**Andrzej Adamski**

# Botnety jako zagadnienie prawno-kryminologiczne na tle doświadczeń amerykańskich


## Streszczenie

*Autor definiuje botnet jako grupę zainfekowanych złośliwym oprogramowaniem komputerów, które są zdalnie kontrolowane przez cyberprzestępców i wykorzystywane przez nich do działań przestępczych na skalę masową. Równocześnie podaje przykłady walki z botnetami w USA, wyrażając pogląd, że amerykański styl tej walki charakteryzuje się silnym przywiązaniem do zasady legalizmu z pragmatycznym podejściem do osiągania zakładanych celów przy użyciu środków prawnych.*


## I. Wprowadzenie

Impulsem do przygotowania artykułu na powyższy temat były dwa wydarzenia z początku tego roku: telefoniczna prośba funkcjonariusza policji o wskazanie adekwatnej podstawy prawnej w kodeksie karnym do postawienia zarzutów zatrzymanemu w Polsce administratorowi botnetu oraz doniesienia prasowe o przejęciu kontroli przez CERT – Polska nad Virutem – „jednym z największych botnetów na świecie, służącym do kradzieży haseł i danych, rozsyłania spamu oraz ataków na sieci firm”[1]. Chociaż oba te wydarzenia nie mają ze sobą bezpośredniego związku, ich koincydencja czasowa stanowi wystarczający powód do zajęcia się tematem i podjęcia próby spojrzenia na fenomen botnetów z perspektywy prawa karnego i kryminologii. Poniższy tekst nie wyczerpuje tego zagadnienia, jest raczej wprowadzeniem do tematu określanego w literaturze przedmiotu mianem „cyberprzestępczości trzeciej generacji”.

Według zgodnej opinii ekspertów głównym źródłem zagrożenia bezpieczeństwa użytkowników Internetu jest obecnie złośliwe oprogramowanie (ang. *malware*). Za najgroźniejszą z jego odmian uważa się *malware* dyna-

[1] T. Grynkiewicz, Cios w Viruta. NASK odcina od sieci groźną sieć cyberprzestępców, „Gazeta Wyborcza” z dnia 18 stycznia 2013 r., http://wyborcza.biz/biznes/1,101562,13259489,Cios_w_Viruta_NASK_odcina_od_sieci_grozna_siec_cyberprzestepcow.html#ixzz2ISda QJbC.

miczny (*dynamic malware*)[2], który umożliwia zdalną kontrolę nad zainfekowanymi komputerami, łączenie komputerów w sieci i wykorzystywanie ich mocy obliczeniowej do skoordynowanych działań przestępczych na skalę masową. Sieci te, zwane botnetami, składają się zazwyczaj z setek tysięcy komputerów rozproszonych po świecie i stanowią kluczowy element infrastruktury informatycznej Internetu służący do popełniania cyberprzestępstw[3]. Na polecenie tzw. botmasterów, czyli osób zarządzających botnetami, zainfekowane komputery „zombi" wykonują – bez wiedzy swoich prawowitych użytkowników – najrozmaitsze, w pełni zautomatyzowane operacje, których finalnym celem jest z reguły przysporzenie korzyści majątkowych cyberprzestępcom.

Oprócz rozsyłania spamu, wymuszania haraczu pod groźbą przeprowadzenie ataku DDoS i okradania posiadaczy rachunków bankowych do pospolitych form zarabiania pieniędzy przy użyciu botnetów zalicza się również handel „kradzioną" informacją. Pochodzi ona najczęściej z zainfekowanych przez *malware* komputerów zombi i jest przedmiotem transakcji kupna–sprzedaży na internetowym czarnym rynku. Jak pokazują badania, w ciągu 10 dni botnet składający się ze 183 tys. komputerów jest w stanie zgromadzić 310000 rekordów danych stanowiących numery rachunków bankowych, kart płatniczych oraz loginów i haseł dostępu do stron internetowych i serwisów społecznościowych. Czarnorynkowa wartość tych informacji jest trudna do oszacowania. Najprostsze wyliczenie, ograniczające się tylko do numerów rachunków bankowych i kar płatniczych, pozwoliło ocenić ich wartość – na podstawie szybko zmieniających się cen czarnorynkowych – w granicach od 83 tys. do 8,3 mln USD[4].

Botnety są coraz częściej wykorzystywane do popełniania cyberprzestępstw. Przesądza o tym nie tylko efektywność tego narzędzia używanego głównie „do zarabiania dużych pieniędzy w krótkim czasie przy niewielkim ryzyku odpowiedzialności karnej", lecz także szereg innych okoliczności. Zalicza się do nich w szczególności rosnącą dostępność botnetów i łatwość ich obsługi, która wbrew pozorom nie wymaga specjalnej wiedzy i umiejętności. Wszystko to sprzyja rozwojowi „internetowego podziemia gospodarczego" i świadczonych tam usług typu *crimeware-as-a-service* (CaaS), dzięki którym można kupić lub wynająć botnet o odpowiedniej konfiguracji, np. do dokonania ataku DDoS, albo zlecić przeprowadzenie takiego ataku na witrynę kon-

[2] Trends for 2011: Botnets and Dynamic Malware, ESET Latin Americ's Lab, November 22nd, 2010, http://www.eset.com/us/resources/white-papers/Trends-for-2011.pdf.

[3] Botnets: Detection, Measurement, Disinfection & Defence, The European Network and Information Security Agency (ENISA), 2011, s. 10.

[4] B. Stone-Gross, et al. 2009. Your Botnet is My Botnet: Analysis of a Botnet Takeover, (w:) 16th Annual ACM Conference on Computer and Communications Security (CCS), 9–13 November 2009, s. 10.

kurencyjnego przedsiębiorstwa za stosowną opłatą. Oferowanie tego rodzaju usług wyszło już „z podziemia", a miejscem ich akwizycji stał się YouTube[5].

„Kamieniem milowym" w historii naturalnej omawianego *instrumentum sceleris* są możliwości budowania własnych botnetów. Jest to idea popularyzowana od kilku lat pod hasłem „zrób to sam" (DIY[6]) w odniesieniu do dostępnego w sieci kodu źródłowego złośliwego oprogramowania i innych komponentów potrzebnych do skompilowania botnetu[7]. Aktualną nowością na czarnym rynku gotowych i w pełni zautomatyzowanych zestawów narzędzi (*toolkits*) do tworzenia botnetów o ewidentnie przestępczym zastosowaniu jest program o nazwie *Citadel Builder*[8]. Chodzi o udoskonaloną wersją bota *Zeus*, opartą na jego kodzie źródłowym, który w 2011 r. wyciekł do Internetu, dając początek licznym odmianom *Zeusa*, do których należy *Citadel*. Główną funkcją *malware'u* z rodziny *Zeusa* jest bezprawne przechwytywanie danych umożliwiających uszczuplenie środków pieniężnych zgromadzonych na rachunkach bankowych dostępnych *on-line*, których posiadaczami są użytkownicy zainfekowanych komputerów. Programy te modyfikują funkcjonowanie przeglądarki internetowej komputera ofiary w taki sposób, aby po zalogowaniu się posiadacza rachunku na stronę banku można było dokonać w jego imieniu transferu środków pieniężnych na konto „pośrednika" współdziałającego z grupą przestępczą i ukryć tę transakcję przed posiadaczem rachunku w trakcie jej realizacji[9].

Szczegółowy opis działania programu *Citadel* zawiera raport zespołu CERT – Polska, który jako jeden pierwszych na świecie zespołów szybkiego reagowania na incydenty naruszające bezpieczeństwo w sieci podjął działania przeciwko wykorzystywaniu domen internetowych do zarządzania botnetami *Citadel*. Według autorów raportu schemat ataku bota jest następujący: „Po zainfekowaniu maszyny, *malware* wstrzykuje się do jednego z procesów działających w systemie operacyjnym użytkownika, co pozwala mu na uniknięcie szybkiego wykrycia. Następnie wstrzykuje się we wszystkie procesy, włączając w to proces przeglądarki internetowej (tzw. atak *man in the brow-*

[5] Jedną z kilkunastu firm, które otwarcie reklamują swoje usługi DDoS na YouTube, jest *Gwapo*. Cena usługi waha się od 5 do 100 USD za godzinę „wyłączenia" z Internetu obiektu ataku, w zależności od jego rozmiarów. Należność inkasowana jest Bitcoinach lub innej „anonimowej" walucie; zob. http://www.youtube.com/watch?v=c9MuuW0HfSA.

[6] Zob. np. DIY Twitter-Controlled Botnet Kit Spotted in the Wild; http://news.softpedia.com/news/DIY-Twitter-Controlled-Botnet-Kit-Spotted-in-the-Wild-142138.shtml.

[7] Por. McAfee Inc. (2006), Virtual Criminology Report 2007 Organized Crime and the Internet: "Creating one's own bot and setting up a botnet is now relatively easy. You don't need specialist knowledge, but can simply download the available tools or even source code".

[8] Zob. na ten temat https://www.botnets.fr/index.php/Citadel_ZeuS_bot.

[9] M. Lee, Four Ways Cybercriminals Profit from Botnets; http://www.symantec.com/connect/blogs/four-ways-cybercriminals-profit-botnets.

*ser*), aby kontrolować informacje, jakie docierają do użytkownika i móc je przechwycić.

Na początku, użytkownik wprowadza swój login oraz hasło do jednej z interesujących atakującego stron. Dane te są wysyłane do serwera, tak jak to się dzieje w przypadku normalnego używania stron internetowych. Złośliwe oprogramowanie jednak kopiuje zadanie HTTP i wysyła je do serwera kontrolującego komputery botnetu (*Command and Control*, w skrócie C&C). Dzięki temu atakujący uzyskuje dostęp do danych logowania ofiary. Zauważmy, że nie ma znaczenia, czy połączenie między komputerem ofiary a serwerem jest szyfrowane, czy też nie – złośliwe oprogramowanie ma dostęp do treści komunikacji przed jego zaszyfrowaniem.

Jednak przechwycenie hasła nie zawsze jest jedynym celem realizowanym poprzez atak tego typu. Przestępca, ponieważ „znajduje sie" w przeglądarce ofiary, jest w stanie również kontrolować zawartość strony prezentowaną użytkownikowi. Umożliwia to wyświetlenie treści niepochodzących z serwera, z którym ofiara sie kontaktuje. Może to służyć np. nakłonieniu użytkownika do przekazania hasła jednorazowego lub podmianie reklam serwowanych na danej stronie na takie, na których zarabia przestępca"[10].

Ten najbardziej chyba technologicznie zaawansowany komercyjny pakiet DIY do zakładania botnetów zyskał ostatnio światowy rozgłos za sprawą komunikatu ogłoszonego w dniu 5 czerwca 2013 r. przez Microsoft[11] i doniesień agencji prasowych[12]. Dowiadujemy się z nich, że w wyniku międzynarodowej operacji, w której oprócz Microsoft Corp. i FBI wzięło udział przeszło 80 podmiotów zagranicznych, zdołano zablokować funkcjonowanie 1492 botnetów *Citadel* rozrzuconych po całym świecie. Hosty 455 z nich znajdowały się w 40 centrach przetwarzania danych w USA. Ośrodki dowodzenia pozostałymi botnetami były zlokalizowane poza Stanami Zjednoczonymi i miały swoje domeny w kilkudziesięciu krajach, głównie europejskich, w tym w Polsce. W ciągu 18 miesięcy bot *Citadel* zainfekował pięć milionów komputerów na świecie, co pozwoliło cyberprzestępcom ukraść ponad 500 milionów USD z rachunków bankowych osób prywatnych lub klientów biznesowych takich instytucji finansowych, jak m.in.: American Express, Bank of America, Citigroup, Credit Suisse, eBay's, PayPal, HSBC, JPMorgan Chase, Royal Bank of Canada i Wells Fargo.

Najbardziej intrygująca część komunikatu Microsoft Corp. stwierdza, że cyberprzestępcy nie zostali zidentyfikowani i pozostają na wolności, jednak

[10] NASK Polska, Raport z dnia 15 kwietnia 2013 r., pt. „Przejęcie domen instancji plitfi botnetu *Citadel*"; http://www.cert.pl/PDF/Raport_Citadel_plitfi_PL.pdf.

[11] Microsoft, financial services and others join forces to combat massive cybercrime ring; http://www.microsoft.com/en-us/news/Press/2013/Jun13/06-05DCUPR.aspx.

[12] Reuters, Exclusive: Microsoft, FBI take aim at global cyber crime ring; http://www.reuters.com/article/2013/06/05/net-us-citadel-botnet-idUSBRE9541KO20130605.

na skutek sprawnie przeprowadzonej akcji międzynarodowej ich potencjał został poważnie osłabiony, co należy uznać za sukces.

Dalecy od akceptacji tej oceny są eksperci z firmy *Sophos*, którzy również monitorowali ekspansję *Citadel* w Internecie i ponad połowy zidentyfikowanych przez siebie domen internetowych związanych z tą sprawą nie znaleźli w wykazie Microsoftu[13]. Mówienie o sukcesie w sytuacji, w której nie zdołano ustalić, kim są sprawcy kradzieży pół miliarda dolarów, budzić może poważne zastrzeżenia także z kryminologicznego punktu widzenia. Wystarczy jednak wziąć pod uwagę całokształt okoliczności towarzyszących decyzji o podjęciu „Operacji b54" oraz jej prewencyjny cel, zorientowany na ochronę przed witymizacją przestępczą wielu użytkowników Internetu, aby zmienić zdanie i uznać, że mamy do czynienia co najmniej z sukcesem połowicznym, odnoszącym się do niektórych aspektów problemu, jakim jest walka z „cyberprzestępczością nowej generacji".

## II. Aspekty kryminologiczne walki z botnetami

Na pierwszy rzut oka *malware* i botnety mogą być postrzegane jako „koło zamachowe" cyberprzestępczości. Bardziej trafna wydaje się jednak opinia, że są one elementami procesu transformacji przestępczości ery społeczeństwa informacyjnego. Kryminolog brytyjski David Wall mówi w tym kontekście o cyberprzestępczości „trzeciej generacji" albo „prawdziwej" cyberprzestępczości, podkreślając tym samym nierozerwalny związek pewnych rodzajów zachowań przestępczych z Internetem, bez którego zachowania te nie byłyby możliwe[14]. Przykładem tego rodzaju zależności jest swoista symbioza spamu z *malware* i botnetami: spam jest często nośnikiem *malware'u*, natomiast botnety są wykorzystywane do rozsyłania spamu. Korelacja ta jest przesłanką interesujących hipotez. Niektórzy autorzy w sprzężeniu zwrotnym spam – botnety upatrują czynnik wzrostu zagrożenia cyberprzestępczością o cechach „samonapędzającego się mechanizmu"[15]. Perspektywicznie mechanizm ten mógłby okazać się bardzo destrukcyjny. Został on jednak w porę dostrzeżony, co pozwoliło na podjęcie środków zaradczych, których efekty dają powody do umiarkowanego optymizmu. Ogólnie mówiąc, zastosowane remedia opierają się na stosunkowo prostym rozumowaniu, które wynika z realistycznej oceny sytuacji. Uznano, że problemu botnetów nie da się rozwiązać ani w istotnym stopniu ograniczyć bez sięgnięcia po niekonwen-

[13] J. Wyke, Was Microsoft's takedown of Citadel effective? Nakedsecurity, Sophos, June 12, 2013; http://nakedsecurity.sophos.com/2013/06/12/microsoft-citadel-takedown/.
[14] D. Wall, Cybercime: The Transformation of Crime in the Information Age, Polity 2007, s. 154.
[15] *Ibidem*, s. 150–153.

cjonalne metody działania, które umożliwią uzyskanie przewagi nad „przeciwnikiem". Ponieważ trudno go zidentyfikować i zlokalizować, a tym samym oskarżyć i osądzić, wybrano inną strategię postępowania. Postanowiono pozbawić cyberprzestępców dostępu do używanych przez nich narzędzi, czyli przejąć kontrolę nad botnetami i sparaliżować, choćby na pewien czas, ich funkcjonowanie. Tego rodzaju działania są podejmowane od 2010 r. z inicjatywy Microsoft Corp. w ramach projektu MARS (*The Microsoft Active Response for Security*), którego celem jest eliminowanie botnetów i związanych z nimi struktur przestępczych oraz pomoc posiadaczom zainfekowanych komputerów w odzyskaniu nad nimi pełnej kontroli[16]. Dwuletnie doświadczenia związane z realizacją tego projektu uzasadniają opinię, że osiągnięcie wspomnianych celów nie jest zadaniem łatwym nawet dla MS.

## 1. Spam, *malware* i botnety

Dostępne dane za lata 2008–2012 wskazują na rosnący udział *malware'u* w globalnym wolumenie „niechcianych wiadomości"[17]. Towarzyszą temu okresowe wahaniach ogólnej liczby tych wiadomości w sieci, będące prawdopodobnie odbiciem „sukcesów" i „porażek" w walce ze spambotnetami. W roku 2008 sześć z nich (Mega–D, Srizbi, Storm, Rustock, Pushdo i Cutwail) generowało 85% spamu w Internecie[18]. W późniejszym okresie proporcja ta utrzymywała się na zbliżonym poziomie, mimo podjętej przez Amerykanów kontrofensywy przeciwko botnetom rozsyłającym spam. Wspomniana inicjatywa, w której oprócz agencji rządowych (FBI) i Microsoft Corp. uczestniczy wiele firm IT i producentów programów antywirusowych, a także indywidualni badacze, polega na przejmowaniu kontroli nad botnetami metodą tzw. *sinkholingu*[19]. Mimo że stosowanie tej metody daje zróżnicowane, często krótkotrwałe rezultaty, stanowi ona obecnie podstawowy oręż w walce z botmasterami.

Początkowo kilka udanych prób przejęcia kontroli na serwerami C&C najbardziej wydajnych spambotnetów przyczyniło się do ograniczenia rozmia-

[16] Zob. http://www.microsoft.com/government/ww/safety-defense/initiatives/Pages/dcu-economic-crime.aspx.

[17] Dane Kasperski Lab wskazują na 13-krotny wzrost liczby załączników do e-maili zawierających *malware* w latach 2009–2012 (odpowiednio: 0,3% i 3,9%). Według Microsoft Corp. (Microsoft Security Intelligence Report, vol. 14, July through December 2012, s. 61) w latach 2008–2012 nastąpił prawie czterokrotny wzrost rozmiarów tego zjawiska (z 1,8% do 6,8%).

[18] A. Al-Bataineh, G. White, Detection and Prevention Methods of Botnet-generated Spam, MIT Spam Conference, MIT, Cambridge, Massachusetts, March 2009, s. 3.

[19] *Sinkholing* polega na przekierowaniu niepożądanego ruchu sieciowego na konkretne adresy IP, gdzie zawartość tego ruchu jest przechwytywana i analizowana. Przekierowanie może być także zrealizowane na nieistniejące adresy IP czy też adresy komputerów, z których ruch jest wysyłany. Wymaga to ścisłej współpracy laboratoriów bezpieczeństwa z dostawcami Internetu, domen oraz usług DNS; cyt. za http://pl.wikipedia.org/wiki/Sinkhole.

rów zjawiska spammingu w Internecie. Bezpośrednio po „wyłączeniu" botnetów Cutwail (sierpień 2010 r.) i Rustock (maj 2011 r.) liczba wiadomości zatrzymywanych przez filtry antyspamowe MS zmniejszyła się z 89.2 mld (lipiec 2010 r.) do 21,9 mld (maj 2011)[20]. Raport firmy *Symantec* wskazuje na kilkunastoprocentowy w skali globalnej spadek liczby e-maili rozpoznanych jako spam w 2011 r. (75,1%) w stosunku do roku 2010 (88,5%). Obniżenie tego wskaźnika autorzy raportu kojarzą głównie z działaniami amerykańskich organów ścigania i wymiaru sprawiedliwości, które unieruchomiły Rustock, powodując z chwilą zajęcia i wyłączenia „wielu jego serwerów C&C znajdujących się na terytorium USA" gwałtowny spadek ilości spamu w sieci: z 51 mld „niechcianych wiadomości" dziennie w tygodniu poprzedzającym operację FBI do 31,7 mld dziennie w tydzień po jej zakończeniu[21]. Statystyka Kasperski Lab również potwierdza spadek udziału spamu w ogólnej liczbie wiadomości przesyłanych pocztą elektroniczną w latach 2010–2012 (84,4% w 2. kwartale roku 2010 w stosunku do 71,5% w 3. kwartale roku 2012). Obserwowaną tendencję tłumaczy się jednak nie tyle zamykaniem spambotnetów, lecz zmianą preferencji reklamodawców internetowych, którzy zamiast poczty elektronicznej wolą korzystać z innych mediów (banery, sieci społecznościowe, reklama kontekstowa i usługi kuponowe) do prowadzenia kampanii reklamowych[22].

## 2. „Walka z wiatrakami"?

Dotychczasowe doświadczenia wskazują, że wygaszenie aktywności botnetu przez zmianę domen internetowych, w których zarejestrowane są oryginalne serwery C&C i przekierowanie ruchu między botami a centrum zarządzania botnetem do serwerów znajdujących się pod kontrolą policji ma ograniczoną skuteczność i na ogół nie oznacza definitywnej likwidacji problemu. Przejęte metodą *sinkholingu* botnety po krótszym lub dużym okresie nieobecności w Internecie najczęściej do niego wracają; z reguły w nowej i ulepszonej wersji, oczywiście po to, by zarządzający nimi ludzie mogli kontynuować lub rozpocząć działalność przestępczą. Sytuacji takich jest wiele i dotyczą one głównie botnetów o dłuższym (6–7-letnim) okresie funkcjonowania. Na przykład wspomniany wyżej Cutwail, który od 2008 r. był czterokrotnie „zdejmowany" z Internetu, by za każdym razem do niego powrócić, w lipcu 2013 r. pracował na pełnych obrotach, generując ok. 25% spamu w sieci[23]. Równie wydajnym źródłem spamu okazał się zapomniany do nie-

[20] Microsoft Security Intelligence…, *op. cit.*, s. 60.
[21] Internet Security Thread Report. 2011 Trends, vol. 17, Published April 2012, s. 31.
[22] Spam in Q3 2012, http://www.securelist.com/en/analysis/204792251/Spam_in_Q3_2012#15.
[23] Trustwave, Spam statistics, https://www.trustwave.com/support/labs/spam_statistics.asp.

dawna Lethic, który przypomniał o swoim istnieniu w 2012 r., trafiając od razu na drugie miejsce listy dziesięciu najgroźniejszych botnetów[24].

Nie brakuje też przykładów świeższej daty, w tym dotyczących botnetów usuniętych z sieci w ramach programu MARS. Trzy z nich – Waledac[25], Kelihos[26] i Rustock[27] nie ustaleni sprawcy próbowali ostatnio uruchomić, i chociaż motywy, jakimi się kierowali, pozostają nieznane, to nie trudno je odgadnąć[28]. Reaktywacja botnetu jest dla doświadczonego bot mastera czynnością stosunkowo nieskomplikowaną, pod warunkiem, że użytkownicy komputerów „zombi" nie zostali poinformowani przez policję o tym, że padli ofiarą przestępstwa i nie usunęli z twardych dysków złośliwego oprogramowania. Komputery takie nadal reagują na sygnały wysyłane przez serwery nowego centrum zarządzania i są gotowe do wykonywania poleceń wydawanych przez bot mastera. W takich okolicznościach „wskrzeszenie" botnetu, który został zamknięty, trwa około miesiąca[29]. Z tego też powodu Departament Sprawiedliwości USA w każdym komunikacie prasowym informującym o przejęciu przez organy ścigania kontroli nad kolejnym botnetem apeluje do opinii publicznej o to, aby chronić własne komputery i dbać o ich bezpieczeństwo przez regularną aktualizację oprogramowania i skanowanie systemu w poszukiwaniu wirusów[30]. W sprawach, które dotyczą blokowania botnetów zainfekowanych szczególnie groźnym malwarem, np. przechwytującym hasła dostępu i inne dane umożliwiające dokonywanie nielegalnych transakcji bankowych, podejmowane są nadzwyczajne środki bezpieczeństwa. W takich przypadkach sądy federalne nakazują policji neutralizację malwaru w komputerach „zombi" oraz informowanie ich użytkowników o możliwości skorzystania w tym celu z dostępnych na rynku programów antywirusowych albo pomocy

[24] Baddest Botnets of 2012, http://www.networkworld.com/slideshow/70773/baddest-botnets-of-2012.html#slide3.

[25] Waledac is Back, Brings New Tools to the Fight, http://www.allspammedup.com/2012/02/waledac-is-back-brings-new-tools-to-the-fight/; Symantec, Return from the Dead: Waledac/Storm Botnet Back on the Rise, http://www.symantec.com/connect/blogs/return-dead-waledacstorm-botnet-back-rise.

[26] The Kelihos botnet, http://en.wikipedia.org/wiki/Kelihos_botnet.

[27] Rustock hiatus ends with huge surge of pharma spam, http://www.symantec.com/connect/blogs/return-dead-waledacstorm-botnet-back-rise.

[28] Według ekspertów firmy *Symantec*, niewielki botnet (10 tys. zainfekowanych komputerów) może wysłać w ciągu godziny 360 mln e-maili. Taka masa spamu oferującego farmaceutyki generuje średnio 28 zamówień o wartości 100 USD każde. Roczny dochód z tej formy marketingu elektronicznego szacuje się na ok. 3,5 mln USD. Zob. Four Ways Cybercriminals Profit from Botnets, http://www.symantec.com/connect/blogs/four-ways-cybercriminals-profit-botnets.

[29] Kaspersky Lab, Spam in the Third Quarter of 2010, http://www.securelist.com/en/analysis/204792147/Spam_in_the_Third_Quarter_of_2010.

[30] Zob. np. Department of Justice Takes Action to Disable International Botnet, Department of Justice, April 13, 2011, http://www.justice.gov/opa/pr/2011/April/11-crm-466.html.

Federalnego Biura Śledczego, którego agenci, mając dostęp do wykazu adresów IP zainfekowanych komputerów, mogą z nich usunąć, za zgodą osoby zainteresowanej, groźnego bota w trybie *on-line*. Druga z tych możliwości wywołała w USA kontrowersje i zaniepokojenie obrońców praw i wolności obywatelskich, w tym Electronic Frontier Foundation[31]. Tym niemniej, skorzystało z niej 19 tysięcy podmiotów pokrzywdzonych przez cyberprzestępców kontrolujących botnet Coreflood[32]. Sprawa ta zasługuje na uwagę ze względu na zastosowane w niej innowacyjne rozwiązania prawne i taktykę postępowania organów powołanych do walki z cyberprzestępczością. Nie można wykluczyć, że doświadczenia amerykańskie[33] w tym względzie staną się drogowskazem dla innych państw i wyznaczą jeden z kierunków rozwoju prawa karnego komputerowego na świecie.

## III. Aspekty prawne walki z botnetami w USA

„Coreflood" to jeden ze starszych botnetów, który pojawił się w Internecie w 2002 r. i w szczytowym okresie swojej aktywności liczył 2,3 mln komputerów „zombi", w większości (80%) używanych w USA. W 2008 r. serwery centrum dowodzenia botnetu zostały spenetrowane przez ekspertów firmy *Dell Secure Works*, a raport z tego rekonesansu potwierdził *stricte* przestępczy charakter działalności administratorów sieci[34]. Okoliczności wszczęcia przeciwko nim dochodzenia nie są jasne. Ze skąpych informacji na ten temat wynika, że pierwsze działania w tym kierunku podjęto w kwietniu 2009 r., gdy jedna z korporacji w stanie Connecticut zawiadomiła policję o zainfekowaniu malwarem kilkuset należących do niej komputerów[35]. Można nawet odnieść wrażenie, że początkowo nie bardzo wiedziano jak zneutralizować botnet Coreflood i zahamować coraz większą aktywność jego administratorów. Tymczasem cyberprzestępcy nie próżnowali. W okresie od marca 2009 do lutego 2010 r. zdołali zgromadzić ponad 190 gigabajtów danych o kluczowym znaczeniu dla bezpieczeństwa kont bankowych i znajdujących się

[31] FBI Hijacks Botnet, Drives it Off the Cliff, https://www.eff.org/press/mentions/1970/1/1-14.

[32] L. Constantine, FBI Remotely Uninstalled Coreflood Malware from 19,000 Computers, June 22nd 2011, http://news.softpedia.com/news/FBI-Remotely-Uninstalled-Coreflood-Malware-from-19-000-Computers-207635.shtml.

[33] Dodajmy: inspirowane doświadczeniami holenderskiego High Tech Crime Unit, który w 2010 r. metodą *singholingu* zneutralizował botnet Bredolab.

[34] Ujawniono m.in. blisko pół miliona przechwyconych przez *malware* loginów i haseł do ponad 35 tys. domen internetowych, w tym banków i innych instytucji finansowych oraz portali społecznościowych. Zob. J. Stewart, The Coreflood Report, August 6, 2008; http://www.secureworks.com/cyber-threat-intelligence/threats/coreflood-report/.

[35] Botnet Operation Disabled; http://www.fbi.gov/news/stories/2011/april/botnet_041411.

na nich depozytów pieniężnych[36], a także zrobić z nich użytek. W konsekwencji, wyrządzili oni szkody sięgające setek tysięcy dolarów co najmniej czterem amerykańskim podmiotom gospodarczym, zanim zdołano sparaliżować ich dalsze poczynania przestępcze[37]. Nastąpiło to dopiero w 2011 r. w następstwie skoordynowanych działań federalnych organów ścigania i wymiaru sprawiedliwości.

W starannie przygotowanym i szybko przeprowadzonym postępowaniu przedprocesowym, do którego ograniczono podjęte kroki prawne, wykorzystane zostały zarówno instrumenty cywilnoprawne, jak i karnoprocesowe. Przy ich pomocy starano się osiągnąć dwa ściśle związane ze sobą cele: pozbawić przestępców możliwości używania botnetu i ochronić ich ofiary, tj. użytkowników komputerów zainfekowanych botem Coreflood, przed dalszą wiktymizacją przestępczą.

W dniu 11 kwietnia 2011 r. Biuro Prokuratora Okręgowego stanu Connecticut wystąpiło do sądu z powództwem cywilnym przeciwko trzynastu nieznanym z imienia i nazwiska („John Doe") pozwanym – o zaprzestanie brania udziału w oszustwach telekomunikacyjnych (*wire fraud*[38]), oszustwach bankowych (*bank fraud*[39]) oraz nielegalnym przechwytywaniu elektronicznych przekazów informacji (*unauthorized interception of electronic communications*[40]) przy użyciu programu komputerowego o nazwie „Coreflood". Pozew zawierał zwięzły opis elementów stanu faktycznego sprawy o istotnym znaczeniu dla rozpatrzenia przez sąd zgłoszonych w pozwie wniosków o zastosowanie środków prawnych mających na celu zabezpieczenie interesów procesowych powoda (United States of America) oraz ochronę interesów pokrzywdzonych przestępstwami popełnianymi przez pozwanych.

---

[36] L. Constantin, FBI Remotely…, *op. cit.*; K. Zetter, With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal; http://www.wired.com/threatlevel/2011/04/coreflood/.

[37] Botnet Operation Disabled, *op. cit.* ("Before we shut down the Coreflood operation, cyber thieves made numerous fraudulent wire transfers, costing companies hundreds of thousands of dollars").

[38] Title 18 US Code § 1343. Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

[39] Title 18 US Code § 1344. Whoever knowingly executes, or attempts to execute, a scheme or artifice, (1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises; shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

[40] Zob. http://www.law.cornell.edu/uscode/text/18/2511.

W paragrafach 2–7 pozwu dokonano ogólnej charakterystyki „wirusa" Coreflood, wyjaśniono czym jest botnet i w jaki sposób jest on kontrolowany przez inny komputer zwany serwerem „command-and-control" (C&C). Prokurator, który przygotował pozew, przedstawił zasady komunikowania się komputerów zainfekowanych malwarem z centrum dowodzenia oraz rolę, jaką w tym zakresie odgrywają adresy IP, system DNS i nazwy domenowe serwerów C&C botnetu Coreflood. Autor pozwu wskazał aktualne nazwy domenowe tych serwerów (jane.unreadmsg.net. i vaccina.medinnovation.org) oraz ich adresy IP (207.210.74.74 i 74.63.232.233). Wyjaśnił przy tym, że mogą się one zmieniać w wyniku ich aktualizacji, której następstwem może być zmiana fizycznej lokalizacji serwerów C&C.

Aby do tego nie dopuścić i wykorzystać sprzyjające okoliczności (nazwy domenowe i adresy IP serwerów C&C wskazywały bowiem na ich aktualną lokalizację w USA), powód wniósł o orzeczenie *ex parte* (tj. bez wysłuchania przez sąd drugiej strony) środka tymczasowego polegającego na temporalnym (14-dniowym) uniemożliwieniu pozwanym określonego postępowania (*temporary restraining order* – TRO). Jest to środek tradycyjnie stosowany systemie *common law* w „stanach wyższej konieczności", który tym razem został wykorzystany do niekonwencjonalnych celów w bezprecedensowy sposób[41].

Zgodnie z żądaniem powoda, na podstawie nakazów sądowych z dnia 12 kwietnia 2011 r. o zastosowaniu TRO oraz zajęciu komputerów, nastąpiło zajęcie pięciu serwerów C&C oraz dwudziestu czterech domen internetowych, za pośrednictwem których zarażone botem Coreflood komputery komunikowały się z tymi serwerami. Jednocześnie, w ramach międzynarodowej pomocy prawnej, organy ścigania Estonii dokonały zatrzymania znajdujących się na terytorium tego kraju serwerów, które wcześniej były wykorzystywane do kontrolowania botnetu Coreflood. Na podstawie tych samych nakazów[42] zastąpiono serwery C&C używane przez przestępców serwerami kontrolowanymi przez FBI. Aby umożliwić im przejęcie komunikacji z komputerami „zombi", sąd nakazał operatorom usług DNS zmienić nazwy domenowe serwerów C&C (jane.unreadmsg.net oraz vaccina.medinnovation.org) na SINKHOLE-00. SHADOWSERVER.ORG oraz SINKHOLE–01.SHADOWSERVER.ORG. Jednocześnie zadysponował, aby serwer substytucyjny „reagował na zapytania przesyłane do domen Coreflood przez wydawanie instrukcji, które spowodują, że program Coreflood zainstalowany w zainfekowanych komputerach przestanie działać, z zastrzeżeniem, że takie instrukcje będą wysyłane tylko do komputerów znajdujących się w USA"[43].

[41] TRO jest krótkoterminowym zezwoleniem sądu na podjęcie przez powoda natychmiastowych działań w celu zapobieżenia wyrządzenia mu przez pozwanego niepowetowanej szkody. Postanowienie o zastosowaniu tego środka zazwyczaj poprzedza *preliminary injunction*.

[42] Zob. http://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm.

[43] Zob. TRO, s. 6; http://www.fbi.gov/newhaven/press-releases/2011/pdf/nh041311_5.pdf.

*Sinkholing* serwerów C&C przyniósł spodziewane rezultaty. Przede wszystkim pozwolił zgromadzić adresy IP zainfekowanych komputerów i zatrzymać w nich działanie bota Coreflood po użyciu komendy „exit" wysyłanej przez serwery znajdujące się pod kontrolą FBI. Komenda ta stanowiła doraźny, ale niezbędny środek do celu. *Malware* Coreflood był bowiem tak zaprogramowany, że uruchamiał się po każdym włączeniu (bootowaniu) zainfekowanego nim komputera i niezwłocznie wysyłał ping do kontrolującego go serwera, aby otrzymać od niego instrukcje. W odpowiedzi oprogramowanie zainstalowane na serwerach FBI przesyłało komendę „stop" po każdym sygnale ping przychodzącym od komputera „zombi". Zastosowana przez organy ścigania taktyka pozwoliła uzyskać niezbędną przewagę nad przeciwnikiem i przejść do kontrofensywy. Zatrzymanie działania bota na zarażonych nim komputerach przejściowo chroniło ich posiadaczy przed dalszymi naruszeniami prywatności i innymi formami pokrzywdzenia. Przede wszystkim jednak uniemożliwiało cyberprzestępcom aktualizację *malware'u*[44], a tym samym zwiększało szanse dostawców programów antywirusowych na przygotowanie sygnatur rozpoznających ostatnią wersję Coreflood[45] i – co najważniejsze – definitywne usunięcie złośliwego programu z zainfekowanych maszyn.

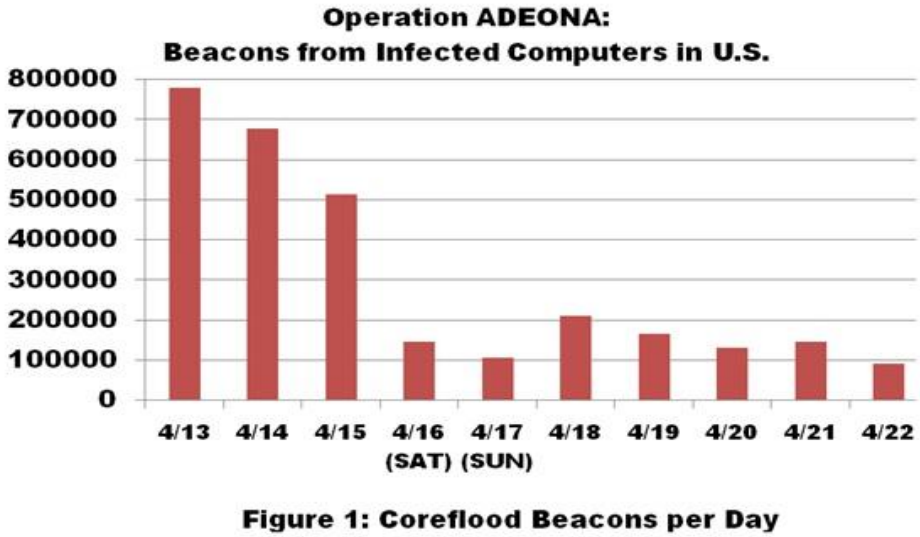
Osiągnięcie tego celu wymagało uruchomienia nowego środka prawnego i przekonania sądu o celowości jego zastosowania. Prokurator federalny w dniu 23 kwietnia 2011 r. wystąpił w związku z tym do sądu z wnioskiem uzupełniającym o zastosowanie *preliminary injunction*[46]. Aby spełnić przesłanki prawne orzeczenia tego środka, posłużono się sugestywną argumentacją, przedstawiając efekty zastosowania *temporary restraining order* (TRO) wydanego przez sąd 12 kwietnia 2011 r. Z przedstawionych na ten temat danych wynikały dwa zasadnicze ustalenia: 1) w ciągu trzech pierwszych dni (13–15 kwietnia 2011 r.) od rozpoczęcia operacji „Adeona", czyli singholowania przez FBI botnetu Coreflood, notowano dziennie po kilkaset tysięcy zgłoszeń zainfekowanych komputerów. Po wydaniu im polecenia „exit" liczba tych sygnałów (pomijając gwałtowny jej spadek w czasie weekendu),

[44] Częściowo zdołali oni dokonać takiej aktualizacji, wykorzystując w tym celu serwery znajdujące się poza jurysdykcją amerykańską – por. F. Y. Rashid, Microsoft, FBI Reprogram Botnet to Remove Coreflood Permanently, eWeek, 2011-04-28, http://www.eweek.com/c/a/Security/Microsoft-FBI-Reprogram-Botnet-to-Remove-Coreflood-Permanently-488081/#sthash. OTdcKVbb.dpuf.

[45] Microsoft Corp. ogłosił komunikat o włączeniu sygnatur trojana Win32/Afcore (alias Coreflood) do swojego sztandarowego narzędzia antywirusowego (Malicious Software Removal Tool) w dniu 13 kwietnia 2011r.; http://blogs.technet.com/b/mmpc/archive/2011/04/13/msrt-april-11-win32-afcore.aspx.

[46] *Preliminary injunction* jest środkiem prawnym o podobnej funkcji do TRO (powstrzymanie pozwanego od określonego postępowania), który na wniosek strony jest stosowany przez sąd po wszczęciu postępowania sądowego w celu powstrzymania strony przeciwnej od określonych zachowań albo zmuszenia jej do określonego zachowania się do czasu merytorycznego rozstrzygnięcia sporu.

stopniowo malała – do 90 tys. w ostatnim, dziesiątym dniu operacji (ryc. 1); 2) dzięki zastosowanej metodzie rozmiary botnetu Coreflood znacznie zredukowano: w USA o 90%, za granicą o 75%[47].




*Ryc. 1. Diagram obrazujący przebieg operacji „Adeona" (źródło: Government's supplemental memorandum in support of preliminary injunction, s. 4).*

Mimo tak spektakularnych wyników prokuratura uznała, że niebezpieczeństwo nie zostało zażegnane i istnieje konieczność kontynuowania działań zapobiegawczych do czasu zlikwidowania botnetu. Podzielając stanowisko prokuratury i przedstawione przez nią argumenty, sąd w dniu 25 kwietnia 2011 r. wydał postanowienie o zastosowaniu *preliminary injunction,* przedłużając okres singholowania botnetu Careflood do czasu merytorycznego rozstrzygnięcia powództwa. Powód nie mając złudzeń co do tego, że może to kiedykolwiek nastąpić, w dniu 14 czerwca 2011 r. wystąpił do sądu z wnioskiem o zmianę *preliminary injunction*. Wnosząc o wykorzystanie substytucyjnego serwera pod kontrolą FBI do zdalnego usunięcia złośliwego oprogramowania z zainfekowanych komputerów „zombi", ograniczył zakres wniosku do komputerów znajdujących się w USA, a jego wykonanie uzależnił od uzyskania od ich właścicieli pisemnej zgody na dokonanie tej czynno-

[47] The Government's supplemental memorandum in support of preliminary injunction; http://www.justice.gov/opa/documents/coreflood-govt-supp.pdf.

ści przez FBI. Do wniosku załączono projekt postanowienia[48]. Sędzia, która je podpisała w dniu 15 czerwca 2011 r., położyła kres działalności przestępczej pozwanych związanej z botnetem Coreflood. Wydaje się, że zarówno w znaczeniu formalnym, jak i faktycznym.

Akordem kończącym postępowanie cywilne w sprawie United States of America v. Joe Does 1–13 był *default judgment*[49] – szczególny rodzaj wyroku zapadającego na korzyść powoda w sytuacji, w której pozwany nie wchodzi z nim w spór, w szczególności nie odpowiada na wezwania sądu i uchyla się od składania środków odwoławczych od postanowień sądowych nakładających na niego w trakcie postępowania określone nakazy, zakazy lub obowiązki (np. *preliminary injunction*). Jednocześnie, na mocy odrębnego postanowienia sądu noszącego tę samą datę (21 czerwca 2011 r.), *preliminary injunction* zastąpiono *permanent injunction*. Zgodnie z pozwem, który precyzował treść tego środka prawnego, sąd nakazał pozwanym usunięcie *malware'u* Coreflood ze wszystkich komputerów, które nie są ich własnością, oraz upoważnił FBI do wykorzystywania serwera substytucyjnego, który emulował działanie serwerów C&C do wykonania wszystkich nakazów sądowych. W rzeczywistości serwer ten działał do dnia 17 czerwca 2011 r., w którym z uwagi na wykonanie wszystkich zadań jego misję uznano za zakończoną.

## IV. Wnioski

Na podstawie analizy dostępnych źródeł internetowych można stwierdzić, że amerykański styl walki z botnetami charakteryzuje się silnym przywiązaniem do zasady legalizmu oraz na wskroś pragmatycznym podejściem do osiągania zakładanych celów przy użyciu środków prawnych. W omawianym przypadku o ich wyborze zadecydowała realistyczna ocena sytuacji oraz racjonalny bilans „zysków i strat". W rezultacie za cel nadrzędny uznano zapobieżenie szkodom grożącym ze strony cyberprzestępców, nie zaś stosowanie represji karnej za popełnione przez nich przestępstwa. Była to decyzja trafna nie tylko z uwagi na trudności związane z ustaleniem tożsamości sprawców, których „identyfikacja" ograniczała się do ustalenia używanych przez nich adresów poczty elektronicznej, na jakie przesyłano im pisma procesowe w toczącym się postępowaniu cywilnym. Wybór takiego trybu postępowania pozwolił na szybkie i skuteczne wykorzystanie tradycyjnych instrumentów cywilnoprocesowych (TRO, *preliminary injunction*) do stosowania w ich ramach nowatorskich rozwiązań technicznych (*sinkholing* serwerów

[48] Zob. project postanowienia na stronie http://www.fbi.gov/newhaven/press-releases/pdf/nh041311_7.pdf.

[49] Zob. ten wyrok na stronie http://www.fbi.gov/newhaven/press-releases/pdf/nh041311_8.pdf.

C&C, zdalne usuwanie złośliwego oprogramowania przez policję), a w konsekwencji doprowadził do zablokowania działalności przestępczej administratorów botnetu Coreflood. Wykorzystane w tym celu przez organy ścigania USA remedia prawne mogą imponować pomysłowością i precyzją wykonania. Z europejskiej perspektywy prawnej, zwłaszcza państw Europy kontynentalnej, są one jednak nie do zaakceptowania. Obowiązujące w tej części świata systemy prawne nie przewidują możliwości stosowania karnoprawnych środków przymusu procesowego (zajęcie komputerów lub domen internetowych) w celach prewencyjnych, a tym bardziej w postępowaniu cywilnym, na dodatek przeciwko pozwanemu o nieustalonej tożsamości. W przeciwieństwie do USA, w Europie, a przynajmniej w niektórych jurysdykcjach europejskich, radzenie sobie z podobnymi problemami prawnymi nie wydaje się możliwe bez udziału i pomocy ustawodawcy. Próby prawidłowego ich rozwiązania w drodze wykładni obowiązujących regulacji prawnych mogą okazać się niewystarczające.

# Botnets as a legal and criminological issue in the context of American experiences

## Abstract

*This paper defines a botnet as dynamic malware used to remotely control infected computers, connect them to networks, and use their performance for coordinated mass-scale crime purposes. Furthermore, it provides examples of the U.S. ways to fight botnets, formulating the view that the American style of the fight against botnets is characterised by strong attachment to the principle of legality, with the pragmatic approach to achieving goals using legal measures.*