ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 797 STUDIA INFORMATICA NR 33 2013

Hanna Pawlak[*]
Roman Nierebiński[**]
PIB Instytut Łączności, Zakład Systemów i Sieci Bezprzewodowych

WYBRANE ASPEKTY SZKODLIWEGO OPROGRAMOWANIA

Streszczenie

W artykule opisano szkodliwe oprogramowanie jako informatyczne zagrożenie dla funkcjonowania wirtualnego świata. Ukazano różnorodność rodzajową takiego oprogramowania, pewne aspekty ekonomiczne i statystyki szkodliwych programów.

Słowa kluczowe: Internet, wirtualny świat, zagrożenia informatyczne, szkodliwe programy

1. Szkodliwe oprogramowanie jako informatyczne zagrożenie

Poszukiwanie rozwiązań w zakresie dystrybucji informacji w rozproszonym środowisku komputerów zaowocowało powstaniem Internetu. Początkowo były to połączone protokołem IP i komunikujące się ze sobą komputery, dające statyczny Internet z informacjami dostępnymi tylko do odczytu. Pojawienie się sieci WWW, a następnie multimedialnych aplikacji spowodowało, że Internet stał się interaktywny i społeczny, z możliwością nie tylko biernego odczytu informacji, ale i jej współtworzenia. Pełną realizacją tej ostatniej cechy jest wirtualny świat.

W tej wirtualnej przestrzeni Internetu, obok systemów, procesów informatycznych, interfejsów dostępu do Internetu oraz innej infrastruktury, aktywnymi aktorami są także ludzie. Odgrywają oni różne role, także negatywne. Tych, dla których charakterystyczne są właśnie działania negatywne, określa się mianem internetowych przestępców działających w swojego rodzaju podziemiu kompute-

[*] h.pawlak@itl.waw.pl
[**] r.nierebinski@itl.waw.pl

rowym i wpływających na ogólne poczucie zagrożenia związane z korzystaniem z sieci. Wachlarz internetowych przestępstw obejmuje różne obszary, poczynając od powszechnie źle ocenianych społecznie zachowań, a kończąc na aktywności hakerów, którzy łamiąc zabezpieczenia, włamują się do systemów i instalują na komputerach prywatnych oraz firmowych różnego rodzaju szkodliwe oprogramowanie. Dla realizacji założonych scenariuszy wirtualnego świata właśnie to szkodliwe oprogramowanie jest bardzo poważnym informatycznym zagrożeniem.

Ogólna liczba przestępców internetowych skorelowana jest z rosnącą liczbą internautów. Trudno ją jednak dokładnie określić, jednak przyjmując pewne założenia, można ją aproksymować. Obecnie liczba użytkowników Internetu, według ITU (2012), wynosi ponad 2,3 miliarda. Zakładając, że na każde 10 tys. internatów tylko 5 z nich produkuje i wprowadza w przestrzeń Internetu szkodliwy kod, to – przy obecnej liczbie użytkowników sieci – ponad milion ludzi w różnych zakątkach świata można nazwać internetowymi przestępcami (ok. 0,5‰ ogólnej liczby internautów).

Wśród twórców szkodliwego oprogramowania znajduje się grupa określająca się jako badacze. Opracowuje ona nowe sposoby infekowania systemów czy np. zwalczania programów antywirusowych. Często właśnie ich programy jako pierwsze (w celach badawczych) dostają się do nowych systemów operacyjnych i wnikają do nowego oprogramowania sprzętu komputerowego. Nie rozprzestrzeniają oni – z założenia – swoich kodów źródłowych, lecz dzielą się tylko wynikami testów i doświadczeniami z innymi na internetowych forach poświęconych tworzeniu szkodliwego oprogramowania. Jednak, zdaniem autorów, ich poczynania nie są bezpieczne. Nie biorą odpowiedzialności za efekty swoich działań, a ich przedsięwzięcia w określonych okolicznościach mogą stanowić poważne zagrożenie informatyczne. Poza tym, niezależnie od intencji, poprzez nielegalne działania stają się częścią podziemia komputerowego.

Szacowanie celów i rodzajów szkodliwego oprogramowania, a także przewidywanie ataków wymierzonych za jego pomocą ze względu na skalę i charakter sieciowy Internetu nie jest łatwe.

2. Ogólna specyfikacja szkodliwego oprogramowania

Szkodliwe oprogramowanie (ang. *malicious software*, skrót *malware*) to aplikacje, skrypty i inne kody programowe, mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera. Kiedyś klasyfikowało

się je jako „wirus" lub „koń trojański". Z czasem cele i wektory infekcji (sposoby atakowania) ewoluowały – obecnie rodzajowa specyfikacja szkodliwego oprogramowania jest szersza, co pokazuje następujące wyszczególnienie:

1. **Wirus** – niewielki kod, który rozprzestrzenia się z pliku do pliku i z komputera na komputer. Dodaje się do istniejących plików – infekcja następuje w momencie uruchomienia już zainfekowanego pliku (nosiciela). Może być zaprogramowany do usuwania lub uszkadzania danych.
2. **Robak** – rozmnaża się, ale nie infekuje innych plików. Instaluje się na danym komputerze jednorazowo, a potem szuka sposobu rozprzestrzeniania się na inne (np. za pomocą poczty). Tworzy jeden niezależny „egzemplarz" swojego kodu – jest to samodzielny program, posiadający wbudowane różne funkcje destrukcyjne.
3. **Koń trojański (Trojan)** – wygląda jak legalne oprogramowanie, ale po uruchomieniu wykonuje szkodliwe działanie. Nie potrafi się samodzielnie rozprzestrzeniać. Umożliwia zdalne przejęcie pełnej kontroli nad zarażonym komputerem. Instalacja następuje poprzez wykorzystanie luk w zabezpieczeniach lub przy użyciu metod socjotechnicznych (np. uruchomienie przez użytkownika niewinnie wyglądającego programu). Może być „zaszyty" w aplikacji pochodzącej ze strony WWW czy w innym pliku (często w spreparowanym pliku graficznym). Po zainstalowaniu się na zaatakowanym komputerze oczekuje na instrukcje. Oprócz możliwości zdalnego wykonywania komend może np. podsłuchiwać komunikację „ofiary" z innymi komputerami, sterować osprzętem komputera (klawiatura, mysz, CD-ROM, monitor) czy rozsyłać spam.
4. ***Spyware*** – zbiera informacje na rzecz autora kodu lub osób trzecich o użytkowniku, np. na temat odwiedzanych stron WWW, haseł, numerów kart kredytowych itp. Często występuje jako ukryty składnik większego programu, odporny na usuwanie i ingerencję użytkownika komputera. Kod może samowolnie zmieniać ustawienia użytkownika, a także uruchamiać pobrane z sieci pliki. Oprogramowanie tego typu zalicza się do tzw. oprogramowania przestępczego (*crimeware*), czyli takiego, które może być użyte w celu popełnienia przestępstwa kryminalnego (np. kradzież tożsamości).
5. ***Rootkit*** – jedno z najniebezpieczniejszych narzędzi hakerskich. Maskuje obecność uruchomionych szkodliwych programów lub procesów, służących do zdalnego administrowania zaatakowanym systemem. Jest trudny do wykrycia, ponieważ nie występuje jako osobna aplikacja. Jego zainstalowanie jest najczęściej ostatnim krokiem po włamaniu do systemu, w którym prowadzona będzie

ukryta kradzież danych lub infiltracja. Do komputera dostaje się często wraz z aplikacją będącą w rzeczywistości Trojanem. Istnieją specjalizowane *rootkity* dla różnych systemów operacyjnych, w tym dla Microsoft Windows.

6. ***Backdoor*** – umyślna luka w zabezpieczeniach systemu dla późniejszego jej wykorzystania. Ten szkodliwy kod może być pozostawiony przez hakera, który włamał się przez inną lukę w oprogramowaniu o przydatności ograniczonej czasowo bądź przez podrzucenie użytkownikowi Trojana. Pozwala przejąć kontrolę nad zainfekowanym komputerem, umożliwiając wykonanie na nim przestępczych czynności administracyjnych, łącznie ze zmianą danych. Podobnie jak koń trojański podszywa się pod pliki i programy, z których użytkownik często korzysta.
7. ***Keylogger*** – odczytuje i zapisuje naciśnięcia klawiszy użytkownika. Dzięki temu adresy, kody i inne cenne informacje mogą dostać się w niepowołane ręce. Pierwsze programowe *keyloggery* były widoczne w środowisku operacyjnym użytkownika, teraz coraz częściej są procesami niewidocznymi. Obok programowych występują także *keyloggery* w postaci sprzętowej.
8. ***Exploit*** – kod, który do zainfekowania systemu wykorzystuje luki w zabezpieczeniach popularnych aplikacji, np. pakietach biurowych czy w przeglądarkach. Umożliwia bezpośrednie włamanie się do komputera ofiary. Wykorzystywany jest w oprogramowaniu zaprojektowanym do kradzieży danych użytkowników komputerów, a także do tzw. ataków ukierunkowanych np. na infrastruktury informatyczne instytucji (cyberszpiegostwo).
9. ***Ransomware*** – zagraża od 2009 roku. Jego działanie polega na wniknięciu do wnętrza atakowanego komputera i zablokowaniu jego funkcji lub zaszyfrowaniu danych należących do użytkownika. Po zainstalowaniu się program rozpoznaje kraj (po adresie IP), wyświetla we właściwym języku komunikat (z logo lokalnego organu władzy, np. policji) o konieczności przelania na podane konto określonej kwoty np. mandatu (okupu). Często dokonanie wpłaty nie zmienia sytuacji i jedynym ratunkiem jest usunięcie szkodnika. Zagrożenie występuje najczęściej na stronach WWW – program dostaje się do komputera po kliknięciu przez użytkownika np. zainfekowanej jego kodem reklamy. Zdarza się również dystrybucja za pośrednictwem poczty e-mail.

Często szkodliwe oprogramowanie ma postać hybrydową, łącząc funkcjonalności kilku rodzajów szkodliwego kodu i stanowiąc tym samym mieszane zagrożenie. Może np. wysyłać automatycznie wiadomości z osadzonym Trojanem i załącznikiem zawierającym innego rodzaju zagrożenia.

Sieci botnet

Do przeprowadzania ataków sieciowych hakerzy posługują się różnymi metodami, w tym często z użyciem tzw. botnetu lub inaczej sieci zombie. Botnet jest to sieć złożona z komputerów zainfekowanych szkodliwym oprogramowaniem, umożliwiającym sprawowanie nad nimi zdalnej kontroli. Właściciel botnetu może zarządzać swoją siecią anonimowo z dowolnego miasta, państwa lub kontynentu. O zainfekowanym komputerze w takiej sieci mówi się, że jest to komputer zombie i jego właściciel zwykle nie ma świadomości, że jest on używany do przestępczych działań. Większość komputerów zombie to komputery użytkowników domowych. Szacuje się, że ich całkowita liczba wynosi kilka milionów i stale rośnie. Już niewielki botnet, składający się z około 3 tys. komputerów, może stać się przyczyną poważnych zagrożeń, jeśli tylko zainfekowane komputery dysponują szybkim połączeniem z Internetem.

Właściciele botnetów rozbudowują swoje sieci, rozsyłając spam ze szkodliwymi załącznikami i odnośnikami. Często też wynajmują je w całości lub ich część za opłatą. Botnety mogą być użyte do przeprowadzania wielu działań przestępczych, poczynając od wysyłania spamu, aż do koordynowania ataków typu DoS lub DDoS.

DoS, atak odmowy usługi (ang. *Denial-of-Sernice*), ma na celu utrudnienie lub całkowite uniemożliwienie działania zasobów Internetu, szczególnie serwerów i stron WWW. Typowy atak DoS polega na przeciążeniu określonego serwera nieustającymi żądaniami i fałszywymi próbami skorzystania z usługi. Powoduje to duże spowolnienie jego działania (WWW usługi otwiera się wolno) albo całkowitą awarię i blokadę usługi (WWW usługi nie działa).

DDoS, atak rozproszonej odmowy usługi (ang. *Distributed Denial of Service*), jest odmianą DoS. Atak przeprowadzany jest na sygnał z wielu zainfekowanych komputerów jednocześnie, a jego celem jest uniemożliwienie lub zawieszenie działania atakowanego systemu lub usługi sieciowej. Są one groźną bronią w rękach internetowych przestępców wymuszających dość często okupy za odstąpienie od ataku. Na szantaż szczególnie narażone są firmy, w których przychody wynikają bezpośrednio z ich aktywności w Internecie i gdzie przerwa w działaniu systemów jest źródłem poważnych strat finansowych (np. serwisy aukcyjne, e-sklepy itp.).

Ataki na usługi używane są także dość często w działaniach ukierunkowanych na serwery rządowe. Atak na komputer rządowy kraju X może nastąpić bezpośrednio z komputera w kraju Y, zarządzanego z użyciem komputera znajdującego się w kraju Z.

3. Aspekt ekonomiczny szkodliwego oprogramowania

Obecnie tworzeniem szkodliwego oprogramowania w większości zajmują się profesjonaliści. Największym niebezpieczeństwem dla społecznej przestrzeni Internetu są ci, którzy sprzedają swoje usługi lub produkty. Coraz częściej organizują się oni w hierarchiczne grupy, wzorując się na legalnych modelach biznesowych. Według firmy Fortinet (2013), przykładowe stawki za usługi takich firm na początku 2013 roku kształtowały się następująco:

– usługi konsultingowe, np. założenie botnetu – 350–400 $,
– infekowanie/rozprzestrzenianie szkodliwego oprogramowania – 100 $ za 1000 instalacji,
– usługi realizowane przez botnety: atak DDoS – 535 $ za 5 godzin dziennie przez tydzień, spam przez e-mail 40 $ za 2 tys. e-maili, spam przez WWW 2 $ za 30 postów,
– zapewnienie jakości, testowanie wykrywalności skanerów itp. – 10 $ miesięcznie,
– szkodliwe programy sieciowe – nawet do 5000 $,
– łamanie zabezpieczeń –1 $ za 1000 złamanych kodów (wykonywane przez zatrudnionych ludzi).

Koszt związany z rozpoczęciem kariery internetowego przestępcy, według analityków amerykańskiej firmy TrendMicro (2013), jest w zasadzie niewielki, bowiem np. kod źródłowy Trojana można nabyć już za około 50 $, zaś instalacja wirusa Zeus, służącego do zdalnej kradzieży danych, na komputerze nabywcy wynosi 35 $, a na komputerze sprzedawcy – 40 $. Wyższe ceny dotyczą zazwyczaj bardziej wyszukanych narzędzi i rozwiązań technicznych.

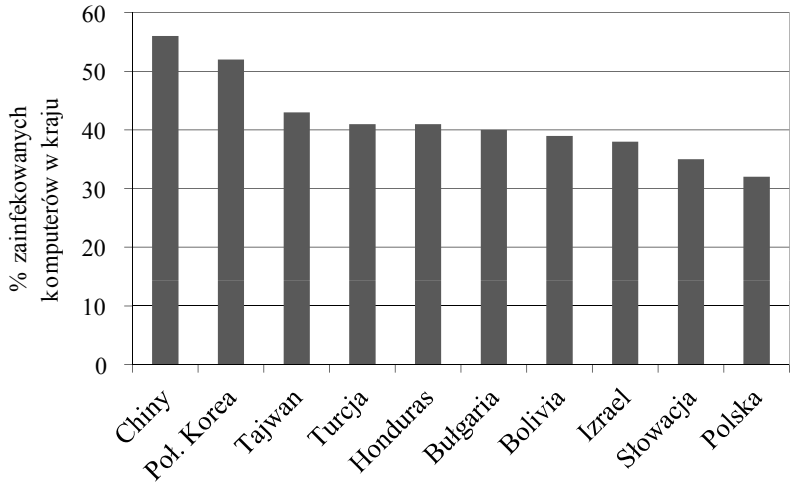
Analitycy tematu wskazują, że działalność internetowych przestępców współtworzy środowisko, w którym coraz większego znaczenia nabiera zysk ekonomiczny. Z drugiej strony legalni uczestnicy wirtualnych światów w związku z atakami na zasoby sieciowe ponoszą coraz większe koszty. Najbardziej uwidacznia się to tam, gdzie prowadzi się rachunek strat i zysków ekonomicznych – wśród biznesowych użytkowników Internetu.

Ponemon Institute na zlecenie HP przeprowadza cykliczne badania szacujące straty firmowe wywołane przestępczością internetową. Raport z ostatniego badania (Ponemon, 2012) pokazuje, że roczne koszty likwidacji skutków cyberataków ponoszone przez amerykańskie instytucje systematycznie rosną. W 2012 roku wyniosły one 8,9 mln $, co oznacza wzrost o 6% w stosunku do 2011 roku i o 38% do 2010 roku. Uwidocznił się także systematyczny wzrost liczby ataków.

W 2012 roku miały miejsce średnio 102 udane ataki na tydzień wobec 72 na tydzień w 2011 roku i 50 w 2010 roku. Ataki stają się coraz bardziej wyrafinowane, o czym świadczy wyraźnie wzrastający czas usuwania ich skutków. W 2012 roku wymagało to średnio 24 dni, podczas gdy w 2011 i 2010 (odpowiednio) 18 i 14 dni. Stosunkowo największe straty ekonomiczne powodują niezmiennie internetowe przestępstwa związane z takimi atakami, jak (w kolejności): szkodliwe oprogramowanie, blokowanie usług, kradzież informacji, przejęcie kontroli nad urządzeniami, a także ataki dokonywane przez osoby działające wewnątrz firmy. W sumie odpowiadają one za ponad 78% rocznych kosztów likwidacji skutków internetowej przestępczości ponoszonych przez firmy w USA.

4. Statystyki szkodliwego oprogramowania

Statystyk szkodliwego oprogramowania stosunkowo najczęściej dostarczają firmy tworzące programowe narzędzia do jego zwalczania. Ich źródłem są obserwacje komputerów klientów, indywidualne zgłoszenia incydentów, a także szeroko zakrojone analizy rynku szkodliwego oprogramowania.

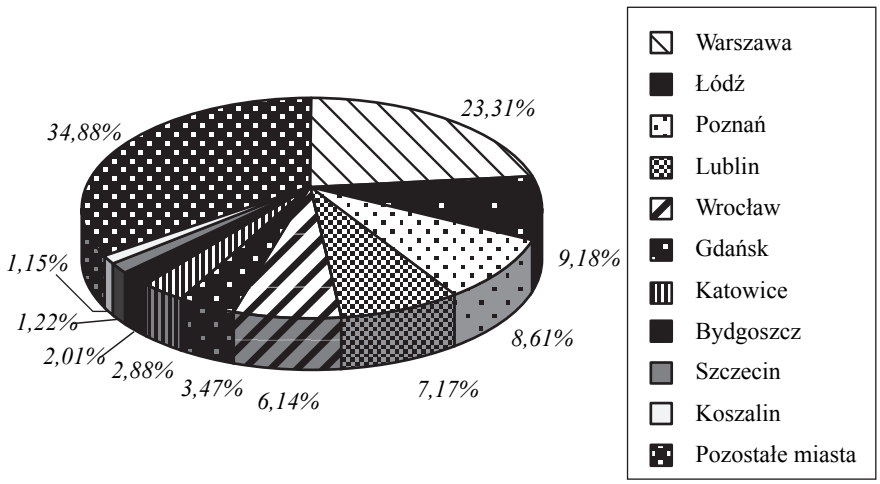


Rysunek 1. Kraje najbardziej zainfekowane szkodliwym oprogramowaniem w 2012 roku
Źródło: opracowanie własne na podstawie rocznego raportu PandaLab (2012).

W 2012 roku, według rocznego raportu amerykańskiej firmy PandaLab (2012), powstało ogółem 27 mln nowych szkodliwych programów (74 tys. dzien-

nie). W większości przypadków (3/4) były to Trojany, których liczba w obiegu od lat stale rośnie. W 2010 roku stanowiły one 56% wszystkich szkodliwych programów, w 2011 roku – 73,3%, a w 2012 roku już 76,6%. W następnej kolejności były to robaki i wirusy. Obserwowane od lat zjawisko geograficznego rozproszenia infekcji utrzymuje się. Na rysunku 1 pokazano 10 państw świata, w których w 2012 roku wyróżniająco duży odsetek krajowych komputerów został zainfekowany szkodliwym oprogramowaniem. W grupie tej znalazła się także Polska (32% zainfekowanych komputerów).

Zjawisko rozproszenia infekcji występuje również w skali lokalnej, różnicując poszczególne regiony w danym kraju. Na rysunku 2 zaprezentowano 10 najczęściej atakowanych szkodliwym oprogramowaniem miast w Polsce według stanu na lipiec 2010 roku, na podstawie badań firmy KasperskyLab (2010).



Rysunek 2. Najczęściej infekowane polskie miasta
Źródło: KasperskyLab (2010).

Na ilustracji widoczne jest, że najczęściej infekowane są komputery w Warszawie (23,3%) i to z dużą przewagą w stosunku do kolejnych, bardzo zagrożonych szkodliwym oprogramowaniem polskich miast.

Firma Norton (2012) ogłosiła raport na temat przestępczości internetowej w 2012 roku, który powstał na podstawie danych zebranych od dorosłych respondentów z 24 krajów, w tym z Polski. Według tego raportu, w ciągu roku z internetowymi przestępstwami zetknęło się ogółem 556 mln osób (w tym

7,2 mln z Polski). Każdego dnia szkodliwym oprogramowaniem atakowanych było około 1,5 mln komputerów, co oznacza średnio 18 ataków na sekundę. Z raportu jasno wynika, że wielu użytkowników Internetu nie zdaje sobie sprawy z obecnych form internetowych przestępstw i skutków szkodliwego oprogramowania dla komputera czy jego zasobów. Aż 40% dorosłych internautów (w Polsce 46%) nie wie, że szkodliwe oprogramowanie może działać w ukryciu, w sposób niezauważalny dla użytkownika komputera. Dodatkowo uzyskane w badaniach dane potwierdzają wyodrębniający się silny trend wzrostu liczby przestępczych incydentów w społecznościowych sieciach i ataków na systemy mobilnych urządzeń.

Społecznościowe sieci są nieodłącznym elementem wirtualnego świata, a najpopularniejsze z nich posiadają miliony stałych użytkowników. Według badania zrealizowanego w 2012 roku przez firmę Harris Interactive na zlecenie KasperskyLab (KasperskyLab, Harris Interactive, 2012), w USA, Europie i Rosji portale społecznościowe regularnie odwiedza aż 56% internautów. Wyniki dowodzą, że pod względem sposobu utrzymywania kontaktów komunikacyjne usługi sieci społecznościowych są prawie równie popularne jak poczta e-mail (zajmują 2. miejsce). Przez internetowych przestępców wykorzystywane są już oba kanały komunikacji. Aż 27% ankietowanych wskazało, że otrzymało różne podejrzane odsyłacze i załączniki w wiadomościach wysłanych zarówno za pośrednictwem portali społecznościowych, jak i programów poczty e-mail. Większość badanych użytkowników portali świadoma jest zagrożeń, jakie mogą wiązać się z sieciami społecznościowymi. Ponad połowa z nich (56%) obawia się ujawniać istotne dla nich dane (numer telefonu, adres itp.), a 63% nie dodaje do grona swoich znajomych osób, których nie zna osobiście, podczas gdy 68% z reguły nie klika odsyłaczy od osób, o których nigdy nie słyszeli. Środki te, mimo że są pewnym zabezpieczeniem, nie zapewniają pełnej ochrony przed infekcją i utratą danych – internetowi przestępcy często uzyskują dostęp do konta użytkownika i rozprzestrzeniają zainfekowane szkodliwym oprogramowaniem odsyłacze do wszystkich jego przyjaciół. Dodatkowo, chociaż większość ankietowanych regularnie komunikuje się z innymi za pośrednictwem portali społecznościowych z wykorzystaniem komputerów (61%), to używanie w tym celu smartfona (47%) lub tabletu (46%) wcale nie jest takie małe. Te nowe interfejsy charakteryzują się jeszcze stosunkowo niskim poziom ochrony przed szkodliwym oprogramowaniem, co może łatwo doprowadzić nie tylko do kradzieży informacji dotyczących konta, ale również do poważniejszych szkód.

Podsumowanie

1. Obecne środowisko twórców szkodliwego oprogramowania jest w pełni profesjonalne i nastawione na zysk.
2. Szkodliwe oprogramowanie szybko nie zaniknie, szczególnie, że jest możliwość zarobienia na tym pieniędzy, a antywirusowe aplikacje powstają w zasadzie w reakcji na już zaistniałe zagrożenie.
3. Średni globalny poziom zagrożenia internetowego wzrasta. Według analityków firmy KasperskyLab (2012), w 2012 roku kształtował się na poziomie 34,7% i był wyższy o 2,4% niż w 2011 roku. W ciągu roku jeden komputer w sieci na trzy był celem ataku przynajmniej raz w roku.
4. Twórcy systemów operacyjnych i aplikacji muszą być szczególnie uwrażliwieni na słabe punkty ich oprogramowania. Konieczność taką potwierdza np. to, że w 2012 roku – na podstawie rocznego raportu firmy KasperskyLab (2012) – na trzecim miejscu pod względem wystąpień znalazły się *exploity* dla systemu Windows i przeglądarki Internet Explorer, które wykorzystywały luki wykryte jeszcze w 2010 roku, związane między innymi z niepoprawnym przetwarzaniem plików JPEG.
5. Każdy użytkownik komputera musi nauczyć się, jak reagować na ciągle zmieniające się środowisko szkodliwego oprogramowania, przede wszystkim instalując ochronne oprogramowanie i na bieżąco aktualizując system operacyjny oraz aplikacje.
6. Szkodliwe oprogramowanie narusza integralność aplikacji społecznej przestrzeni Internetu, a także bezpieczeństwo oraz prywatność uczestników tego świata i wobec tego jego autorzy w każdym przypadku – niezależnie od intencji – powinni być ścigani prawem.
7. Zapewnienie bezpieczeństwa, prywatności oraz zaufania w sieci jest działaniem priorytetowym, szczególnie wobec zbliżającego się Internetu Rzeczy (*Internet of Things* IoT). Otaczające nas wszelakiego rodzaju rzeczy, stanowiąc część Internetu, będą się ze sobą komunikować z wykorzystaniem protokołu IP w społecznym, zawodowym i prywatnym interesie ludzi i będzie niedopuszczalne, by wskutek działania szkodliwego oprogramowania zaczęły np. wysyłać nieprawdziwe sygnały (Pawlak i Nierebiński, 2010).

Bibliografia

Fortinet (2013), *Cyberprzestępczość w 2013 roku*, raport, www.fortinet.pl (dostęp luty 2013).

ITU (2012), *Key statistical highlights: ITU data release June 2012*, www.itu.int/ITU-D/ict/statistics/material (dostęp wrzesień 2012).

KaspersakyLab (2010), *Szkodliwe programy w Polsce - lipiec 2010*, raport, www.viruslist.pl/ (dostęp styczeń 2012).

KaspersakyLab (2012), *Kaspersky Security Bulletin 2012***,** www.kaspersky.com (dostęp luty 2013).

KasperskyLab, Harris Interactive (2012), *Kaspersky lab consumer_survey*, raport, www.kaspersky.com/downloads/pdf/kaspersky_lab_consumer_survey_report_eng_final.pdf (dostęp luty 2013).

Norton (2012), *2012 Norton Cybercrime Raport*, raport, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf (dostęp luty 2013).

PandaLab (2012), *2012 Annual Report PandaLabs*, raport, http://press.pandasecurity.com/press-room/reports/ (dostęp styczeń 2013).

Pawlak H., Nierebiński R. (2010), *Skutki społeczno-ekonomiczne Future Internet*, raport, www.itl.waw.pl (dostęp luty 2013).

Ponemon (2012), *2012 Cost of Cyber Crime Study: United States*, raport, www.ponemon.org (dostęp luty 2013).

TrendMicro (2013), informacje prasowe, www.trendmicro.pl/ (dostęp luty 2013).

SOME ASPECTS OF MALICIOUS SOFTWARE

Summary

This work describes the malware as a threat to the functioning of the computer virtual world. It shows a variety of generic such software, economic aspects of such programs and some statistics about them.

Translated by Hanna Pawlak

Keywords: Internet, virtual world, computer threats, malware