b0167612ea130970b-pi

[8] Tłumienie oznacza działania wymienione w art. 4 konwencji o cyberprzestępczości.

[9] Jeśli na przykład zalew PING jest wykorzystywany do ataku DoS lub DDoS, można sobie wyobrazić całą sytuację jako ciągłe połączenie (i późniejsze rozłączenie) z określonym numerem telefonu. Powoduje to sytuację, w której zaatakowany numer telefonu nie może wykonać własnego połączenia (funkcja dzwonienia jest zablokowana), ale żaden z dzwoniących (atakujących) nie uzyskuje żadnych danych przechowywanych na zaatakowanym telefonie.

[10]Zob. art. 228 ust. 1 TZK:

"Kto cudzą rzecz niszczy, uszkadza lub czyni bezużyteczną i przez to powoduje szkodę w cudzym mieniu, która nie jest nieznaczna, podlega karze pozbawienia wolności do roku, zakazu prowadzenia działalności albo przepadku rzeczy lub innej wartości majątkowej".

Niewielka szkoda oznacza szkodę w wysokości co najmniej 5 000 CZK (zob. art. 138 ust. 1 TZK)

[11]Czy te szkody zostaną wyegzekwowane od każdego atakującego? Czy też szkody te zostaną "rozdysponowane" pomiędzy atakujących?

4.15. Rozpowszechnianie szkodliwych treści

Obecnie można wyróżnić dwa podstawowe typy rozpowszechniania szkodliwych treści. Są to: **rozpowszechnianie niedozwolonych rodzajów pornografii** oraz **rozpowszechnianie treści** nawołujących **do nienawiści i ekstremistycznych.**

W przypadku rozpowszechniania **zabronionych rodzajów pornografii** chodzi głównie o rozpowszechnianie materiałów pornograficznych przedstawiających stosunek ze zwierzętami oraz rozpowszechnianie (lub samo posiadanie) "pornografii dziecięcej" (materiałów przedstawiających lub w inny sposób wykorzystujących dziecko - osobę poniżej 18 roku życia lub osobę, która sprawia wrażenie dziecka). Rzeczywiste metody rozpowszechniania są bardzo różnorodne. Począwszy od zwykłego oferowania tego rodzaju pornografii do pobrania, poprzez umieszczanie jej w Internecie, rozpowszechnianie w sieciach wymiany komputerów, wysyłanie pocztą elektroniczną itp.

Wykorzystywanie dzieci do produkcji materiałów pornograficznych, a następnie rozpowszechnianie takich materiałów jest jedną z form przestępczości, którą zobowiązała się ścigać większość krajów świata, niezależnie od tego, czy ratyfikowały one Konwencję o cyberprzestępczości. Mimo że w tej dziedzinie podejmowane są znaczne działania (nie tylko przez państwa, organizacje pozarządowe i inne), problem wykorzystywania seksualnego dzieci w Internecie nadal pozostaje aktualny.

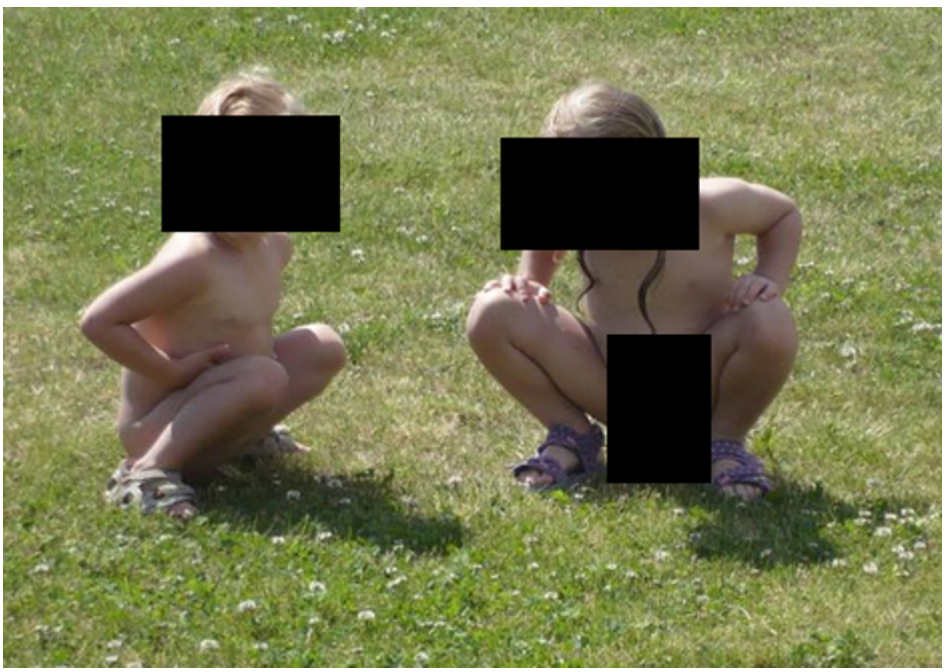
Zjawisko pornografii dziecięcej towarzyszy społeczeństwu od pierwszych chwil, gdy możliwe stało się utrwalenie na jakimkolwiek nośniku (papier, film itp.) samego faktu wykorzystania. Prawda jest jednak taka, że Internet umożliwił masowe rozpowszechnianie takich materiałów wśród indywidualnych użytkowników, a także większy stopień anonimowości.

Problem, jaki stwarza Internet i cyberprzestrzeń, wiąże się z wcześniejszym stwierdzeniem, że *"Internet nie zapomina"*. Jeśli jakikolwiek materiał jest przesyłany lub transmitowany za pośrednictwem TIK, zawsze może istnieć gdzieś jego kopia. Przykładem z Czech, gdzie użytkownicy sami tworzą materiały pokazujące nagie dzieci, jest portal www.rajce.net. Portal ten z pewnością nie został stworzony jako środowisko do rozpowszechniania jakichkolwiek materiałów pornograficznych lub w inny sposób obraźliwych (istnieją inne strony do tego celu), jednak użytkownicy nie przestrzegają podstawowych zasad serwisu rajce.net, a w szczególności artykułu 13, który mówi:

*"**Treści przedstawiające nagie osoby**, w szczególności **poniżej 18 roku życia**, **mogą być umieszczane na Rajce wyłącznie w prywatnych albumach zabezpieczonych hasłem**; pozostałe postanowienia niniejszego regulaminu, w szczególności zakaz umieszczania treści pornograficznych lub treści bezprawnie ingerujących w prawo do ochrony dóbr osobistych osób trzecich, pozostają w tym przypadku nienaruszone."*

Niemniej jednak na tej stronie można znaleźć wiele zdjęć, choć stworzonych w dobrych intencjach (np. rozpowszechnianie zdjęć między członkami rodziny mieszkającymi daleko od siebie), które są atrakcyjne dla każdego, także dla potencjalnego napastnika. Dodatkowe informacje publikowane na tej stronie lub korelacja danych z innych źródeł dostępnych w Internecie znacznie ułatwiają np. napastnikowi znalezienie potencjalnej ofiary.

Problemem jest nie tyle samo zamieszczanie zdjęć nagich osób (ze świadomością replikacji danych), co fakt, że dane te są dostępne dla wszystkich użytkowników, a nie tylko dla ograniczonej grupy (np. wspomnianej rodziny).



Zdjęcie z rajce.net (zdjęcie jest dostępne dla wszystkich użytkowników)

Podsumowując, chcę powiedzieć, że zdecydowanie nie mam nic przeciwko robieniu zdjęć dzieciom (lub dzieleniu się niektórymi zdjęciami z najbliższą rodziną), aby zachować piękne wspomnienia. Mam jednak problem z bezmyślnym udostępnianiem tych zdjęć każdemu w cyberprzestrzeni.

Jednym z najnowszych projektów, w ramach którego podjęto problem wykorzystywania dzieci w Internecie, była praca organizacji Terre des Hommes Netherlands (THN). Firma ta stworzyła wirtualną dziesięcioletnią filipińską dziewczynkę, **Sweetie.** Sweetie przez dziesięć dni udzielała się na czatach internetowych i kontaktowało się z nią około 20 000 mężczyzn. Tysiąc z nich oferowało jej pieniądze w zamian za seks w sieci.

Szef projektu, Hans Guyt, powiedział na konferencji prasowej w Hadze, że ten rodzaj przestępczości wymaga nowego sposobu prowadzenia działań policyjnych. "*Ani drapieżcy, ani ich ofiary nie spotkają się z nami podczas naszych dochodzeń*" - powiedział.

"Stworzyliśmy wirtualną tożsamość, która reprezentowała 10-letnią Filipinkę".

"Nie przyciągnęliśmy nikogo, dopóki sam nie zaoferował nam pieniędzy" - powiedział Guyt.

Aktywiści chcieli zwrócić uwagę na rosnący problem wykorzystywania dzieci za pośrednictwem kamer internetowych. Nazywają to zjawisko "*internetową turystyką seksualną*".[1]

Możliwości stosowania sankcji karnych w Republice Czeskiej

W przypadku tworzenia, posiadania lub rozpowszechniania materiałów mieszczących się w pojęciu pornografii dziecięcej, użytkownik może zostać ukarany na podstawie **paragrafu 192** (Produkcja i inne dysponowanie pornografią dziecięcą), paragrafu **193** (Wykorzystywanie dziecka do produkcji pornografii) Kodeksu karnego. Karalny jest również udział w przedstawieniu pornograficznym lub innym podobnym przedstawieniu, w którym bierze udział dziecko (**§ 193a** TZK). Uzyskanie dostępu do pornografii dziecięcej za pomocą technologii informacyjnej lub komunikacyjnej jest również karalne (**paragraf 192(2)** kodeksu karnego).

Przestępstwem jest także produkowanie, importowanie, eksportowanie, transportowanie, oferowanie, publiczne udostępnianie, pośredniczenie, wprowadzanie do obiegu, sprzedawanie lub przekazywanie w inny sposób innemu użytkownikowi utworu fotograficznego, filmowego, komputerowego, elektronicznego lub innego utworu pornograficznego, który pokazuje przemoc lub brak szacunku dla człowieka lub który opisuje, przedstawia lub w inny sposób przedstawia stosunek seksualny ze zwierzęciem (**art. 191 ust. 1** kodeksu karnego).

W przypadku **rozpowszechniania nienawistnych i ekstremistycznych przekazów** obejmuje to w szczególności wspieranie i promowanie ruchu, który w oczywisty sposób zmierza do ograniczenia praw i wolności człowieka, wyrażanie sympatii do takiego ruchu, głoszenie nienawiści rasowej, etnicznej, narodowościowej, religijnej, klasowej lub nienawiści do innej grupy osób. Obejmuje ono także rozpowszechnianie zniesławienia za pomocą technologii informatycznych oraz, co nie mniej ważne, wysyłanie nękających wiadomości, które mieszczą się w pojęciu stalkingu lub cyberstalkingu.

Sprawy te mogą dotyczyć szeregu przestępstw, takich jak. **§ 184** (Zniesławienie), § **353 (**Groźby), § **354** (Groźne prześladowanie), § **355** (Zniesławienie narodu, rasy, grupy etnicznej lub innej grupy osób), **§ 356** (Nawoływanie do nienawiści wobec grupy osób lub do ograniczenia ich praw i wolności), **§ 403** (Zakładanie, wspieranie i promowanie ruchu mającego na celu tłumienie praw i wolności człowieka), **§ 404** (Manifestowanie sympatii dla ruchu mającego na celu tłumienie praw i wolności człowieka), **§ 405** (Zaprzeczanie, kwestionowanie, aprobowanie i usprawiedliwianie ludobójstwa) Kodeksu karnego.

Możliwości ścigania karnego w Polsce

W Polsce obowiązują następujące artykuły Kodeksu karnego:

Artykuł 200b. Publiczne rozpowszechnianie treści pedofilskich

Artykuł 202. Prezentowanie i rozpowszechnianie pornografii

---

[1] Więcej informacji można znaleźć na stronie:

Wygenerowany komputerowo "Słodziak" łapie internetowych drapieżników [online]. [cyt. 2016-08-19]. Dostępny pod adresem: http://www.bbc.com/news/uk-24818769

Holendrzy stworzyli wirtualną dziewczynę. Pomogła złapać ponad tysiąc pedofilów. [online]. [cyt. 19.8.2016]. Dostępny pod adresem: http://zpravy.idnes.cz/virtualni-holcicka-pomohla-lapit-tisic-pedofilu-fuu-/zahranicni.aspx?c=A131106_210025_zahranicni_zt

Film o **Sweetie** jest dostępny w Internecie: https://www.youtube.com/user/sweetie.

4.16. Cyberataki na sieci społecznościowe

Większość z opisanych wcześniej cyberataków (np. złośliwe oprogramowanie, phishing, spam itp.) może być przeprowadzana w środowisku sieci społecznościowych. Powodem, dla którego cyberataki na sieci społecznościowe zostały opisane oddzielnie, jest to, że przede wszystkim (ale nie wyłącznie) mają one miejsce w środowisku sieci społecznościowych.

Do takich ataków należą:

1. Cyberprzemoc
2. Cybergrooming
3. Sexting
4. Cyberstalking

4.15.1. Cyberprzemoc

W prawdziwym świecie znęcanie się polega na tym, że napastnik próbuje fizycznie lub psychicznie zranić, upokorzyć, ośmieszyć lub znieważyć inną osobę. Cyberprzemoc przenosi "klasyczne prześladowanie" do świata wirtualnego i pozwala atakującemu na użycie narzędzi i środków, które mogą mieć znacznie większy wpływ na ofiarę niż miałoby to miejsce w świecie rzeczywistym. Ze względu na wykorzystanie technologii informacyjno-komunikacyjnych i trwałość danych w cyberprzestrzeni cyberprzemoc pozwala na powtarzające się ataki na ofiarę, nawet jeśli w świecie rzeczywistym jest ona geograficznie oddalona od miejsca, w którym była pierwotnie nękana.

Cyberprzemoc może być powiązana z "tradycyjną" przemocą (np. nagranie ataku fizycznego na ofiarę, a następnie umieszczenie go w sieci). Aby można było mówić o cyberprzemocy, konieczne jest, aby do nękania wykorzystywano technologie informacyjne i komunikacyjne lub usługi oferowane w cyberprzestrzeni.

Objawy cyberprzemocy obejmują:

- **Poczucie anonimowości** (napastnik zwykle ma poczucie, że dzięki Internetowi nie można go wyśledzić).
- **Nieograniczony atak** (dzięki technologiom teleinformatycznym atakujący nie musi się martwić o czas i przestrzeń do przeprowadzenia ataku. Znęcanie się jest możliwe w każdej chwili, z każdego miejsca i przez każdego. Sam atak wymaga też znacznie mniej wysiłku niż w przypadku "tradycyjnego" zastraszania).
- **Nieograniczony zasięg napastników** (w przeciwieństwie do świata rzeczywistego, w świecie wirtualnym nie ma znaczenia wiek, płeć, siła fizyczna, pozycja napastnika w grupie itp. Dręczycielem może być dowolna osoba).
- **Nieograniczona przestrzeń i zasoby** (Internet zapewnia atakującemu de facto nieograniczoną przestrzeń i zasoby do zastraszania). Napastnik może wielokrotnie zamieszczać obraźliwe uwagi, komentarze, zdjęcia i filmy na różnych portalach, w sieciach społecznościowych itp. On może te materiały udoskonalać i "ulepszać").
- **Trudne do wykrycia** (w przeciwieństwie do tradycyjnego zastraszania, cyberprzemoc może nie mieć zewnętrznych oznak, takich jak siniaki, brak pieniędzy itp.)
- **Trwałość** [Klasyczne nękanie polega zwykle na powtarzających się pojedynczych atakach, ale częściowy atak zawsze kończy się dla ofiary. W przypadku cyberprzemocy wystarczy na przykład jeden SMS, e-mail itp., a ofiara wciąż do nich wraca (lub jest im stale przypominana, wysyłana itp.) i może żyć w traumie przez wiele miesięcy. Obraźliwe SMS-y, e-maile, zdjęcia itp. są bardziej trwałe niż pojedyncze ataki fizyczne].[1]

Najczęstsze przejawy cyberprzemocy:

1. Oszczerstwa, zastraszania, obrażania, wyśmiewania lub innego rodzaju zawstydzania (sieci społecznościowe, poczta elektroniczna, SMS, czat, ICQ, Skype, gry itp.)

2. Wykonywanie nagrań audio, wideo lub fotografii, ich obróbka graficzna lub inna, a następnie publikacja w celu zaszkodzenia (ośmieszenia) wybranej osobie.

3. Nagrywanie filmów, w których ofiara jest fizycznie atakowana lub w inny sposób psychicznie wykorzystywana i wyśmiewana. Filmy te są następnie publikowane w Internecie (tzw. Happy Slapping).

4. Tworzenie stron internetowych, kont społecznościowych (modyfikowanie oryginalnych lub tworzenie nowych profili), portali dyskusyjnych itp., które obrażają, zniesławiają lub poniżają konkretną osobę.

5. Nadużycie cudzego konta - kradzież tożsamości (poczta elektroniczna, dyskusja itp.).

6. Prowokowanie i atakowanie użytkowników na forach dyskusyjnych (czatach itp.).

7. Ujawnianie sekretów innych osób.

8. Wymuszenia przez telefon komórkowy lub Internet.

9. Nękanie i prześladowanie przez dzwonienie, wysyłanie wiadomości tekstowych lub dzwonienie.[2]

Konsekwencje niektórych ataków:

- **Amanda Todd** (15 lat). Historię, która przydarzyła się Amandzie, można obejrzeć w jej własnym filmie wideo dostępnym pod adresem: youtu.be/vOHXGNx-E7E

Amanda popełniła samobójstwo.

- **Rebecca Ann Sedwick, lat** 12, była nękana w sieci przez prawie rok, a w 2013 r. popełniła samobójstwo. Prześladowanie zaczęło się po tym, jak Rebeka przez pewien czas spotykała się z chłopakiem. Jej matka powiedziała dziennikarzom, że jej córka otrzymywała wiadomości takie jak: "Jesteś brzydka", "Dlaczego jeszcze żyjesz" i "Idź się zabić". Sytuacja zaostrzyła się do tego stopnia, że matka wycofała córkę ze szkoły w Crystal Lake i usunęła jej konto na Facebooku. Podobno musiała opuścić szkołę. Przez resztę roku matka uczyła ją w domu. We wrześniu rozpoczęła naukę w innej szkole. Wszystko zaczęło się układać, a Rebeka świetnie sobie radziła w nowej szkole. Jednak potajemnie zarejestrowała się w nowych aplikacjach, w tym w komunikatorach Kik Messenger i Ask.fm, a prześladowania zaczęły się na nowo, gdy zaczęła pytać w sieci o swoją nadwagę. Szeryf Judd powiedział, że dziewczyna była "absolutnie sterroryzowana" w mediach społecznościowych.[3]
- **Ghyslain Raza** (14 lat, Kanada), znany jako Star Wars Kid.

. Ghyslain Raza sfilmował się, odgrywając scenę walki z Gwiezdnych wojen. Próbował naśladować postać Dartha Maula. Koledzy z klasy ukradli nagranie i umieścili je w Internecie dla rozrywki innych. W ciągu kilku tygodni nagranie to obiegło cały świat, było wielokrotnie edytowane i wywołało powstanie wielu stron internetowych i blogów wyśmiewających chłopca. Fani Ghyslaina napisali petycję do twórców "Gwiezdnych wojen", aby obsadzić go w jednym z epizodów. Był nawet parodiowany w programach telewizyjnych (np. South Park, American Dad, Veronica Mars). Ghyslain przeszedł załamanie psychiczne i musiał poddać się długotrwałemu leczeniu.[4]

- **Anna Halman** (14 lat, Polska). Pięciu kolegów z klasy znęcało się nad Anną na oczach całej klasy (zerwali z niej ubranie i udawali, że ją gwałcą). Nagrali całą scenę telefonem komórkowym i zagrozili dziewczynie, że opublikują nagranie w Internecie. Później tak właśnie zrobili, umieszczając nagranie na YouTube. Dla Anny miała to być zemsta za to, że nie chciała umówić się z którymś z chłopaków. Anna popełniła samobójstwo.[5]
- **Jessica Logan** (18 lat, USA). Po rozstaniu były chłopak Jessiki opublikował jej intymne zdjęcia, które wysyłała mu, gdy jeszcze się spotykali. Jessica była wówczas narażona na ciągłe wyśmiewanie przez kolegów z klasy. Ataki na nią nasiliły się po tym, jak anonimowo wystąpiła w telewizji, by ostrzec innych przed zagrożeniami związanymi z sextingiem. Jessica popełniła samobójstwo.[6]

Możliwości stosowania sankcji karnych w Republice Czeskiej

Cyberprzemoc (podobnie jak tradycyjne znęcanie się) nie jest sama w sobie przestępstwem ani wykroczeniem. To zawsze zależy od działań dręczyciela. Jeśli zachowanie to przybrało formę np. fizycznego uszkodzenia ciała ofiary, szantażu lub zastraszania jej, wówczas może dojść do zastosowania np. **sekcji 146** (Uszkodzenie ciała) lub **sekcji 145** (Poważne uszkodzenie ciała), **sekcji 175 (**Szantaż) Kodeksu karnego. W przypadku nękania i prześladowania osoby można skorzystać z przepisów paragrafu **354** Kodeksu Karnego (Niebezpieczne prześladowanie). Jednak w przypadku cyberprzemocy, która może przejawiać się np. w ciągłym ośmieszaniu, zawstydzaniu i wyrządzaniu szkód psychicznych za pośrednictwem technologii informacyjno-komunikacyjnych, zastosowanie niektórych z powyższych przepisów będzie problematyczne, a nawet niemożliwe.

Możliwości ścigania karnego w Polsce

W Polsce jest to regulowane przez:

Artykuł 212 kodeksu karnego - zniesławienie

Oraz

***Art. 190** § 1 Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub szkodę osoby najbliższej, jeżeli groźba wzbudza w zagrożonym uzasadnioną obawę, że będzie spełniona, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

§ 2. ściganie odbywa się na wniosek pokrzywdzonego.

4.15.2. Cybergrooming

Cybergrooming to czyn polegający na psychologicznej manipulacji osobą (zazwyczaj z wykorzystaniem socjotechniki), dokonywany za pośrednictwem Internetu lub technologii informacyjno-komunikacyjnych (np. telefonów komórkowych itp.). Celem cybergroomingu jest wzbudzenie w ofierze fałszywego zaufania i skłonienie jej w ten sposób do osobistego spotkania. Efektem takiego spotkania może być atak fizyczny, seksualny lub inny na ofiarę. Ofiarami cybergroomingu mogą być zarówno dzieci, jak i dorośli.[7] Według statystyk, najczęściej ofiarami są dziewczęta w wieku od 13 do 17 lat.[8]

"Manipulacja psychologiczna w cybergroomingu trwa zazwyczaj przez długi okres czasu - od około 3 miesięcy do kilku lat. Ten okres czasu zależy bezpośrednio od metody manipulacji i naiwności ofiary. Zdarzają się przypadki, że drapieżnik manipulował dzieckiem przez 2-3 lata, zanim doszło do osobistego spotkania i wykorzystania seksualnego. Należy również wziąć pod uwagę pełnoletniość dziecka - napastnik mógł mieć kontakt z dzieckiem, gdy było ono niepełnoletnie, ale do ataku dojdzie dopiero po osiągnięciu przez nie pełnoletniości (oczywiste jest, że kary za seksualne wykorzystywanie nieletniego i małoletniego są bardzo różne)."[9]

Cybergrooming ma różne etapy:

1. Zdobycie zaufania i próba odizolowania ofiary od otoczenia (napastnik zmienia tożsamość, jest bardzo cierpliwy)
2. Przekupywanie prezentami lub różnymi usługami, budowanie relacji przyjacielskich
3. Uzależnienie emocjonalne ofiary od osoby napastnika
4. Spotkanie osobiste
5. Molestowanie seksualne, wykorzystywanie dzieci lub inne napaści[10]

Dzieci zagrożone to:

1. *młodzież/nastolatkowie* (zainteresowani seksualnością człowieka, chętni do rozmowy na ten temat),
2. *Dzieci z niską samooceną lub brakiem wiary w siebie* (łatwiej izolują się emocjonalnie lub fizycznie),
3. *dzieci z problemami emocjonalnymi, ofiary w trudnej sytuacji życiowej* (często szukają zastępstwa za swoich rodziców i potrzebują pomocnej dłoni),
4. *dzieci są naiwne i nadmiernie ufne* (chętniej angażują się w rozmowy online z nieznajomymi, trudniej im rozpoznać ryzykowną komunikację).

Możliwości stosowania sankcji karnych w Republice Czeskiej

Osoba dopuszczająca się cybergroomingu może swoim zachowaniem wypełniać znamiona niektórych przestępstw wymienionych w Kodeksie karnym. Z reguły, w zależności od charakteru działań napastnika, będą to przestępstwa z paragrafu **168** (Handel ludźmi), paragrafu **171 (**Ograniczenie wolności osobistej), paragrafu **175 (**Wymuszenie), paragrafu **185 (**Gwałt), paragrafu **187 (**Wykorzystanie seksualne), paragrafu **201 (**Zagrożenie edukacji dziecka), paragrafu **209 (**Oszustwo), paragrafu **353 (**Groźby), paragrafu **354 (**Niebezpieczne prześladowanie) Kodeksu karnego.

Inna możliwa definicja cybergroomingu mówi, że jest to ***"zachowanie użytkowników Internetu, którego celem jest wzbudzenie fałszywego zaufania u dziecka będącego ofiarą i skłonienie go do osobistego spotkania". Efektem takiego spotkania może być wykorzystywanie seksualne ofiary,*** *przemoc fizyczna wobec niej, wykorzystywanie jej do prostytucji dziecięcej, produkcja pornografii dziecięcej itp.*[11] W tym kontekście można skorzystać z **przepisu** szczególnego zawartego w **rozdziale 193b** (Nakłanianie do bezprawnego kontaktu z dzieckiem) kodeksu karnego.

Możliwości ścigania karnego w Polsce

W czerwcu 2010 r. weszła w życie nowelizacja Kodeksu karnego. W Kodeksie karnym pojawia się zupełnie nowy typ przestępstwa, uregulowany w art. 200a k.k., tzw. grooming, czyli uwodzenie przez Internet. Chodzi o osoby, które za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązują kontakt z małoletnim poniżej 15 roku życia, dążąc do wprowadzenia go w błąd, wyzyskania jego błędu lub niezdolności do zrozumienia sytuacji albo bezprawnej groźby spotkania. To przestępstwo jest zagrożone karą do 3 lat pozbawienia wolności.

Kto składa małoletniemu poniżej lat 15, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej, samą propozycję obcowania płciowego, poddania się lub innej czynności seksualnej albo udziału w produkowaniu lub utrwalaniu treści pornograficznych i zmierza do jej realizacji, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

4.15.3. Sexting

Jedną z form niebezpiecznego zachowania, zwłaszcza w środowisku portali społecznościowych, jest sexting. Termin sexting powstał z połączenia słów sex i texting, stąd jego znaczenie. Jest to wysyłanie drogą elektroniczną wiadomości tekstowych, zdjęć lub filmów o treści seksualnej. Takie materiały o charakterze seksualnym mogą być umieszczane w sieciach społecznościowych lub innych miejscach przechowywania danych bezpośrednio przez samych autorów lub przez innego użytkownika, który uzyskał dostęp do takich materiałów. Najczęściej odbywa się to poprzez dobrowolne umieszczanie plików o treści seksualnej, które zostały pobrane przez samego nadawcę.

Następnie (po zakończeniu komunikacji, związku lub z innego powodu) sprawca wykorzystuje uzyskane materiały wrażliwe do zastraszania lub szantażu. W niektórych przypadkach sprawca może żądać dalszych zdjęć lub nagrań wideo pod groźbą publikacji takiego materiału, zmuszając w ten sposób ofiarę za pomocą przymusu psychologicznego do wykonania i utrwalenia kolejnych materiałów, których sprawca żąda na własny użytek lub z zamiarem udostępnienia ich w Internecie (w przypadku dzieci - udostępnienia ich na stronach poświęconych pornografii dziecięcej). Drugim wariantem zachowania sprawcy jest wykorzystanie uzyskanych materiałów do innych celów przymusu (np. odnowienie związku partnerskiego, podjęcie czynności seksualnych, przesłanie kwoty pieniężnej itp.) pod groźbą opublikowania uzyskanych wcześniej zdjęć lub nagrań wideo (pierwotnie dobrowolnie przesłanych przez sprawcę ofierze).

Wyniki badań nad ryzykownymi zachowaniami czeskich dzieci w środowisku internetowym[12] 2014, przygotowanych przez Centrum Profilaktyki Ryzykownej Komunikacji Wirtualnej Wydziału Edukacji Uniwersytetu Palackiego w Ołomuńcu we współpracy z portalem Seznam.cz, pokazują, że 9,86% dzieci zamieściło w Internecie "seksowne" zdjęcie lub filmik, na którym są częściowo lub całkowicie nagie. Spośród 28 232 respondentów 12,14% stwierdziło, że wysłało komuś taki materiał przez Internet/telefon komórkowy.

W przypadku sextingu udział ofiary w akcie jest niezaprzeczalny, gdyż to ona jest autorką zdjęcia lub filmu, ale po wysłaniu materiału traci ona całkowitą kontrolę nad dalszym "życiem" danych.

Możliwości stosowania sankcji karnych w Republice Czeskiej

W przypadku opublikowania zdjęć innej osoby bez jej zgody, osoba zainteresowana może dochodzić ochrony swoich praw w postępowaniu cywilnym

Jeśli dana osoba wygłosi fałszywe oświadczenie na temat innej osoby (jak to miało miejsce w sprawie *Roztahovačky*), które może w istotny sposób narazić na szwank jej poważanie wśród współobywateli, w szczególności zaszkodzić jej zatrudnieniu, zakłócić jej relacje rodzinne lub wyrządzić jej inną poważną szkodę, można powołać się na **paragraf 184** (Zniesławienie) Kodeksu karnego.

Szczególnym przypadkiem jest sytuacja, w której dochodzi do pozyskania materiałów audiowizualnych przedstawiających dziecko i ich nadużywania. Jeśli napastnik zachęca dziecko do tworzenia, a następnie przesyłania zdjęć, filmów lub transmisji online przed kamerą internetową (które przedstawiają dziecko nagie, obnażone lub w inny sposób wzbudzające podniecenie seksualne), może popełnić przestępstwo z **paragrafu 193** (Wykorzystywanie dziecka do produkcji pornografii) Kodeksu karnego.

Sexting bardzo często objawia się także tym, że sprawca zmusza ofiarę do przesyłania dodatkowych materiałów (zdjęć, filmów, transmisji na żywo itp.), grożąc, że jeśli ich nie prześle, materiały, które już posiada, zostaną opublikowane w Internecie lub udostępnione rodzinie czy znajomym. Tym samym popełnia on przestępstwo z **paragrafu 175(1)** (Wymuszenie) Kodeksu Karnego.

Osoba, która dopuści się sekstingu, może również popełnić przestępstwo z paragrafu **192** (Produkcja i inne sposoby pozbywania się pornografii dziecięcej) lub **paragrafu 201** (Zagrożenie edukacji dziecka) Kodeksu karnego.

Możliwości ścigania karnego w Polsce

Zgodnie z polskim prawem zabronione są następujące działania:

- produkcja w celu rozpowszechniania;
- nagranie;
- rozpowszechnianie;
- prezentowanie;
- posiadanie i przechowywanie;
- import

materiałów pornograficznych z udziałem małoletniego - osoby poniżej 18 roku życia (art. 202 Kodeksu karnego). Takie działania są zagrożone karą pozbawienia wolności od 8 miesięcy do 10 lat. Warto również zauważyć, że rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody (art. 191a Kodeksu karnego) jest zagrożone karą pozbawienia wolności od 3 miesięcy do 5 lat.

4.15.4. Cyberstalking

Cyberstalking jest połączeniem słów cyber i stalking. Pierwotnie słowo stalking było używane przez myśliwych do tropienia zwierzyny aż do jej zabicia. Stalking w dzisiejszym rozumieniu został po raz pierwszy użyty w latach 90. w opracowaniu Meloya[13] , który zdefiniował stalking jako niebezpieczne prześladowanie przez znanego lub nieznanego sprawcę, który ściga ofiarę w taki sposób, że wywołuje poczucie zagrożenia lub strachu. To prześladowanie musi być długotrwałe.

Cyberstalking to działanie polegające na wielokrotnym kontaktowaniu się z ofiarą, np. poprzez wysyłanie wiadomości SMS, e-maili, rozmowy telefoniczne, VoIP, komunikatory itp. Zachowanie napastnika zwykle eskaluje i zwykle powoduje, że ofiara obawia się o swoją prywatność, zdrowie lub życie. *Cyberstalkerzy* są zazwyczaj uporczywi i systematyczni, a nierzadko zdarza się, że mają kilka fałszywych tożsamości, których używają do kontaktowania się z ofiarą. Cyberstalker może również demonstrować swoją siłę i władzę, np. zamieszczając informacje o życiu ofiary, które może uzyskać z różnych źródeł internetowych.

Możliwości stosowania sankcji karnych w Republice Czeskiej

Stalking lub cyberstalking może, pod pewnymi warunkami, podlegać przepisom **sekcji 354** (Niebezpieczne prześladowanie) Kodeksu karnego. Podstawowe warunki obejmują, że napastnik musi "*uporczywie kontaktować się z* ofiarą przez dłuższy czas za *pomocą środków komunikacji elektronicznej, pisemnej lub innej*" oraz . Takie zachowanie może wywołać u ofiary uzasadnioną obawę o swoje życie lub zdrowie albo życie i zdrowie osób jej bliskich. Okolicznością obciążającą zgodnie z **paragrafem 354(2)(a)** Kodeksu karnego jest fakt, że wspomniany czyn został popełniony na dziecku.

Możliwości ścigania karnego w Polsce

Zgodnie z polskim kodeksem karnym stalking można popełnić na dwa sposoby. Poprzez uporczywe nękanie osoby (art. 190a § 1 Kodeksu karnego) lub podszywanie się pod nią (art. 190a § 2 Kodeksu karnego). Zakwalifikowanie określonego zachowania jako stalkingu zależy od spełnienia przez sprawcę kilku warunków.

Pierwszą główną cechą stalkingu jest uporczywość działań sprawcy. Oznacza to, że tylko nieliczne czyny naruszające wolność psychiczną człowieka mogą być uznane za stalking. W uproszczeniu można powiedzieć, że stalking w swojej pierwszej postaci (§1) polega na co najmniej kilkukrotnym nękaniu innej osoby. Zachowania, które kwalifikują się jako nękanie, mogą być różne, np. dokuczanie, niepokojenie, wysyłanie listów lub wykonywanie telefonów. Konieczność stwierdzenia uporczywości działań sprawcy. Pojedyncze działania nie są zabronione przez prawo, są powszechne w naszym codziennym życiu. W niektórych przypadkach mogą one zostać zakwalifikowane jako wykroczenie polegające na złośliwym zakłóceniu porządku publicznego. Tylko wielokrotne i długotrwałe zachowanie sprawcy, który nie ma zamiaru zaprzestać swoich działań mimo próśb pokrzywdzonego, może być uznane za stalking.

[1] Por. *Co to jest cyberprzemoc i jak się objawia?* [online]. [cyt. 19.8.2016]. Dostępne od:

http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html

Więcej na temat *cyberprzemocy* zob. np. *Cyberbullying I, II* [online]. [cyt. 19.8.2016]. Dostępny pod adresem: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

[2] Por. dalej: *Czy wiesz, co to jest KYBERSHIKANA?* [online]. [cyt. 19.8.2016]. Dostępny pod adresem: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

[3] *Dwunastoletnia dziewczynka popełniła samobójstwo po prawie rocznym okresie cyberprzemocy.* [online]. [cyt. 2016 Aug 19]. Dostępny pod adresem: https://www.novinky.cz/zahranicni/amerika/313386-dvanactileta-divka-se-zabila-po-temer-rocni-sikane-na-internetu.html

http://www.ceskatelevize.cz/ct24/svet/246314-dalsi-sebevrazda-kvuli-socialnim-sitim-divka-skocila-z-veze/

[4] *Cyberprzemoc I, II* [online]. [cyt. 19.8.2016]. Dostępny pod adresem: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

[5] *Cyberprzemoc I, II* [online]. [cyt. 19.8.2016]. Dostępny pod adresem: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

Następnie: *Jessica Logan - Dalsza część opowieści.* [cit.8.8.2016]. Dostępny pod adresem: http://nobullying.com/jessica-logan/

[6] Ibid.

[7] *Komunikacja zagrożeń: cyberprzemoc* [online]. [cyt. 19.3.2014]. Dostępny pod adresem: http://www.e-nebezpeci.cz/index.php/rizikova-komunikace/kybergrooming

[8] CHOO, Kim-Kwang Raymond. *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences* [online]. Canberra: Australian Institute of Criminology, c2009, [cyt. 19 marca 2014]. ISBN 978-1-921532-33-7. Dostupné z: http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf

[9] KOPECKÝ, Kamil. W: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cyt.19.3.2014]. Dostępny pod adresem: http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a

[10] *Cyberprzemoc.* [online]. [cyt. 2016-08-19]. Dostępny pod adresem: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

[11] KOPECKÝ, Kamil. W: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cyt. 2014-03-19]. Dostępny pod adresem: http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a

[12] *Badania nad ryzykownymi zachowaniami czeskich dzieci w środowisku internetowym 2014* [online]. [cit.19.8.2016]. Dostępny pod adresem: https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace

[13] MELOY, Reid J. *STALKING (OBSESYJNE ŚLEDZENIE): PRZEGLĄD PRELIMINARNYCH BADAŃ* [online]. [cyt. 2015 Oct 3]. Dostępny pod adresem: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf

4.17. Kradzież tożsamości

Kradzież tożsamości to atak, w którym dochodzi do kradzieży wirtualnej tożsamości[1] , a raczej do przejęcia kontroli (stałej lub tymczasowej) nad tą tożsamością. Motywem działania atakującego może być zysk finansowy, ale także inne korzyści, takie jak dostęp do informacji o innych osobach, dostęp do danych firmowych itp. które są związane z faktem, że atakujący działa w imieniu innej osoby.

Z reguły działania napastnika polegają na jednoczesnym popełnieniu kilku czynów zabronionych. Pierwszym przestępstwem w kradzieży tożsamości jest złamanie danych uwierzytelniających lub zainstalowanie złośliwego oprogramowania w systemie komputerowym ofiary w celu uzyskania dostępu do tożsamości wirtualnej.

Po uzyskaniu dostępu do tożsamości zaatakowanej osoby, uzyskane informacje mogą zostać wykorzystane do ataku na tę osobę, a także tożsamość może zostać wykorzystana do ataku na inną osobę. Faktyczny atak na inną ofiarę za pomocą skradzionej tożsamości jest dla atakującego znacznie łatwiejszy, ponieważ ta druga ofiara zwykle nie posiada informacji o błędnej tożsamości osoby (pierwszej ofiary), z którą na przykład regularnie się komunikuje i wymienia poufne dane.

Wracając do kwestii botnetów, jednym z typowych zadań złośliwego oprogramowania, które jest instalowane po podłączeniu systemu komputerowego do botnetu, jest automatyczne pozyskiwanie danych o użytkownikach zainfekowanego systemu komputerowego - kradzież tożsamości. Botmaster może następnie wykorzystać pozyskane dane w dowolnym momencie, podszywając się pod konkretną osobę lub sprzedając te dane osobom trzecim.[2]

Zazwyczaj skradzione tożsamości są wykorzystywane do:

- przeprowadzanie ataków typu phishing lub złośliwe oprogramowanie w obrębie listy użytkowników, z którymi komunikuje się osoba o skradzionej tożsamości,

- wysyłanie spamu,

- uzyskanie informacji, które nie są publicznie dostępne (np. informacje o strukturze firmy, ustawieniach zabezpieczeń innych usług itp,)

- uzyskanie dostępu do innych usług. Wiele serwisów internetowych umożliwia zmianę hasła po prostu przez podanie adresu e-mail. Ponieważ osoba atakująca kontroluje konto e-mail atakowanej osoby, może również zmienić wiele innych usług powiązanych z tym kontem.

Możliwości stosowania sankcji karnych w Republice Czeskiej

Jeśli środki bezpieczeństwa zostaną pokonane i uzyskany zostanie nieuprawniony dostęp do tożsamości ofiary, spełnione zostaną znamiona przestępstwa z **paragrafu 230(1)** (Nieuprawniony dostęp do systemu komputerowego i nośnika informacji) Kodeksu karnego. Używając złośliwego oprogramowania w tym samym celu, atakujący popełnia czyn z paragrafu 230(2) kodeksu karnego. Jeśli celem kradzieży tożsamości jest uzyskanie nieuzasadnionej korzyści dla siebie lub innej osoby, można również zastosować przepisy **paragrafu 230(3)** kodeksu karnego. Jeśli napastnik kradnie tożsamość w celu oszukania innej osoby, tj. wprowadzenia jej w błąd w celu wzbogacenia się, taki czyn może być również oceniany na podstawie **paragrafu 209** (Oszustwo) Kodeksu karnego.

Możliwości ścigania karnego w Polsce

Zgodnie z art. 190a § 2 Kodeksu karnego, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej, podlega karze pozbawienia wolności do lat trzech

---

[1] Tożsamość wirtualna to dowolna tożsamość lub awatar wykorzystywany przez daną osobę do interakcji w cyberprzestrzeni (np. poczta elektroniczna, konto w sieci społecznościowej, gra, różne rynki internetowe, system komputerowy itp.) Nie ma znaczenia, czy tożsamość wirtualna jest prawdziwa czy fałszywa, tzn. czy reprezentuje osobę, czy też jest całkowicie sztuczną tożsamością, pozbawioną rzeczywistych podstaw.

[2] Więcej szczegółów w PLOHMANN, Daniel, Elmar GERHARDS-PADILLA i Felix LEDER. *Botnety: wykrywanie, pomiar, dezynfekcja i obrona.* ENISA, 2011, s. 22 [online]. [cyt. 17.5.2015]. Dostępny pod adresem: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

4.18. APT (Advanced Persistent Threat - zaawansowane trwałe zagrożenie)

Termin APT można dosłownie przetłumaczyć jako "zaawansowane i uporczywe zagrożenie". Jest to długotrwały, systematyczny cyberatak ukierunkowany na docelowy system komputerowy lub technologie informacyjno-komunikacyjne docelowej organizacji. Sam atak wykorzystuje różnorodne techniki i dość duże zasoby, a zazwyczaj atakowane mogą być cele drugorzędne (systemy komputerowe organizacji, np. poprzez powtarzające się ataki DoS lub inne) w celu odwrócenia uwagi od celu głównego (infiltracja firmy za pomocą złośliwego oprogramowania), który następnie jest atakowany.

"Celem APT jest zazwyczaj wydobycie strategicznie cennych danych niejawnych lub niepublicznych, ograniczenie operacyjności celu lub zajęcie pozycji umożliwiającej przyszłe wdrożenie wspomnianych działań. Podejmowanie działań, które spełniają definicję APT, wymaga wysokiego poziomu wiedzy specjalistycznej, znacznych zasobów finansowych oraz umiejętności długoterminowego dostosowywania się do działań ofiary. Charakter APT przyjmują więc głównie podmioty państwowe, grupy przez nie kontrolowane i sponsorowane lub wyspecjalizowane zorganizowane grupy przestępcze. [1]

Rzeczywisty atak APT składa się zazwyczaj z:

- zdobycie informacji o celu ataku (zbieranie informacji z otwartych źródeł, wykorzystanie socjotechniki itp.)
- właściwego ataku:
    - Wybór odpowiednich środków (złośliwe oprogramowanie, tworzenie tożsamości pod przykrywką itp.)
    - Jeśli system można zaatakować z zewnątrz, to jest on atakowany
    - Jeżeli system nie jest dostępny z zewnątrz, można zastosować inne techniki w połączeniu z socjotechniką (np. spear phishing, kradzież tożsamości itp.).
- przejęcia kontroli nad niektórymi systemami komputerowymi, umocnienia pozycji w zaatakowanej sieci komputerowej
- gromadzenia danych i informacji i przesyłania ich do napastnika
- eksploracji danych

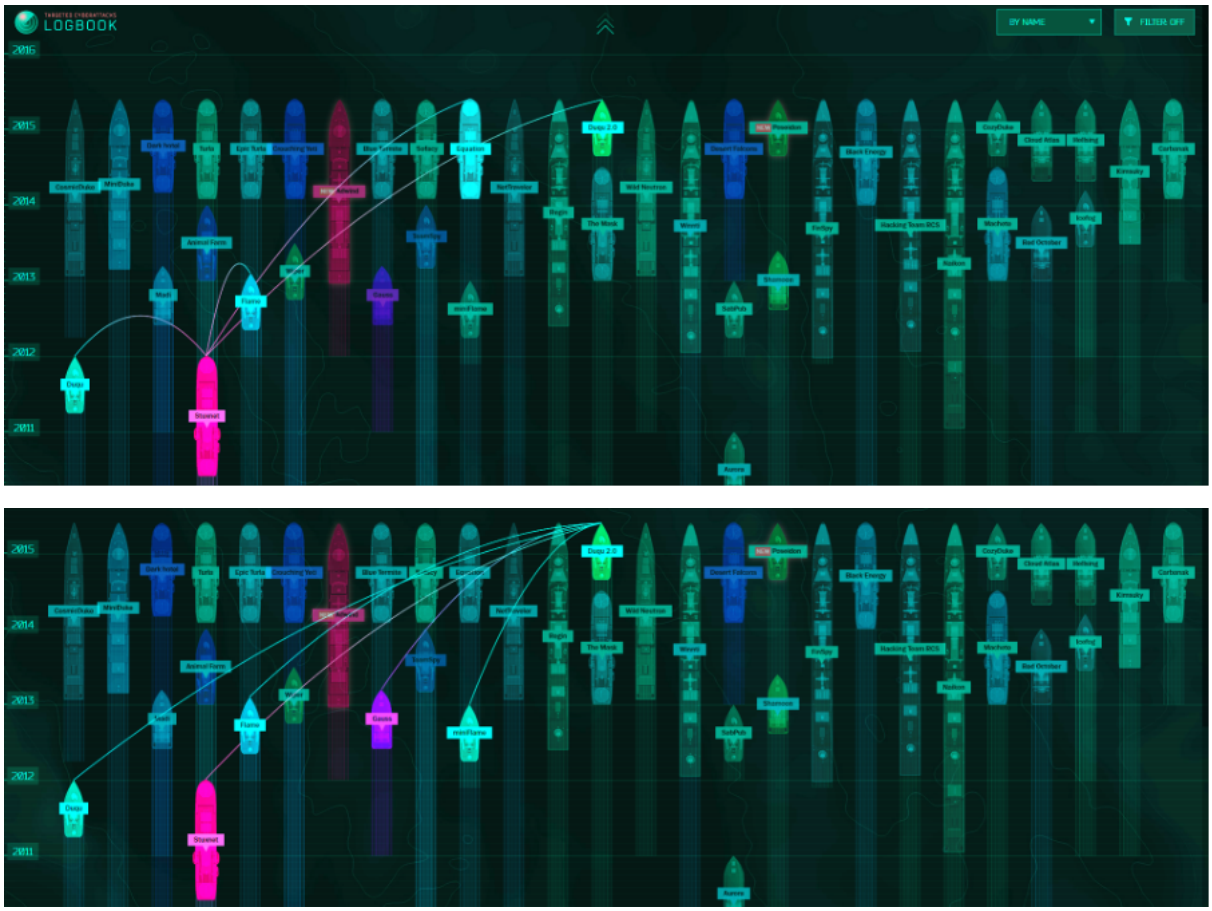
Podczas ataku APT napastnicy mogą stosować inne rodzaje ataków na wybrany cel, w zależności od uzyskanych danych i informacji.

APT można wyświetlić, wykorzystując jego cykl życia:

Przebieg ataku APT[2]

Rzeczywisty atak APT może trwać od kilku miesięcy do wielu lat, a atak może obejmować stosunkowo długie okresy, w których aktywność atakującego jest minimalna. Prowadzenie dużej liczby podobnych operacji przeciwko różnym celom jednocześnie nie jest wyjątkiem. [3]

Na stronie internetowej Kasperky Lab (https://apt.securelist.com/#firstPage) znajduje się graficzna prezentacja znanych ataków APT, zawierająca informacje o tym, kiedy po raz pierwszy pojawiła się próbka szkodliwego oprogramowania, kiedy atak APT został wykryty, gdzie głównie działa (informacje o geolokalizacji, główne zaatakowane systemy operacyjne, liczba celów itd. Poniższe dwa printscreeny pokazują pierwotne wiązanie złośliwego oprogramowania Stuxnet (między innymi) z Duqu 2.0, a następnie wiązanie Duqu 2.0 z innym złośliwym oprogramowaniem.



Wyświetlanie ataków ATP wraz z ich współzależnościami[4]

Możliwości stosowania sankcji karnych w Republice Czeskiej

Ewentualna odpowiedzialność karna napastników przeprowadzających atak APT zależy wyłącznie od ich działań, które mogą przybrać formę dystrybucji złośliwego oprogramowania, ataków phishingowych, kradzieży tożsamości itp.

Możliwości ścigania karnego w Polsce

Analizując atak APT pod kątem naruszeń prawa obowiązującego w Polsce, należy wziąć pod uwagę, że gdyby atak został przeprowadzony na wszystkich jego etapach, popełniono by co najmniej kilka wykroczeń. Zgodnie z obowiązującymi przepisami prawa można rozważyć przeprowadzenie ataku APT:

- hakowanie na podstawie art. 267 § 1 Kodeksu karnego

- przestępstwo wytwarzania lub udostępniania urządzeń lub programów komputerowych, haseł i kodów z art. 269b kodeksu karnego

- oszustwo komputerowe z art. 287 Kodeksu karnego

Inne przestępstwa, które mogą wystąpić w fazie wdrażania, to:

- sabotaż komputerowy z art. 269 Kodeksu karnego,

- sprowadzenie niebezpieczeństwa dla życia, zdrowia lub mienia na podstawie art. 165 Kodeksu karnego,

- niszczenie, uszkadzanie, usuwanie danych informatycznych z art. 268a Kodeksu karnego,

- zakłócenia w działaniu systemu komputerowego lub sieci teleinformatycznej w trybie art. 269a.

Atak APT może być również równoznaczny ze szpiegostwem w rozumieniu art. 130 § 3 Kodeksu karnego.

---

[1] *Zaawansowane trwałe zagrożenie.* [online]. [cyt. 2016-08-20]. Dostępny pod adresem: https://www.isouvislosti.cz/advanced-persistent-threat

[2] *Zaawansowane trwałe zagrożenie - cykl życia.* [online]. [cyt. 2016 Aug 20]. Dostępny pod adresem: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg

[3] Więcej informacji można znaleźć na stronie: *Zaawansowane trwałe zagrożenie.* [online]. [cyt. 2016 Aug. 20]. Dostępny pod adresem: https://www.isouvislosti.cz/advanced-persistent-threat

Zaawansowane trwałe zagrożenie (Advanced Persistent Threat, APT). [online]. [cyt. 2016 Aug 20]. Dostępny pod adresem: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

Zaawansowane trwałe zagrożenia: jak działają. [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://www.symantec.com/theme.jsp?themeid=apt-infographic-1

Jak działają APT? Cykl życia zaawansowanych trwałych zagrożeń (infografika). [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://blogs.sophos.com/2014/04/11/how-do-apts-work-the-lifecycle-of-advanced-persistent-threats-infographic/

[4] *Dziennik ukierunkowanych ataków cybernetycznych.* [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://apt.securelist.com/#secondPage

4.19. Cyberterroryzm

W kontekście ataków cybernetycznych nie można zapominać o terroryzmie, który jest jednym z aktualnych zagrożeń globalnych, a jego dynamiczny rozwój i rozprzestrzenianie się można zaobserwować na całym świecie.

Terroryzm można podzielić ze względu na jego formę na *śmiercionośny* i *nieśmiercionośny*, przy czym pierwsza grupa charakteryzuje się stosowaniem konwencjonalnych środków realizacji przemocy (*konwencjonalne* - ataki dokonywane przy użyciu powszechnie dostępnych środków walki, takich jak broń palna, oraz *niekonwencjonalne* - nadużywanie broni masowego rażenia). Natomiast **nieśmiercionośne formy terroryzmu**[1] lub ataki wykorzystujące nowoczesne narzędzia w połączeniu ze środkami śmiercionośnymi są **bardziej powszechne w** obszarze Internetu.

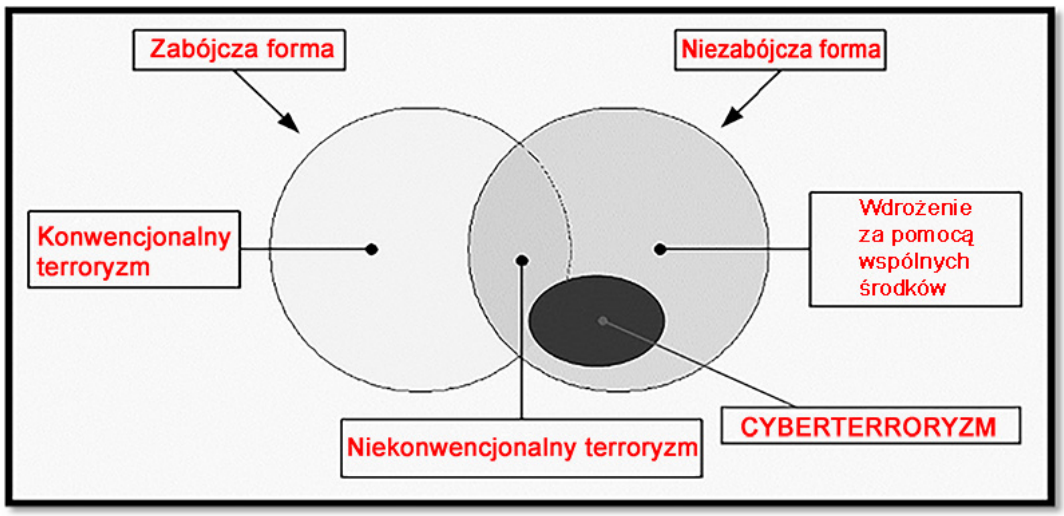
Do konwencjonalnej formy terroryzmu nieśmiercionośnego zalicza się niżej wymienione podgrupy:

- *Terroryzm nieuzbrojony*.

- *Cyberterroryzm*, który jest jednym z największych zagrożeń XXI wieku. Zasada ta polega przede wszystkim na nadużywaniu technologii informacyjno-komunikacyjnych (w tym Internetu) jako środka i środowiska do przeprowadzania ataków. Podobnie jak w przypadku konwencjonalnego ataku terrorystycznego, jest to działanie zaplanowane, zwykle motywowane politycznie lub religijnie i przeprowadzane przez małe, niezorganizowane militarnie struktury. Celem tych grup jest przede wszystkim wpływanie na opinię publiczną. Ze względu na szybkie rozprzestrzenianie się technologii informacyjnych i komunikacyjnych na całym świecie cyberterroryzm stanowi poważne zagrożenie i jest coraz częściej wykorzystywany przez grupy terrorystyczne.[2]

- *Terroryzm medialny*, w którym dochodzi do planowego nadużywania środków masowego przekazu i innych środków psychologicznych w celu wywarcia wpływu na opinie całej populacji lub grup docelowych.

Zależność tę najlepiej obrazuje schemat przedstawiony na poniższym rysunku.



Przedstawienie form terroryzmu, w tym cyberterroryzmu

Globalny charakter środowiska informacyjnego i telekomunikacyjnego umożliwia przekazywanie informacji i koordynację działań terrorystycznych na całym świecie. Według doniesień, na przykład atak na WTC w Nowym Jorku został zorganizowany przy użyciu Internetu.

Istnieją też inne przypadki nadużywania Internetu do rozpowszechniania szkodliwych informacji lub prowadzenia operacji psychologicznych związanych z terroryzmem medialnym. Internet jest w znacznym stopniu wykorzystywany do rozpowszechniania propagandy, ideologii lub zastraszania, na przykład w formie publikacji egzekucji więźniów w Internecie[3] , rekrutacji i mobilizacji nowych działaczy, sympatyków lub sponsorów, propagowania aktów terrorystycznych i zachęcania osób do ich popełniania. Strony internetowe grup terrorystycznych często zawierają instrukcje wykonania improwizowanej broni lub propagandę skierowaną do młodego pokolenia.

Internet stwarza dość wyjątkowe możliwości dla grup i jednostek ekstremistycznych i terrorystycznych, zwłaszcza w zakresie szybkiej i stosunkowo tajnej komunikacji, gdy jest wykorzystywany do wymiany informacji i instrukcji służących planowaniu i koordynowaniu działań lub przekazywaniu środków finansowych.

Prawie wszystkie grupy i organizacje terrorystyczne mają swoje strony internetowe. Są one zazwyczaj publikowane w kilku językach, a ponadto istnieją specjalne strony skierowane do dzieci i kobiet, zawierające komiksy lub kreskówki, w których można znaleźć np. historie zamachowców-samobójców. [4]

Strona TravelWest.info po ataku napastników

Możliwości stosowania sankcji karnych w Republice Czeskiej

Z punktu widzenia prawa karnego zachowanie to może wypełniać znamiona przestępstwa z **art. 311 par. 2** (Atak terrorystyczny), **§ 355 (**Zniesławienie narodu, rasy, grupy etnicznej lub innej grupy osób), § **356** (Nawoływanie do nienawiści wobec grupy osób lub do ograniczenia ich praw i wolności), § **364 (**Podżeganie do popełnienia przestępstwa), § **403 (**Tworzenie, wspieranie i promowanie ruchu mającego na celu tłumienie praw i wolności człowieka) oraz **§ 404** (Wyrażanie sympatii dla ruchu mającego na celu tłumienie praw i wolności człowieka) Kodeksu Karnego.

Możliwości ścigania karnego w Polsce

W Polsce do realizacji ataku cyberterrorystycznego stosuje się art. 265-269 oraz art. 287 Kodeksu karnego, a w zależności od skutków ataku cyberterrorystycznego zastosowanie mogą mieć także niektóre inne artykuły Kodeksu karnego, takie jak:

Artykuł 163. Doprowadzenie do katastrofy

Artykuł 164. Sprowadzenie niebezpieczeństwa katastrofy

Artykuł 165. Wprowadzenie zagrożenia ogólnego

Artykuł 173. Spowodowanie wypadku drogowego

Artykuł 174. Wprowadzenie bezpośredniego zagrożenia wypadkiem drogowym

---

[1] Można sobie jednak wyobrazić kombinację tych ataków. Więcej informacji na ten temat można znaleźć np:

Wyłącznie: Wirus komputerowy zaatakował amerykańską flotę dronów. [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://www.wired.com/2011/10/virus-hits-drone-fleet/

[2] JIROVSKÝ, Václav. *Cyberprzestępczość to nie tylko hakerstwo, cracking, wirusy i trojany bez tajemnic.* Praga: Grada, 2007, s. 129.

[3] **Przesłany adres URL nie jest ocenzurowany i zawiera drastyczne materiały filmowe!** Zob. na przykład:

OGLĄDAJ: ISIS pozbywa się więźniów żywcem, wysadza zakładników w powietrze za pomocą RPG, a innych zabija ładunkami wybuchowymi - wideo z grafiką. [online]. [cyt. 2016 Aug 20]. Dostępny pod adresem: https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382

Niepokojące nagranie wideo ISIS pokazuje bojowników ścinających głowy czterem więźniom i strzelca zabijającego kupujących na targu. [online]. [cyt. 2016 Aug 20]. Dostępny pod adresem: http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017

[4] JIROVSKÝ, Václav. *Cyberprzestępczość to nie tylko hakerstwo, cracking, wirusy i trojany bez tajemnic.* Praga: Grada, 2007, s. 138.

Zob. też np:

Cyberterroryzm: Jak groźne jest zagrożenie ze strony cyberkalifatu ISIS? [online]. [cyt. 2016-08-20]. Dostępny pod adresem: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html

Wydział Hakowania Państwa Islamskiego [online]. [cyt. 2016 sierpień 20]. Dostępny pod adresem: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355

4.20. PODSUMOWANIE

ℹ️

- Znaczna część cyberprzestępczości wykorzystuje lub przenosi powszechnie znane rodzaje przestępstw (np. oszustwa, naruszenie praw autorskich, kradzież, zastraszanie itp.) do środowiska cyfrowego, gdzie można je popełnić "lepiej, szybciej i skuteczniej" niż w świecie rzeczywistym. Ataki czysto cybernetyczne mogą obejmować np. hakerstwo, ataki DoS i DDoS, botnety itp.
- Wraz z rozwojem usług opartych na zasadzie as-a-service w środowisku cyberprzestępczym pojawiło się wiele platform (zazwyczaj podziemnych, darknetowych forów), na których oferowane są usługi, które można określić jako **Crime-as-a-service**. Powstaje zatem *"złośliwe oprogramowanie* lub szara strefa*", w której* niemal każdy użytkownik może popełnić cyberprzestępstwo.
- W rozdziale przedstawiono podstawowe ataki cybernetyczne. Przedstawiono typowy modus operandi, a także możliwości zastosowania sankcji prawnokarnych za te czyny.
- Cyberprzestępczość można zdefiniować jako czyn skierowany przeciwko komputerowi lub sieci komputerowej albo jako czyn, w którym komputer jest wykorzystywany jako narzędzie do popełnienia przestępstwa. Fakt, że sieć komputerowa lub cyberprzestrzeń jest środowiskiem, w którym odbywa się ta działalność, jest niezbędnym elementem, aby definicja cyberprzestępstwa miała zastosowanie.

🗝️

SŁOWA KLUCZOWE, KTÓRE WARTO ZAPAMIĘTAĆ

- inżynieria społeczna
- botnet
- złośliwe oprogramowanie
- oprogramowanie ransomware
- spam
- oszustwo
- phishing
- pharming
- oszustwo
- hakowanie
- krakowanie
- DoS, DDoS
- APT

❓

PYTANIA KONTROLNE

- W jaki sposób przejawia się inżynieria społeczna?
- Co to jest botnet i jak działa?
- Jakie są topologie botnetów?
- Czy można ścigać właściciela botnetu?
- Co to jest złośliwe oprogramowanie?
- Jakie są najczęstsze przejawy złośliwego oprogramowania?
- Jakie są najczęstsze wektory infekcji złośliwym oprogramowaniem?
- Co to jest oprogramowanie ransomware i jak się ono zazwyczaj objawia?
- Co to jest phishing i jak najczęściej przeprowadza się ten atak?
- Jaka jest różnica między phishingiem a pharmingiem?
- Co to jest hakerstwo?
- Jak objawia się pękanie?
- Jaka jest różnica między hakerstwem a crackingiem?
- Co to jest atak DoS i jak działa?
- Jaka jest różnica między DoS a DDoS?
- Co można zakwalifikować jako rozpowszechnianie wadliwych treści?
- Co to jest APT?

5. Wnioski

Jestem głęboko przekonany, że cyberprzestrzeń nie może stać się środowiskiem, w którym można bezkarnie popełniać wszelkie przestępstwa. Z drugiej strony, należy ustalić zasady i warunki, aby nie stała się ona środowiskiem, w którym dominuje cenzura i represje. Zrównoważenie tych dwóch poziomów jest kluczowym warunkiem stosowania, a przede wszystkim przestrzegania zasad obowiązujących w cyberprzestrzeni, zarówno prawnych, jak i moralnych.

Jeśli chodzi o stosowanie ewentualnych norm prawa karnego do niektórych rodzajów cyberataków, należy zauważyć, że nie jest możliwe ściganie na drodze karnej najbardziej niebezpiecznych zachowań, które nie są zapisane w kodeksach karnych danego kraju. Prawo karne jest środkiem *ultima ratio* i jako takie musi być bardzo precyzyjne, aby nie ingerować w prawa i wolności jednostek w stopniu większym niż jest to absolutnie konieczne.

Oprócz państwa w ochronę cyberprzestrzeni i jej użytkowników zaangażowane są różne organizacje prywatne. Uważam, że jeśli chcemy skutecznie walczyć z cyberprzestępczością, to powinna istnieć bardziej efektywna współpraca między organizacjami prywatnymi (zwłaszcza ekspertami IT, zespołami CSIRT itp.) a administracją publiczną (państwową) lub organami ścigania, tak aby możliwe było reagowanie w odpowiednim czasie i w odpowiedni sposób na coraz bardziej wyrafinowane formy cyberprzestępczości lub cyberataków.

Jak powiedziałem na wstępie, *"życie bez technologii informacyjnych i komunikacyjnych jest dla naszego społeczeństwa nie do pomyślenia lub niemożliwe"*.

Moim zdaniem nie ma sensu zwalniać się z obowiązku stosowania TIK i usług związanych z tymi technologiami. Celem tej monografii nie było zmuszenie użytkowników do odinstalowania Facebooka i niekorzystania z usług Google czy innych serwisów. Celem było zwrócenie uwagi na potencjalne zagrożenia związane z korzystaniem z TIK i usług z nimi związanych. W tym kontekście warto przypomnieć cytat *Scientia est potentia* (**wiedza to potęga, wiedza i wiedza to** *potęga*, **wiedza to władza**). W przypadku TIK i usług związanych z TIK należy wiedzieć, czym są te technologie i usługi, co robią i do czego służą.

Ograniczanie negatywnych zjawisk w cyberprzestrzeni i dążenie do zmian musi zatem koniecznie zaczynać się od użytkowników końcowych, ponieważ w cyberprzestrzeni to oni są zazwyczaj pierwszymi ofiarami napastnika. Jednocześnie to użytkownicy są organem, który może określić, jakie usługi, dane lub informacje będą poszukiwane, przechowywane i udostępniane w cyberprzestrzeni.

Uważam, że kształcenie i szkolenie użytkowników powinno być istotną częścią procesu przenikania technologii informacyjno-komunikacyjnych do naszego życia. Budowanie kompetencji informacyjnych powinno być nierozerwalnie związane z tworzeniem, dystrybucją i promocją produktów lub usług związanych z technologiami informacyjno-komunikacyjnymi. Rzeczywista edukacja w tym zakresie, a raczej zapoznanie z możliwymi zagrożeniami, ryzykiem i negatywnymi aspektami informatyki, powinna być częścią nauczania wszystkich form studiów na wszystkich poziomach edukacji.

"Nikt nie popełnia większego błędu niż ten, kto

nie robi nic, uważając, że to, co może zrobić, jest bezcelowe. "

Edmund Burke

6. Wykorzystana literatura

1. *10 najbardziej znanych grup hakerskich* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: https://www.hackread.com/10-most-notorious-hacking-groups/

2. *7 typów motywacji hakerów* [online]. [cyt. 2015-08-16]. Dostępny pod adresem: https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

3. *7 typów hakerów, których powinieneś znać.* [online]. [cyt. 2015-08-16]. Dostępny pod adresem: https://www.cybrary.it/0p3n/types-of-hackers/

4. *Zaawansowane trwałe zagrożenie - cykl życia.* [online]. [cyt. 2016 Aug 20]. Dostępny pod adresem: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg

5. *Zaawansowane trwałe zagrożenie (Advanced Persistent Threat, APT).* [online]. [cyt. 2016 Aug 20]. Dostępny pod adresem: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

6. *Zaawansowane trwałe zagrożenie.* [online]. [cyt. 2016-08-20]. Dostępny pod adresem: https://www.isouvislosti.cz/advanced-persistent-threat

7. *Zaawansowane trwałe zagrożenia: jak działają.* [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://www.symantec.com/theme.jsp?themeid=apt-infographic-1

8. *Adware.* [online]. [cyt. 2016-08-10]. Dostępny pod adresem: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking

9. *Android Ransomware atakuje także Twój Smart TV!* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: https://thehackernews.com/2016/06/smart-tv-ransomware.html

10. *Rozkład udziału wersji systemu Android w rynku wśród posiadaczy smartfonów na maj 2016 r.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

11. BALIGA, Arati, Liviu IFTODE i Xiaoxin CHEN. Zautomatyzowane powstrzymywanie ataków typu Rootkits. *Computers & Security*, 2008, vol. 27, nr 7-8, s. 323-334.

12. BAUDIŠ, Pavel. Programy typu rootkit. Kolejne zagrożenie dla systemu Windows. *CHIP*, 2005, nr 7, s. 14.

13. *Uważaj na fałszywe aplikacje Android Prisma Apps Running Phishing, Malware Scam* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://www.hackread.com/fake-android-prisma-app-phishing-malware/

14. *Botnet - historyczna lista botnetów.* [online]. [cyt. 2016-08-15]. Dostępny pod adresem: http://www.liquisearch.com/botnet/historical_list_of_botnets

15. *Botnet.* [cyt. 8.7.2016]. Dostępny pod adresem: http://research.omicsgroup.org/index.php/Botnet

16. *Botnet.* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: https://en.wikipedia.org/wiki/Botnet

17. *Botnety.* [online]. [cyt. 2016-07-15]. Dostępny pod adresem:

18. *Botnety: nowe zagrożenie w Internecie.* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://www.lupa.cz/clanky/botnety-internetova-hrozba/

19. *Boty i botnety - rosnące zagrożenie.* [online]. [cyt. 11.8.2016]. Dostępny pod adresem: https://us.norton.com/botnet/

20. *Spamer Buffalo idzie do więzienia na 7 lat za spamowanie.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality

21. CARL, Glenn, Richard BROOKS i Rai SURESH. Wykrywanie odmowy usługi na podstawie falek. *Computers & Security*, 2006, vol. 25, nr 8, s. 600-615.

22. CHOO, Kim-Kwang Raymond. *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences* [online]. Canberra: Australian Institute of Criminology, c2009, [cyt. 19 marca 2014]. ISBN 978-1-921532-33-7. Dostupné z: http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf

23. *Co to jest botnet i jak się rozprzestrzenia?* [online]. [cit.15.7.2016]. Dostępny pod adresem:

24. *Co to jest cyberprzemoc i jak się objawia?* [online]. [cyt. 19.8.2016]. Dostępny pod adresem: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html

25. *Co kryje się w załącznikach oszukańczych wiadomości e-mail?* [online]. [cyt. 15.8.2016]. Dostępny pod adresem: https://blog.nic.cz/2014/07/23/co-sa-skryva-v-prilohe-podvodnych-e-mailov-2/

26. *Co to jest rozszerzenie pliku SCR* [online]. [cit.14.8.2016]. Dostępny pod adresem: http://www.solvusoft.com/cs/file-extensions/file-extension-scr/

27. *Zwalczanie cyberprzestępczości w erze cyfrowej.* [online]. [cyt. 2016 maj 7]. Dostępny pod adresem: https://www.europol.europa.eu/ec3

28. *Wygenerowany komputerowo "Słodziak" łapie internetowych drapieżników* [online]. [cyt. 2016-08-19]. Dostępny pod adresem: http://www.bbc.com/news/uk-24818769

29. *Skazany spamer kwestionuje prawo obowiązujące w Va.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm

30. *Cyberterroryzm: Jak groźne jest zagrożenie ze strony cyberkalifatu ISIS?* [online]. [cyt. 2016-08-20]. Dostępny pod adresem: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html

31. *Cyberprzestępczość.* [online]. [cyt. 1.2.2015]. Dostępny pod adresem: http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime; także.

32. *Cyfrowy świat Digi Dooma*, 2008, ISSN 1802-047X. [online]. [cyt. 14 sierpnia 2016]. Dostępny pod adresem: http://**www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html**

33. *Obliczenia rozproszone.* [online]. [cyt. 2.11.2013]. Dostępny pod adresem: http://dc.czechnationalteam.cz/

34. *Niepokojące nagranie wideo ISIS pokazuje bojowników ścinających głowy czterem więźniom i strzelca zabijającego kupujących na targu.* [online]. [cyt. 2016 Aug 20]. Dostępny pod adresem: http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017

35. DOČEKAL, Daniel. Bruce Schneier: *Internet rzeczy przyniesie ataki, których nie jesteśmy w stanie sobie wyobrazić.* [online]. [cyt. 10.8.2016]. Dostępny pod adresem: http://www.lupa.cz/clanky/bruce-schneier-internet-veci-prinese-utoky-ktere-si-neumime-predstavit/

36. DOČEKAL, Daniel. *Google: Oprogramowanie typu adware infekuje miliony urządzeń i szkodzi reklamodawcom, witrynom internetowym i użytkownikom.* [online]. [cyt. 10.8.2016]. Dostępny pod adresem: http://www.lupa.cz/clanky/google-adware-napada-miliony-zarizeni-a-poskozuje-inzerenty-weby-i-uzivatele/

37. Protokół dodatkowy. ETS nr 189 Protokół dodatkowy do Konwencji o cyberprzestępczości, dotyczący kryminalizacji czynów o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

38. DODGE, Ronald. C., Curtis CARVE i Aaron J. FERGUSON. Phishing dla zwiększenia świadomości bezpieczeństwa użytkowników. *Computers & Security*, 2007, vol. 26, nr 1, s. 73-80.

39. *Dwunastoletnia dziewczynka popełniła samobójstwo po prawie rocznym okresie cyberprzemocy.* [online]. [cyt. 2016 Aug 19]. Dostępny pod adresem: https://www.novinky.cz/zahranicni/amerika/313386-dvanactileta-divka-se-zabila-po-temer-rocni-sikane-na-internetu.html

40. *Estonia odzyskuje siły po potężnym ataku DDoS.* [online]. [cytowany 4 marca 2010] Dostępny w: http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

41. *Wyłącznie: Wirus komputerowy zaatakował amerykańską flotę dronów.* [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://www.wired.com/2011/10/virus-hits-drone-fleet/

42. *Zwalczanie cyberprzestępczości: patrole cybernetyczne i internetowe zespoły dochodzeniowo-śledcze w celu wzmocnienia strategii UE.* [online]. [cyt. 10.7.2016]. Dostępny pod adresem: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827

43. *Klony Flappy Bird przyczyniają się do wzrostu liczby złośliwego oprogramowania mobilnego.* [online]. [cyt. 2016-08-14]. Dostępne od: http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx

44. *Mobilne oprogramowanie ransomware FLocker przenosi się na telewizory Smart TV.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/

45. *Francja rezygnuje z kontrowersyjnego prawa Hadopi po wydaniu milionów* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy i.

46. *Lodówka przyłapana na wysyłaniu spamu w ramach ataku botnetowego.* [online]. [cyt. 2016 maj 17]. Dostępny pod adresem: http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

47. GONZÁLES-TALAVÁN, Guillermo. Prosty, konfigurowalny filtr antyspamowy SMTP. *Computers & Security*, 2006, vol. 25, nr 3, s. 229-236.

48. GOODMAN, Marc. *Wizja przestępczości w przyszłości* [online]. [cyt. 13.11.2014]. Dostępny pod adresem: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071

49. *Google twierdzi, że najlepsze oszustwa phishingowe mają 45-procentowy wskaźnik skuteczności.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/

50. GREENBERG, Andy. *Hakerzy zdalnie przechwycili Jeepa na autostradzie - ze mną w środku.* [online]. [cyt. 2016 maj 4]. Dostępny pod adresem: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

51. GRIFFITHS, Mark. Przestępczość komputerowa i hakerstwo: poważny problem dla policji? The *Police Journal,* 2000, vol. 73, nr 1, s. 18-24.

52. GŘIVNA, Tomáš i Radim POLČÁK. *Cyberprzestępczość i prawo*. Praga: Audytorium, 2008 r.

53. *Hakerzy podszywają się pod Anonymous i grożą atakami na czeskie firmy [*online]. [cyt. 16.8.2015]. Dostępny pod adresem: http://www.lupa.cz/clanky/hackeri-vydavajici-se-za-anonymous-hrozi-utokem-na-ceske-firmy-chteji-zaplatit/

54. *Hakerzy zaatakowali użytkowników Facebooka*. [online]. [cyt. 16.8.2015]. Dostępny pod adresem: http://tech.ihned.cz/c1-37133210-hackeri-zautocili-na-uzivatele-facebooku-chteli-jejich-hesla

55. HILL, Kaszmir. *Ci dwaj gracze Diablo III ukradli wirtualną zbroję i złoto - i zostali oskarżeni w IRL* [online]. [cyt. 2015-08-10]. Dostępny pod adresem: http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/

56. *Historyczna lista botnetów.* [online]. [cyt. 2016-08-15]. Dostępny pod adresem: http://jpdias.me/botnet-lab//history/historical-list-of-botnets.html

57. *Historyczne mapy sieci komputerowych*. [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html

58. HOŘEJŠÍ, Jaromír. *Fałszywy nakaz egzekucji zagraża użytkownikom czeskich banków* [online]. [cit.15.8.2016]. Dostępny pod adresem: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

59. *Jak działają APT? Cykl życia zaawansowanych trwałych zagrożeń (infografika).* [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://blogs.sophos.com/2014/04/11/how-do-apts-work-the-lifecycle-of-advanced-persistent-threats-infographic/

60. *Jak używać programu Wireshark do przechwytywania, filtrowania i sprawdzania pakietów.* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

61. *Wydział Hakowania Państwa Islamskiego* [online]. [cyt. 2016 sierpień 20]. Dostępny pod adresem: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355

62. *Jessica Logan - Dalsza część opowieści.* [cyt. 2016-08-08]. Dostępny pod adresem: http://nobullying.com/jessica-logan/

63. JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [Wydanie 2. zaktualizowane. 2. edycja: AFCEA, 2015, s. 57 i 73 [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

64. JIROVSKÝ, Václav i Oldřich KRULÍK. Podstawowe definicje związane z tematem. *Magazyn Bezpieczeństwa*, 2007, t. 14, nr 2, s. 47.

65. *Sędzia, 69-latek, który ściągał dziecięce porno, narażony na "katastrofalne upokorzenie".* [online]. [cyt. 2009-09-01]. Dostępny pod adresem: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

66. *The Kevin Mitnick Case: 1999* [online]. [cyt. 2.11.2011]. Dostępny pod adresem: http://www.encyclopedia.com/doc/1G2-3498200381.html

67. KOLOUCH, Jan, Pavel BAŠTA i in. *Cyberbezpieczeństwo*. Praga: CZ.NIC, 2019. ISBN 978-80-88168-31-7.

68. KOLOUCH, Jan. Ewolucja kampanii phishingowych i kampanii typu "Business Email Compromise" w Republice Czeskiej. W: *Badania naukowe i stosowane w naukach o zarządzaniu w wojsku i społeczeństwie*. Budapeszt: National University of Public Service, 2018, s. 83-100. ISSN 2498-5392

69. KOLOUCH, Jan. *Cyberprzestępczość.* Praga: CZ.NIC, 2016. REPUBLIKA CZESKA, REPUBLIKA CZESKA, REPUBLIKA CZESKA. ISBN 978-80-88168-15-7

70. KOLOUCH, Jan i Andrera KROPÁČOVÁ. Ransomware. W: ZHUANG, Xiaodong. *Recent Advances in Computer Science: Proceedings of the 19th International Conference on Computers*. B.m.: B.n., 2015, s. 304-307. recent Advances in Computer Engineering Series, [No. 32]. ISBN 978-1-61804-320-7. ISSN 1790-5109.

71. *Cyberprzemoc.* [online]. [cyt. 2016-08-19]. Dostępny pod adresem: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

72. *Cyberprzemoc I, II* [online]. [cyt. 19.8.2016]. Dostępny pod adresem: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

73. *Cyberprzemoc I, II* [online]. [cyt. 19.8.2016]. Dostępny pod adresem: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

74. LEVY, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly edia, s. 32-41. ISBN 978-1449388393.

75. LI, Tao, GUAN, Zhihong, WU, Xianyong. Modelowanie i analiza rozprzestrzeniania się aktywnych robaków w oparciu o systemy P2P. *Computers & Security*, 2007, vol. 26, nr 3, s. 213-218.

76. *Złośliwe oprogramowanie, chaos i zatrzymanie McColo.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/

77. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO i Pedro GARCÍA-TEODORO. Ocena ataku DoS o małej szybkości przeciwko serwerom aplikacji. *Computers & Security*, 2008, vol. 27, nr 7-8, s. 335-354.

78. MATĚJKA, Michał. *Przestępstwa komputerowe.* Praga: Computer Press, 2002

79. MELOY, Reid J. *STALKING (OBSESYJNE ŚLEDZENIE): PRZEGLĄD PRELIMINARNYCH BADAŃ* [online]. [cyt. 2015 Oct 3]. Dostępny pod adresem: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf

80. MINAŘÍK, Pavel. *Wireshark - analiza pakietów dla każdego.* [online]. [cit.18.8.2016]. Dostępny pod adresem: https://www.systemonline.cz/it-security/wireshark-paketova-analyza-pro-vsechny.htm

81. MITNICK, Kevin D. i William L., SIMON. *Duch w przewodach: moje przygody jako najbardziej poszukiwanego hakera na świecie*. New York: Little, Brown & Co, 2012. ISBN 9780316037723.

82. MITNICK, Kevin D. *Sztuka włamywania się: prawdziwe historie kryjące się za wyczynami hakerów, intruzów i oszustów*. Indianapolis: Wiley, c2006. ISBN 0-471-78266-1.

83. MUELLER, Robert. [online]. [cit.3.4.2013]. Dostępny pod adresem: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

84. *Największy atak hakerski potwierdzony. Zagrożone setki milionów użytkowników* [online]. [cyt. 16.8.2015]. Dostępny pod adresem: https://www.novinky.cz/internet-a-pc/bezpecnost/405260-nejvetsi-hackersky-utok-potvrzen-v-ohrozeni-jsou-stovky-milionu-uzivatelu.html

85. *Nowe oprogramowanie Ransomware szyfruje pliki gier.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/

86. NIGAM, Ruchna. *Oś czasu botnetów mobilnych.* [online]. [cyt. 2016-07-12]. Dostępny pod adresem: https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf ;

87. *OWASP, XSS* [online]. [cyt. 2016-07-15]. Dostępne pod adresem: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

88. *Password Sniffer Spy.* [online]. [cyt. 2016-08-18]. Dostępny pod adresem: http://securityxploded.com/password-sniffer-spy.php

89. *Raport Tresnds dotyczący aktywności phishingowej.* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

90. *Phishing w liczbach: statystyki dotyczące phishingu, które trzeba znać w 2016 r.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://blog.barkly.com/phishing-statistics-2016

91. PLETZER, Valentin. Oprogramowanie szpiegowskie zdemaskowane. *CHIP*, 2007, nr 10, s. 116-120.

92. PLOHMANN, Daniel, Elmar GERHARDS-PADILLA i Felix LEDER. *Botnety: wykrywanie, pomiar, dezynfekcja i obrona.* ENISA, 2011 [online]. [cytowany 17 maja 2015], s. 14. Dostępny w: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence.

93. *Policyjne oprogramowanie ransomware.* [online]. [cyt. 14.8.2016]. Dostupné z: https://www.f-secure.com/documents/996508/1018028/multiple_ransomware_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000

94. *Security Insights: Ransomware sześć razy inne.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://www.root.cz/clanky/postrehy-z-bezpecnosti-ransomware-sestkrat-jinak/

95. *POŽÁR, Josef. Bezpieczeństwo informacji*. Pilzno: Aleš Čeněk, 2005

96. *Uważaj na zgłoszenia o rzekomym niezapłaconym roszczeniu - to oszustwo.* [online]. [cyt. 15.8.2016]. Dostępny pod adresem: https://www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/

97. *Należy uważać na zawiadomienie o żądaniu przejęcia przed przejęciem - jest to oszustwo.* [online]. [cyt. 15.8.2016]. Dostępny pod adresem: https://www.csirt.cz/news/security/?page=87

98. PROSISE, Chris i Kevin MANDIVA. *Reagowanie na incydenty i informatyka śledcza, wydanie drugie.* Emeryville: McGraw-Hill, 2003

99. RAK, Roman i Radek KUMMER. Zagrożenia informacyjne w latach 2007 - 2017. *Magazyn Bezpieczeństwa*, 2007, t. 14, nr 1, s. 4.

100. *Ransomware.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://www.trendmicro.com/vinfo/us/security/definition/ransomware

101. *Komunikacja zagrożeń: cyberprzemoc* [online]. [cyt. 19.3.2014]. Dostępny pod adresem: http://www.e-nebezpeci.cz/index.php/rizikova-komunikace/kybergrooming

102. SCHNEIER, Bruce. *Przestępczość: Następna wielka rzecz w Internecie.* [online]. [cyt. 6.11.2007]. Dostępne na stronie https://www.schneier.com/crypto-gram/archives/2002/1215.html

103. SCHNEIER, Bruce. *Internet rzeczy zmieni wielkie włamania w prawdziwe katastrofy.* [online]. [cyt. 10.8.2016]. Dostępny pod adresem: https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster

104. SCHNEIER, Bruce. *Siedem typów hakerów.* [online]. [cyt. 16.8.2015]. Dostępny pod adresem: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html

105. SCHRYEN, Guido. Wpływ umieszczania adresów e-mail w Internecie na otrzymywanie spamu: analiza empiryczna. *Computers & Security*, 2007, vol. 26, nr 5, s. 361-372.

106. Selfmite - *Android SMS robak Selfmite powraca, bardziej agresywny niż kiedykolwiek.* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html

107. *Złośliwy kod jest kierowany* na *telefony komórkowe i rozprzestrzenia się jak lawina.* [online]. [cyt. 17.5.2016]. Dostępny pod adresem: https://www.novinky.cz/internet-a-pc/bezpecnost/401956-skodlivy-kod-cili-na-mobily-siri-se-jako-lavina.html

108. *Śledzenie przesyłek Poczty Czeskiej lub nowy szkodnik.* [online]. [cit.14.8.2016]. Dostępny pod adresem: http://www.viry.cz/sledovani-zasilky-ceske-posty-aneb-nova-havet/

109. SMEJKAL, Vladimír, Tomáš SOKOL i Martin VLČEK. *Prawo komputerowe.* Praga: C. H. Beck, 1995

110. Smejkal, Władimir. Przestępczość w środowisku systemów informatycznych a rekodyfikacja kodeksu karnego. Trestněprávní revue, 2003, t. 2, nr 6, s. 161.

111. SMEJKAL, Vladimir. *Cyberprzestępczość.* Pilzno: Aleš Čeněk, 2015

112. *Statystyki i fakty dotyczące spamu* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://www.spamlaws.com/spam-stats.html

113. *Statystyki spamu*. [online]. [cyt. 14.8.2016]. Dostępny pod adresem: https://www.spamcop.net/spamstats.shtml

114. STRAUS, Jiří i in. *Metodologia kryminalistyczna.* Pilzno: Aleš Čeněk, 2006

115. *Stuxnet.* [online]. [cyt. 2016-07-23]. Dostępny pod adresem: https://cs.wikipedia.org/wiki/Stuxnet

116. *Dziennik ukierunkowanych ataków cybernetycznych.* [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://apt.securelist.com/#secondPage

117. TAYLOR, Harriet. *W jaki sposób "Internet rzeczy" może okazać się zgubny.* [online]. [cyt. 17.6.2016]. Dostępny pod adresem: http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html

118. *Uścisk dłoni TCP krok po kroku.* [online]. [cyt. 18.8.2016]. Dostępny pod adresem: http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000

119. *The Internet Organised Crime Threat Assessment (iOCTA) 2014* [online]. [cyt. 10.8.2015]. Dostępny pod adresem: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

120. *The Malware Museum @ Internet Archive*. [online]. [cyt. 17.5.2016]. Dostępny pod adresem: https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/

121. *Świadectwo byłego hakera.* [online]. [cyt. 26.9.2008]. Dostępny pod adresem: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html

122. *Pierwsze mobilne szkodliwe oprogramowanie: jak Kaspersky Lab odkrył Cabir.* [online]. [cyt. 29.6.2015]. Dostępny pod adresem: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir

123. Tinba: *W32. Tinba (Tinybanker).* [online]. [cyt. 2016-08-15]. Dostępny pod adresem: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf

124. *Porada miesiąca lipiec 2016 - Unikaj phishingu*. [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/

125. *Czołowy spamer skazany na prawie cztery lata.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: http://www.pcworld.com/article/148780/spam.html

126. Konwencja o cyberprzestępczości. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

127. *Podręcznik Organizacji Narodów Zjednoczonych dotyczący zapobiegania i kontroli przestępczości komputerowej.* [online]. [cyt. 2016-08-20]. Dostępny pod adresem: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

128. *Wojny botnetów - jak działają botnety.* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://tmp.testnet-8.net/docs/h9_botnet.pdf

129. *Czy wiesz, co to jest KYBERSHIKANA?* [online]. [cyt. 19.8.2016]. Dostępny pod adresem: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

130. *Badania nad ryzykownymi zachowaniami czeskich dzieci w środowisku internetowym 2014* [online]. [cit.19.8.2016]. Dostępny pod adresem: https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace

131. *Ostrzeżenie! Ponad 900 milionów telefonów z systemem Android jest podatnych na nowy atak "QuadRooter".* [online]. [cyt. 2016-08-10]. Dostępny pod adresem: https://thehackernews.com/2016/08/hack-android-phone.html

132. *OGLĄDAJ: ISIS pozbywa się więźniów żywcem, wysadza zakładników w powietrze za pomocą RPG, a innych zabija ładunkami wybuchowymi - wideo z grafiką.* [online]. [cyt. 2016 Aug 20]. Dostępny pod adresem: https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382

133. **WILSON Tracy, V.** *Jak działa phishing.* [online]. [cyt. 14.8.2016]. Dostępny pod adresem: http://computer.howstuffworks.com/phishing.htm

134. Xshqi - *robak na Androida w chińskie walentynki.* [online]. [cyt. 2016-08-14]. Dostępny pod adresem: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/

135. *Yahoo bada, czy haker rzeczywiście posiada dane 200 milionów kont.* [online]. [cyt. 16 sierpnia 2015]. Dostępny pod adresem: http://www.lupa.cz/clanky/yahoo-resi-jestli-hacker-opravdu-ma-udaje-o-200-milionech-tamnich-uctu/

136. YAR, Majid. Hakerstwo komputerowe: kolejny przypadek przestępczości nieletnich? *The Howard Journal*, 2005, t. 44, nr 4, s. 387-399.

137. ZETTER, Kim. *Czy pasażerowie mogą włamać się do samolotów komunikacyjnych?* [online]. [cit.5.5.2016]. Dostępny pod adresem: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/

138. *Znów pojawiły się fałszywe doniesienia*. [online]. [cyt. 15.8.2016]. Dostępny pod adresem: https://www.csirt.cz/news/security/?page=97