Technologie cyfrowe

Artur Kalinowski

Zakład Cząstek i Oddziaływań Fundamentalnych

Pasteura 5, pokój 4.15

Artur.Kalinowski@fuw.edu.pl

Semestr letni 2014/2015

Polski wkład w świat cyfrowy

Kapitalizacja: wartość spółki giełdowej szacowana jako iloczyn liczby akcji i ich kursu.

Maj 2015: kapitalizacja CD Projekt Red: 2.2 mld PLN

kapitalizacja Jastrzębskiej Spółki Węglowej: 1.8 mld PLN

Reklama gry Wiedźmin 3 na Times Square, NY, USA

Polski wkład w świat cyfrowy

Listopad 2014: premiera gry „This War of Mine” wyprodukowanej przez studio 11BIT z Warszawy. Po premierze akcje spółki wzrosły o 500%. **96% graczy, używających pewnej platformy cyfrowej dystrybucji gier uważa grę za dobrą.**

11BIT - notowania spółki

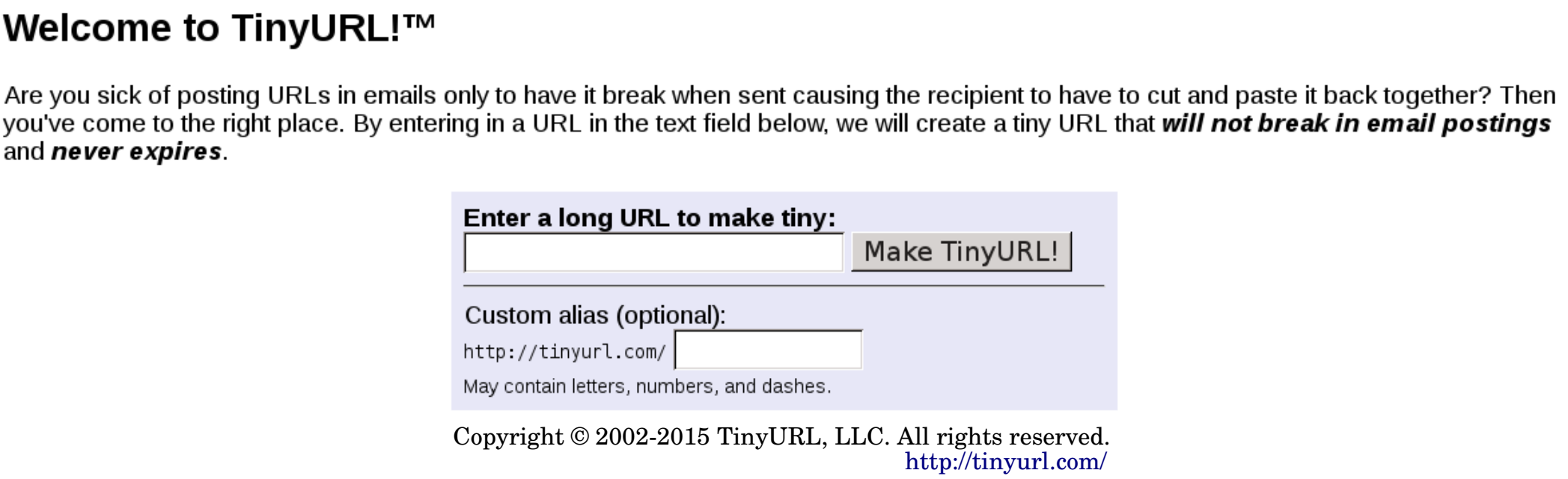
Rynek notowań:	**New Connect**
Kurs odniesienia:	**11,00 zł** (14-09-11)
Data początkowa:	**2014-09-12**
Data końcowa:	**2015-05-18**
Zmiana:	**477,27%**
Zmiana:	**52,50 zł**
Minimum:	**8,50 zł** (14-10-20)
Maksimum:	**82,82 zł** (15-02-13)
Średni:	**50,57 zł**

Usługi internetowe: aplikacje

Dokumenty: dokumenty biurowe przechowywane na dyskach zdalnych mogą być edytowane przez wiele osób jednocześnie. Pozwala to na wspólną pracę, bez konieczności fizycznego spotykanie się współpracujących osób.

Usługi internetowe: skracanie URL

Skracanie adresów URL: usługa polegająca na zamianie długich adresów URL na skrócone wersje, łatwiejsze do przekazania innym osobom. Usługodawca prowadzi bazę danych w której zapisuje pełny i skrócony URL. Użytkownik, wpisując krótką wersję komunikuje się z serwerem usługodawcy, który przekierowuje go na stronę wskazywaną przez pełny URL. Przykładowe serwisy: bit.ly, goo.gl, tinyurl.com



Usługi internetowe: skracanie URL

Google url shortener

Paste your long URL here:

Google

brain.fuw.edu.pl/edu/Slajdy_z_wyk%C5%82ad%C3%B3w_2C

Shorten URL

All goo.gl URLs and click analytics are public and can be accessed by anyone.

Clicks for the past: two hours | day | week | month | **all time**

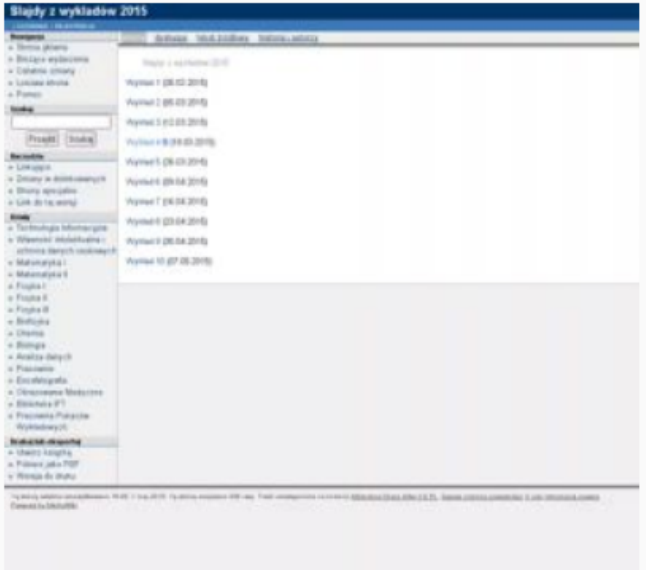
	LONG URL	CREATED	SHORT URL		CLICKS
☐	brain.fuw.edu.pl/edu/Slajdy...	0 minute ago	goo.gl/DLzWdm	Details	0

Hide Hidden URLs remain public, but are removed from your history 1 - 1 of 1

http://goo.gl/DLzWdm

0 minute ago - details

http://brain.fuw.edu.pl/edu/Slajdy_z_...



©2012 Google https://goo.gl/

Bezpieczeństwo w internecie

Bezpieczeństwo: stałe połączenie i korzystanie z internetu wystawia użytkowników na szereg zagrożeń. Zagrożenia można luźno podzielić na dwie kategorie:

• **związane z obecnością w internecie** – zagrożenia typu wirusy, kradzież tożsamości (od numeru IP/MAC po tożsamości w świecie cyfrowym), przejęcie komputera

• **związane z wymianą danych** – zagrożenia kradzieży poufnych danych wymienianych drogą cyfrową, np. kodów do kanałów dostępu do zasobów (haseł, identyfikatorów)

Świadome korzystanie z technologii cyfrowych wymaga znajomości możliwych zagrożeń, oraz podejmowania co najmniej podstawowych środków zaradczych.

Phishing

Phishing: próba wyłudzenia poufnych informacji. Wykradanie poufnych danych zachodzi zwykle przy użyciu poczty internetowej, lub portali społecznościowych. Złodziej podszywa się pod zaufaną osobę lub instytucję i prosi o podanie poufnych danych.

użytkownik cb-allegro3 <cb-allegro3@o2.pl> napisał:

W sprawie przestępstwa na serwisie Allegro

Bardzo prosimy o reakcję na poniższego e-maila najpóźniej w przeciągu 4 godzin od jego odczytania.

Witam serdecznie,

Niniejszą wiadomość otrzymują Państwo ponieważ w dniu 09.05.2011, osoba podpisująca się Państwa nazwą użytkownika Allegro dokonała **nielegalnego** zakupu towarów o łącznej wartości 8,400 PLN za pośrednictwem serwisu aukcyjnego Allegro. Z zebranych przez nas oraz **przez policję** dowodów wynika, że oszust, za pośrednictwem Państwa konta Allegro, opłacił towar za pomocą karty kredytowej po przez system Płatności Allegro, a następnie poprosił sprzedawcę o wysyłkę towaru na pewien adres w Warszawie, który obecnie jest sprawdzany przez odpowiednie służby.

Chcielibyśmy pomóc Państwu rozwiązać tę sytuację, gdyż jesteśmy świadomi faktu, iż oszustwa mogła dokonać osoba trzecia po uzyskaniu nielegalnego dostępu do Państwa konta. W tym celu jednak jesteśmy zmuszeni przeprowadzić dokładną weryfikację Państwa tożsamości, aby upewnić się, czy dane użyte przez oszusta podczas dokonania kradzieży faktycznie nie należą do Państwa. W tym celu prosimy o **niezwłoczną** odpowiedź na niniejszego e-maila oraz uwzględnienie w treści następujących informacji:

- Aktualny adres zamieszkania
- Data urodzenia
- Potwierdzenie, czy użyczali Państwo dostępu do swojego konta osobom trzecim
- Numer Państwa karty kredytowej / debetowej
- Data ważności w/w karty
- Kod CVV w/w karty (3 cyfrowy kod znajdujący się z tyłu karty obok jej numeru)
- Pełne imię oraz nazwisko posiadacza karty

W najbliższym czasie prawdopodobnie skontaktuje się z Państwem telefonicznie bądź osobiście przedstawiciel stołecznej policji - bardzo prosimy o udzielenie im wszelkich informacji o które mogą prosić.

Przydatne informacje

- Zapraszamy również do zapoznania się z Regulaminem Allegro.pl

Phishing

Phishing: próba wyłudzenia poufnych informacji. Wykradanie poufnych danych zachodzi zwykle przy użyciu poczty internetowej, lub portali społecznościowych. Złodziej podszywa się pod zaufaną osobę lub instytucję i prosi o podanie poufnych danych.

Przykładowy mail:

From: mBank [mailto:no-reply@eurometrex.org]
Sent: Tuesday, March 24, 2015 11:29 AM
Subject: [spam] Dostep do serwisu zostal zablokowany

Zablokowany dostęp do serwisu w Internecie.

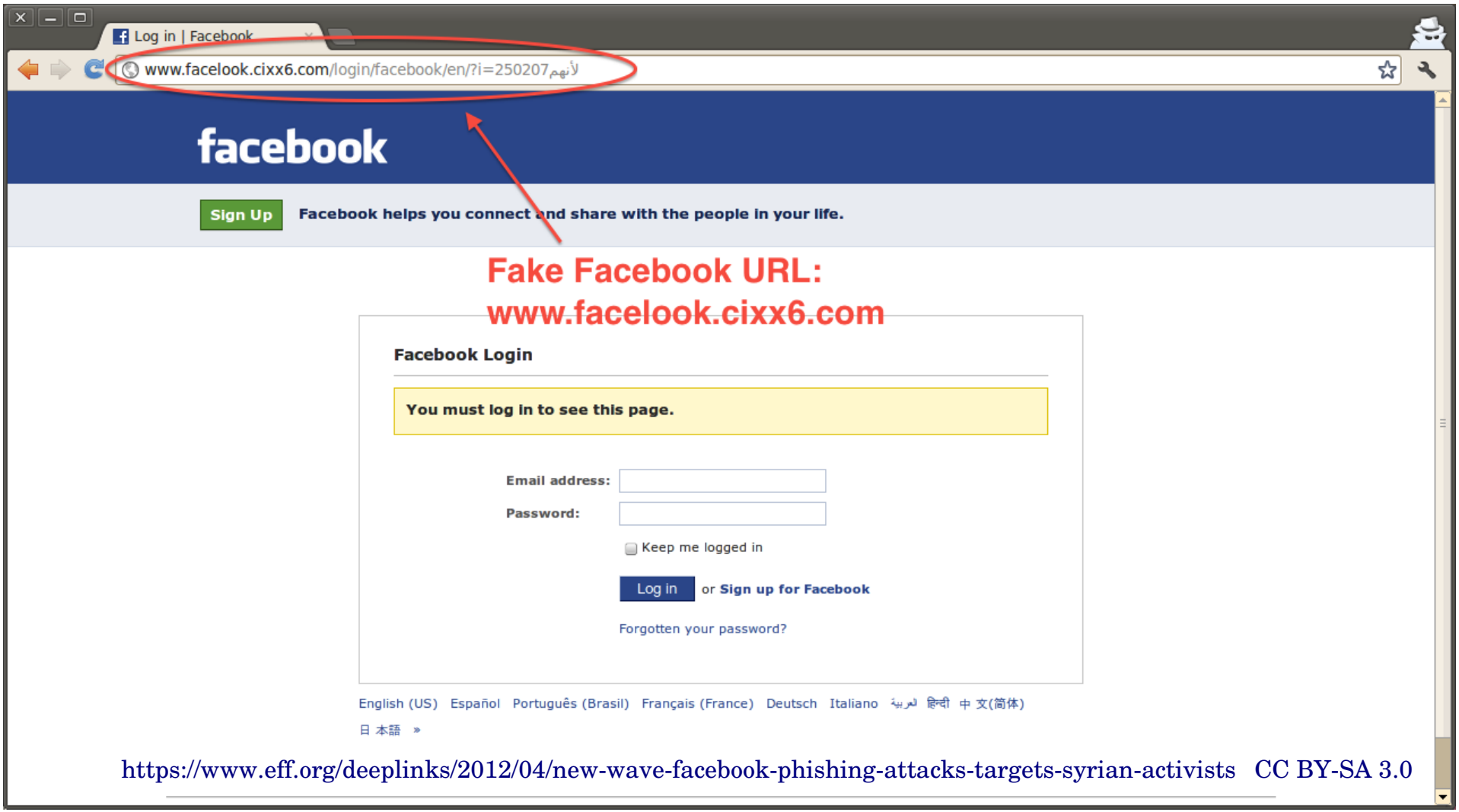
Dostęp do serwisu został zablokowany. Aby przywrócić kliknij w link:

https://online.mbank.pl/pl/Login

http://www.mbank.pl/aktualnosci/post,6228,mbank-ostrzega-klientow-przed-nowym-zagrozeniem-sugerujacym-blokady-rachunkow.html

Phishing

Phishing: próba wyłudzenia poufnych informacji. Wykradanie poufnych danych może też zajść przez **skierowanie do fałszywego portalu logowania.**



https://www.eff.org/deeplinks/2012/04/new-wave-facebook-phishing-attacks-targets-syrian-activists

Phishing: zabezpieczenie

• żaden administrator jakiegokolwiek serwisu WWW czy pocztowego nie będzie żądał od użytkownika podania w odpowiedzi na mail jego hasła logowania. Obecność takiego żądania jest bezbłędną wskazówką, że mamy do czynienia z fałszywką.

• nie można ufać treści emaila na podstawie wyświetlanego przez aplikację pocztową adresu nadawcy. Jest on równie łatwy do sfałszowania, jak adres nadawcy na kopercie listu papierowego - nie jest on (zazwyczaj) w żaden sposób weryfikowany.

• do serwisów zabezpieczonych logowaniem należy wchodzić jedynie poprzez odręczne wpisanie adresu (np. usosweb.fuw.edu.pl) w okienku adresowym przeglądarki

http://www.fuw.edu.pl/informacje-okwf/news0792.html

Pharming

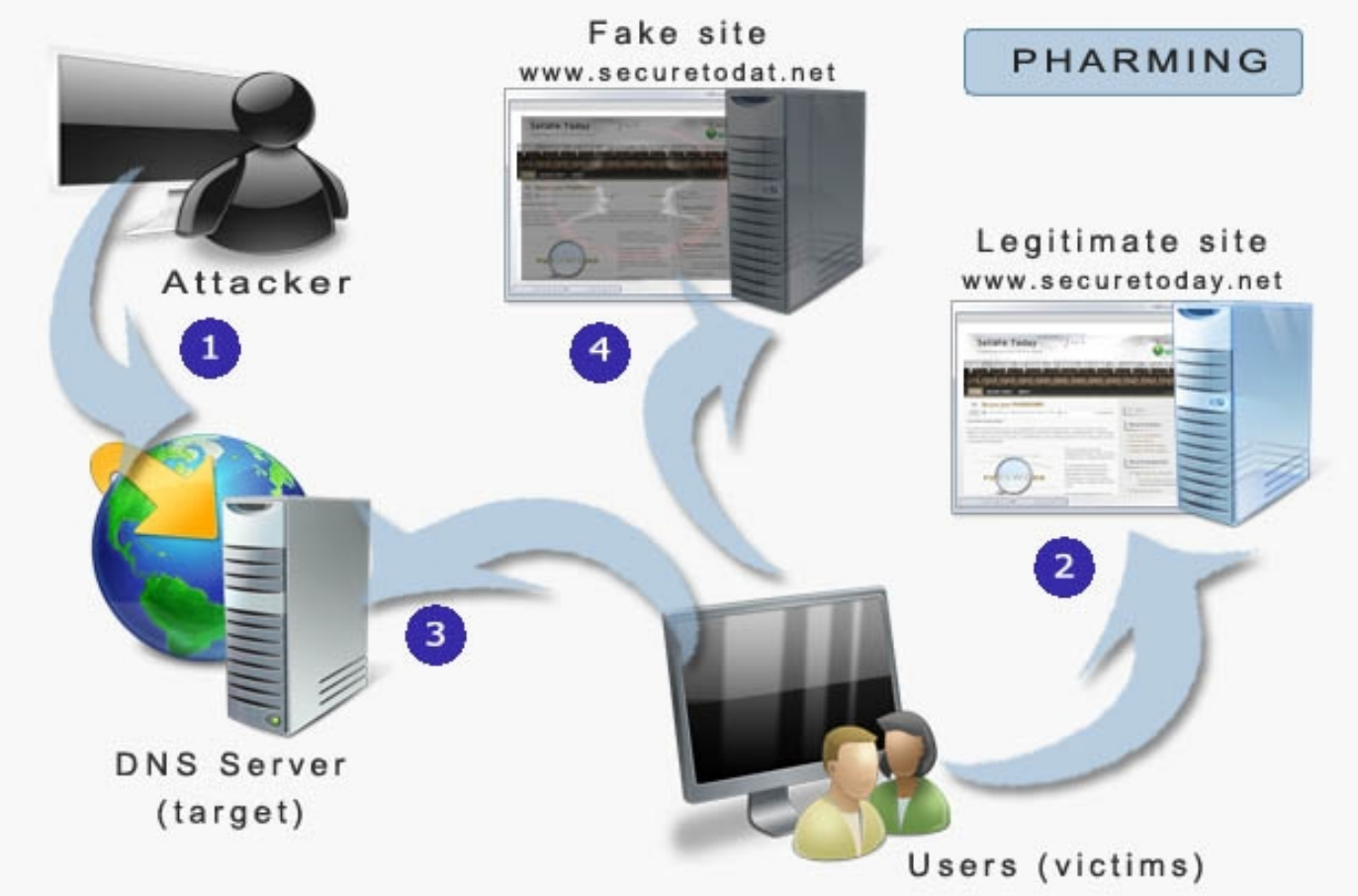
Pharming: próba wyłudzenia poufnych informacji przez przekierowanie użytkownika na fałszywą stronę, **nawet jeśli ten wpisał poprawny URL**.

• atak może polegać na sfałszowaniu bazy DNS (zatruciu (*ang. poisson*) serwera DNS), w ten sposób, że zaufany adres w formacie DNS (np. www.mojBank.com) zostaje skojarzony z adresem IP serwera złodzieja

• atak może polegać na instalacji na komputerze lub trasowniku użytkownika programów (typu trojan) fałszujących powiązania DNS – IP rozwiązywane przez wysyłaniem zapytań do zewnętrznego serwera DNS

Pharming

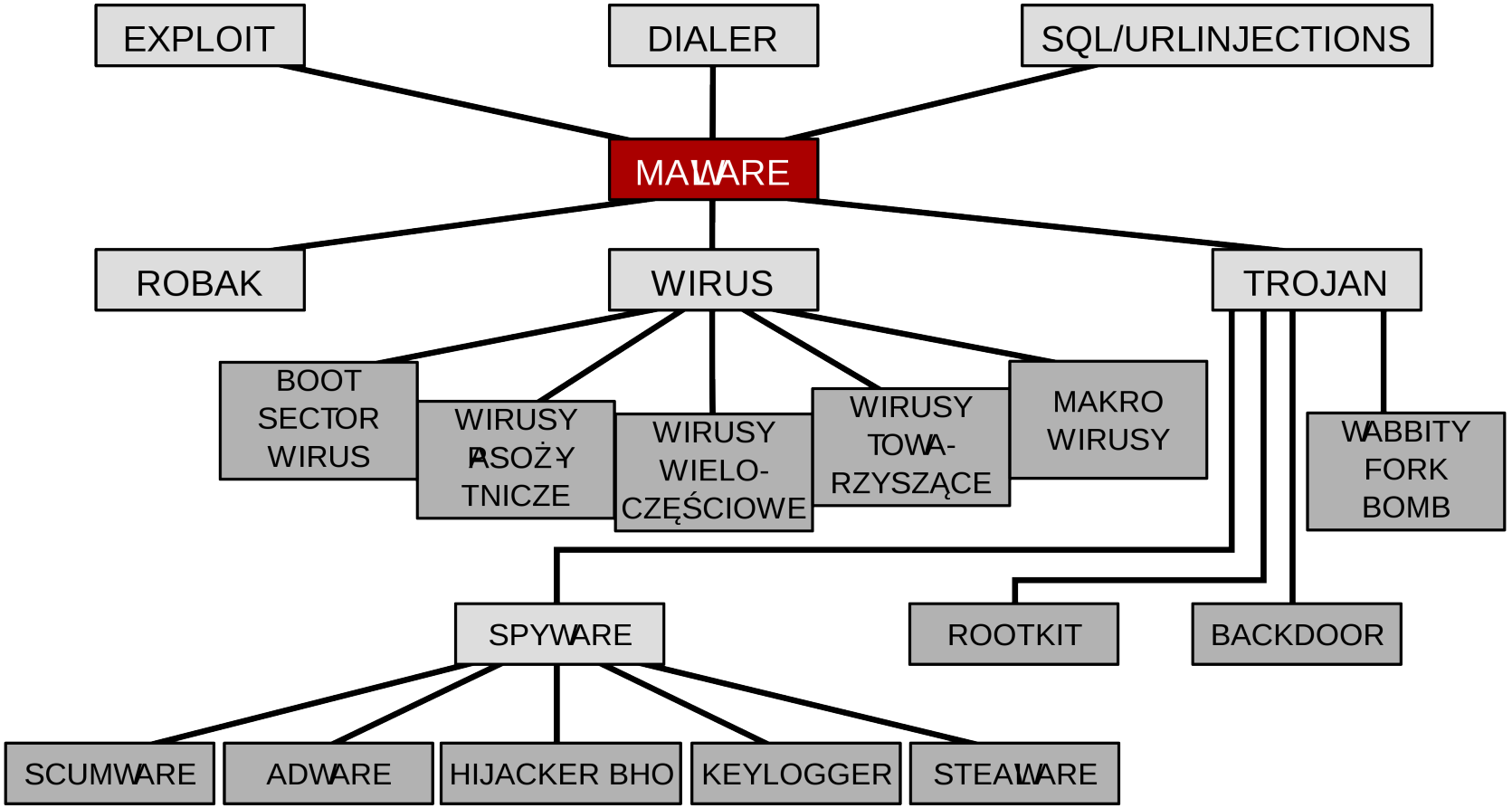
Pharming: próba wyłudzenia poufnych informacji przez przekierowanie użytkownika na fałszywą stronę, **nawet jeśli ten wpisał poprawny URL**.



http://www.securetoday.net/tag/pharming/

Malware

Złośliwe oprogramowanie (ang. malicious software, malware): programy komputerowe mające na celu szkodliwe działania na rzecz użytkownika i/lub innych użytkowników przez użycie sprzętu należącego do użytkownika.



Rodzaje malware

Wirus: program lub fragment wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika.

Robak (*ang. worm*): złośliwe oprogramowanie podobne do wirusów, rozmnażające się tylko przez sieć. W przeciwieństwie do wirusów nie potrzebują programu „żywiciela". Często powielają się pocztą elektroniczną.

Trojan: nie rozmnaża się jak wirus, ale jego działanie jest równie szkodliwe. Ukrywa się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku zgodnego z jego nazwą, trojan wykonuje operacje w tle szkodliwe dla użytkownika, np. otwiera port komputera, przez który może być dokonany atak włamywacza

http://pl.wikipedia.org/wiki/Złośliwe_oprogramowanie

Tylne drzwi

Tylne drzwi (*ang. backdoor*): luka w ograniczeniach dostępu do zasobów, która może być wykorzystana do przejęcia kontroli nad komputerem. Często luka jest tworzona przez włamywaczy (*ang. hacker*), którzy korzystają z błędów w oprogramowaniu używanym przez użytkownika.

historia z 2003 roku: w kodzie jądra linuksa odkryto następujące dwie linie, które były dodane do repozytorium przez do tej pory nieznaną osobę:

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
        retval = -EINVAL;
```

Zamierzony błąd w warunku instrukcji „*if*” przyznawał użytkownikowi uprawnienia administratora (użytkownika *root* w systemie linux).

Tylne drzwi

Tylne drzwi (*ang. backdoor*): jedną z najbardziej popularnych luk używanych przez włamywaczy jako tylne drzwi są domyślne hasła i identyfikatory dostępu do urządzeń, w szczególności trasowników bezprzewodowych.

D-Link Router Default Passwords:

Vendor – Model	Access Type	Username	Password
DI624 – D-LINK	HTTP	admin	password
d-link – 504g adsl router	HTTP	admin	admin
DLINK – 604	Multi	n/a	admin
d-link – ads500g	HTTP	admin	admin
dlink – adsl	HTTP	admin	admin
D-Link – D-704P	Multi	admin	(none)
D-Link – D-704P	Multi	admin	admin

Tylne drzwi

Tylne drzwi (*ang. backdoor*): jedną z najbardziej popularnych luk używanych przez włamywaczy jako tylne drzwi są domyślne hasła i identyfikatory dostępu do urządzeń, w szczególności trasowników bezprzewodowych.

Nazwa użytkownika i hasło do konfiguracji routera/modemu z funkcją routera

Jakie są nazwa użytkownika i hasło routera lub modemu z funkcją routera w usłudze Bezprzewodowego Internetu [redacted]

Obydwa rodzaje urządzeń są wstępnie przygotowane przez producentów do pracy, więc dla standardowego użytkowania nie jest wymagana ich dalsza konfiguracja. Jeśli jednak zajdzie potrzeba zalogowania się na modem Thomson, Technicolor, Cisco lub router Netgear należy:

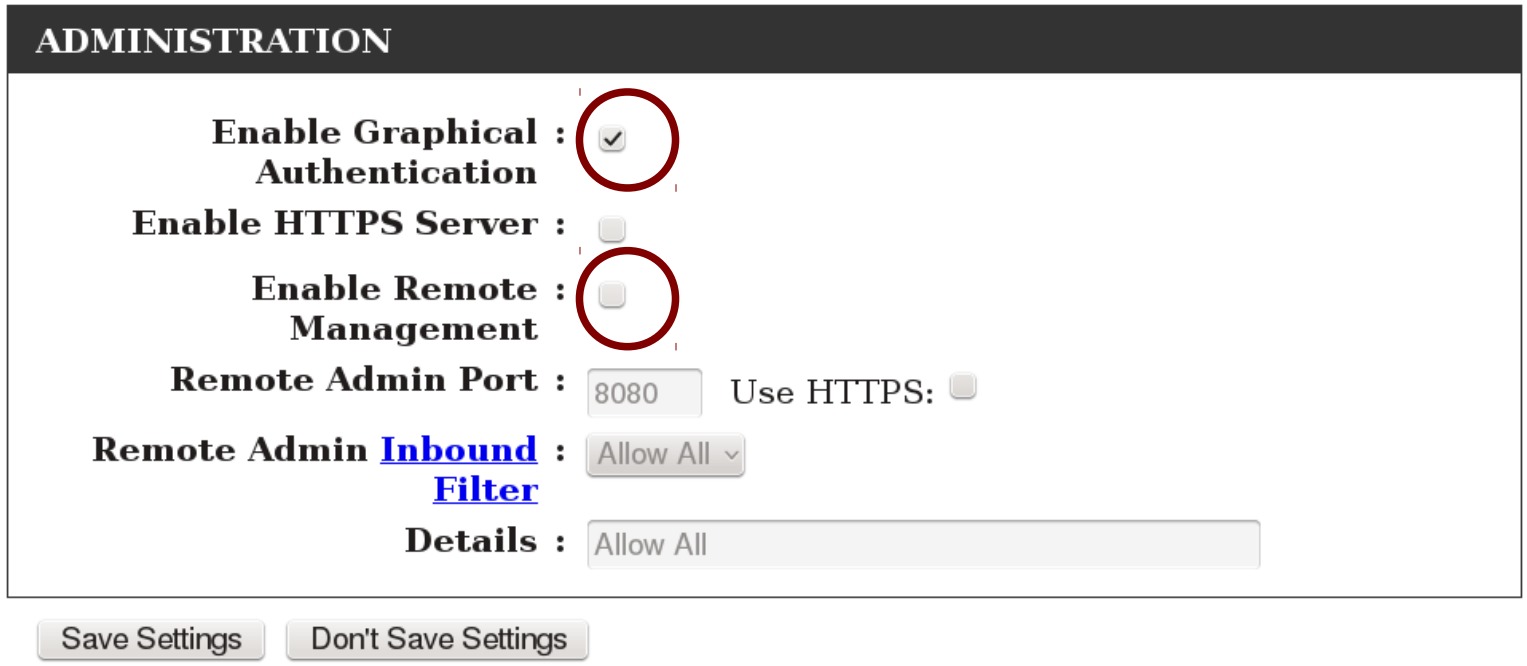
- w przypadku modemów Thomson TWG850 i TWG870: pod adresem http://192.168.0.1 pozostawić pustą nazwę użytkownika, a w pozycji hasło wpisać **admin**;
- w przypadku modemów Technicolor TC7200 i Ubee EVW3226: pod adresem http://192.168.0.1 jako nazwę użytkownika i hasło wpisać **admin**;
- w przypadku modemów Cisco EPC3925 i EPC2425: pod adresem http://192.168.1.1 pozostawić puste nazwę użytkownika i hasło;
- w przypadku routera Netgear: pod adresem http://192.168.1.1 jako nazwę użytkownika podać **admin**, a w pozycji hasło wpisać **password**. Konfiguracja możliwa jest **tylko na komputerze podłączonym do routera**. W przeciwnym razie okno logowania nie zostanie wyświetlone.

Nazwę użytkownika i hasło można oczywiście zmienić (szczegóły dostępne są w Dokumentach i instrukcjach). Należy pamiętać jednak, że po zrestartowaniu modemu Thomson/Technicolor/Cisco lub routera Netgear do ustawień fabrycznych, dane te wracają do pierwotnych ustawień.

Tylne drzwi: zabezpieczenie

- zawsze należy zmienić domyślne hasła i identyfikatory konta administratora urządzenia (komputera, trasownika, itd.)

- w przypadków trasowników bezprzewodowych należy wyłączyć możliwość zarządzania zdalnego, oraz włączyć dodatkowe metody autoryzacji



Rootkit

Rootkit (*ang. Rootkit*): pakiet (*ang. Kit*) złośliwego oprogramowania, którego część ma za zadanie ukrycie plików i procesów (wykonywanych programów) włamywacza przed użytkownikiem komputera. Programy wchodzące w skład rootkita mogą oszukiwać oprogramowanie antywirusowe, co powoduje, że wykrycie działającego rootkita jest bardzo trudne.

historia z lat 2005 – 2007: firma Sony BMG do muzyki nagranej na płytach CD dołączyła rootkita. Pakiet instalował się na komputerach użytkownika bez jego wiedzy i zgody. Pakiet miał zapobiegać kopiowaniu muzyki przez użytkownika, oraz przesyłać dane o działaniach użytkownika do firmy Sony.
Po fali krytyki firma Sony BMG udostępniła program do deinstalacji pakietu, który instalował dodatkowe oprogramowanie, kolekcjonował adresy e-mail użytkowników i wprowadzał dodatkowe nieszczelności w zabezpieczeniach systemu operacyjnego.

Rootkit

Rootkit (*ang. Rootkit*): pakiet (*ang. Kit*) złośliwego oprogramowania, którego część ma za zadanie ukrycie plików i procesów (wykonywanych programów) włamywacza przed użytkownikiem komputera. Programy wchodzące w skład rootkita mogą oszukiwać oprogramowanie antywirusowe, co powoduje, że wykrycie działającego rootkita jest bardzo trudne.

historia z lat 2005 – 2007: jedną z reakcji firmy Sony BMG w osobie Dyrektora firmy Sony była wypowiedź:

> Mr. THOMAS HESSE (President, Sony BMG Global Digital Business): Most people, I think, don't even know what a Rootkit is, so why should they care about it?

http://www.npr.org/templates/story/story.php?storyId=4989260

Lista obecności

Robak ILOVEYOU

historia z maja 2000 roku: w 4 maja 2000 roku do wielu osób dotarł e-mail o tytule ILOVEYOU, wraz z załącznikiem o nazwie "LOVE-LETTER-FOR-YOU.TXT.vbs". Po otwarciu załącznika robak wykonywał kilka operacji na komputerze ofiary:

• nadpisywał pliki o rozszerzeniach typu *.JPG, *.GIF, *.WAV swoją własną zawartością dodając rozszerzenie .VBS (rodzaj wykonywalnego programu)

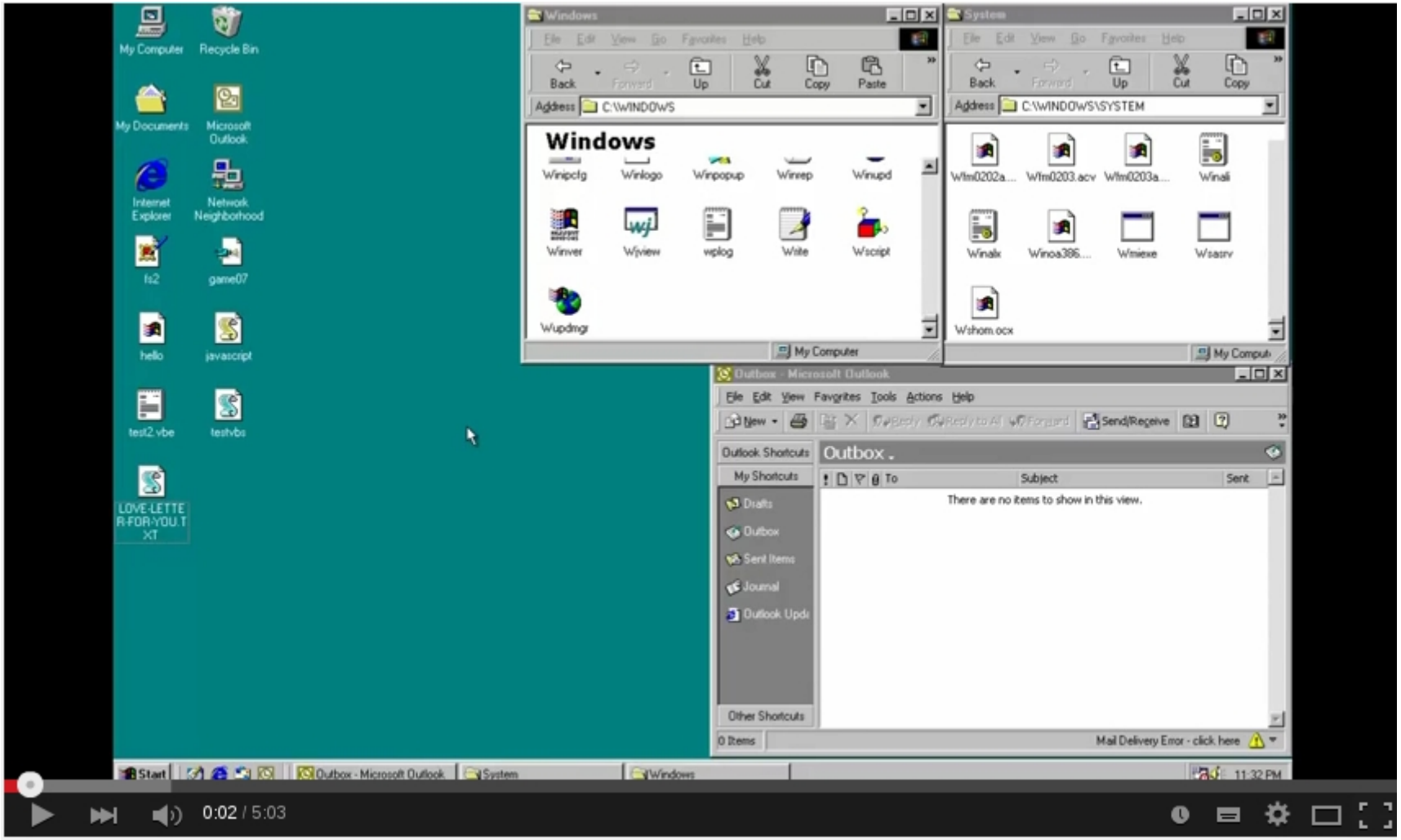
• ładował trojana, który służył do kradzieży haseł użytkownika

• robak wysyłał oryginalny e-mail do wszystkich osób znajdujących się w książce adresowej użytkownika

Robak zainfekował komputery w ponad połowie firm w USA i około 100 000 serwerów poczty w Europie.

Szacuje się, że spowodował straty wysokości 5 – 9 MLD $

Robak ILOVEYOU

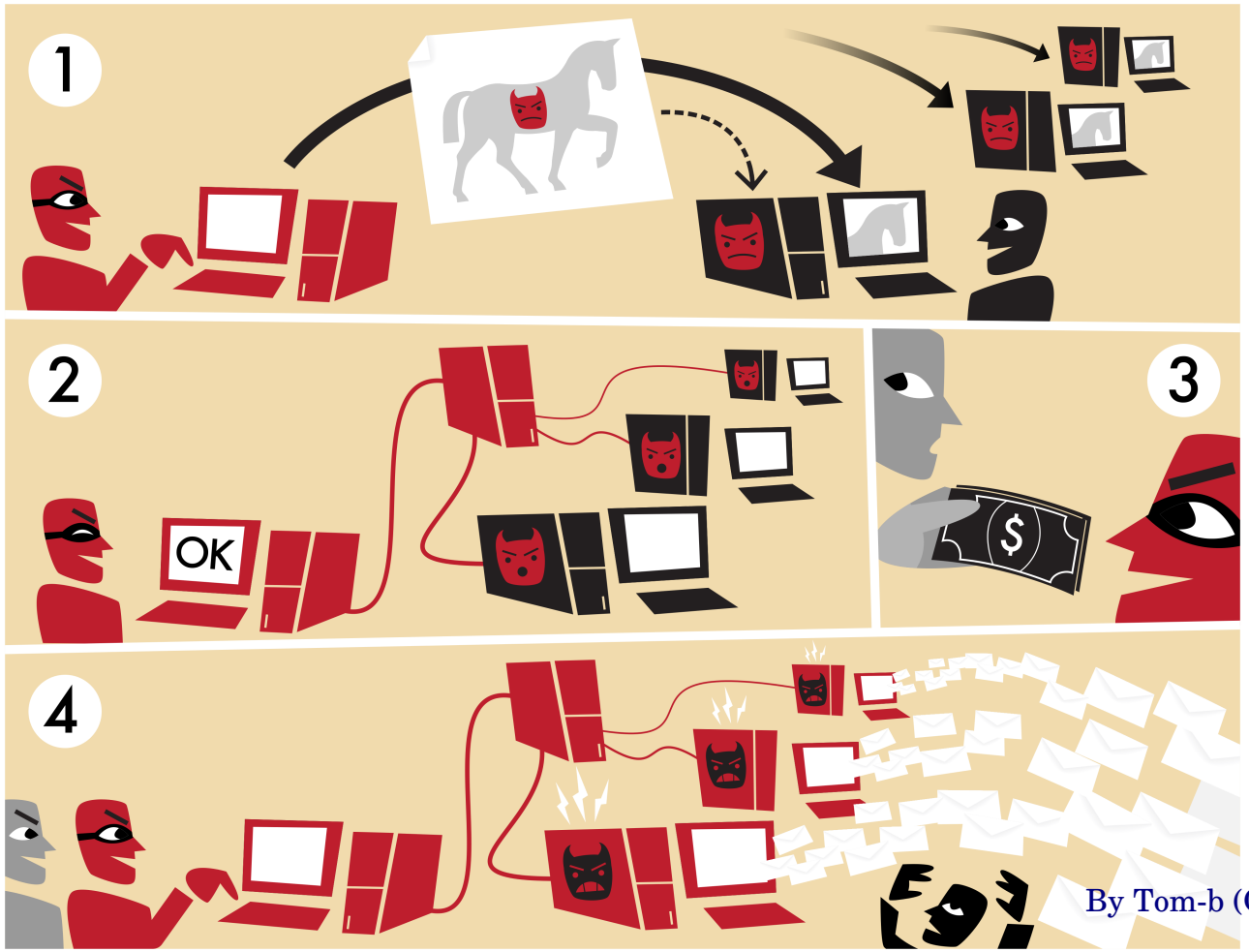


Robak Stuxnet

http://www.antibody.tv/projects/stuxnet.html

Botnet

Botnet (*ang. robot + net*): grupa komputerów, które przy użyciu malware znajdują się pod kontrolą przestępców. Komputer w sieci bootnet określany jest mianem *zombie*. Zasoby *bootnetu* są sprzedawane przez ich "właścicieli" innym przestępcom, którzy wykorzystują je w niecnych celach.



Wykorzystanie botnetów

DDOS (*ang. Distributed Denial of Service*): atak mający na celu tymczasowe zablokowanie działania wybranej usługi internetowej poprzez zmasowane żądania wykonania tej usługi. Najprostszy przypadek to blokada serwera WWW przez zbyt dużą liczbę żądań wyświetlenia danej strony. **Koszt tygodniowego ataku zaczyna się od 150$**

E-mail spam: komputery wchodzące w skład botnetu są używane do rozsyłania niechcianej poczty elektronicznej (*ang. spam*). **Spam stanowi 66% listów elektronicznych.**

http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q1-2014

Ataki DDOS


Digital Attack Map
Map
Gallery
Understanding DDoS
FAQ
About
August 31 2013
World Map
Table
Embed
Bandwidth (Gb)
Type
Source Port
Duration
Dest. Port
Web (80/443)
DNS (53)
Other
Attacks where source and destination are unknown
Type of Attack
between two countries
internal
either source or dest. unknown
no source, no dest.
Total Attack Bandwidth (All Countries), Gb
Sep 1
2013
Most Active Countries (normalized)
As source
As destination

Malware na Androida

Android: raporty firm Kaspersky i Symantec wskazują na lawinowy wzrost liczby programów typu malware dla systemu Android.

Mobile Cyber Threads, Kaspersky LAB, Październik 2014:

- dziesięciokrotny wzrost liczby ataków między 08.2013 a 03.2014
- 59% ataków skierowanych na kradzież pieniędzy ofiary
- trojany wysyłające wiadomości SMS stanowiły 57% wszystkich programów malware
- liczba trojanów skierowanych na usługi bankowości mobilnej wzrosła 14 razy

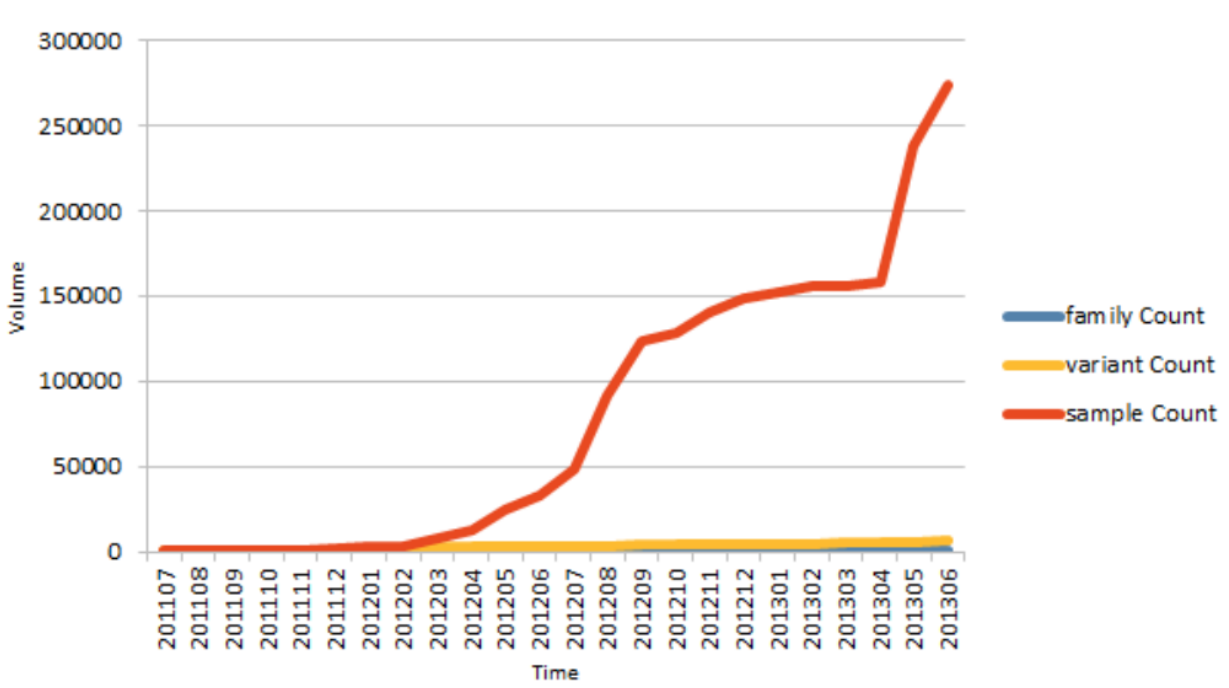


Figure 11. Android malware growth

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/madware_and_malware_analysis.pdf

Malware na Androida

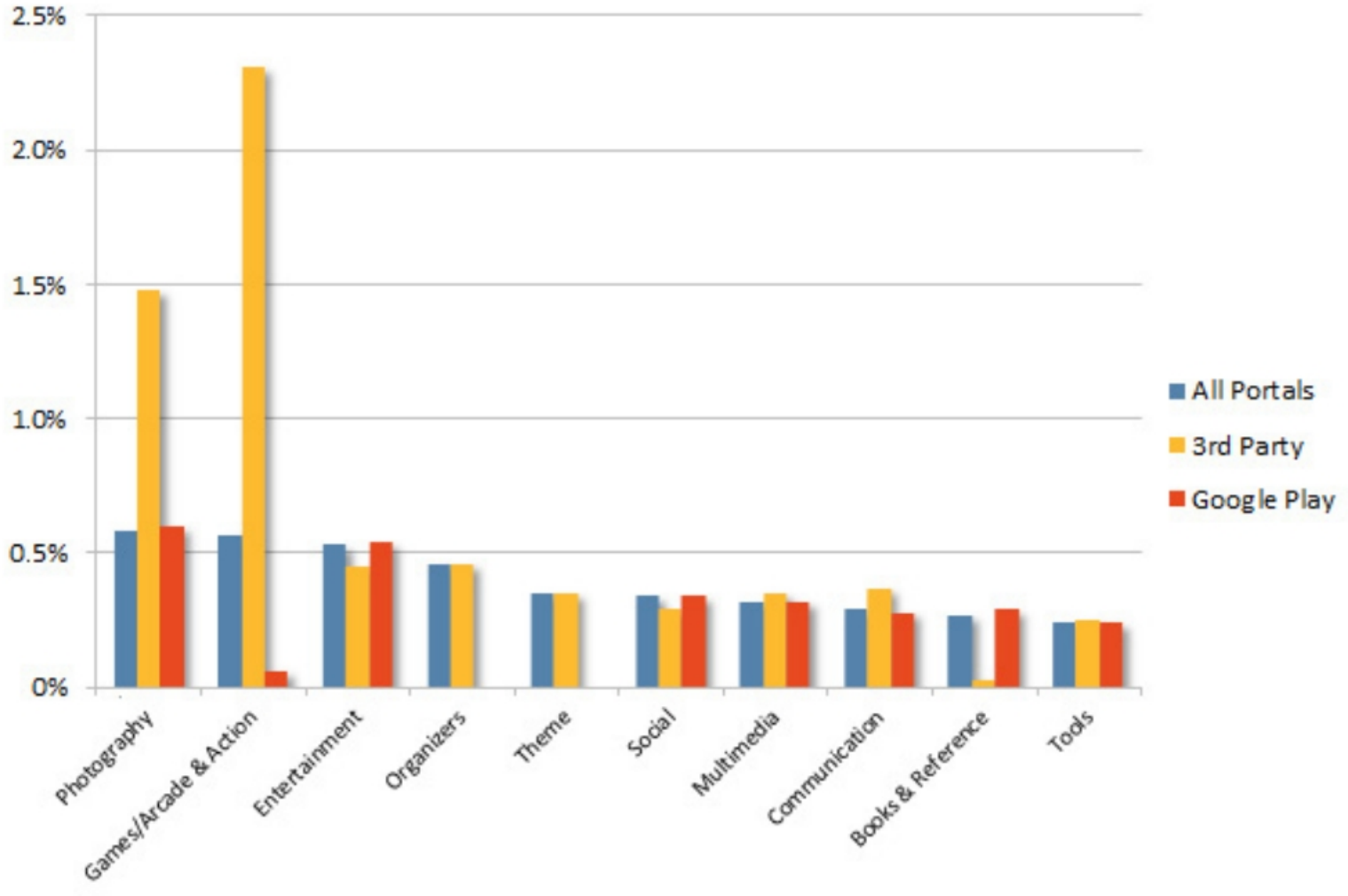


Figure 12. Top ten app categories with the highest percentage of malware

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/madware_and_malware_analysis.pdf

Malware na Androida

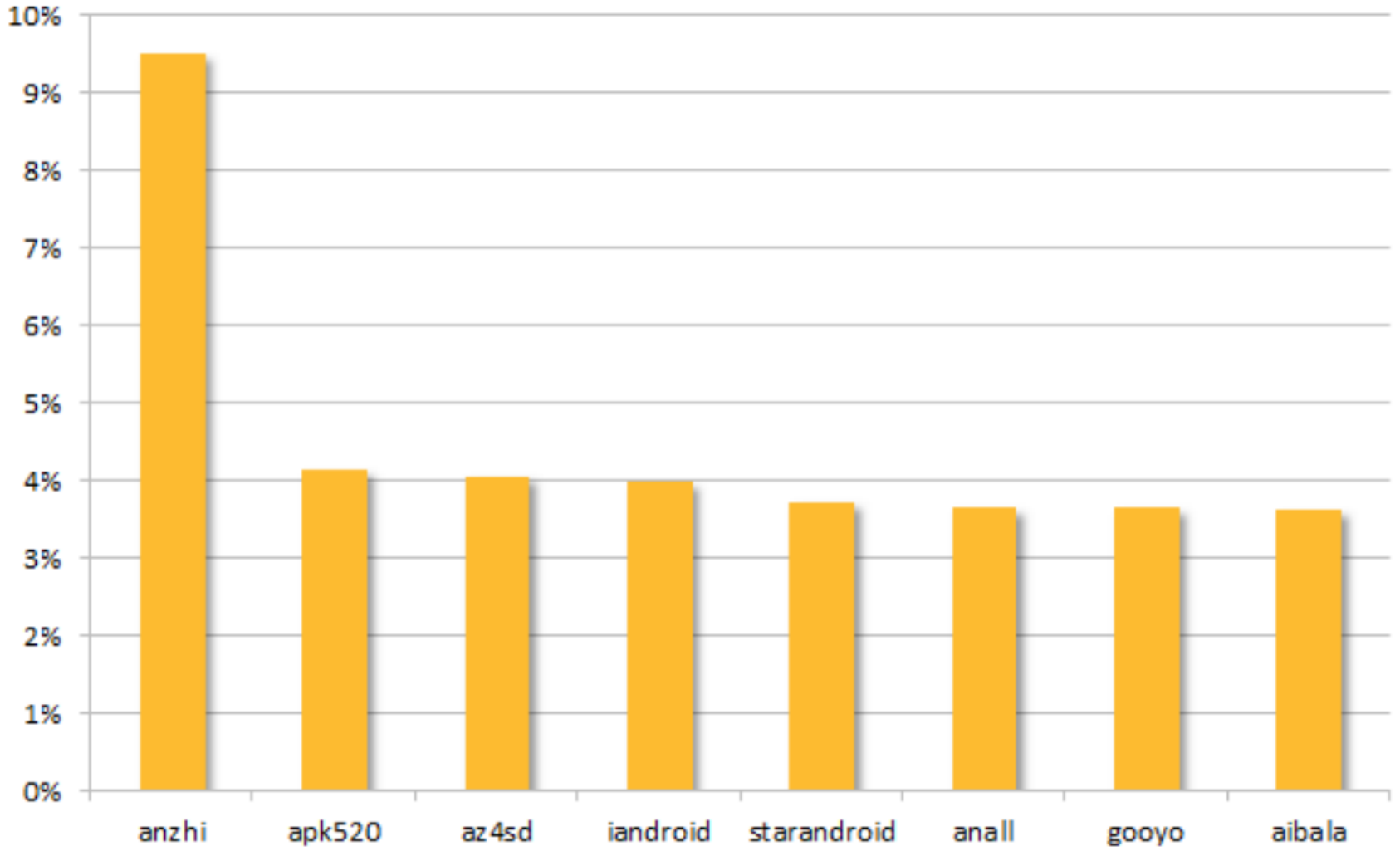


Figure 13. Third-party app stores hosting the most malware from January to June 2013

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/madware_and_malware_analysis.pdf

Zagrożenia w Polsce 2014 – raport CERT Polska:

280 000 komputerów: tyle komputerów było średnio infekowanych w Polsce w 2014 roku

zainfekowane załączniki: najbardziej popularna metoda zarażania

bankowość elektroniczna: wzrost ataków ukierunkowanych na tę dziedzinę. Cztery z największych znanych bootnetów są ukierunkowane na tę dziedzinę.

witryny Prezydenta RP i GPW: witryny ważnych instytucji w Polsce padły ofiarą ataków DDOS w 2014 roku

malware na Androida: jest obecne w Polsce, ale nadal nie jest znaczącym problemem

Botnety w Polsce

Poz.	Procent zainfekowanych adresów IP	Maksymalna dzienna liczba unikalnych adresów IP	Numer AS	Nazwa Operatora
1	4,02%	27 354	12912	TMobile Polska
2	2,44%	15 607	39603	P4 (Play)
3	2,31%	13 693	21021	Multimedia Polska
4	2,09%	30 520	12741	Netia
5	1,71%	9 051	29314	Vectra
6	1,68%	92 340	5617	Orange Polska
7	1,54%	3 837	20960	TK Telekom
8	1,44%	19 099	8374	Plus
9	0,95%	14 544	6830	UPC Polska
10	0,78%	2 528	43939	Internetia

Tabela 1. Dane dotyczące infekcji u polskich operatorów.

Zagrożenia w Polsce 2014 – raport CERT Polska

Botnety w Polsce

Poz.	Nazwa botnetu	Liczba adresów IP	Udział procentowy
1	Conficker	62 221	22,19%
2	ZeroAccess	32 460	11,57%
3	Zeus (w tym Citadel i pochodne)	25 311	9,03%
4	Sality	14 003	4,99%
5	Zeus GameOver	12 513	4,46%
6	Ircbot	10 768	3,84%
7	Bankpatch	6 086	2,17%
8	Banatrix	5 385	1,92%
9	Virut	4 014	1,43%
10	Kelihos	3 922	1,40%
	Pozostałe	103 750	37,00%

Tabela 2. Największe botnety w Polsce.

Zagrożenia w Polsce 2014 – raport CERT Polska

Internetowe BHP

Aktualizacja oprogramowania: w każdym rodzaju oprogramowania są znajdowane błędy. Zawsze należy aktualizować wszelkie programy do ich najnowszej wersji.

Program antywirusowy: na każdym urządzeniu należy korzystać z programów antywirusowych z włączona opcją skanowania każdego pliku ściągniętego z Internetu.

Zapora sieciowa: na komputerach stacjonarnych zawsze należy mieć uruchomiony program kontrolujący które programy mogą komunikować się z internetem i jakie dane przychodzące są dopuszczane do komputera.

E-maile: należy uważać na wszelkie wiadomości nieznanego pochodzenia, w szczególności na załączniki wykonywalne.

Źródła oprogramowania: należy korzystać jedynie z zaufanych źródeł oprogramowania.