CYBERNIEBEZPIECZEŃSTWO

OMÓWIENIE CYBERBEZPIECZEŃSTWA I ZŁOŚLIWEGO WYKORZYSTANIA CYBERPRZESTRZENI

Co-funded by the
Erasmus+ Programme
of the European Union

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

Omówienie cyberbezpieczeństwa i złośliwego wykorzystania cyberprzestrzeni

Rui Miguel Silva[1], Ivan Zelinka[2]

[1] Lab UbiNET - Bezpieczeństwo informatyki i cyberprzestępczość / LISP – Laboratorium Informatyki, Politechniczny Instytut Beja, Superior and Management School, Rua Pedro Soares, s / n, 7800-295 Beja, Portugalia

[2] Katedra Informatyki, Wydział Elektryczny i Nauk Komputerowych, VSB-TUO, 17. Listopada 2172/15, 708 00 Ostrava-Poruba, Republika Czeska

Abstrakt

Cyberprzestrzeń wkracza w nasze życie od lat we wszystkich dziedzinach życia współczesnych społeczeństw. Gry i zabawy, informacje, od sportowych do politycznych i kulturalnych, rozpowszechnianie osiągnięć naukowych, działania rządowe i publiczne - wszystkie te dziedziny tworzą nową rzeczywistość ekonomiczną i finansową. Obecnie „Ludzie i pieniądze" są w cyberprzestrzeni, a to sprawia, że tam skupia się dziś działalność przestępcza. Z drugiej strony cyberprzestrzeń zapewnia dostęp z każdego miejsca na kuli ziemskiej do innych zakątków świata za jednym kliknięciem myszy. Cyberprzestępczość i wszystkie inne „cyber", jak bezpieczeństwo cybernetyczne, obrona cybernetyczna, wojna cybernetyczna, cyberterroryzm, cyberhaktywizm, czyli szpiegostwo cybernetyczne, pojawiły się w świecie rzeczywistym. Niniejszy wykład będzie przeglądem najnowszej sytuacji, gdy idzie o złe lub złośliwe użycia cyberprzestrzeni spowodowane słabością zabezpieczeń a przy tym znacznymi zyskami z wykorzystania cyberprzestrzeni jako platformy złośliwego działania.

Słowa kluczowe: bezpieczeństwo cybernetyczne, hakowanie, cyberprzestępczość, cyberterroryzm

Wprowadzenie

Żyjemy w nowoczesnym świecie, w którym technologie otaczają nas na każdym kroku. Mądre telefony zawierające system operacyjny, który budzi cię rano, pokazując najnowsze aktualności i prognozę pogody. W drodze do pracy dostrzegasz technologię zapakowaną w twój samochód. W swojej pracy musisz wybrać - ciężką pracę lub skorzystanie z technologii i spędzanie czasu przed ekranem komputera. Po prostu nie można sobie wyobrazić życia w 21 wieku bez technologii.

Współczesny wiek coraz bardziej zmierza w kierunku globalizacji i wzajemnych połączeń. Istnieją inne opcje łączności - powszechną praktyką jest posiadanie telefonu nieprzerwanie podłączonego do sieci operatora komórkowego i korzystającego z transmisji danych. Ponadto połączenie bezprzewodowe jest obecne w budynkach, możesz łączyć się w środkach publicznego transportu i wkrótce w samolocie. Czas płynie, wciąż nowe i nowe urządzenia łączą się codziennie na całym świecie - od komputerów, tabletów, telefonów, telewizorów po zegarki, okulary i inne przenośne urządzenia. W najbliższych latach twój dom, samochód, pralka, blender, sztućce zostaną połączone ... w końcu nawet ty sam.

Wszystkie pozytywne sprawy mają ciemną stronę. Analiza wszystkich możliwych negatywów potrzebowałby osobnej pracy filozoficznej. Czytelnik zostanie zatem zapoznany z jednym ważnym i bardzo obszernym tematem, który otwiera rozwój technologii – bezpieczeństwem komputera, a zwłaszcza złośliwym kodem (znanym również jako złośliwe oprogramowanie). Każdy człowiek jest niedoskonały, co znajduje również odzwierciedlenie w technologiach takich jak systemy komputerowe. Im bardziej świat się łączy i systemy stają się bardziej rozbudowane, tym więcej możliwości nabywają przestępcy. Pamiętaj, że złośliwe kody nie są kierowane tylko na komputer ale także na inne urządzenia elektroniczne, które mogą być narażone na atak. Czytelnik powinien pamiętać, że takie urządzenia mogą zakłócać jego życie prywatne i mogą zawierać dane osobowe lub inne cenne dane. W tym systemy bankowości komputerowej, które zarządzają Twoimi finansami.

Oczywiste jest, że nieuprawnione manipulowanie takimi systemami może wyrządzić szkody osobom, grupom, instytucjom i całym krajom w skali globalnej. Poczujesz poważne konsekwencje, jeśli staniesz się ofiarą przestępcy i jego atak będzie zakończony powodzeniem. Te inicjatywy skłoniły mnie do dalszego myślenia: „Jak łatwo można wykonać udany atak? Jak mogę zostać zaatakowany w cyfrowym świecie i jakie mogą być prawdziwe konsekwencje? Czy systemy są chronione w jak największym stopniu, aby wyeliminować ryzyko?"

Te pytania wywołały moje zainteresowanie tym zagadnieniem. Dlatego spróbuję wcielić się w rolę atakującego, aby lepiej zrozumieć taktykę przestępcy i wykorzystać tę wiedzę w celu lepszego

zapobiegania atakom i ich wykrywania. Będę następnie wykorzystywać tę wiedzę w celu poprawy bezpieczeństwa systemów, którymi zarządzam, i programów, które stworzyłem. Informacje teoretyczne i praktyczne są również udostępniane tym, którzy chcą uczestniczyć w zwiększaniu bezpieczeństwa systemów komputerowych.

Informacje odgrywają w dzisiejszych społecznościach kluczową rolę. W początkowym okresie rozszerzania się technologie komputerowe w ostatnich dziesięcioleciach koncentrowano się na przesyłach i jak największej dostępności. Na ochronę prawie nikt uwagi nie zwracał, ponieważ jej konsekwentne zastosowanie sprawia że rozwiązania IT stają się droższe a osiągnięcie wyżej wymienionych celów podlega ograniczeniom. Na przełomie tysiącleci liczba różnorodnych ataków na systemy komputerowe osiągnęła jednak takie rozmiary a straty przez nie zadawane stały się tak znaczące, że nastąpiło otrzeźwienie i na pierwszy plan wysunęła się ochrona informacji znajdujej się w komputerach. Dzisiaj przeciętny użytkownik ma do dyspozycji niezawodny program antywirusowy, zaporę ogniowa, aktualizacje Windows, oprogramowanie antyszpiegowskie, filtry antyspamowe, system operacyjny w wersji zaawansowanej i systemy backupu danych. W ciągu najbliższych lat potrzeba będzie coraz więcej specjalistów ds. bezpieczeństwa. Według opinii czołowych światowych ekspertów ds. Bezpieczeństwa i zgodnie z naszym codziennym doświadczeniem ich liczba powinna być czterokrotnie większa. Choć bezpieczeństwu systemów komputerowych poświęca się bez porównania większą uwagą niż w poprzednich latach, ale jednocześnie znacznie wzrosła liczba i poziom skomplikowania technologii, które są niezbędne do skutecznej ochrony. Dzisiaj minęły już czasy naiwnych ataków, gdy piętnastoletni haker był w stanie sprzed 15 lat wyzwalanie wystukać skrypty i włamać się do systemu. Choć w przypadku jednego lub dwóch największych serwerów WWW w Internecie (przypadek Mafiaboy, rok 2000), autorami ataków byli już dobrzy specjaliści. Oprócz ulepszeń nasza obrona, a mianowicie zaawansowana technologia, jest w stanie wyśledzić atakujących. Wymieńmy przypadki niektórych incydentów z roku 2008:

- Błąd w systemie DNS wykryty przez Dana Kaminskiego: korzystanie z tzw. paradoksu urodzinowego, aby udowodnić fałszowanie komunikacji z serwerem DNS i uszkodzenie jego cache zagroziło całej infrastrukturze internetowej pozwalając na przekierowywanie dowolnych serwerów WWW i e-mail. Tylko dzięki szerokiej współpracy wielu zainteresowanych podmiotów na całym świecie (producenci serwerów DNS, operatorzy, ISP, ...), które miały zostać dotknięte tym błędem doszło do jego eliminacji pomyłki przed jej szerszą publikacją. Nie wiemy, czy błąd został wykryty i wykorzystany zanim ujawnił go Dan Kaminski.

- Pierwsze szkodliwe oprogramowanie przeniknęło już także do kosmosu - robak W32. Gammima AG został schwytany na międzynarodowej stacji kosmicznej IIS w notebooku jednego z rosyjskich astronautów.

- Kilka lat temu na konferencji BlackHat skupił uwagę na możliwości stworzenia uniwersalnego rootkita dla routera Cisco. Routery tych marek obsługują około 2/3 Internetu, gdyby stworzenie takich rootkitów się powiodło hakerzy mogliby uzyskać ogromną moc.

-We Francji kowboj ukradł pieniądze z konta bankowego prezydentowi Nicolasowi Sarkozy'emu. Nie było to działanie na poziomie zorganizowanej grupy, ale dwie małe malwersacje finansowe. Czy nie trzeba uznać, że celem takiego ataku mógłby stać się każdy?

-W Chile ujawniono, że nieznany kowboj wykradł i opublikował w Internecie nazwiska i dane sześciu milionów chilijskich obywateli.

- Wykryto błąd zabezpieczeń w nowym Boeingu 787 pozwalający na uzyskanie przez pasażera z jego sprzętu dostępu do sieci używanych przez przyrządy pokładowe. Komentarz jest chyba zbyteczny.

- Oczywiście nowoczesny telefon komórkowy jest narażony na ataki za pomocą Bluetooth lub MMS. Na przykład w przypadku niektórych popularnych wersji Motorola RAZR do instalacji szkodliwego oprogramowania wystarczy tylko odebrać MMS z zainfekowanym plikiem JPEG. Taki telefon można następnie zmusić na przykład do przekazywania wszystkich rozmów i wiadomości tekstowych W przyszłości czekam także na botnet utworzony przez telefon komórkowy.

- Błędy bezpieczeństwa miały zostać wykryte w ekspresach do kawy marki Jura F90 (elektryczny ekspres do kawy ma interfejs umożliwiający sterowanie na odległość). Na pierwszy rzut oka brzmi to nawet zabawnie, ale w istocie udany atak może prowadzić do tego przechwycenia komputera PC z systemem Windows używanego do sterowania ekspresem. Obecnie rzecz dotyczy interesującego ewenementu, ale nie jest odległy czas, kiedy prawie każdy elektroniczny zestaw w sektorze konsumenckim, w tym elektryczne gniazdko ścienne będzie miało swój własny adres IPv6 (tak zwany inteligentny dom). Powierzchnia potencjalnych przestępstw znowu wzrośnie.

- W październiku 2008 r. Ponownie wykryto błąd w prądzie wewnętrznym systemu RPC (Windows (2000, XP, 2003, Vista, 2008). Za wykorzystaniem błędów możliwe jest na zdalnym systemie uruchomienie dowolnego kodu pod kontem systemowym (tj. w najgorszym przypadku do instalacji) rootkita). Zagrożenie jest tak istotne, że Microsoft opublikował łatkę poza zwykłym terminem aktualizacji systemu (co drugi wtorek w miesiącu). Tym razem Microsoft miał szczęście, ponieważ błąd wykryto wcześniej niż znalazła go strona przeciwna, w przeciwnym razie z największym prawdopodobieństwem czekałby nas atak podobnego robaka jak słynny W32. Blaster w 2003 roku.

Ataki na systemy komputerowe z pewnością nie zanikają a raczej będą, zdaniem autorów, rok po roku się nasilać. Co więcej - według wybitnego programu antywirusowego firmy McAfee, z grubsza od 2007 roku internetowy świat przestępczy zmienił się w tym sensie, że zniknęli młodzi hakerzy (tak zwani skrypciarze), którzy tworzyli wirusy i wykonywali hakerskie ataki po prostu dla zabawy lub z

ciekawości. Zastępują ich zorganizowane gangi, zawodowi przestępcy. Dzisiaj w tej dziedzinie w dużej mierze celem jest zdobycie pieniędzy. Pojawiła się cała szara strefa, w której możliwe są usługi hakerów, twórców spyware i demise botów – można to dziś kupić jak każdą inną usługę.

Zagrożenia rosną, a więc musimy poszerzyć naszą wiedzę, aby im się z powodzeniem przeciwstawiać. W walce z dowolnym antagonistą należy go dobrze poznać - jego grę, zdobycze, narzędzia i motywy. Działania, wiedza i umiejętności, które służą do tego celu, zwykle zwane są hakowaniem etycznym, prowadzonym przez ludzi, którzy są potem w stanie odizolować „złych" hakerów. Informacje zawarte w tej i podobnych publikacjach nie wystarczą, by zapobiec nadużyciom i atakom na operacje komputerowe. Konieczna jest bardziej solidna edukacja dotycząca rozwiązywanie tych problemów. Niemniej jednak pomimo gigantycznej różnorodności motywów i intencje wszystkie hakerskie działania łączy ciekawość i tęsknota za poznawaniem.

Firma i osoby prywatne muszą wiedzieć, w jaki sposób dochodzi do uszkodzeń komputera. Co jest genezą ataków komputerowych, jak należy się najlepiej przygotować. Muszą mieć świadomość, jak się z nimi zmierzyć. Uważamy, że istnieją dwa kluczowe aspekty, które prowadzą do ataków komputerowych, najpierw brak cyberbezpieczeństwa, a po drugie złośliwe wykorzystanie cyberprzestrzeni.

Brak cyberbezpieczeństwa

Pierwszą kwestią, która prowadzi do braku cyberbezpieczeństwa, jest dostęp do informacji. Uzyskanie informacji o osobie fizycznej lub firmie jest dzisiaj możliwe i bardzo łatwe dla każdego z dostępem do Internetu. Dzięki tym informacjom w większości przypadków możliwe jest zidentyfikowanie słabych punktów, technicznych lub ludzkich, co pozwala na ułożenie planu udanego ataku. Czasami informacja jest dostępna dla każdego, w innych przypadkach powiązanie zebranych informacji z wykorzystaniem, a nawet bez wykorzystania technik i narzędzi wywiadowczych prowadzi do takich informacji, które pomagają w zaplanowaniu ataku. Proces gromadzenia informacji wykorzystuje dwa rodzaje procedur: zasoby w Internecie i specjalistyczne narzędzia opracowane specjalnie w celu gromadzenia określonego rodzaju informacji. Niektóre przykłady zasobów w Internecie to: (i) prosta wyszukiwarka Google lub inne wyszukiwarki; (ii) witryny gromadzące dane statystyczne, takie jak „www.alexa.org"; (iii) archiwum internetowe, które przechowuje każdą stronę, która pojawia się w Internecie pod adresem „www.archive.org"; (iv) czarne listy, na przykład serwerów sieciowych lub e-mailowych „www.dnsbl.info"; (v) lub informacje o systemie operacyjnym i serwerze internetowym oraz oprogramowaniu strony docelowej, takie jak „www.netcraft.com". Przykłady specjalistycznych narzędzi dla gromadzenie informacji to: (i) „DNSENUM" dostępny pod

adresem „github.com/fwaeytens/dnsenum”, który używa Systemu Nazw Domen do zebrania informacji o celu, takich jak „nameservers”, „MX record” lub „reverse lookups on netranges”; (ii) „WHOIS” dostępny w kilku odmianach dających informacje o zarejestrowanych domenach, w tym informacje techniczne i związane z zarządzaniem w firmach docelowych; (iii) „TheHarvester” dostępny na „github.com/laramies/theHarvester” który gromadzi informacje takie jak „konta e-mail”, „nazwy subdomen”, „nazwiska pracowników” lub „wirtualne nazwy hostów ”; (iv) „Metagoofil” dostępny pod adresem „Github.com/laramies/metagoofil”, który wyodrębnia metadane dokumentów publicznych takich jak PFD, DOC między innymi, które są dostępne dla docelowej strony internetowej i na podstawie tych informacji można uzyskać „nazwy użytkownika”, „nazwiska”, „ścieżki w systemie komputerowym” w którym dokumenty zostały wygenerowane, a wszystko to może być przydatne dla lepszego planowanie ataków; (v) lub wreszcie „NAMP” dostępny pod adresem „Github.com/nmap/nmap”, który pozwala między innymi na identyfikację lub na przynajmniej bardzo łatwe odgadnięcie w docelowym systemie komputerowym systemu operacyjnego, otwartych portów i oprogramowania działającego na tych portach.

Oprócz łatwego gromadzenia informacji i otwartego dostępu, ogromna popularność dostępu do Internetu oferowanego przez firmy telekomunikacyjne, walczących o większe liczby klientów, którzy używają ich jako dostawców usług internetowych, ogromnie rozprzestrzeniła dostęp do Internetu do wielu domów w tzw. społeczeństwach rozwiniętych. Wielu zwykłych klientów korzysta z subskrypcji, również tak zwanych „usług pakietowych”, które obejmują telewizję, telefon i Internet, a w niektórych przypadkach także telefony komórkowe, a nawet mobilne połączenia internetowe z wysokim pasmem. Korzystając z tych „usług pakietowych”, wielu użytkowników ma stałe połączenie z Internetem w swoich domach. Czasami, jeśli nie w większości przypadków, bez środków bezpieczeństwa, takich jak antywirus lub zapory ogniowe. Poza tym uważamy, że wielu użytkowników stara się uzyskać w Internecie ze źródeł pirackich darmową zawartość, taką jak muzyka, filmy, książki techniczne, między innymi używając protokołów udostępniania plików peer-to-peer i platform takich jak BitTorrent. Ten proces może doprowadzić do wykorzystania luk w zabezpieczeniach komputera użytkowników cyberprzestrzeni, takich jak backdoory, które pozwalają hakerom przejąć kontrolę nad zainfekowanym komputerem. Inną częstą czynnością wśród użytkowników cyberprzestrzeni jest korzystanie z wyszukiwarek w celu uzyskania bezpłatnych odtwarzaczy lub czytników plików, takich jak odtwarzacze „AVI”, „MPEG3” lub „MPEG4” lub czytnik „PDF”. Proste wyszukiwanie z trzema słowami „bezpłatny”, „pobierz” i „czytnik” w Google daje 27 700 000 wyników. Zaufanie stron do pobierania nie budzi wątpliwości zwykłego użytkownika cyberprzestrzeni, który uważa, że wystarczy kliknąć, pobrać oprogramowanie i zainstalować na swoim komputerze. Takie zachowanie wynika z bardzo słabej cyberkultury, w której bezpieczeństwo

cybernetyczne nie jest jeszcze na właściwym miejscu. Tymczasem jednocześnie użytkownicy mogą używać komputerów do uzyskiwania dostępu do bankowości internetowej lub przesyłania osobistych danych finansowych na platformy e-administracji. Ten brak edukacji cybernetycznej, która zapewniłaby użytkownikom cyberprzestrzeni wiedzę na temat zagrożeń w cyberprzestrzeni, jest najważniejszym elementem niepewności cybernetycznej.

Jak sugerowano we wstępie do tego dokumentu, oprogramowanie zawsze będzie miało luki, nawet ze względu na złożoność integracji oprogramowania, która importuje biblioteki i moduły oprogramowania, które nie zostały poprawnie sprawdzone. Z powodu niedostatecznej dbałości o bezpieczeństwo ze strony programistów, z powodu „niezbyt dobrych" umiejętności programistycznych lub wielu innych aspektów zawsze powinniśmy liczyć się z lukami w oprogramowaniu. Ale oprócz luk w oprogramowaniu istnieją również konfiguracje domyślne lub słabe. Ten aspekt jest czasem wykorzystywany przez hakerów do przeprowadzania udanych ataków mimo braku luk w oprogramowaniu. Na przykład konfiguracja systemów o nazwie użytkownika „admin" i bez hasła lub systemów o nazwie użytkownika równej imieniu użytkownika i słabych haseł, takich jak „12345678". Te karykaturalne przykłady nie są rzadkie. Wchodząc nieco w świat słabych konfiguracji, niektórzy administratorzy systemu utrzymują dobrze znane porty we wspólnych usługach, takich jak dostęp SSH na porcie 22, co prowadzi do ataków siłowych na ich systemy, wykorzystujące na przykład aplikacje takie jak Hydra do automatyzacji ataku, który następnie musi mieć „głupiego" użytkownika ze słabym hasłem, aby skutecznie zaatakować cały system. Z innej perspektywy słabych konfiguracji, często mamy do czynienia z faktem, że wiele zespołów instalujących dostawców usług internetowych pozostawia domyślne nazwy użytkowników i hasła skonfigurowane na klientach routera, tym samym narażając ich klientów na łatwe ataki. To niewiarygodnie nieodpowiedzialne zachowanie występuje w wielu prawdziwych zdarzeniach.

Luki w oprogramowaniu i słabe konfiguracje są publicznie ogłaszane i służą do tego znormalizowane notacje. Luki w oprogramowaniu są znormalizowane we „wspólnych lukach w zabezpieczeniach i narażeniach" (CVE) dostępnych na stronie „cve.mitre.org/", a słabe konfiguracje są znormalizowane we „wspólnym zestawianiu konfiguracji" (CCE) dostępnym na stronie „nvd.nist.gov/cce/index.cfm". Te dwie notacje są częścią większego zestawu języków, notacji i systemów klasyfikacji, promowanych przez MITER i NIST oraz inne organizacje, jako sposób zarządzania cyberbezpieczeństwem. Jednocześnie jednak te publiczne ogłoszenia o lukach w zabezpieczeniach i słabych konfiguracjach mogą być pomagać sumiennym szefom bezpieczeństwa (CSO), a także mogą pomóc hakerom, którzy czekają na te ogłoszenia, by podjąć próbę zaatakowania mniej sumiennych CSO. Zatem te same informacje mogą pomóc w dobrym lub złośliwym wykorzystaniu cyberprzestrzeni. W następnej części skupimy się na niektórych złośliwych zastosowaniach cyberprzestrzeni.

Złośliwe wykorzystanie cyberprzestrzeni

Istnienie „repozytoriów luk”, takich jak National Vulnerability Database (NVD) pod adresem „nvd.nist.gov”, umożliwia i ułatwia wyszukiwanie znanych luk. Tak więc normalnym sposobem myślenia atakującego powinno być po zebraniu dobrych informacji o jego celu przeszukiwanie repozytoriów podatności, w poszukiwaniu znanych luk, które mógłby zbadać dla osiągnięcia swojego celu. Ale wiedza na temat podatności, którą można zbadać, nie umożliwia zbadania samej luki, potrzebny jest exploit, który mógłby wykorzystać tę lukę. Tymczasem luka wskazuje na pewien słaby punkt w rozwoju oprogramowania, który może być wykorzystany do złamania bezpieczeństwa oprogramowania, exploit to konkretny element oprogramowania, który skutecznie „wykorzystuje lukę w celu wykorzystania” oprogramowanie. Exploit jest więc praktyczną bronią, a nie hipotezą, nie jest to konceptualny, ani nawet teoretyczny sposób eksploracji. W tej części naszej podróży znajdują się „repozytoria exploitów”, takie jak na przykład Baza danych exploitów pod adresem „www.exploit-db.com”, która w chwili pisania tego tekstu ma zarchiwizowane 37 771 exploitów. Jeśli więc haker ma cel do zaatakowania, może wykonać trzyetapową procedurę: 1) Zbieranie informacji; 2) repozytoria podatności; 3) Wykorzystuj repozytoria.

Czasami jednak hakerzy nie mają określonego celu, po prostu mają wiedzę na temat podatności i odpowiedniego exploita do użycia, więc w tym scenariuszu haker nie dba o to, kto jest celem lub ofiarą, po prostu chce znaleźć kogoś podatnego na exploit, który posiada. W takich sytuacjach cyberprzestrzeń ma również odpowiedź; istnieją „repozytoria Dork”, takie jak „Baza danych hakerskich Google” (GHDB) na stronie „www.exploit-db.com/google-hacking-database”. Dorks to wyrażenia, które można wykorzystać w wyszukiwarkach takich jak Google, aby znaleźć witryny, które są podatne na pewien rodzaj luki. Wśród różnych rodzajów wykrytych luk znajdują się na przykład: (i) „Wrażliwe serwery”; (ii) „wrażliwe pliki”; (iii) „Wrażliwe informacje o zakupach online”; (iv) „Dane dotyczące sieci lub podatności”; (v) lub „Strony zawierające portale logowania”.

Istnieją więc „repozytoria luk”, „repozytoria exploitów”, „repozytoria Dork”, co więcej, istnieją systemy operacyjne specjalnie przeznaczone do hakowania systemów bezpieczeństwa komputerowego, takie jak „Kali Linux” dostępne na stronie „www.kali.org ”, A także frameworki, które ułatwiają ponowne wykorzystanie i rozwój exploitów, takich jak„ Metasploit ”dostępnych na „github.com/rapid7/metasploit-framework” lub„ www.metasploit.com ”, który jest już dołączony do Kali Linux. Możemy łatwo stwierdzić, że zasoby operacyjne do złośliwego korzystania z Internetu znajdują się w sieci i są dostępne dla wszystkich.

Oprócz zasobów operacyjnych, o których mowa w ostatnich akapitach, cyberprzestrzeń zapewnia również natywną tarczę ochronną ze względu na swój światowy obszar geograficzny, gdzie w

odległości kliknięcia myszą moglibyśmy zamówić działania z jednego do dowolnego innego zakątka świata, dając złośliwym użytkownikom cyberprzestrzeni (i) „fizyczny dystans" oraz (ii) „brak potrzeby kontaktu wzrokowego" z ofiarami, tarczę ochronną.

Nauka odgrywa także dużą rolę w złośliwym wykorzystaniu cyberprzestrzeni, ponieważ kryptografia, a mianowicie „kryptografia klucza publicznego" lub „kryptografia asymetryczna", zapewnia naukowe wsparcie poufności, uwierzytelnienia, a także bezpieczny sposób negocjowania nowego klucza do szyfrowania komunikacji za pośrednictwem Diffie - Algorytm Hellmana używającego w tym przypadku szyfrów „Symmetric Cryptography", takich jak dobrze znany, bezpieczny i szybki Advanced Encryption Standard (AES).

To właśnie naukowe wsparcie daje początek dwóm najważniejszym technologiom służącym do złośliwego wykorzystania cyberprzestrzeni, a mianowicie: komunikacji anonimowej i monetom kryptograficzne.

Niemniej jednak możliwość ustanowienia anonimowej komunikacji opiera się na dobrej zasadzie, która polega na ochronie prywatnych informacji o osobistych życzeniach i umożliwia ochronę danych osobowych. Ta sama możliwość pozwala również na wykorzystanie cyberprzestrzeni z anonimizacją przez tych, którzy mają złośliwe zamiary. Ta równowaga między ochroną danych osobowych i prawem do prywatności użytkowników cyberprzestrzeni z jednej strony, a zwalczaniem złośliwego użytkowania cyberprzestrzeni z drugiej strony, jest z pewnością jednym z największych wyzwań dla społeczności informatycznych i prawniczych w nadchodzących latach. Projekty takie jak „The Onion Router" (TOR) dostępne na stronie „www.torproject.org", które w znacznym stopniu przyczyniają się do rozpowszechniania korzystania z DarkWeb, umożliwiając anonimowe przeglądanie i publikowanie niebezpiecznych treści, takich jak sprzedaż narkotyków, zabójstwo na zlecenie, rynek broni lub zawartość pedofilska, mocno przyczyniając się do złośliwego wykorzystania cyberprzestrzeni. Jednak z powodu pewnych braków protokołu TOR jego prawdziwa anonimowość stała się wątpliwa, a powstają nowe projekty, takie jak projekt Riffle dostępny na stronie „github.com/kwonalbert/riffle".

Crypto Coins, po raz pierwszy został przedstawiony pod koniec 1994 r. przez grupę Cyberpunks w dokumencie o nazwie „Cyphernomicon" jako marzenie o cyfrowej gotówce i handlu elektronicznym bez zależności od banków centralnych. W 2008 r. Artykuł zatytułowany „Bitcoin: elektroniczny system gotówki Peer-to-Peer" [1] opublikowany pod pseudonimem „Satoshi Nakamoto" tworzy pierwszą monetę kryptograficzną. Bitcoiny mają genetycznie trzy główne cechy: (i) Wsparcie kryptograficzne za pomocą kryptografii asymetrycznej; (ii) Walidacja transakcji dokonywanych przez społeczność tak zwanych „górników", do których każdy mógł dołączyć przy użyciu określonego protokołu transakcji; (iii) Wysoki poziom anonimizacji. Od tego czasu powstało wiele innych monet

kryptograficznych opartych na oryginalnej propozycji Bitcoinów. Choć korzystanie z Bitcoinów nie powinno być bezpośrednio powiązane ze złośliwym wykorzystaniem cyberprzestrzeni, w rzeczywistości większość działań związanych z cyberprzestępczością wykorzystuje Bitcoiny jako formę płatności. Na przykład raport Europolu „Internetowa ocena zagrożenia przestępczością zorganizowaną 2015" [2], koncentrujący się na płatnościach transakcyjnych za kilka cyberprzestępstw, odnotowuje, że spośród dziesięciu wymienionych tam klas przestępstw Bitcoiny były obecne w ośmiu. Inne spojrzenie na to samo badanie pokazuje nam, że w „Płatnościach ofiar" Bitcoiny były we wszystkich dwóch rodzajach cyberprzestępstw, w „Płatnościach kryminalnych na rzecz przestępstw" Bitcoiny były obecne w czterech z sześciu rodzajów cyberprzestępstw. Bitcoiny były również obecne w pozostałych dwóch klasach cyberprzestępstw związanych z „Opłatami za legalne usługi" i „Przepływami pieniędzy". Możliwe jest jednak płacenie bitcoinami na przykład w firmie spożywczej „SubWay" lub za bilety lotnicze na „aBitSky" dostępne na „www.abitsky.com". Z drugiej strony liczba monet kryptograficznych rośnie bardzo szybko. 21 kwietnia 2016 r. było 675 różnych rodzajów kryptowalut, 16 maja 2017 r. było ich 722, we wrześniu 2017 r. było ich 867. Kolejnym interesującym faktem na temat ewolucji monet kryptograficznych jest to, że rozwijają się specjalne rodzaje monet kryptograficznych, których główną cechą jest wzmocnienie anonimizacji transakcji, nawet bardziej niż oferują to Bitcoiny. Jest to np. „Monero" dostępne na „github.com/monero-project/monero" i „Dash" dostępne na „github.com/dashpay/dash". W 2016 r. pojawiły się dwa inne podmioty ze środowiska naukowego, a mianowicie „Zcoin" dostępny na „github.com/zcoinofficial/zcoiniorze" i „ZCash" dostępny na „github.com/zcash / zcash ". Istnieją również specjalne aplikacje do prania transakcji Bitcoin, takie jak na przykład ta dostępna na „app.bitlaundry.com". Rynek transakcji Bitcoin jest również ważnym punktem analizy, ponieważ na przestrzeni prawie półtora roku, od kwietnia 2016 r. wartość Bitcoin wzrosła prawie dziesięciokrotnie Do 21 kwietnia 2016 r. Jeden bitcoin wyniósł około 381 euro, do 16 maja 2017 r., jeden bitcoin wyniósł około 1607 euro, a do chwili pisania tego tekstu, czyli do września 2017 r., jeden bitcoin wyniósł 3637 euro. Wartości te pochodzą ze strony „www.kraken.com".

Co ciekawe, ten okres, w ciągu ostatniego półtora roku, zwrócił szczególną uwagę na specjalny rodzaj cyberprzestępczości, ataki „Ransomware", które wykorzystują Bitcoiny do zapłaty od ofiar. Czy może to być zbieg okoliczności? Pozostawiamy to jako sugestię do dalszego czytania. Wreszcie, w szczególności w odniesieniu do Bitcoinów lub ogólnie monet kryptograficznych, należy badać technologię o nazwie BlockChain, w której rejestrowane są transakcje Bitcoin. W rzeczywistości technologia ta jest obsługiwanym kryptograficznie sposobem chronologicznej rejestracji własności. Dzięki tej technologii, dzięki temu mechanizmowi rejestracji własności, możliwe jest zagwarantowanie prawa do czegokolwiek (nie tylko monet kryptograficznych), a walidacja tego

prawa jest dokonywana przez całą społeczność, która chce wziąć udział w walidacji. Potęga tej technologii może doprowadzić nas do świata całkowicie zarządzanego przez maszyny, w którym mogliby zarejestrować swoją własność i udowodnić to komukolwiek, maszynie lub człowiekowi - czy należy to uznać za złośliwe wykorzystanie cyberprzestrzeni?

Wreszcie chcemy krótko skupić się na wykorzystaniu cyberprzestrzeni przez terrorystów [3]. Jako mechanizm propagandy i szkolenia (rekrutacja, radykalizacja i podżeganie), czasopisma online, takie jak „Dabiq" i „Rumiyah" z Państwa Islamskiego lub „Inspirować" z Al-Kaidy, są wykorzystywane do rozpowszechniania doktryny, gloryfikacji heroicznych działań terrorystycznych, samouczki do budowania broni od podstaw i przy użyciu tanich materiałów. Są gry komputerowe, w których bohaterami są wojownicy dżihadystów, lub platformy takie jak strona „jihadology.net", przy użyciu których wiele działań i informacji jest swobodnie rozpowszechnianych na całym świecie. Grupy terrorystyczne mają własne szyfry, takie jak „Asrar Al Dardashah" - pierwszy islamski program do szyfrowania wiadomości błyskawicznych. Służy to uzyskiwaniu wsparcia finansowego, przez zwolenników, a nawet przez ogół społeczeństwa lub poprzez działania związane z cyberprzestępczością. Jako platforma planowania, za pomocą protokołów anonimizacji w DarkWeb, do komunikacji między nimi lub w celu uzyskania informacji. Jako platforma zagrożeń z możliwością rozprzestrzeniania strachu. Jako platforma ataku, z możliwością wpływania nie tylko na struktury cyberprzestrzeni, a także na krytyczne infrastruktury, które mogą wpływać na populacje i cele w świecie rzeczywistym, np. na w celu rozmnażania wirusów biologicznych w systemach dystrybucji wody ze względu na dystrybucję do wszystkich domów, a także ponieważ nie można infekcji zatrzymać jednym kliknięciem ze względu na cechy fizyczne systemu.

Wnioski

W tym artykule krótko ujawniamy niektóre złośliwe zastosowania cyberprzestrzeni. Jesteśmy przekonani, że cyberbezpieczeństwo jest ściśle powiązane z solidną praktyczną wiedzą na temat procedur i technik hakerów. Edukacja cybernetyczna, a mianowicie edukacja w zakresie bezpieczeństwa cybernetycznego, jest niezbędna nie tylko dla technicznych jednostek firm i organizacji, ale także dla każdego użytkownika cyberprzestrzeni. Rosnące wykorzystanie cyberprzestrzeni w działaniach finansowych i egovernment wymaga szybkiej i zorganizowanej edukacji na temat zagrożeń związanych z cyberprzestrzenią.

Dwie maksymy przestępczości, które brzmią: „Gdzie są pieniądze, są przestępstwem" i „Gdzie są ludzie, są przestępstwa", dotyczą także cyberprzestrzeni, a fakty, na które wskazaliśmy w niniejszym artykule, pokazują pilną potrzebę zorganizowania edukacji w zakresie bezpieczeństwa

cybernetycznego, od edukacji podstawowej poprzez szkołę średnią, do firm i organizacji w całym społeczeństwie. Wierzymy, że lepszym sposobem na osiągnięcie edukacyjnego sukcesu w szerokiej populacji jest demonstracja procedur hakerskich, techniki, zasobów, a także sposobu myślenia. Nasz artykuł to skromny wkład w działania na długiej drodze do lepszej i bezpieczniejszej cyberprzestrzeni.

Przypisy

[1] S. Nakamoto, „Bitcoin: elektroniczny system kasowy peer-to-peer", 2008.

[2] Europol, „Internetowa ocena zagrożenia przestępczością zorganizowaną 2015", 2016 r.

[3] Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości, „Wykorzystanie Internetu do cele terrorystyczne ", 2012

Autorzy - biografie

Rui Miguel Silva urodził się 4 lutego 1971 r. W Beja w Portugalii.

W 1996 r. uzyskał dyplom „Systemy informatyczne i inżynieria komputerowa" w Wyższym Instytucie Technicznym na Politechnice w Lizbonie, następnie uzyskał tytuł magistra i doktora w dziedzinie „Inżynierii elektrycznej i komputerowej" również w Wyższym Instytucie Technicznym na Politechnice w Lizbonie, odpowiednio w 2002 i 2009 r. Od 2002 roku koncentruje się na stosowaniu ofensywnego bezpieczeństwa, a mianowicie na inwazyjnych technikach systemów komputerowych, współpracując z kilkoma krajowymi i międzynarodowymi organizacjami w dziedzinie bezpieczeństwa cybernetycznego i cyberprzestępczości, takimi jak Portugalska Agencja Bezpieczeństwa Narodowego, armia portugalska, portugalska akademia wojskowa, Prokuratoria Generalna Portugalii, policja kryminalna i wyspecjalizowana grupa ds. cyberprzestępczości INTERPOLu.

Rui Miguel Silva jest profesorem w Politechnice w Beja, Portugalia, od dwudziestu lat. Pełnił kilka funkcji kierowniczych, takich jak Dyrektor Departamentu Inżynierii lub Koordynator kursu inżynierii informatycznej. Obecnie jest szefem laboratorium UbiNET - „Bezpieczeństwo informatyki i cyberprzestępczość" oraz koordynatorem kursu magistra inżyniera bezpieczeństwa informatycznego.

Rui Miguel Silva jest autorem i współautorem około 40 publikacji naukowych i był współzałożycielem trzech firm, poświęcając swoją działalność badawczą nauce stosowanej w dziedzinie ofensywnych zabezpieczeń. Jego zainteresowania koncentrują się teraz na „Prewencyjnych testach penetracyjnych", aby umożliwić firmom ciągłe utrzymywanie świadomości i ochronę systemów przed lukami w zabezpieczeniach i słabymi konfiguracjami. Jest „genetycznie entuzjastycznym" badaczem w zakresie stosowania niekonwencjonalnych algorytmów i procedur do łamania systemów informatycznych.

Ivan Zelinka pracuje obecnie na Politechnice Ostrawskiej (VŠB-TU), Wydziale Elektrycznym i Informatyki. Ukończył kolejno Politechnikę w Brnie (1995 - mgr), UTB w Zlinie (2001 - doktorat) i ponownie na Politechnice w Brnie (2004 - prof. Prof.) I VSB-TU (2010) - profesor). Przed karierą akademicką zajmował stanowiska technika TELECOM, specjalisty komputerowego (HW + SW) i nadzorcy banku komercyjnego (operacje komputerowe i LAN). Podczas swojej kariery akademickiej zaproponował i otworzył ponad 10 różnych wykładów. Został również zaproszony na wykłady na uniwersytetach w różnych krajach UE, a także na prezentacje i tutoriale na różnych konferencjach i sympozjach. Odpowiada za nadzorowanie grantu badawczego z czeskiej agencji grantowej GAČR o nazwie „Metody obliczeń miękkich w kontroli", był współinicjatorem grantu FRVŠ – „Laboratorium obliczeń równoległych". Dr Zelinka uczestniczył również w licznych grantach i dwóch projektach UE jako członek zespołu (5PR-RESTORM) i jako kierownik (7PR-PROMOEVO) czeskiego zespołu. Obecnie jest kierownikiem Wydziału Informatyki Stosowanej. Przez cały okres swojej kariery nadzorował liczne studia magisterskie i licencjackie oraz prace dyplomowe, pełnił rolę promotora doktorantów, w tym studentów z zagranicy. Został wyróżniony nagrodą Siemensa za doktorat i otrzymał nagrodę od czasopisma Software News za książkę o sztucznej inteligencji. Ivan Zelinka jest członkiem British Computer Society, IEEE (komitet czeskiej Section of Computational Intelligence), a także zasiada w międzynarodowych komitetach programowych różnych konferencji i trzech czasopism międzynarodowych (Soft Computing, SWEVO, Editorial Council of Security Revue.) Jest autorem licznych artykułów w czasopismach oraz książek w języku czeskim i angielskim .