mgr Przemysław Mazurczak
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych
ORCID 0000-0001-5968-3019

WYKORZYSTANIE BOTNETÓW W CYBERPRZESTĘPCZOŚCI. ANALIZA WYBRANYCH PRZYPADKÓW

USE OF BOTNETS IN CYBER CRIME. ANALYSIS OF SELECTED CASES

Streszczenie
W opracowaniu przedstawiono analizę zagrożeń wynikającą z aktywności w Internecie sieci typu botnet. Sieci botnet są bardzo powszechnym narzędziem wśród cyberprzestępców, umożliwiają pozyskiwanie dużej ilości danych z komputerów zarażonych wirusem tworzącym daną sieć podporządkowaną w pełni jej twórcy. Obecnie istnieje wiele niezidentyfikowanych botnetów stanowiących zagrożenie dla użytkowników Internetu, te, które zidentyfikowano i zdiagnozowano są odpowiedzią na problem jak niebezpiecznym narzędziem w rękach cyberprzestępców jest botnet.

Słowa kluczowe: botnet, cyberbezpieczeństwo, cyberzagrożenia, komputer, sieć

Abstract
The article presents threat analysis resulting from botnet activity on the Internet. Botnet networks are a very common tool among cyber criminals, they enable the acquisition of large amounts of data from computers infected with the virus that creates the given network fully subordinated to its creator. Currently, there are many unidentified botnets that pose a threat to Internet users, those that have been identified and diagnosed are the answer to the problem of how dangerous a botnet is in the hands of cybercriminals.

Keywords: botnet, cybersecurity, cyber threats, computer, network

Wstęp

W Polsce, pomimo ciągle rosnącej liczby publikacji, wiedza na temat najnowszych trendów dotyczących zagrożeń płynących z sieci i systemów komputerowych stanowi rodzaj wiedzy specjalistycznej, niedostępnej i często niezrozu-

miałej dla dużej części społeczeństwa[1]. Brak aktualnej wiedzy o najnowszych zagrożeniach stanowi zagrożenie dla internautów i przyczynia się do lekceważenia środków bezpieczeństwa, niezauważania przez pokrzywdzonych włamań do ich systemów komputerowych, niewielkiej gotowości ofiar przestępstw do angażowania Policji w ich ściganie oraz w niskiego prawdopodobieństwa wykrycia sprawcy. Wobec tego, przestępczość zorganizowana czerpie znaczne zyski finansowe przy niewielkim ryzyku pociągnięcia do odpowiedzialności karnej. Przeciwdziałanie tej przestępczości jest niezwykle trudne i kosztowne. Wymaga nie tylko nakładów finansowych, organizacyjnych czy technicznych, ale także zwiększenia świadomości użytkowników sieci oraz organów ścigania o zagrożeniach powodowanych cyberprzestępczością.

Rozwój cyberprzestępczości następował wraz ze wzrostem społeczeństwa informacyjnego. Już na początku lat 60 dwudziestego wieku w USA, kiedy pojawiły się pierwsze komputery, przestępcy myśleli nad sposobami i możliwościami wdrożenia nowych technologii i wykorzystania ich do celów przestępczych. Nieustanny postęp technologiczny dostarczał cyberprzestępcom nowe narzędzia. Pojawiły się krypto waluty, które zrewolucjonizowały rynek wymiany pieniądza, oraz pozwalały na dokonywanie anonimowych płatności, co znalazło szczególne zainteresowanie w obszarze przestępczości.

Główną przyczyną rozwoju cyberprzestępczości są możliwości osiągnięcia bardzo wysokich zysków przy stosunkowo niskim ryzyku. Kradzieże w cyberprzestrzeni są najczęściej popełnianym cyberprzestępstwem na świecie. Zgodnie z raportem McAfee „The Economic Impact of Cybercrime" z 2018 roku globalne straty związane z cyberprzestępczością wynoszą ok. 600 miliardów dolarów, czyli ok. 0,8% globalnego PKB[2]. Zainteresowanych cyberprzestępczością jest dużo, niski próg wejścia w obszar technologiczny i dostęp do sztucznej inteligencji pozwala na wykorzystanie najnowszych technologii przy stosunkowo niskich kosztach. Z raportu wynika też, że są kraje, które sprzyjają rozwojowi cyberprzestępczości, do takich „oaz spokoju dla przestępczości" należą między innymi Rosja czy Korea Północna, gdzie trafia większość zysków z działalności cyberprzestępców.

Przestępcy szukają pieniędzy tam gdzie jest ich najwięcej, wobec tego cześć cyberprzestępczości skierowana jest w sektor bankowy. Kradzież pieniędzy z banku to marzenie wielu przestępców, w dzisiejszych czasach tradycyjne napady na bank z bronią w ręku należą już do rzadkości. Istnieje niezwykle duże ryzyko niepowodzenia oraz ujęcia sprawców takiego napadu. W przypadku ataków zdalnych sytuacja zmienia się diametralnie. Przestępca ma dużo większe szansę na powodzenie przy minimalistycznych szansach na ujęcie. Zakładając taki scenariusz, cyberprzestępcy stworzyli jedno z najskuteczniejszych narzędzi do okradania banków – Botenet o mitycznie brzmiącej nazwie ZEUS.

---

1 M. Siwicki, *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 7.

2 https://www.forbes.pl/gospodarka/globelne-koszty-cybeprzestepczosci-raport-mcafee-za-2017-rok/0k5qgr7, (dostęp 14.01.2020).

Charakterystyka sieci botnet

Botnetem nazywamy grupę zainfekowanych złośliwym oprogramowaniem komputerów np. robakiem lub trojanem pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach stworzonej sieci. Urządzenia wchodzące w skład botnetu nazywane są botami, aby botnet mógł istnieć, muszą go tworzyć, co najmniej dwa zainfekowane złośliwym oprogramowaniem urządzenia. Celem twórców każdego botnetu jest zainfekowanie jak największej ilości komputerów i urządzeń podłączonych do Internetu. Botnety mogą składać się nawet z kilkunastu milionów botów. Do znanych botnetów należą na przykład: Mirai, Conficker, Zeus, Waledac, Mariposa i Kelihos.

Historia botnetów rozpoczyna się na końcu XX wieku. Dokładnie 2 listopada 1988 r. został uruchomiony wirus typu „robak" o nazwie Morris Worm, który potrafił automatycznie infekować komputery podłączone do internetu. Wirus zainfekował ponad 6 tysięcy komputerów, co stanowiło wówczas około 10% globalnej sieci. Straty wywołane programem oszacowano na ok. 100 milionów dolarów, a programista został skazany na prace społeczne i grzywnę[3].

Inny przypadek, dotyczył USA i incydentu jaki miał miejsce w lutym 2000r. Młody piętnastoletni Kanadyjczyk Michael o pseudonimie „MafiaBoy" wykorzystał swój program do zaatakowania najczęściej odwiedzanych stron w USA. Ofiarą padły między innymi CNN[4], Yahoo oraz Amazon. Incydent odbił się szerokim echem w prasie i zaowocował pilnymi spotkaniami ekspertów od bezpieczeństwa w Białym Domu[5]. Incydent był klasycznym atakiem typu DDoS (Distributed Denial of Service)[6] z wykorzystaniem metody rozproszonej odmowy usługi. Już wtedy eksperci ds. bezpieczeństwa zdawali sobie sprawę, że ataki zespolonej sieci komputerów będą stanowić w przyszłości poważne zagrożenie – mieli racje. Kilka lat później ataki DDoS były tak popularne, że nastoletni hakerzy mogli swobodnie wyłączać z użycia serwery www wykorzystując architekturę pozyskanych botów.

Specyfika działania botnetów opiera się o wykorzystanie mocy obliczeniowej sprzężonych ze sobą komputerów. Botnety są tworzone przez wirusy i robaki komputerowe, czyli samoreplikujące się programy, które w odróżnienia od klasycznego wirusa nie potrzebują pliku wykonalnego do infekcji. Robak jest pod tym względem samodzielny i potrafi się rozprzestrzeniać w sieci poprzez wykorzystywanie luk w systemie operacyjnym lub naiwności użytkownika. Wirusy lub robaki rozprzestrzeniają się wykorzystując różne kanały komunikacji, najczęściej poprzez spam w poczcie email, ale także przez komunikatory internetowe oraz podszywają się pod oprogramowanie dostępne do pobrania w internecie.

Botnety obecnie stanowią duże zagrożenie, scalenie nawet kilkunastu komputerów podłączonych do internetu może być użytecznym narzędziem dla cyber-

[3] https://en.wikipedia.org/wiki/Morris_worm, (dostęp 14.01.2020).
[4] Cable News Network – amerykańska telewizja informacyjna.
[5] K. Poulsen, Haker. *Prawdziwa historia szefa cybermafi*, Wydawnictwo Znak, Kraków 2011, s. 43.
[6] Blokowanie dostępu do usług w sieci Internet poprzez generowanie sztucznego ruchu.

przestępców. Nie ma konkretnych danych, co do liczby botnetów na świecie. Botnety mogą być wykorzystane do różnego rodzaju ataków w tym DDoS, kradzieży danych, pieniędzy, sabotażu czy inwigilacji.

Botnety charakteryzują się wielozadaniowością, potrafią jednocześnie wykorzystywane do wielu czynności. Cyberprzestępcy najczęściej wykorzystują Botnety do:

- rozsyłania spamu, niechcianej korespondencji zawierającej linki lub załączniki ze złośliwym oprogramowaniem lub treści reklamowe. Szacuje się, że nawet 80% spamu w internecie rozsyłane jest przez komputery *zombie* będące częścią czyjegoś botnetu. Adresu wykorzystywane do rozsyłania spamu trafiają na „czarne listy" operatorów pocztowych przez co często trafiają do zakładki „spam" lub są całkowicie blokowane. Jednak cyberprzestępcy znaleźli już sposób na obejście blokad operatorów pocztowych. Komputer zarażony wirusem, należąc do danego botnetu może rozsyłać spam z wykorzystaniem dostępnych komunikatorów w tym poczty właściciela, czatów, itp. Dzięki temu spam jest o wiele bardziej skuteczny i niebezpieczny. Wysyłany z zaufanego adresu mail czy komunikatora jest odbierany jako „zaufane źródło" np. poprzez sieć znajomych na portalu Facebook.
- prowadzenia ataków typu DDoS. Atak tego typu jest bardzo prostym i niezawodnym atakiem. Polega na wyczerpaniu dostępnej pamięci serwera poprzez przepełnienie a w konsekwencji przeciążenie i zawieszenie działania danej usługi lub usług. Cyberprzestępcy wykorzystują połączone ze sobą Botnetem komputery zombie i dokonują masowego wejścia na dany serwer, w wyniku przeciążenia serwer zostaje zablokowany. Cyberprzestępcy często żądają okupu za ustąpienie ataku, a firmy często się na niego godzą, jest to szybsze niż działanie orangów ścigania. Hipotetycznie cyberprzestępca posiadający botnet liczący ok 100 tysięcy botów, jest w stanie zawiesić na pewien czas nawet duże serwisy stramingowe, których architektura utrudnia dokonanie skutecznego ataku DDoS[7].
- kradzież prywatnych i wartościowych danych. Komputer zarażony wirusem znajdujący się wewnątrz jakiegoś botnetu stanowi interesujące dla cyberprzestępców źródło pozyskania prywatnych danych. Cyberprzestępcy interesują się w szczególności numerami kart kredytowych, prywatnymi zdjęciami, korespondencją oraz loginami i hasłami do różnych serwisów i usług np. do banków. Zebrane dane są wykorzystywane w różny sposób; prywatne zdjęcia i korespondencja mogą służyć do szantażu, karty kredytowe do kradzieży a loginy, hasła i dane osobowe mogą stać się przedmiot sprzedaży.
- generowania fałszywych kliknięć na reklamy online. Niektóre agencje reklamowe płacą za wyświetlanie reklam, płatność odbywa się w systemie PPC (ang. Pay-Per-Click). Właściwe dużego botnetu przy pomocy komputerów *zombie* może wygenerować w ciągu jednego dnia kilka tysięcy unikatowych

[7] https://bitdefender.pl/masywny-13-dniowy-atak-ddos-botnetu-na-serwis-streamingowy/, (dostęp 14.01.2020).

kliknięć z kilu tysięcy różnych komputerów. Dzięki temu właściciel botnetu może osiągać wysokie zyski z reklam, w które klikają jego boty. Botnet działa jako pasożyt wykorzystując zdolności operacyjne zespolonych komputerów. Od czasu powstania Bitcoina i kryptowalut istnieją botnety „kopacze" które wykorzystują swoje możliwości do pozyskiwania wirtualnej waluty.

Klasyfikacja sieci botnet

Botnety najczęściej klasyfikuje się ze względu na ich architekturę oraz protokoły sieciowe wykorzystywane do komunikacji pomiędzy zainfekowanymi komputerami. Klasyfikując botnety ze względu na architekturę, wyróżnia się botnety scentralizowane oraz zdecentralizowane[8].

W modelu scentralizowanym zainfekowane komputery są podłączone do serwera zarządzającego zwanego C&C (Command and Control). Każdy zainfekowany komputer po nawiązaniu komunikacji z C&C rejestrowany jest w bazie danych, która przechowuje między innymi dane dotyczące adresów IP oraz lokalizacji komputerów stanowiących botnet. Właściciel botnetu sprawuje bezpośrednią kontrolę poprzez wydawanie komend w panelu sterowania. Botnety tego typu są proste w obsłudze, ale również stosunkowo łatwo je zneutralizować, bo są podpięte do konkretnego najczęściej jednego serwera C&C. Wystarczy przejąć lub unieszkodliwić serwer żeby usunąć całe zagrożenie.

W modelu zdecentralizowanym – P2P *(ang. Peer-to-peer)* sytuacja jest bardziej skomplikowany, gdyż botnet posiada strukturę rozproszoną. Oznacza to, że każdy z zarażonych wirusem komputer może pełnić rolę serwera zarządzającego. Architektura tego botnetu pozwala cyberprzestępcy na dostęp do sieci botnetu za pośrednictwem poszczególnych komputerów. Każdy pojedynczy bot posiada listę „sąsiednich" maszyn i za pomocą pojedynczego serwera administrator botnetu może wydawać polecenia dla całej sieci bez wyróżniania roli serwera C&C. W praktyce tworzenie zdecentralizowanych botnetów jest dość trudne. Każdemu nowo zainfekowanemu komputerowi należy dostarczyć listę botów – „sąsiadów", z którymi połączy się w sieć botnet. Zwalczanie zdecentralizowanych botnetów jest jednak znacznie trudniejsze niż zwalczanie scentralizowanych sieci[9]. Unieszkodliwienie pojedynczego komputera spowoduje jedynie odcięcie od sieci tylko części botów.

Czasami tworzone są sieci botnet o modelu mieszanym. Struktura taka, ułatwia cyberprzestępcy przekazywanie listy „sąsiadów" nowo zainfekowanym komputerom, które komunikują się z serwerem centralnym, od którego otrzymują listy botów a następnie przełączane są na komunikację typu P2P. Dzięki temu łatwiej jest zarządzać siecią przy zachowaniu maksymalnej ostrożności, co do wykrycia i zneutralizowania takiego botnetu.

[8] R. Kasprzyk, M. Paź, Z. Tarapata, *Modelowanie i symulacja cyberzagrożeń tupu botnet*, [w:] „Symulacja w Badaniach i Rozwoju" Vol. 6, No. 2/2015: 1-15, s.3

[9] Ibidem.

Botnet ZEUS

Zeus jest wirusem komputerowym modyfikującym wygląd stron internetowych w celu wyłudzenia pieniędzy. Program tworzy Botnet czyli sień zarażonych komputerów, którymi zarządzają zdalnie cyberprzestępcy. Zeus jest jednym z największych botnetów funkcjonujących obecnie w Internecie. Znany jest także pod nazwami: Zbot, PRG, Wsnpoem, Gorhax, Kneber[10]. Boty Zeusa są końmi trojańskimi, których głównymi zadaniami są: kradzież danych dotyczących kont bankowych z wykorzystaniem wbudowanych keyloggerów przechwytujących wciśnięte na klawiaturze przyciski. Zeus to multifunkcjonalne narzędzie do prowadzenia ataków wymierzonych w użytkowników sektora bankowego. Poza kradzieżą danych wirus umożliwia generowanie kampanii phishingowych i tworzenie fałszywych stron internetowych łudząco przypominających te oryginalne. Wielkość botnetu Zeus szacuje się na kilkanaście milionów zainfekowanych komputerów, z czego 3.6 milionów znajduje się w USA[11]. Ofiarą botnetu padły m. in. przedsiębiorstwa: Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon oraz BusinessWeek. Do 29 października 2009 roku botnet wysłał ponad 1.5 milionów wiadomości phishingowych do serwisu Facebook. W dniach 14-15 listopada 2009 botnet wysłał około 9 milionów sfałszowanych wiadomości podszywając się pod firmę Verizon Wireless[12].

Zeus jest programem atakującym wyłącznie komputery i urządzenia pracujące na systemie Windows. Zarażenie komputera wirusem ZEUS następuje najczęściej przez nieumyślne pobranie droppera, czyli programu zawierającego wstrzyknięty załącznik do pobrania złośliwego oprogramowania. Wykorzystywana jest do tego metoda drive-by-download. Metoda to polega na tym, że do kodu strony znajdującej się na serwerze wstrzykiwany jest złośliwy skrypt zawierający odnośnik do witryny serwującej szkodliwe oprogramowanie. Po wejściu na podobnie zmodyfikowaną stronę następuje niewidoczne dla użytkownika przekierowanie do szkodliwego adresu, uruchomienie exploita (programu wykorzystujący błędy w strukturze oprogramowania), a następnie pobranie i instalacja szkodliwego oprogramowania na komputerze ofiary[13].

Koń trojański po pobraniu jest uruchamiany na komputerze ofiary, wirus jest zaszyfrowany za pomocą algorytmów kryptograficznych i zdalnie aktualizowany, dlatego trudne jest jego wykrycie przez programy antywirusowe. Wszystko odbywa się poza wzrokiem użytkownika. Zeus wstrzykuje się w dwa najważniejsze procesy systemowe w zależności od wersji oprogramowania, wcześniej do procesu winlogin.exe odpowiadającym za funkcję logowania oraz do explorer.exe, który odpowiada za wyświetlanie interfejsu Windowsa. Oba procesy są niezbędne przy pracy na środowisku Windowsa. Wstrzyknięty w proces kod pobiera z ser-

[10] https://www.cert.pl/wp-content/uploads/2011/01/zeus_report.pdf, dostęp 14.01.2020).
[11] Ibidem.
[12] https://www.cert.pl/news/single/analiza-bota-zeus/, (dostęp 14.01.2020).
[13] https://mojafirma.infor.pl/e-firma/warsztat/269231,Czym-jest-driveby-download-poradnik.html, (dostęp 14.01.2020).

wera zewnętrznego plik konfiguracyjny zawierający listę atakowanych banków, stron, wykorzystywane wektory ataków, etc.. Po załadowaniu informacji z pliku konfiguracyjnego Zeus przechwytuje krytyczne dla bezpieczeństwa użytkowników informacje (głównie informacje logowania) i okresowo wysyła je do serwera zewnętrznego. Najwięcej ataków z wykorzystaniem botnetu Zeus odbywało się w latach 2009-2012, wtedy w Polsce Bankowość elektroniczna dopiero się rozwijała. Wirus podmieniał wygląd oryginalnej strony banku ofiary na spreparowaną i wymuszał logowanie do serwisu transakcyjnego. Wirus również wysyłał do ofiary fałszywą wiadomość sms służącą rzekomej autoryzacji płatności. W rzeczywistości była to próba włączenia przelewów bez autoryzacji z wykorzystaniem „zaufanego urządzenia". W Polsce ofiarami padli użytkownicy dwóch banków, ING Banku śląski oraz mBanku.

Wielkość botnetu Zeus według raportu Cert oszacowano na kilkanaście milionów zainfekowanych komputerów, z czego 3.6 milionów znajdowało się w USA. Ofiarą botnetu padły m. in. przedsiębiorstwa: Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon oraz BusinessWeek. Do 29. października 2009 roku botnet wysłał ponad 1.5 milionów wiadomości phishingowych do serwisu Facebook. W dniach 14-15 listopada 2009 botnet wysłał około 9 milionów sfałszowanych wiadomości podszywając się pod firmę Verizon Wireless. W dniu 14. czerwca 2010 roku firma Trustee udostępniła raport na temat skompromitowanych z pomocą Zuesa kart kredytowych piętnastu amerykańskich banków. W dniu 1. Października 2010 roku FBI[14] poinformowało o istnieniu międzynarodowej grupy cyberprzestępcy odpowiedzialnej za włamania do amerykańskich komputerów i kradzieży około 70 milionów dolarów. W USA aresztowano 90 osób, aresztowania nastąpiły także w Wielkiej Brytanii i na Ukrainie[15].

Botnet Zeus trafił także w Polskich użytkowników Internetu. Cert Polska[16] monitorował jego aktywność od stycznia 2009 roku. Najwięcej ataków w latach 2009-2010 było ukierunkowane na sektor bankowy i dwa polskie banki PKO BP oraz ING Bank Śląski. Oba te banki znalazły się w ponad dwustu plikach konfiguracyjnych wirusa[17]. Zespół Cert Polska, co roku rejestrował nowe przypadki użycia wirusa lub jego zmodyfikowanych wersji. Np. w 2012 r. zarejestrowano 246 564 unikalnych adresów IP, z których był generowany ruch przez boty Zeusa[18]. W 2013 po wielu publikacjach kodów Zeusa liczba generowanych przez wirusa polskich IP zmalała do 12193 sztuk[19]. Rok później ta tendencja została utrzymana na podobnym poziomie 12 513[20]. W 2015 r. można było zaobserwować dalsze spadki aktywności wirusa, wówczas aktywność botnetu stanowiła jedynie 3,60% aktywności

[14] Federal Bureau of Investigation – amerykańska agencja rządowa zajmująca się przestępstwami wykraczającymi poza granice danego stanu.
[15] https://www.cert.pl/wp-content/uploads/2011/01/zeus_report.pdf, (14.01.2020).
[16] CERT(Computer Emergency Response Team) Polska – zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet.
[17] https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2010.pdf, (14.01.2020).
[18] https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2012.pdf, (dostęp 14.01.2020).
[19] https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2013.pdf, (dostęp 14.01.2020).
[20] https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2014.pdf, (dostęp 14.01.2020).

wszystkich botnetów w polskim Internecie. Wielkość Zeusa w 2015 określono 5305 generowanych IP. Rok później aktywność trojan była znikoma, zaobserwowano jedynie 6 przypadków[21]. W kolejnych latach nie odnotowano już żadnej istotnej aktywności, wirus był już zbadany i znany na całym świecie, dlatego nie stanowił już zagrożenia.

Mimo, że ZEUS w cyberprzestępczości jest już starym wirusem, ciągle pojawiały się jego nowe, ulepszone wersje. W roku 2012 pojawiła się odmiana wirusa: Citadel oraz Zues-P2P, który dokonywał modyfikacji popularnych przeglądarek internetowych. Rok później, gdy technologia mobilna zaczęła być bardziej powszechna cyberprzestępcy stworzyli specjalną wersję wirusa atakującą systemy w smartfonach. Oprogramowanie działało w systemach opartych na Androidzie i zachęcało do aktualizacji swoich aplikacji bankowych. Pobranie aplikacji skonstruowanej przez cyberprzestępców pozwalało na dostęp do smartfonu, co w konsekwencji zazwyczaj kończyło się przejęciem haseł autoryzacyjnych sms i ostatecznie kradzieżą wszystkich dostępnych na koncie środków.

Kilka lat później w 2016 r. Związek Banków Polskich na swojej oficjalnej stronie dodał komunikat o pojawieniu się kolejnych zagrożeń wirusem bankowym. Banki ostrzegały przed nową wersją Zeusa o nazwie ZITMO, który nakłaniał użytkowników usług bankowości elektronicznej do instalacji złośliwego oprogramowania na komputerach, tabletach i smartfonach, szczególnie z systemem operacyjnym Android, wykorzystywanych w usługach bankowości elektronicznej[22]. Wirus tradycyjnie miał na celu kradzież haseł oraz smsów i sesji autoryzujących umożliwiających wykonanie operacji przelewów w serwisach bankowości elektronicznych i aplikacjach mobilnych.

Obecnie struktura wirusa Zeus jest bardzo dobrze znana, mimo tego nie brakuje nowych rozwiązań dotyczących ataków na użytkowników bankowości elektronicznej. Istnieje wiele programów stosujących mechanizmy Zeusa oraz socjotechnikę do wyłudzenia danych. Najnowsze rozwiązania mogą być nawet oparte o architekturę podstawy systemów, np. afera z Huawei w 2019 r. dotycząca rzekomego szpiegowania Amerykanów przez Chiny.

Rozwój technologii mobilnych wywołał zainteresowanie wśród inżynierów zajmujących się tworzeniem złośliwego oprogramowania, w 2015 r. miał miejsce atak wymierzony w rosyjskie urządzenia mobilne. Trojan AndroidZbot został stworzony do wykradania pieniędzy z kont bankowych i stanowił poważne zagrożenie dla użytkowników bardzo popularnego systemu Android. Wirus miał zdolność do wykradania loginów i haseł innych poufnych danych, poprzez wyświetlanie fałszywych formularzy autoryzacyjnych na ekranach roboczych różnych aplikacji. Pojawianie się tych formularzy było generowane przez cyberprzestępców. Wirus maskował się pod popularną aplikacją „sklepu google play" dlatego nie zwracał na siebie uwagi przeciętnych użytkowników. Kluczowym dla wirusa momentem była prośba o udzielenie uprawnień administratora. Udzielenie tych uprawnień

[21] https://www.cert.pl/PDF/Raport_CP_2016.pdf, (dostęp 14.01.2020).

[22] https://www.bnpparibas.pl/szkolenie/bezpieczenstwo-test/alerty-dotyczace-bezpieczenstwa/zlosliwe-oprogramowanie-zeus, dostęp 14.01.2020).

powodowało przejęcie całkowitej kontroli nad urządzeniem. W ten sposób cyberprzestępcy wykradali numery kart kredytowych razem z poufnymi kodami CVV[23] i udzielali autoryzacji na przelewy wychodzące z aplikacji bankowych ofiary.

Infekcja wirusem najczęściej następowała przez pobieranie niecertyfikowanych aplikacji z innych źródeł niż podaje Google, np. pirackich gier lub programów z pełną licencją na Androida. W momencie, gdy nowo zainfekowane urządzenie zostanie zarejestrowane na serwerze, trojan otrzymał polecenie sprawdzenia konta bankowego użytkownika. Jeśli wykryje dostępność środków, automatycznie przesyła określoną sumę pieniędzy na konta bankowe cyberprzestępców. Tym samym Android. Trojan Zbot[24] potrafił uzyskać dostęp do kont bankowych użytkowników urządzeń z Androidem i w ukryciu wykradać pieniądze, używając specjalnych komend sms wymaganych przez usługi bankowości online. Ponadto, ofiara nawet nie zdawała sobie sprawy z zaistniałej kradzieży, gdyż trojan przechwytywał wszystkie przychodzące wiadomości SMS pochodzące od banków i zawierające kody służące do weryfikacji transakcji[25]. Mimo, że wirus był typowym „bankowym botnetem" posiadał także unikatową funkcję wykradania różnych poufnych danych. Odbywało się to z użyciem fałszywych formularzy do wprowadzania informacji, generowanych na podstawie komend otrzymanych z serwera i zaprojektowanych w celu stworzenia iluzji, że przynależą one do niektórych programów. Mimo, że jest to klasyczny atak phishingowy, to sposób, w jaki, w tym konkretnym przypadku, został on przeprowadzony jest dość unikalny.

Urządzenia zainfekowane przez Android ZBota były podłączone do swoich zdalnych węzłów tworząc niezależne botnety. Każdy botnet składa się z dziesiątek, a nawet tysięcy zaatakowanych urządzeń. Oznacza, że ten trojan stał się produktem komercyjnym i jest dystrybuowany poprzez podziemne sklepy dla hakerów, w których może być kupowany przez pojedynczych cyberprzestępców lub przez zorganizowane grupy twórców wirusów.

Robak Conficker

Conficker to jeden z groźniejszych znanych samoreplikujących się programów komputerowych. Pojawił się w 2008 r. a rok później Microsoft wyznaczył nagrodę w postaci 250 tysięcy dolarów dla każdego, kto może udzielić skutecznych informacji na temat twórcy tego wirusa. Złośliwe oprogramowanie wykorzystało lukę w systemach Windows Server Service polegającą na zajęciu przez program większego obszaru pamięci niż zarezerwował na ten cel programista. Dzięki luce, program mógł wyłączyć usługi bezpieczeństwa, takie jak Windows defender oraz aktualizacje oprogramowania systemowego. Pracując na nieaktualnym systemie, wirus łączył się z serwerem i pobierał dodatkowe złośliwe oprogramowanie,

[23] Kod CVV (Card Security Code) jest specjalnym kodem umieszczonym na kartach płatniczych.

[24] Zbot jest bardzo szkodliwym trojanem, który jest używany do wykradania danych osobistych, takich jak hasła, loginy i inne prywatne informacje.

[25] https://news.drweb-av.pl/show/?i=9754&lng=pl, (dostęp 14.01.2020).

umożliwiające kolejne działania w tym gromadzenie danych z komputera, samo replikację przez USB[26] i komunikatory a także całkowite przejęcie komputera ofiary i poddanie go pod kontrolę cyberprzestępcy.

Conficker zdołał zainfekować ponad 7 milionów komputerów na całym świecie[27]. Conficker infekował nawet systemy militarne i większość komputerów osobistych na zachodzie Europy. Został uznany przez Common Vulnerabilities and Exposures (Program Departamentu Bezpieczeństwa USA) za jeden z dziesięciu największych zagrożeń komputerowych dla obu ameryk. Conficker był tak tak bardzo „udanym" malware, ponieważ jego wektorami ataku były słabości systemu Windows XP[28], który był w owych latach najbardziej popularnym systemem na świecie. Do dziś wiele urządzeń wciąż pracuje na systemie Windows XP, pomimo tego, że system ten od dawna nie jest wspierany przez Microsoft. Mimo upływu lat, wciąż wirus pozostaje aktywny na wielu urządzeniach. Specjaliści z CERT Orange nazywają go „żywym archaicznym wykopaliskiem" twierdzą, że podczas skanowania ruchu sieciowego wciąż natrafiają na incydenty związane z aktywnością tego wirusa[29].

Conficker uderzył także w polską cyberprzestrzeń. Najbardziej aktywny był w 2015 r. Wówczas liczba unikalnych adresów IP, z których był generowany ruch botnetu wynosiła 22 899[30]. Dzięki działaniu Orange Polska, aktywność wirusa została ograniczona i rok później 9 410 adresów IP. W 2017 r. – 3759, zaś rok później zaobserwowano nieznaczny wzrost aktywności – 4 529 adresów IP.

Podsumowanie

Botnety są powszechnym zjawiskiem w Internecie. Każde urządzenie podłączone do Internetu może zostać zainfekowane przez wirusa tworzącego botnet. Nie istnieje uniwersalne narzędzie, które w sposób skuteczny i kompleksowy będzie w stanie obronić urządzenia przed infekcją ze strony wirusów. Podobnie jest w biologicznym życiu, nie ma szczepionek na wszystkie wirusy na świecie, tak samo nie ma też programu, który będzie w stanie zatrzymać wszystkie zagrożenia.

Obronę przed zagrożeniami typu botnet podzieliłem na dwie kategorie. Pierwszą z nich jest Wsparcie z, zewnątrz, czyli wszelkiego rodzaju programy antywirusowe i mechanizmy automatycznego reagowania na zagrożenia w cyberprzestrzeni, a także systemy wspomagające te procesy np. wbudowany w Windows program Windows Defender. Druga kategoria dotyczy wiedzy posiadanej przez

[26] USB (od ang. Universal Serial Bus), uniwersalna magistrala szeregowa – komputerowe złącze komunikacyjne.

[27] https://avlab.pl/conficker-czyli-najbardziej-niebezpieczny-malware-w-historii (dostęp 14.01.2020).

[28] Windows XP, wersja systemu operacyjne firmy Microsoft .

[29] https://www.cert.orange.pl/aktualnosci/archaiczny-malware-nieprzerwanie-zywy, (dostęp 14.01.2020).

[30] https://www.cert.pl/PDF/Raport_CP_2015.pdf, (dostęp 14.01.2020).

użytkownika i umiejętności poruszania się w cyberprzestrzeni w tym znajomość podstawowych mechanizmów działania cyberprzestępców oraz ograniczone zaufanie w Internecie. Użytkownik świadomy zagrożeń, ostrożny i zapobiegliwy ma niską szansę, że jego urządzenie stanie się częścią botnetu. Dlatego istotną kwestią jest edukacja cyberbezpieczeństwa w szkołach już od najmłodszych lat. Wykształcone społeczeństwo jest w stanie lepiej unikać ataków ze strony cyberprzestępców, niż takie, które reaguje impulsywnie i bezkrytycznie podejmuje swoje decyzję w cyberprzestrzeni nie zdając sobie sprawy z wielu cyberzagrożeń.

Zagrożenia wynikające z działań cyberprzestępców korzystających z sieci botnet są niezwykle istotne w kontekście utrzymania bezpieczeństwa w cyberprzestrzeni. Wysoka dynamika zmian w cyberprzestrzeni zwiększa potrzebę zwrócenia uwagi na problem botnetów. Nie wystarczy jedynie obserwacja i analiza ruchu sieciowego oraz reakcje na występujące incydenty. Rośnie potrzeba posiadania umiejętności wczesnego wykrywania i unieszkodliwiania botnetów we wczesnym stadium ich rozwoju. Istotną kwestią jest też uruchamianie odpowiednich metod ochrony w przypadku już wykrytych incydentów i dostosowania się do dużej dynamiki zmian w formach ataków.

Internet będący fundamentem cyberprzestrzeni posiada bardzo podatną na ataki infrastrukturę. Od jego bezpieczeństwa zależy prawidłowe funkcjonowanie państwa, organizacji i społeczeństwa. Botnety stanowią duże zagrożenie zarówno dla osób prywatnych jak i dużych firm i korporacji. W niektórych przypadkach wyznaczone były wysokie nagrody za ujawnienie twórców najbardziej znanych botnetów na świecie.

Analizowane w artykule przypadki znanych botnetów tj. Zeus, AndroidBot i Conficker wskazują na rosnący trąd w cyberprzestępczości. Cechą wspólną omawianych botnetów jest ich cel, który łączy ze sobą funkcję kradzieży pieniędzy z kont bankowych użytkowników oraz pozyskiwanie wrażliwych informacji, haseł i loginów. W sieci wciąż działa wiele niezidentyfikowanych botnetów. Te, które zostały zdiagnozowane i w części stanowią bardziej obiekt historyczny niż realne zagrożenie pokazują kierunek rozwoju cyberprzestępczości, a tym kierunkiem są właśnie nowe duże botnety pracujące w strukturze rozproszonej, trudne do zidentyfikowania, dobrze zaszyfrowane działające w ukryciu przed użytkownikiem. Każdy z nas może być częścią jakiegoś botnetu, nawet przez długie lata. Najskuteczniejszą obroną przed botnetami jest aktualizacja swojej wiedzy, uważne czytanie i zwracanie uwagi na szczegóły, gdyż w większości przypadków do zainfekowania dochodzi właśnie z winy użytkownika.

Bibliografia

1. https://avlab.pl/conficker-czyli-najbardziej-niebezpieczny-malware-w-historii.
2. https://bitdefender.pl/masywny-13-dniowy-atak-ddos-botnetu-na-serwis-streamingowy/.
3. https://en.wikipedia.org/wiki/Morris_worm.

4. https://mojafirma.infor.pl/e-firma/warsztat/269231,Czym-jest-driveby-download-poradnik.html.
5. https://news.drweb-av.pl/show/?i=9754&lng=pl.
6. https://www.bnpparibas.pl/szkolenie/bezpieczenstwo-test/alerty-dotyczace-bezpieczenstwa/zlosliwe-oprogramowanie-zeus.
7. https://www.cert.orange.pl/aktualnosci/archaiczny-malware-nieprzerwanie-zywy.
8. https://www.cert.pl/news/single/analiza-bota-zeus/.
9. https://www.cert.pl/PDF/Raport_CP_2015.pdf.
10. https://www.cert.pl/PDF/Raport_CP_2016.pdf.
11. https://www.cert.pl/PDF/Raport_CP_2017.pdf.
12. https://www.cert.pl/wp-content/uploads/2011/01/zeus_report.pdf.
13. https://www.cert.pl/wp-content/uploads/2015/11/Raport_CERT_Polska_2011.pdf.
14. https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2010.pdf.
15. https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2012.pdf.
16. https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2013.pdf.
17. https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2014.pdf.
18. https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf.
19. https://www.forbes.pl/gospodarka/globelne-koszty-cybeprzestepczosci-raport-mcafee-za-2017-rok/0k5qgr7.
20. K. Poulsen, *Haker – prawdziwa historia szefa cybermafii*, Wydawnictwo Znak Literanova, Kraków 2011.
21. M. Siwicki. 2013. *Cyberprzestępczość*. Wydawnictwo C.H. Beck, Warszawa 2013.
22. R. Kasprzak, M. Paź, Z. Tarapata. *Modelowanie i symulacje cyberzagrożeń typu botnet*, [w:] „Symulacja w Badaniach i Rozwoju" Vol. 6, No. 2/2015: 1-15.