Janusz Janczyk

W głębi Internetu – inne zastosowania informatyki

Dydaktyka Informatyki 9, 114-125

2014

Janusz JANCZYK

W GŁĘBI INTERNETU – INNE ZASTOSOWANIA INFORMATYKI

IN THE DEPHTS OF THE INTERNET – OTHER APPLICATIONS OF COMPUTER SCIENCE

Słowa kluczowe: Internet, cyberterroryzm, hackerzy, wojna sieciowa
Keywords: Internet, cyber-terrorism, hackers, netwar

Streszczenie

Internet wywodzi się z projektów wojskowych, lecz stał się pierwszym elektronicznym środowiskiem komunikacji społecznej. Funkcjonalność Internetu pozwala wykorzystywać go do różnych celów, nie zawsze etycznych, czy zgodnych z prawem. Ciemna strona Internetu – *darknet*, jest wykorzystywana do wielu celów. Szczególne miejsce w tym opracowaniu ma kontekst instytucjonalnego cyberterroryzmu w Internecie. Zostały też opisane typy ataków sieciowych dla celów prowadzenia działań destrukcyjnych i inwigilacji. Celem jest deskrypcja środowiska społecznego sieci dla uzyskania obrazu tak kontrowersyjnych zastosowań informatyki.

Summary

The Internet originates from military projects, but became the first electronic communication environment. The functionality of the Internet allows to use it for various purposes, does not always ethical or lawful. The dark side of the Internet – Darknet, is used for many purposes. The special place in this paper is the institutional context of cyber-terrorism on the Internet. In this paper have also been described types of network attacks for the purpose of conducting destructive activities and surveillance. The aim is description of the social environment network to obtain an image of controversial applications of computer science.

Wstęp

Wśród zastosowań społecznych dziedziny nauki, jaką jest informatyka, niewątpliwie największą karierę zrobiły sieci komputerowe – zwłaszcza rozległe, czyli Internet. Czym jest obecnie Internet? Każdy ma na ten temat własne zdanie i jednocześnie znakomita większość podziela opinię, iż wpływ tego produktu informatyki jest duży, może nawet zbyt duży, na życie współczesnego człowieka. Najbardziej rozpowszechnioną funkcjonalnością Internetu jest World Wide

Web (WWW), pomimo że w zamyśle twórców miał służyć do celów naukowych. W 1992 roku fizyk Tim Berners-Lee obmyślił sposób integracji źródeł informacji w Internecie dla potrzeb własnych dokumentów i użył do tego hipertekstu, wykreowanego jeszcze w latach 60. XX wieku przez Teda Nelsona. Nie zdawał sobie sprawy z wykreowania WWW, a pewnie nie przypuszczał, że w tak krótkim czasie spowoduje burzę w społeczeństwie. Informacja niesiona poprzez strony WWW jest multimedialna i o pełnym spektrum tematycznym. Olbrzymi obszar zastosowań hipertekstu w Internecie, a szczególnie jego dostępność i łatwość stosowania nie tylko oszałamia, ale wciąga i uzależnia. Trzeba zaznaczyć, że racjonalne, w stosunku do zamysłu twórców WWW, wykorzystanie Internetu jest tylko wierzchołkiem góry lodowej możliwych zastosowań[1]. Należy się zastanowić, czy naprawdę możliwy jest dostęp do wszelkiego rodzaju poglądów, opinii czy wiadomości, skoro WWW oferuje ich tyle, że za krótko żyjemy, aby je chociażby pobieżnie przejrzeć. Z technicznego punktu widzenia, przy tak szybkim rozwoju środków przenoszenia i przetwarzania informacji, niepozbawione racjonalności jest globalne sieciowe połączenie społeczeństw, określane mianem McLuhan'owskiej „globalnej wioski", która w ostatniej dekadzie usilnie egzemplifikuje idee zwarte w teorii chaosu.

1. Czym się zajmują hackerzy

Poindeksowana zawartość informacyjna Internetu nie jest tak intrygująca i tajemnicza dla badacza zagadnień społeczności sieciowych, co bliżej nieokreślone ciemne obszary globalnej sieci – tzw. ***darknet***. Pierwszoplanowa trudność dotyczy liczby witryn prywatnych osób, które nie potrafią włączyć ich do indeksowanych zasobów Internetu. Są to osoby poznające podstawy edycji stron WWW, które przy pomocy standardowego oprogramowania, nawet biurowego, realizują tego typu projekty. Zapewne wiele dokumentów tak powstałych zawiera wiele interesujących informacji, ale nie mogą zaistnieć w Internecie bez procedury publikacji. Szczególnie istotni są tutaj ci użytkownicy Internetu, którzy posiadają stałe łącza i we własnych komputerach uruchomili serwery usług WWW. Często tego typu netizeni nie wiedzą o konieczności zarejestrowania swoich serwerów przynajmniej w jednym serwisie wyszukiwawczym lub katalogu tematycznym.

Istotną rolę pełnią w powstawaniu problemów społecznych i technicznych w Internecie domorośli eksperci, zwani potocznie ***hackerami***. Chociaż ich liczba jest niewielka w stosunku to użytkowników sieci, to silnie oddziałują na całe

[1] Por. J. Janczyk, *Racjonalność użytkowania Internetu* [w:] *Racjonalność myślenia, decydowania i działania*, red. L.W. Zacher, Wyd. WSPiZ, Warszawa 2000

społeczeństwo. Wraz z rozwojem Internetu i jego upowszechnieniem problem hackerstwa otrzymał najwyższy priorytet. To dzięki hackerom powstało pojęcie „firewall", za którym kryje się oprogramowanie systemów informatycznych o najwyższej jakości zabezpieczeń. Za hackera uważany jest każdy kto potrafi „poskromić system komputerowy" lub „rozpruć system komputerowy", przy czym nie jest to jego własny system i nie posiada do niego praw dostępu. Ze względu na średnią wieku (są to głównie młodociani przestępcy), hackerów często nazywa się przestępcami w krótkich spodenkach (ang. *short-pants criminals*). Nieco inaczej hackera definiuje angielski słownik *The New Hacker's Dictionary – The Jargon File*[2]. Podaje on, że hacker to osoba mająca duże umiejętności programistyczne i bardzo bogatą wiedzę o komputerach oraz systemach operacyjnych, aplikacjach i lukach w nich występujących. W takim znaczeniu za hackera uważany byłby kiedyś nawet Bill Gates. Z kolei B. Landreth, były hacker, wyróżnia następujące kategorie hackerów: nowicjuszy, studentów, turystów, wandali i złodziei.[3] Charakterystyczną cechą takiego podziału są pobudki, dla których dokonywane są przestępstwa oraz oczekiwane zyski z tych działań. Do nowicjuszy zalicza się początkujących hackerów, których interesują gry komputerowe, nowsze oprogramowanie lub zawartość zbiorów danych. Trudno jest określić zakres działań nowicjuszy w stosunku do systemów informatycznych, które uległy ich „poskromieniu". W kategorii studentów znajdują się wszelkiego rodzaju amatorscy badacze i analitycy, którzy są zainteresowani poznaniem różnych systemów informatycznych. Nie są oni nastawieni na wyrządzanie szkód, lecz tylko na zaspokojenie własnej ciekawości lub wypróbowanie umiejętności. Dla turystów systemy komputerowe są swego rodzaju łamigłówką, do której po rozwiązaniu więcej nie wracają. Wandale to kategoria, którą kieruje głównie chęć dokonywania zniszczeń w systemach komputerowych. Satysfakcję dla tej grupy użytkowników stanowi totalna destrukcja „rozprutego" systemu. Kategoria złodziei, najliczniej reprezentowana, ma najwięcej wspólnego z przestępstwami tradycyjnymi, chociaż komputer jest im w działaniu nieodzowny. Złodziei można uznać za typowych przestępców po odpowiednim przeszkoleniu informatycznym (kursie doskonalącym), a Internet ułatwia im zadanie, chociażby poprzez: informacje o szczegółach systemów informatycznych (listy dyskusyjne np. turystów, studentów, czy nawet nowicjuszy), serwery z oprogramowaniem specjalistycznym (crack's) do włamań[4], tworzenia lub podrabiania elektro-

[2] Por. *The New Hacker's Dictionary*, http://www.ccil.org/jargon/jargon.html (20.09.2012).

[3] Por. B. Landreth, *Out of the Inner Circle. A Hacker's Guide to Computer Seciurity*, Washington 1985.

[4] Jednym z bardziej znanych tego typu serwisów był http://astalavista.box.sk (obecnie właściwy serwis dostępny jest w tylko darknecie).

nicznych kart kredytowych[5], jak i do tworzenia listy haseł dostępu do najprzeróżniejszych zabezpieczonych serwerów[6].

Pierwszy ujawniony i najsłynniejszy hacker świata, Kevin Mitnick, twierdzi, że najsłabszym ogniwem zabezpieczeń systemów komputerowych są ludzie. On sam nigdy nie stosował aplikacji hackerskich. Według niego najskuteczniejszą metodą było poznanie odpowiedniej osoby i tzw. social engineering, czyli wykorzystanie słabości psychiki ludzkiej[7]. W przeciwieństwie do Mitnicka inni hackerzy tworzą i używają oprogramowania do swoich poczynań w sieci. Metod włamań do sieciowych systemów komputerowych jest wiele i można je podzielić na kilka grup:

- BO (*Buffer Overflow*) – to najpopularniejsza metoda ataku w Internecie; wykorzystuje błędy logiczne w oprogramowaniu komputerów;
- DoS (*Denial of Service*) – polega na blokowaniu działania serwerów sieciowych poprzez wysyłanie wielu zmodyfikowanych pakietów IP;
- DDoS (*Distributed Denial of Service*) – atak DoS wykonany jednocześnie z wielu komputerów (np. botnetu);
- Wirusy, robaki i konie trojańskie[8] – są znane prawie wszystkim użytkownikom Internetu;
- Sniffing – polega na przechwytywaniu haseł dostępu[9];
- Spoofing – czyli podszywanie się pod cudzy adres IP;
- Session hijacking – to dynamiczna odmiana spoofingu;
- Network snooping – wykorzystanie zaawansowanych analizatorów sieci w celu doboru najefektywniejszej metody ataku.

2. Gdzie pracują hackerzy

Trzeba zauważyć, że rozróżnienie zastosowań typowych od nietypowych (przestępczych) komputerów jest trudne. Granica między nimi jest cienka lub niewyraźna. Takie rozumowanie jest błędne pomimo, że w środkach masowego przekazu afirmuje się działania przestępcze poprzez następujące określenia: „legalne szpiegostwo gospodarcze", „legalny wywiad gospodarczy"[10]. Szpiego-

[5] Np.: Cmaster3 lub Cwizard1.

[6] Np.: McKiler PL, HackNet czy Socket Demon1.3.

[7] Por. J. Janczyk, *Social problems resulting from information contents of the Internet*, Congress Papers: *Innovations for an e-Society. Challenges for Technology Assessment*, session II – *New Media and Culture*, Berlin 2001.

[8] Te grupy specjalizowanego oprogramowania są często w potocznym znaczeniu używane zamiennie.

[9] Hackerzy używają najczęściej kilku metod zdobywania haseł: brutal force, słownika, podsłuch w sieci lub powtórne logowanie.

[10] Por. J. Janczyk, *„Cienie" Internetu a edukacyjne możliwości zastosowań technologii informacyjnej*, „Transformacje" listopad 2002, 1–4/2002.

stwo w sposób naturalny kojarzy się z działaniami nielegalnymi, a wywiad jest określeniem obojętnym, przez co obejmuje również działania legalne. W tym kontekście „New York Times" ujawnił, że od 2010 roku Agencja Bezpieczeństwa Narodowego USA (NSA) wykorzystuje swoje ogromne zbiory danych do tworzenia zaawansowanych wykresów powiązań społecznych większości amerykanów. Dzięki nim możliwa jest identyfikacja: współpracowników, miejsc przebywania w określonym czasie, towarzyszy podróży i innych danych osobowych[11]. Usprawiedliwieniem działań NSA jest syndrom zagrożenia terroryzmem i cyberterroryzmem. W 2013 roku, po sześcioletnim śledztwie, amerykańska firma Mandiant opublikowała raport, według którego Chińska Armia Ludowa posiada jednostkę cyberterrorystycznej formacji[12]. Raport nazywa formację hackerską jako APT1 i określa jej lokalizację w niepozornym 12-piętrowym budynku na przedmieściach Szanghaju. Formacja jest oznaczona w chińskiej armii jako jednostka 61398. Współpracownicy tej formacji, w liczbie sięgającej nawet kilku tysięcy mają za swój główny cel instytucje państwowe oraz organizacje i firmy w Stanach Zjednoczonych. To, że nasilające się w ostatnich latach ataki na amerykańskie cele pochodzą z Chin, nie jest niczym nowym dla NSA Stanów Zjednoczonych. Ten raport stanowi pierwsze, tak poważne oskarżenie chińskiego rządu o prowadzenie szeroko zakrojonych cyberterrorystycznych działań. NSA nie należy do organizacji świętych, gdyż podejrzewana jest o cyberataki od czasu konfliktu w Zatoce Perskiej w 1991 roku, a do tych celów wypuściła do Internetu takie robaki, jak: Stuxnet, Duqu i Flame. Działania amerykańskiej agencji doprowadziły do tego, że Stanom Zjednoczonym zagraża już nie tylko Chińska formacja cyberterrorystyczna, lecz także coraz mocniejsza irańska siatka rządowych hackerów. Interesujące spostrzeżenia w związku z powyższym poczynił C. Raiu szef działu badań Kaspersky Lab na konferencji Cyber-Security Summit w 2013 roku[13]. Stwierdził między innymi, że w sieci funkcjonuje wiele cyberbroni, o których użytkownicy, a nawet specjaliści od zabezpieczeń sieciowych, nie mają pełnej wiedzy, gdyż jest trudna do wykrycia i monitorowania. Wyraził też opinię, że do początku 2013 roku za większość aktywnego w Internecie złośliwego oprogramowania odpowiedzialni byli „klasyczni" cyberprzestępcy, których główną motywacją były pieniądze. Od tego czasu specjaliści z Kaspersky Lab odnotowują coraz większą aktywność najróżniejszych agend rządowych i wojskowych. Specjalizują się one w przeprowadzaniu ataków informatycznych i wykradaniu danych. Wspomniani specjaliści dzielą takie

[11] Por. wiadomości w serwisie New York Times, *N.S.A. Gathers Data on Social Connections of U.S. Citizens,* http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?_r=0 (14.12.2013).

[12] Por. *Cynerterroryści w chińskiej armii*, „PC World" 4/2013.

[13] Por. *Hacker na państwowej posadzie*, „PC World" 4/2013.

akcje na dwie grupy działania: celem pierwszej jest zakłócenie funkcjonowania jakiegoś państwa, instytucji lub organizacji (taki efekt spowodował wirus Stuxnet zakłócając pracę irańskich instalacji atomowych), celem drugiej są operacje szpiegowskie, przeprowadzane z wykorzystaniem narzędzi informatycznych (działanie wirusa Duqu, który miał poczynić rekonesans przed atakiem Stuxnet). Operacje hackerskie inspirowane i prowadzone przez organizacje rządowe mają na celu nie tylko inne rządy, lecz coraz częściej firmy. Ataki takie są prowadzone dla pozyskania poufnych danych (np. kodu źródłowego oprogramowania) lub z myślą o uzyskaniu dostępu do rządowych systemów IT, co dotyczy firm współpracujących z instytucjami publicznymi. Do tych celów, jak twierdzą specjaliści z Kaspersky Lab, wykorzystywany był i po modyfikacjach jest wirus Flame. Polska armia nie chce dłużej pozostawać w tyle i jak twierdzi minister obrony narodowej T. Siemoniak, w 2014 roku nowo powołana jednostka Centrum Operacji Cybernetycznych ma zajmować się odpieraniem ataków elektronicznych i prowadzeniem cyberwojny[14]. Pan minister zdaje sobie sprawę, że wojsko do tej jednostki rekrutować będzie hackerów i to nie koniecznie do sortów mundurowych. Zatrudnianie specjalistów od włamań hackerskich, infiltracji elektronicznej oraz przeciwdziałania podobnym atakom nie jest w polskim wojsku niczym nowym. Z usług takich specjalistów chętnie korzysta Służba Kontrwywiadu Wojskowego, a wzmacnianiem bezpieczeństwa sieciowego zajmują się hackerzy w Narodowym Centrum Kryptologii. Centrum to uważane jest za odpowiednik amerykańskiej NSA. Wypada także wspomnieć o przetargu MON i Narodowego Centrum Badań i Rozwoju z 2013 roku na stworzenie oprogramowania i sprzętu elektronicznego do prowadzenia walki elektronicznej[15]. Projekt obejmował stworzenie botworma (inteligentnego robaka) na tyle szkodliwego, aby mógł on niepostrzeżenie infekować i inwigilować komputery innych państw, paraliżować ich systemy komunikacyjne i informatyczne, a także przejmować i neutralizować wrogie oprogramowanie szpiegowskie. Polityka MON w tej sprawie jest co najmniej niejasna, gdyż najpierw dokumenty przetargowe opublikowano na stronie instytucji współpracującej z ministerstwem, a potem okazuje się, że przetarg ktoś wygrał, ale nie wiadomo kto i dokumenty związane z projektem są niekompletne.

Wiele informacji o prowadzeniu nielegalnej działalności instytucji państwowych pochodzi ze źródeł oficjalnych i są publikowane w prasie specjalistycznej, nie tylko on-line. Z problematyką państwowego cyberterroryzmu spotkałem się już w 2004 roku na międzynarodowej konferencji „Społeczeństwo – Ryzyko – Demokracja w kontekście integracji, globalizacji i trwałego rozwoju",

[14] Por. *Polska armia stawia na hackerów*, „PC World" 2/2014.
[15] Por. tamże.

zorganizowanej przez Center for impact assessment studies and forecasting, przy Akademii Leona Koźmińskiego w Warszawie. P. Sienkiewicz w swoim wystąpieniu silnie zaakcentował, że od czasu konfliktu Falklandy-Malwiny prowadzone są prace badawczo-rozwojowe we wszystkich nowoczesnych armiach świata w celu wykorzystania Internetu do działaniach wojskowych – wojennych i wywiadowczych (tzw. walka elektroniczna). W tym wystąpieniu zostały zaprezentowane także: typowy schemat Sieciocentrycznego Pola Walki (skrót ang. NCW), założenia dla strategii Infowar, Cyberwar i Netwar, ale co szczególnie interesujące diagram wyodrębniający cyberterroryzm państwowy i niepaństwowy. Zawartość pól diagramu po graficznej obróbce własnej prezentuje rysunek 1.

Rysunek 1. Cyberterroryzm w ujęciu P. Sienkiewicza[16]

Schemat zaprezentowany przez P. Sienkiewicza dopiero po kilku latach znalazł odbicie w nielicznych publikacjach specjalistycznych i wiadomościach głównych dzienników międzynarodowych (dostępnych nie tylko on-line). Nie powinno dziwić takie zestawienie groźnych możliwości zastosowań Internetu, gdyż cyberprzestrzeń bierze swój rodowód od wojskowego projektu Stanów Zjednoczonych ARPANET. Najdziwniejsze jest w tym to, że w tę „sieć sieci" złapano w skali globalnej całe społeczeństwo i wykorzystuje się jego zasoby do prowadzenia działań nie tylko nieetycznych, ale i nielegalnych, niezgodnych z prawami człowieka. Tych zinstytucjonalizowanych działań cyberterro-

[16] Por. P. Sienkiewicz, H. Świeboda, *Niebezpieczna przestrzeń cybernetyczna,* „Transformacje", 1–4 (47–50)/2006.

rystycznych nie będą ścigać żadne organy władzy – choćby międzynarodowej (np. ONZ), gdyż wszystko odbywa się w majestacie prawa.

3. Do czego służą botnety

Wypada przyjrzeć się obecnie nietypowym zastosowaniom zasobów sprzętowo-programowych przeciętnych użytkowników Internetu, którzy bez wiedzy udostępniają swoje komputery i łącza internetowe, sieciowym przestępcom. Według pierwszych doniesień BBC[17] podziemie w Internecie szybko się rozrosło w 2004 roku, gdyż ponad 30 tys. komputerów dziennie było przyłączanych do tajnych sieci, które rozpowszechniały spam i wirusy. Pół roku wcześniej tylko 2 tys. komputerów działających na systemie Windows było przyłączanych codziennie do tych tzw. botnetów. W Internet Security Threat Report[18] z tego samego roku firma Symantec doniosła również, że Internetowi przestępcy codziennie przejmują kontrolę nad 30 tys. komputerów i czynią to głównie za sprawą robaków, zawierających moduł „backdoor". Prób zainfekowania komputerów przez Internet w 2008 roku odnotowywano ok. 75 tys. dziennie, a Symantec określiła zainfekowane maszyny jako „sieć komputerów zombie"[19]. Raport podaje, że połączone w sieć „zombie PC" służą przestępcom przeważnie do rozsyłania spamu oraz przeprowadzania ataków DDoS. Sytuacja w Internecie się nie zmienia, gdyż jak poinformowano uczestników konferencji Black Hat USA 2013 – skala przejęć komputerów Zombie sięgnęła 150 tys. dziennie[20]. Powstaje pytanie: do czego jeszcze, oprócz ataków DDoS, wykorzystuje się taką liczbę przejętych komputerów. Producenci oprogramowania antywirusowego są zdania, że większość spamu trafiającego via e-mail jest zasługą „armii zombie PC". Są to ofiary ataku robaków internetowych takich, jak: Sobig, MyDoom, czy też Bagle'a. Każdy z tych insektów zawiera ukryte w kodzie procedury, które umożliwiają zdalne przejęcie kontroli nad maszyną i wykorzystanie jej do rozsyłania spamu, ale także przeprowadzania ataków metodą DDoS na serwery internetowe (np. znany atak w sprawie ACTA z 2012 r.). Firma Akamai Technologies[21] świadcząca usługi dla największych korporacji i serwisów internetowych (Goo-

[17] Por. *Net security threats growing fast,* http://news.bbc.co.uk/1/hi/technology/ 3666978.stm, (20.09.2009).

[18] Por. D. Cieślak**,** *Internet pełen zombie*, http://www.pcworld.pl/news/70746.html (21. 09.2009).

[19] J. Janczyk, *Technical and Organizational Crises in Nets,* TRANSFORMACJE Special Issue 2005–2007, Warszawa 2008.

[20] Por. *Parada pomysłów na łamanie zabezpieczeń*, „PC World" 10/2013.

[21] Por. S. Górski, *Zombie PC: zmora naszych czasów*, http://www.pcworld.pl/news/ 68560.html (12.07.2011).

gle, Yahoo!, Microsoft), winą za awarie serwerów w pierwszym półroczu 2004 r. obarczyła właśnie „armię zombie PC". Specjaliści z brytyjskiej firmy antywirusowej Sophos są zdania, iż 40% spamu w Cyberprzestrzeni jest zasługą działania wirusów: Sobiga, MyDooma i Bagle'a. Z kolei firma Sandvine zajmująca się bezpieczeństwem sieci ocenia, iż zainfekowane komputery mogą być odpowiedzialne nawet za 80% niechcianej korespondencji. „Zombie PC" oprócz dystrybucji spamu i ataków DDoS mogą służyć między innymi do rozsyłania groźnych wirusów, pobierania pornografii i wykradania prywatnych informacji bez wiedzy użytkownika. C. Theriault, konsultantka ds. bezpieczeństwa w firmie Sophos twierdzi, że komputer osobisty może stać się bezwolnym przekaźnikiem wszelkiego typu śmieci i niebezpiecznych pakietów danych, jakie można znaleźć w Internecie, rozsyłającym je do setek, czy tysięcy niewinnych użytkowników. Według specjalistów z firmy Sophos w 2004 r. na całym świecie działało ponad 500 tysięcy komputerów „Zombie PC". Inne źródła podały, że mogło ich być nawet 2 miliony. Z badań firm Earthlink oraz Webroot Software wynika, że co trzeci komputer posiada zainstalowane oprogramowanie typu spyware, które może skrycie rejestrować poufne dane i wysyłać je do zdalnego komputera w Internecie[22]. Hackerom w większości przypadków nie zależy na naszych danych finansowych, zdjęciach, czy też prywatnej korespondencji. Dla nich ważny jest dodatkowy komputer, który powiększa „armię komputerów zombie", inaczej zwanych botnetem. Niełatwo jest określić, czy nasz komputer jest już „zombie PC". Symptomami mogącymi świadczyć o przejęciu kontroli nad naszym komputerem mogą być:

- nadmierna aktywność dysku twardego;
- podwyższone wykorzystanie połączenia sieciowego;
- nagłe i niespodziewane ruchy kursora na ekranie (odbywające się bez udziału użytkownika);
- niespodziewane wiadomości w skrzynce pocztowej (od osób, których nie znamy ze wstawionym początkiem tematu – Re:).

Wspomniane „zombie PC" kolekcjonowane przez hackerów są organizowane w sieci, które, jak większość rzeczy i usług, są wystawiane na sprzedaż. Stąd niektórzy badacze problematyki spamu określają je nazwą handlową „botnets", pewnie dlatego, że brzmi dla celów marketingowych znacznie lepiej niż „armia zombie PC". Jeden ze specjalistów od spamu S. Linford[23], szef firmy Spamhaus uważa, że ponad 70% niezamawianej korespondencji jest dziełem „botnetów" – sieci komputerów, nad którymi zdalnie przejęto kontrolę. Według niego każda

[22] Por. D. Cieślak, *W poszukiwaniu szpiegów: 1/3 komputerów zainfekowana*, http://www.pcworld.pl/news/ 67804.html (21.09.2009).

[23] Por. S. Górski, *Większość spamu generują botnety*, http://www.pcworld.pl/news/70837.html (23.09.2009).

grupa zajmująca się rozsyłaniem spamu, posiada własny „botnet" lub korzysta z takiej sieci, utworzonej przez innych. Dla przykładu S. Linford podaje grupę spamerów z Florydy, którzy wykorzystują „bonety" utworzone przez Rosjan. Każdego tygodnia, ponad 100 tysięcy komputerów zaprzęganych było do rozsyłania spamu w ich „bonetach", bez wiedzy ich właścicieli. „Bonety" rozsyłają spam, dopóki nie zostaną wciągnięte na „czarną listę" przez firmy antyspamowe. Wtedy właściciel takiego „bonetu" może go sprzedać innym użytkownikom, którzy mogą jeszcze wykorzystać taką sieć komputerów do przeprowadzania ataków DDoS. Jakiej nazwy byśmy nie użyli dla ogromnej rzeszy przejętych przez hackerów komputerów, to zjawisko „botnets" przybiera na sile i stanowi poważny zasób sieciowy dla instytucjonalnego cyberterroryzmu. O instytucjach wykorzystujących zasoby Internetu do działań nielegalnych ukazuje się nieco informacji w różnego rodzaju publikatorach, ale czy wszystkie lub chociażby większość ma szansę na ujawnienie? Trzeba w tym miejscu nieco szerzej opisać wspomniany już obszar Internetu, czyli tzw. darknet.

4. Darknet to nie tylko anonimowość

Anonimowość w Internecie od jego zarania była postrzegana jak dobro naturalne, była niezbywalnym prawem człowieka. Wraz z rozwojem usług sieciowych już w nowym milenium anonimowość w swej naturze Internetu została utracona. Takie sieci w Internecie, jak FreeNet (projekt rozwijany od 2000 r.) i TOR (rozwijany od 2004 r.) powstały w celu zapewnienia ochrony prywatności internautów, zwłaszcza w krajach totalitarnych. Korzystają z tych sieci internauci, którzy nie życzą sobie, aby ich działania zostały odkryte i wykorzystywane przeciwko nim. Z tej anonimowości korzystają różni ludzie, zatem FreeNet i TOR mają swoją drugą „ciemną stronę", czego raczej nie życzyli sobie ich twórcy. Wspomniany darknet (Ciemna sieć), zwany także Hidden Services (Ukryte Usługi) lub Deep Web (Głęboki Internet), jest nośnikiem usług dla tej gorszej strony anonimowości[24]. Almanachem wiedzy o darknecie i zarazem jego symbolem jest Hidden Wiki (Ukryta Wikipedia), zawierająca hasła dotyczące treści, których nie można znaleźć w Internecie, których wyszukiwarka Google nie znajdzie. Deep Web kryje wszystko to, co w znanym przeciętnym użytkownikom w Internecie jest zabronione, a więc: wszelkiej maści pornografia (także dziecięca), fora dla terrorystów i miłośników wszystkich odmienności, podręczniki hackingu i poradniki przygotowywania substancji psychoaktywnych w warunkach domowych oraz wiele innych. Ta ciemna strona Internetu uchodzi w opiniach wielu użytkowników, którzy niby przypadkiem tam zajrzeli, za ściek lub rynsztok informacyjny, którym płyną najbardziej cuchnące odpady działal-

[24] Por. *Darknet – ciemna strona sieci*, „PC World" 11/2013.

ności ludzkiej w sieci. Do informacji zawartych w darknecie nie można dostać się za pośrednictwem Google, czy innego legalnego oprogramowania. Do zasobów ciemnej strony Internetu trzeba dołączyć świadomie, instalując odpowiednie oprogramowanie i mając jasną intencję poszukiwania tego, co zakazane i nielegalne lub chcąc pozostać w Internecie anonimowym użytkownikiem. Po ciemnej stronie sieci nie funkcjonują wyszukiwarki, a użytkownicy muszą polegać na zbiorach odsyłaczy. Witryny w tej sieci są bardzo prymitywne, a ich oprawa graficzna przypomina Internet z lat 90. XX wieku. Punktem startowym w ciemnej stronie Internetu jest najczęściej witryna TorDir, która jest niczym innym, jak katalogiem linków, agregującym mnóstwo odnośników do innych stron. Nie wszystkie odsyłacze zawsze działają, a zawartość stron jest dostępna tylko wtedy, kiedy właściciel serwera włączy go i zaloguje się w sieci. To jeszcze jedna typowa cecha darknetu, odróżniająca go od zwykłej sieci. Jeśli jednego dnia są dostępne jakieś strony, drugiego mogą one już nie działać, ale za to są dostępne zupełnie inne, których wcześniej nie było.

Istnienie darknetu samo w sobie nie wpływa na bezpieczeństwo internautów. Ciemna sieć funkcjonuje poza użytkownikami Internetu, a jeśli nawet legalne dane gdzieś na łączach mieszają się z brudnymi danymi, nie powoduje to żadnych kolizji. Należy pamiętać, że przestępcy, ci instytucjonalni i prywatni, przygotowują pod osłoną darknetu ataki różnego rodzaju (wymienione wyżej) dotyczące całego Internetu, które w efekcie mogą dotknąć każdego użytkownika. Każdy internauta może być zamieszany w tego typu działania, bez jego wiedzy i przyzwolenia.

Zakończenie

Wraz z początkiem XXI wieku szczególnie dwa zjawiska zdominowały myślenie o przyszłości: globalizacja (gospodarka, kultura, polityka) i szybki rozwój technologii informacyjnej (szczególnie Internetu). To właśnie Internet stanowi najbardziej wyrazisty przykład globalizacji systemów informacyjnych. Życie w globalnym społeczeństwie informacyjnym jest jednoznaczne z istnieniem człowieka w społeczeństwie sieciowym, gdyż, jak stwierdził chociażby M. Castells, „żyjemy bowiem w galaktyce Internetu”[25]. Internet jest dobrodziejstwem dla wszelkich działań ludzkich, także dla bezprawnych i nieetycznych działań profesjonalnych przestępców, terrorystów, hackerów i crackerów.

Na zakończenie drobna ciekawostka, którą podały dwie agencje prasowe w różnym czasie: Serwis USA Today[26] już w 2008 r., a serwis Russia Today

[25] M. Castells, *Galaktyka Internetu*, Dom Wydawniczy REBIS, Poznań 2003.

[26] Por. w serwisie USA Today: *Your next gadget may come with a pre-installed virus*, http://usatoday30. usatoday.com/tech/news/computersecurity/2008-03-13-factory-installed-virus_n.htm (2.12.2010).

(obecnie RT)[27] w 2013 r. Poinformowały one, że w procesie produkcji urządzeń elektronicznych służących do komunikacji on-line (np. laptopach, tabletach) przeinstalowane są wirusy. Cała wina została zrzucona na producentów urządzeń w Chinach, lecz kto zlecił instalację oprogramowania z wirusami trudno zgadnąć. USA Today przypisują tego typu działania NSA, a RT rządowi chińskiemu. Za tego typu działaniami z pewnością nie stoją tak wyklęci i ścigani domorośli hackerzy.

Bibliografia

Castells M., *Galaktyka Internetu*, Dom Wydawniczy REBIS, Poznań 2003.

Chinese-made laptops' latest feature: Pre-installed viruses, http://rt.com/ news/nitol-microsoft-malware-pre-installed-laptops-054/ (25.04.2013)

Cieślak D.**,** *Internet pełen zombie*, http://www.pcworld.pl/news/70746.html (21.09.2009).

Cieślak D., *W poszukiwaniu szpiegów: 1/3 komputerów zainfekowana*, http://www.pcworld.pl/news/ 67804.html (21.09.2009).

Cynerterroryści w chińskiej armii, „PC World" 4/2013.

Darknet – ciemna strona sieci, „PC World" 11/2013.

Górski S., *Większość spamu generują botnety*, http://www.pcworld.pl/ news/70837.html (23. 09.2009).

Górski S., *Zombie PC: zmora naszych czasów*, http://www.pcworld.pl/news/68560.html (12. 07.2011).

Hacker na państwowej posadzie, „PC World" 4/2013.

Janczyk J, *Racjonalność użytkowania Internetu* [w:] *Racjonalność myślenia, decydowania i działania*, red. L.W. Zacher, Wyd. WSPiZ, Warszawa 2000.

Janczyk J., *„Cienie" Internetu a edukacyjne możliwości zastosowań technologii informacyjnej,* „Transformacje" 1–4/2002.

Janczyk J., *Social problems resulting from information contents of the Internet*, Congress Papers: *Innovations for an e-Society. Challenges for Technology Assessment*, session II – *New Media and Culture*, Berlin 2001.

Janczyk J., *Technical and Organizational Crises in Nets*, "Transformacje" Special Issue 2005–2007.

Landreth B., *Out of the Inner Circle. A Hacker's Guide to Computer Seciurity*, Washington 1985.

N.S.A. Gathers Data on Social Connections of U.S. Citizens, http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?_r=0 (14.12.2013).

Net security threats growing fast, http://news.bbc.co.uk/1/hi/technology/3666978.stm (20. 09.2009).

Parada pomysłów na łamanie zabezpieczeń, „PC World" 10/2013.

Polska armia stawia na hackerów, „PC World" 2/2014.

Sienkiewicz P., Świeboda H., *Niebezpieczna przestrzeń cybernetyczna*, „Transformacje", 1–4 (47–50)/2006.

The New Hacker's Dictionary, http://www.ccil.org/jargon/jargon.html.

Your next gadget may come with a pre-installed virus, http://usatoday30.usatoday.com/tech/news/computersecurity/2008-03-13-factory-installed-virus_n.htm (02.12.2010).

[27] Por. w serwisie RT: *Chinese-made laptops' latest feature: Pre-installed viruses*, http://rt.com/news/nitol-microsoft-malware-pre-installed-laptops-054/ (25.04.2013).