



Garnkiem miodu w zombie

Detekcja, analiza, dns-blackholing sieci botnet.

Borys Łącki – Patryk Dawidziuk

<http://www.logicaltrust.net>

XIX Górska Szkoła Informatyki – Szczyrk 2008



LogicalTrust

departament bezpieczeństwa IT Business Consulting Experts Sp. z o.o. świadczący usługi w wybranych obszarach bezpieczeństwa IT.

- audyty,
- testy penetracyjne,
- inżynieria odwrotna,
- analiza ryzyka,
- hardening,
- analiza malware.



Podstawy teoretyczne

- co to jest botnet – informacje ogólne
 - armia komputerów zainfekowana trojanami (botami)
 - słucha rozkazów od serwera zarządzającego (C&C)
 - wykonuje polecenia także legalnego właściciela
 - **rozprzestrzenia się**



Topologie sieci botnet

- scentralizowana – boty łączą się do centrum zarządzania (serwer Command and Control, C&C) i słuchają rozkazów
 - komunikacja przy wykorzystaniu protokołów http oraz irc



Topologie sieci botnet

- peer-to-peer (p2p) – boty łączą się do wykrytych innych pośredników w sieci – w efekcie docierają do centrum zarządzania
 - komunikacja przy wykorzystaniu protokołów istniejących (np. gnutella lub własnych)
 - fast-flux



Topologie sieci botnet

- przypadkowa (random) – jest to topologia przyszłości, którą badacze postrzegają jako następny krok w ewolucji botnetów
 - komunikacja w oparciu o ... ?
 - C&C ciężkie do wykrycia
 - wydłużająca czas życia bota



Podstawy teoretyczne

„poznacie ich po owocach (...)” Mat. 7:16



Podstawy teoretyczne

- boty skanują adresy IP w poszukiwaniu podatności na ataki
 - wykorzystują luki znane
 - ... i nie znane (0 day)
 - szukają użytkowników końcowych
 - ... i podatnych serwerów (injections)
- wysyłają spam z zachętą do kliknięcia linka infekującego



Podstawy teoretyczne

- coraz rzadziej wysyłają maile ze złośliwymi załącznikami
- coraz częściej wysyłają linki do stron z fałszywymi kodekami
- ... lub do kartek okolicznościowych



Podstawy teoretyczne

- podstawowe sposoby wykorzystania botnetu
 - DDoS – terroryzm dla zysku lub z innych powodów
 - spam – więcej niż 80% wszystkich emaili
 - fraudy – w bardzo szerokim ujęciu
 - inne przestępstwa



Virustotal to **usługa udostępniająca skanowanie plików** i szybkie rozpoznawanie wirusów, robaków, trojanów i wszelkiego rodzaju podejrzanego oprogramowania, które jest identyfikowane przez dostępne na rynku programy antywirusowe. [Więcej informacji...](#)

Plik **unknown** otrzymany 2008.06.18 23:52:36 (CET)
Obecny status: **zakończono**
Wynik: **12/33 (36.36%)**

[Zwiezły](#)

Wynik: 12/33 (36.36%)

Antywirus	Wersja	Ostatnia aktualizacja	Wynik
AhnLab-V3	-	-	-
AntiVir	-	-	-
Authentium	-	-	W32/Heuristic-KPP Eldorado
Avast	-	-	Win32:Delf-KNF
AVG	-	-	-
BitDefender	-	-	Trojan.Dropper.Delf.Crypt.C
CAT-QuickHeal	-	-	Backdoor.IRCBot.dok
ClamAV	-	-	-
DrWeb	-	-	-
eSafe	-	-	-
eTrust-Vet	-	-	-
Ewido	-	-	-

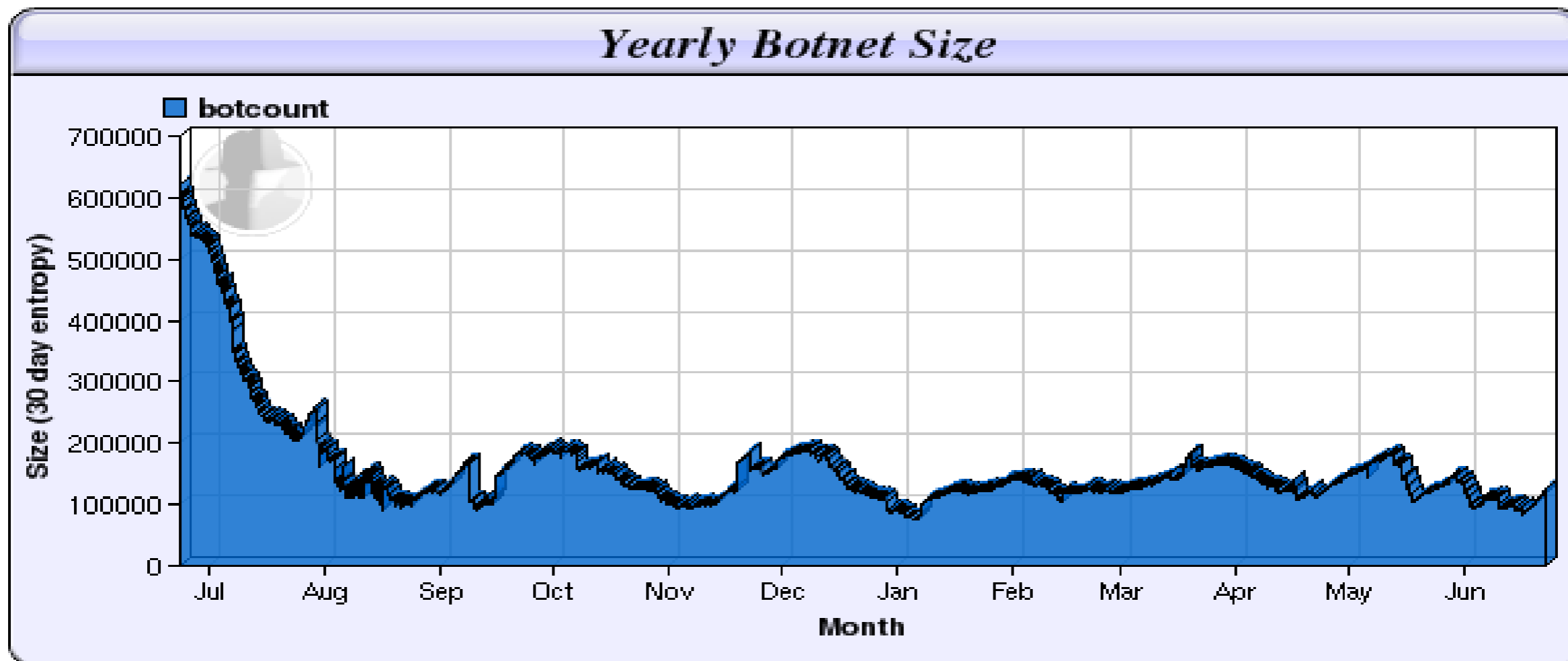


Fakty

- 2008.03 – Kraken/Bobax botnet
~ **400 000** zainfekowanych maszyn
- 2008.04 – Konferencja RSA (SecureWorks)
~ **1 000 000**
- 2008.04 – Srizbi botnet
~ **350 000**
- 2008.06 - Malicious Software Removal Tool
~ **700 000** – Taterf (1 dzień!)



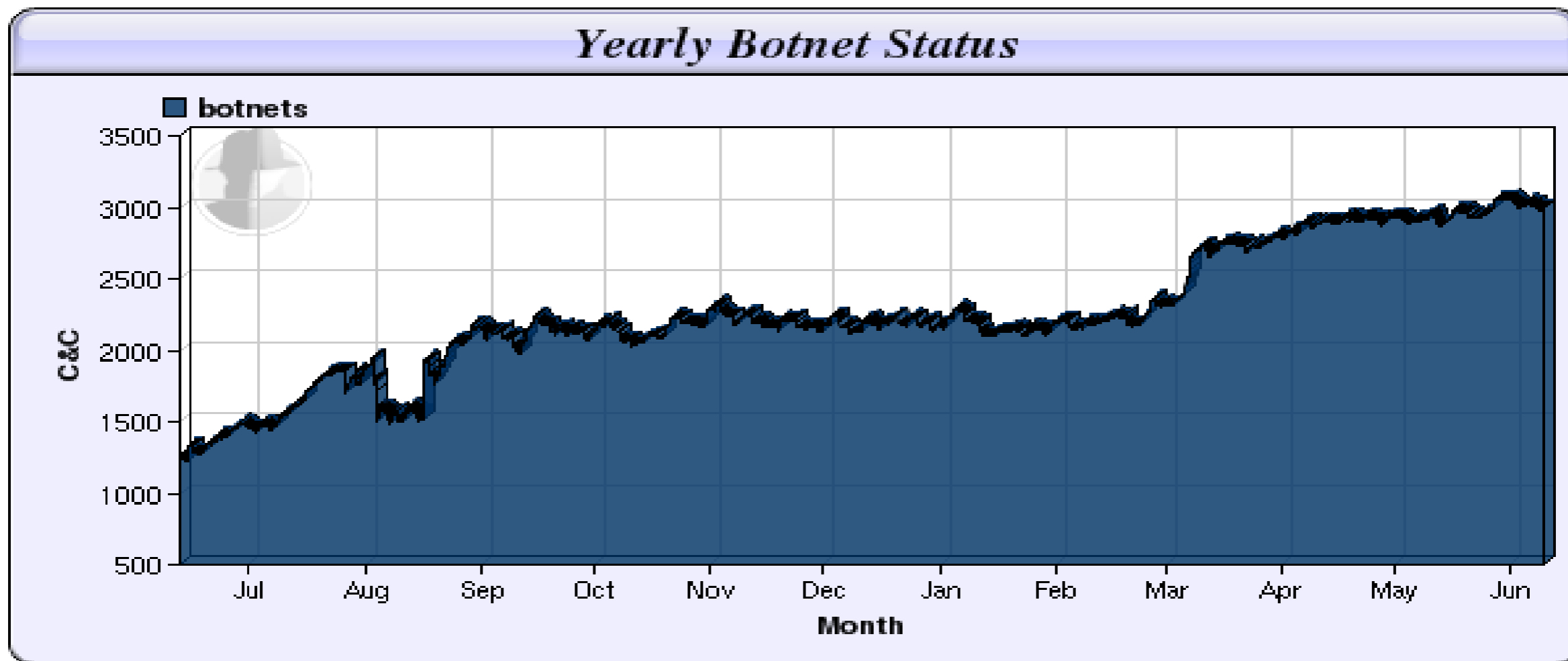
Fakty



Źródło: www.shadowserver.org



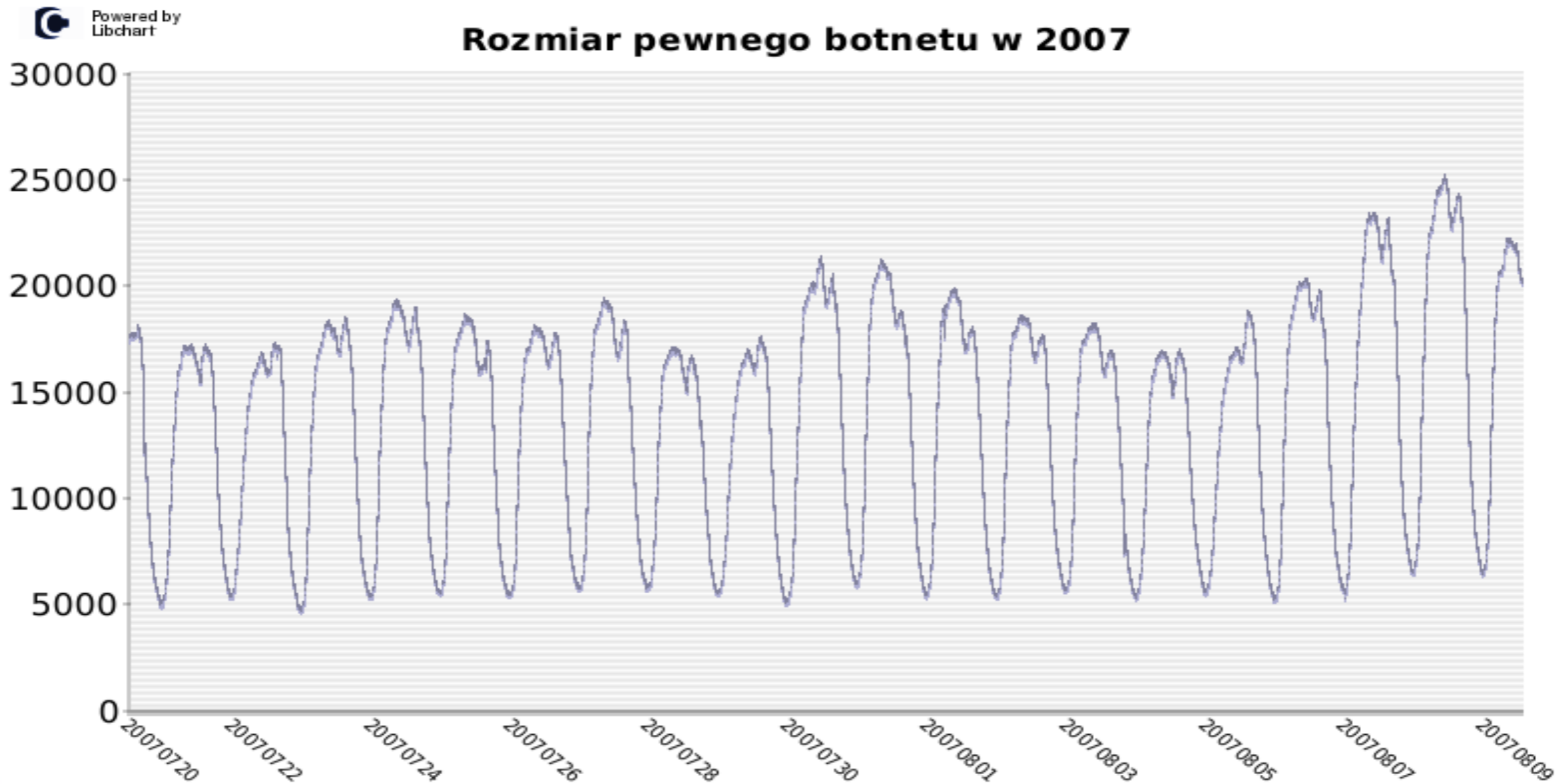
Fakty



Źródło: www.shadowserver.org



Fakty





SPAM

Upload: 256 Kb/s = 32 KB/s

1 spam = 11 KB

Średnia ilość botów: 13862

$32 * 13862 * 3600 = 159690240$ KB /h = 156 GB /h

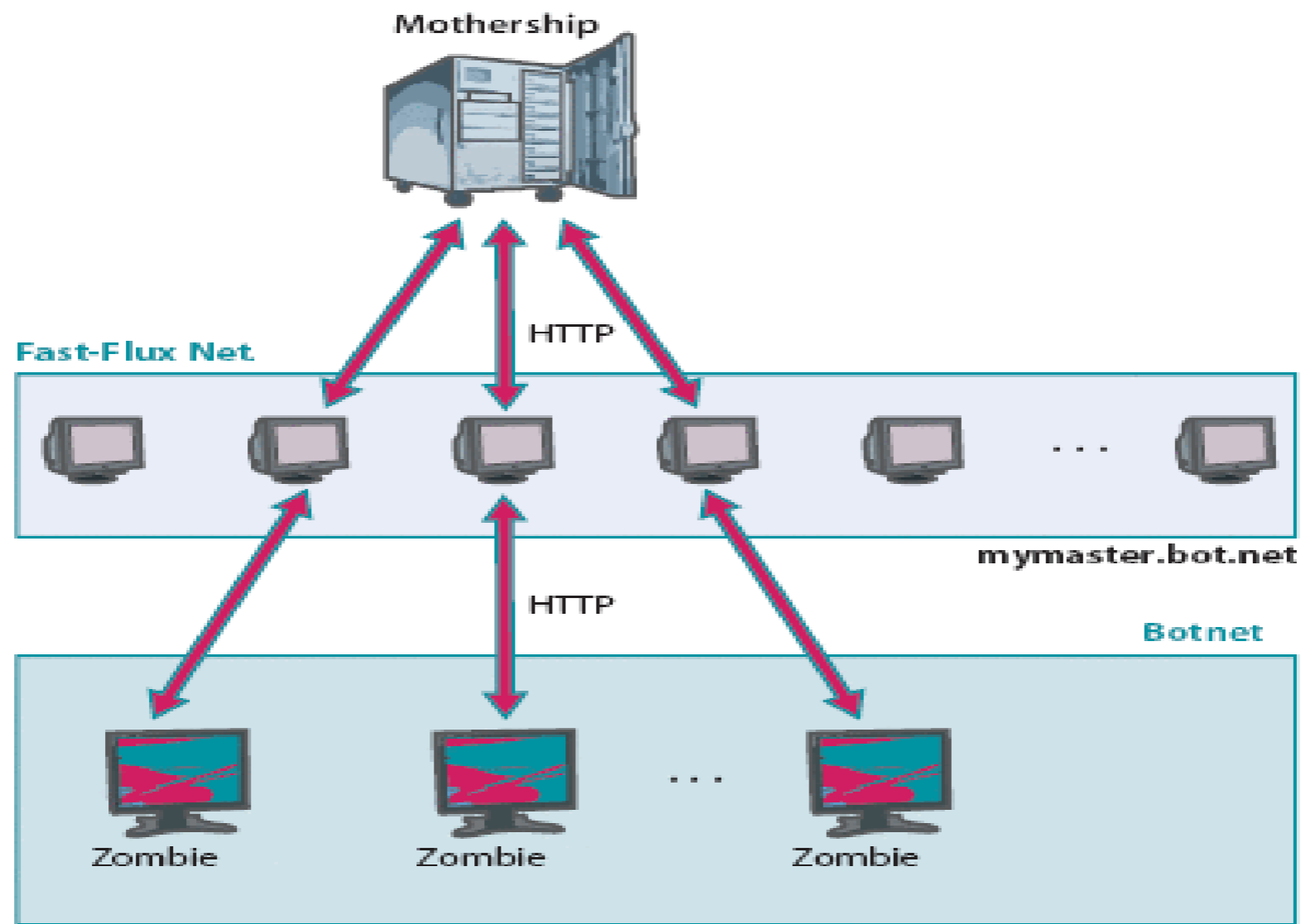
$159690240 / 11 = 14.517.294$ wiadomości typu spam /h

348.415.056 wiadomości typu spam / dziennie



Fakty

FastFlux



+ P2P

Źródło: <http://www.heise-online.pl>



Fakty - WWW

- **2008.03**
> 100 000 wyników wyszukiwarki Google zarażonych
(TV.com, News.com, ZDNetAsia.com)
- **2008.04**
Niebezpieczna reklama Flash w serwisie USATODAY.com
- **2008.05**
Ponad 500 000 podmienionych stron (w 24 godziny)



Narzędzia

- **Zeus**

- multigenerator
- cena: 700 dolarów

RSA Anti-Fraud Command Center - ponad 150 różnych wersji

- **Mpack**

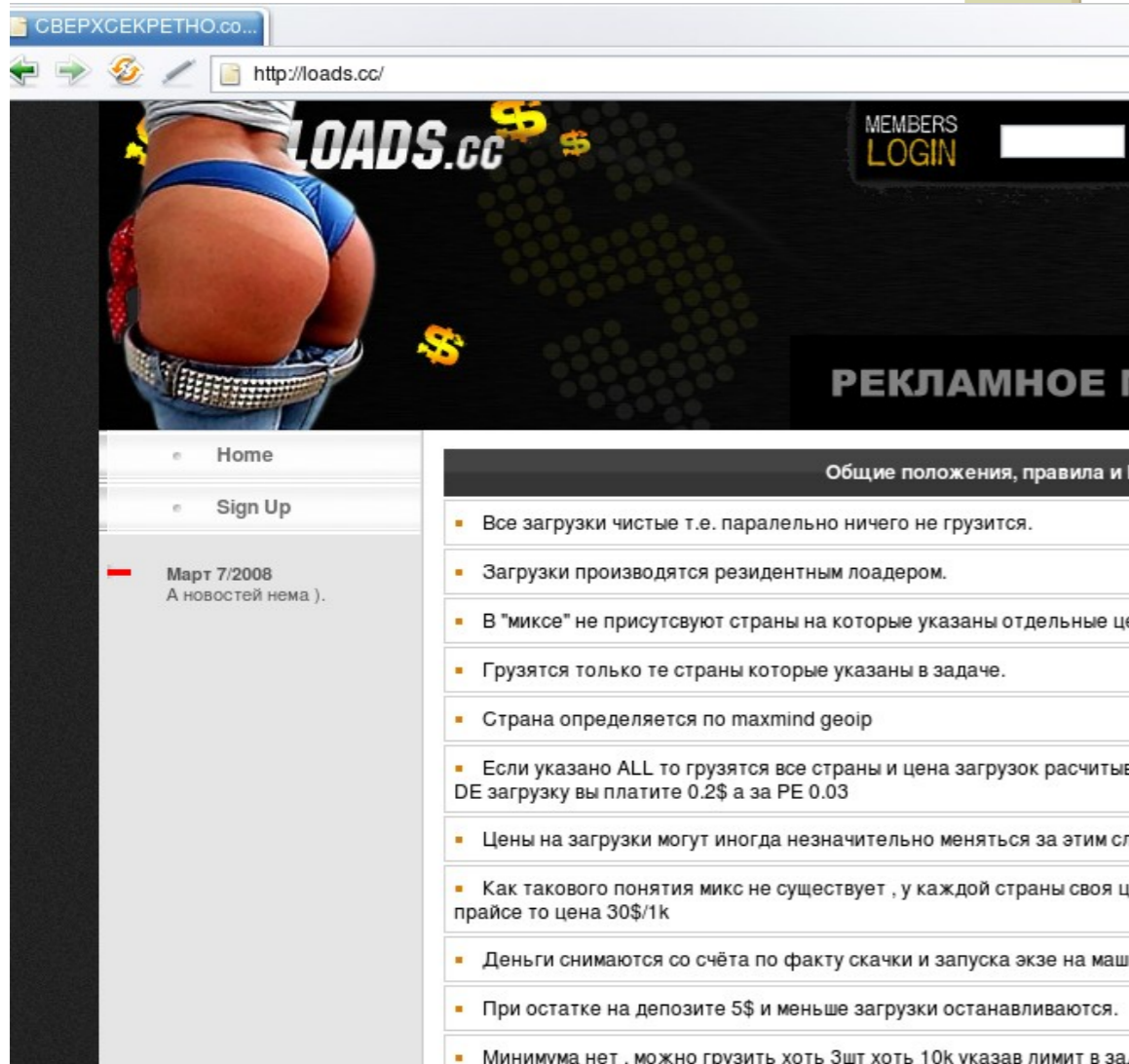
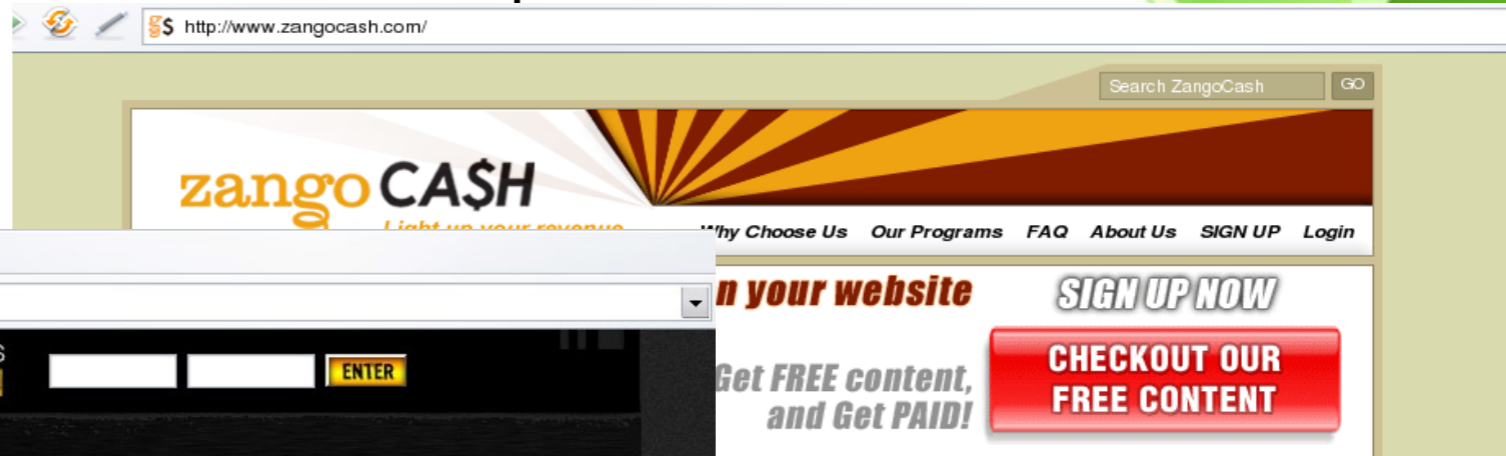
- oparty na PHP malware kit produkowany przez rosyjskich hakerów
- cena: < 1000\$ [+ 50\$ - 150\$ aktualizacje]
- (IE 0 day - 10 000\$)

- **DreamSystem**

- system łatwego zarządzania sieciami botnet [via WWW]
- cena: 750\$ [aktualizacje zawarte w cenie]



Adware \$





Czarny rynek \$\$\$

```
<cUrl> 4,0[5,4]4,5[1,5]5,1[0,1 ...:::SELLING >>> HACKED HOST [((cPANEL + FTP))] (12
$)-//-PHP MAiLER 2 INBOX (8$)-//-c99/r57 SHELLS (9$)-//-EMAIL SPIDER GOLD V9 [((FUL
L VERSiON))] (30$)-//-PRIV8 PHP GOOGLE Rfi SCANNER [((SCRIPT))] (26$)-//-PERL Rfi S
CANNER [((SCRIPT))] (28$)-//-ANY WEB SCRiPT/TEMPLATE (55$)-//-MAILING LIST US/UK/IN
DIA (1mb 10$)-//-ALSO DESIGNING CUSTOM SCAM PAGEz (26$) !!! RiPPERS/TIME WASTERS/LO
NG TALKERS ---> DIE !! ONLY SERiOUS
<\2Legit> 9,1I Am 8,1Western1,8Union9,1 Confirmer Cashing Out Male Cvv2's With Dob
+ Ssn And Full Infos Also Need Paypal Drop Wtih Atm Debit Card For Instant Cashout
Msg Me For Deal.
<Geezer> 0,4 I am selling:- Declined Fullz + Fresh socks4/5 (any country) + All Sca
m Pages(BOA/PayPal/Aol/Hotmail/Yahoo) and others + DDsoHTTP with serial key - I acc
ept E-Gold == I need US unspammed fresh leads + CPanel
đ luxmarket/#ccpower has requisite people for bulk cc orders, Needs direct supplier
s. your share is 50%
<Droper> contact me for any cashout in US,UK and Canada,through transfer and Billpa
y also pick up Wu&MG anyname,and i have drop for merchandise, need a good spammer f
or long term deal
<uznt> 4,1I have photos of these items: CCs(visa, mastercard), Drive licences(UK, m
ale, female), Passports(UK, male, female), student cards. Also have photos of China
, Mongolia, Russia, Vietnam Visas(documents, not cards). PM me
```



Zarobki \$\$\$

DDoS:

„Czy strona twojej firmy jest nadal niedostępna? Występuje problem z twoją stroną i oferujemy Wam rozwiązanie tego problemu. Koszt naprawy wynosi 480 000 jenów (~ 10 000 zł). Jeśli nie uiścicie opłaty, możecie spodziewać się dalszych problemów.”

**Straty na poziomie 50 milionów jenów dziennie (1 mln zł)
- tydzień!** (Atak o sile 6 GB/s)

- 2008.03

Ponad 30.000 maszyn PC oraz Mac wygenerowało ruch na poziomie **10 Gb/s**.



Zarobki \$\$\$

- **18 latek Owen Thorn Walker**

Oskarżony o szereg przestępstw związanych z „hakingiem”

Straty jakie spowodował botnet to około 20 mln dolarów

- Wywiady [1 osoba !!!]

- **Phisher:** 30.000 osób / 3000 - 4000 dolarów / dzień

- **Spamer:** 10.000 - 15.000 dolarów / dzień



Detekcja

- sposoby wykrywania wrogiej działalności w sieci
 - badanie ruchu na określone porty (pod kątem skanowania)
 - sposobów jest wiele, każdy inny, ale każdy robi dokładnie to samo, zlicza ilość pakietów na określone porty w określonym okresie czasu



Detekcja

- wysyłanie spamu
 - skrypt spamdetector.sh – bash i ngrep
 - detekcja najlepiej na punkcie styku ze światem
 - niestety na bieżąco jest ciężko i zasobożernie



Detekcja

- analiza ruchu na porty IRCa
 - większość ujawnianych przypadków to sterowanie botnetem przy pomocy serwera IRC
 - np. ircproxy - <http://ircproxy.packetconsulting.pl>
 - można na żywo podglądać konwersacje klient-serwer
 - ngrep - cały ruch na żywo (pcap)



Detekcja

- Fraudy
 - przeważnie są wykrywane po fakcie
 - o masowych fraudach najczęściej informuje prokuratura
 - fraudy nastawione na kradzież danych czy tożsamości mogą pozostać niezauważone przez długi czas



Nepenthes

- co to jest
 - HoneyPot (z ang. garnek miodu)
 - oprogramowanie udające prawdziwy system operacyjny, pozwalające na zastawienie pułapki na agresorów
 - podobnych narzędzi jest wiele:
 - Capture-HPC, HoneyC, Pehunter, Google Hack HoneyPot, Honeymole, Capture BAT, Honeysnap, HoneyBow, High Interaction HoneyPot Analysis Toolkit (HIHAT)



Nepenthes

- podstawy działania
 - nasłuchuje na portach emulując znane luki w wiodącym systemie operacyjnym
 - zaatakowany, potrafi przechwycić exploita w celu jego późniejszej analizy (np. w którymś z darmowych sandboxów, sunbelt czy norman)
- sandbox
 - środowisko pozwalające na uruchomienie programu w pod ścisłą kontrolą wraz z logowaniem każdej akcji



Nepenthes

- możliwości
 - pojedynczy nepenthes może działać jako samodzielna jednostka
 - ...może być też częścią sieci detekcji malware'u
 - przechwycone exploity potrafi automatycznie przesłać, do któregoś z sandboxów (np. Norman)
 - logowanie na irc jako ciekawostka



Nepenthes

- przykładowe analizy pochodzące z exploitów przesłanych do sandboxa



Nepenthes

- **nic nie wykryto**

- nepenthes-744f7bb406891c512b0c19ae4a5d7489-msnmsgr.exe : Not detected by Sandbox (Signature: NO_VIRUS)
-
- [General information]
- * File length: 152576 bytes.
- * MD5 hash: 744f7bb406891c512b0c19ae4a5d7489.
-
- [Process/window information]
- * Terminates AV software.
-
- (C) 2004-2008 Norman ASA. All Rights Reserved.



Nepenthes

- anti debug/emulation code present –
zabezpieczone przed podglądaniem
- nepenthes-9a93ca2265a2c01ac0386d298f032975-xhost.exe : Not detected by Sandbox
(Signature: NO_VIRUS)
-
- [General information]
- * Anti debug/emulation code present.
- * File length: 224256 bytes.
- * MD5 hash: 9a93ca2265a2c01ac0386d298f032975.
-
- (C) 2004-2008 Norman ASA. All Rights Reserved.



Nepenthes

- boty patchujące system, żeby nikt inny nie wykorzystał tej samej luki (tak, one istnieją)



Nepenthes

- [Network services]
 - * Attempts to delete share named "Admin\$" on local system.
 - * Attempts to delete share named "C\$" on local system.
 - * **Downloads file from**
<http://download.microsoft.com/download/6/1/5/615a50e9-a508-4d67-b53c-3a43455761bf/WindowsXP-KB835732-x86-ENU.E>
 - as C:\WINDOWS\TEMP\patch.exe.
 - * Connects to "download.microsoft.com" on port 80 (TCP).
 - * Opens URL:
download.microsoft.com/download/6/1/5/615a50e9-a508-4d67-b53c-3a43455761bf/WindowsXP-KB835732-x86-ENU.EXE.
- [Process/window information]
 - * Creates a mutex hrx 0.2 by h4x..
 - * Will automatically restart after boot (I'll be back...).
 - * **Attempts to open C:\patch.exe /passive /quiet /norestart.**



Statystyki

Data pierwszego ataku:	2007-02-16 18:34:23
Data ostatniego ataku:	2008-06-23 18:39:18

Wszystkich ataków:	3.287.461
--------------------	------------------

Unikalnych źródłowych adresów IP:	120.779
Unikalnych docelowych adresów IP:	5.876
Unikalnych plików malware:	12.521



Statystyki

- maksymalna ilość ataków ze źródłowego IP:
 - xxx.xxx.28.115 - **198.099**
- minimalna ilość ataków ze źródłowego IP:
 - xxx.xxx.102.15 - **1**
- maksymalna ilość ataków do docelowego IP:
 - xxx.xxx.61.156 - **30.003**
- minimalna ilość ataków do docelowego IP:
 - xxx.xxx.58.19 - **3**



Statystyki

Maksymalna ilość ataków dla malware:
b65a426bee4440171ad6ed7143cc93ba (md5)
339.364

Ataków na minutę:

4,63

Ataków na godzinę:

277,86

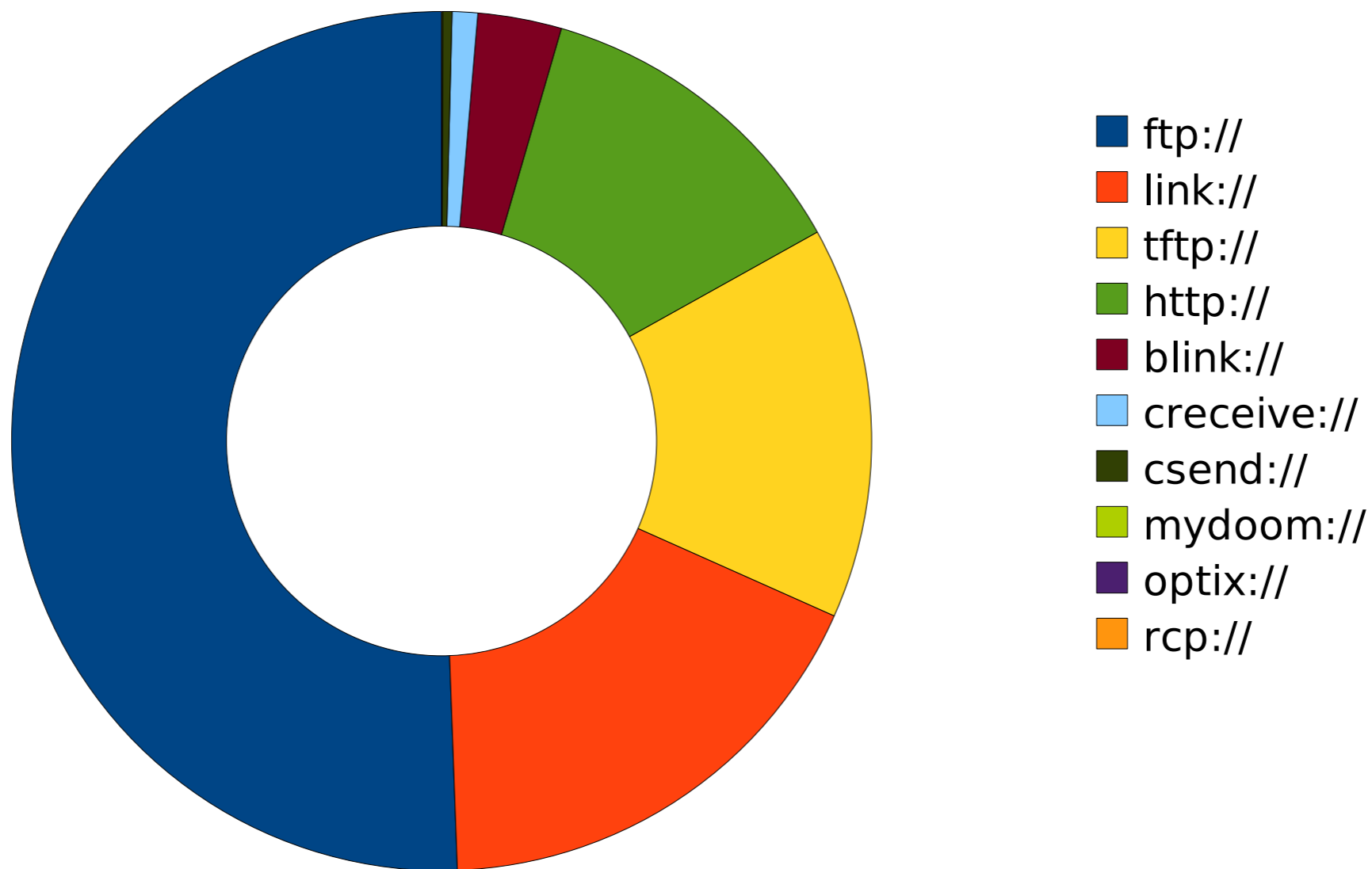
Ataków na dzień:

6668,66



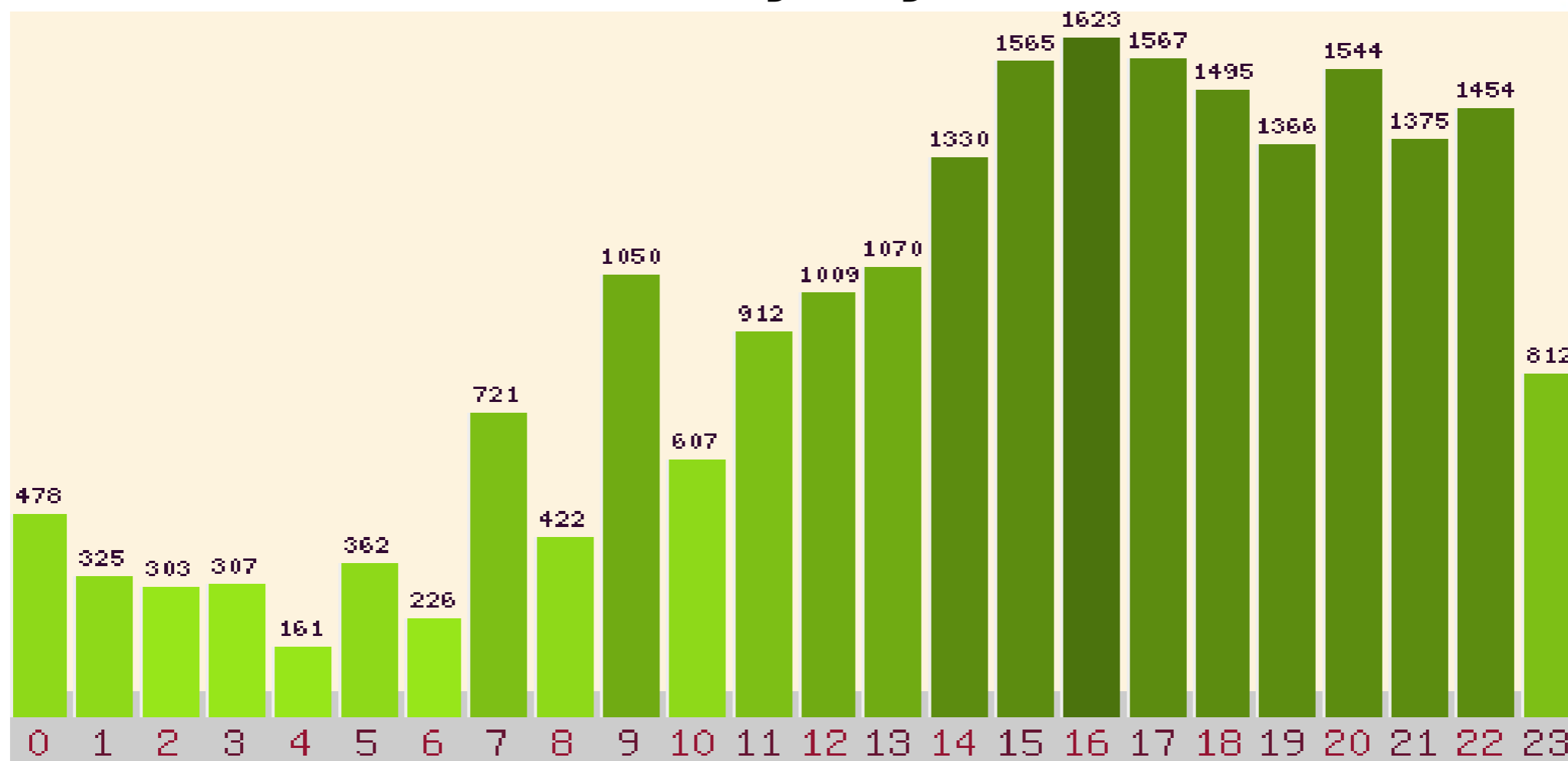
Statystyki

Malware Download Protocol





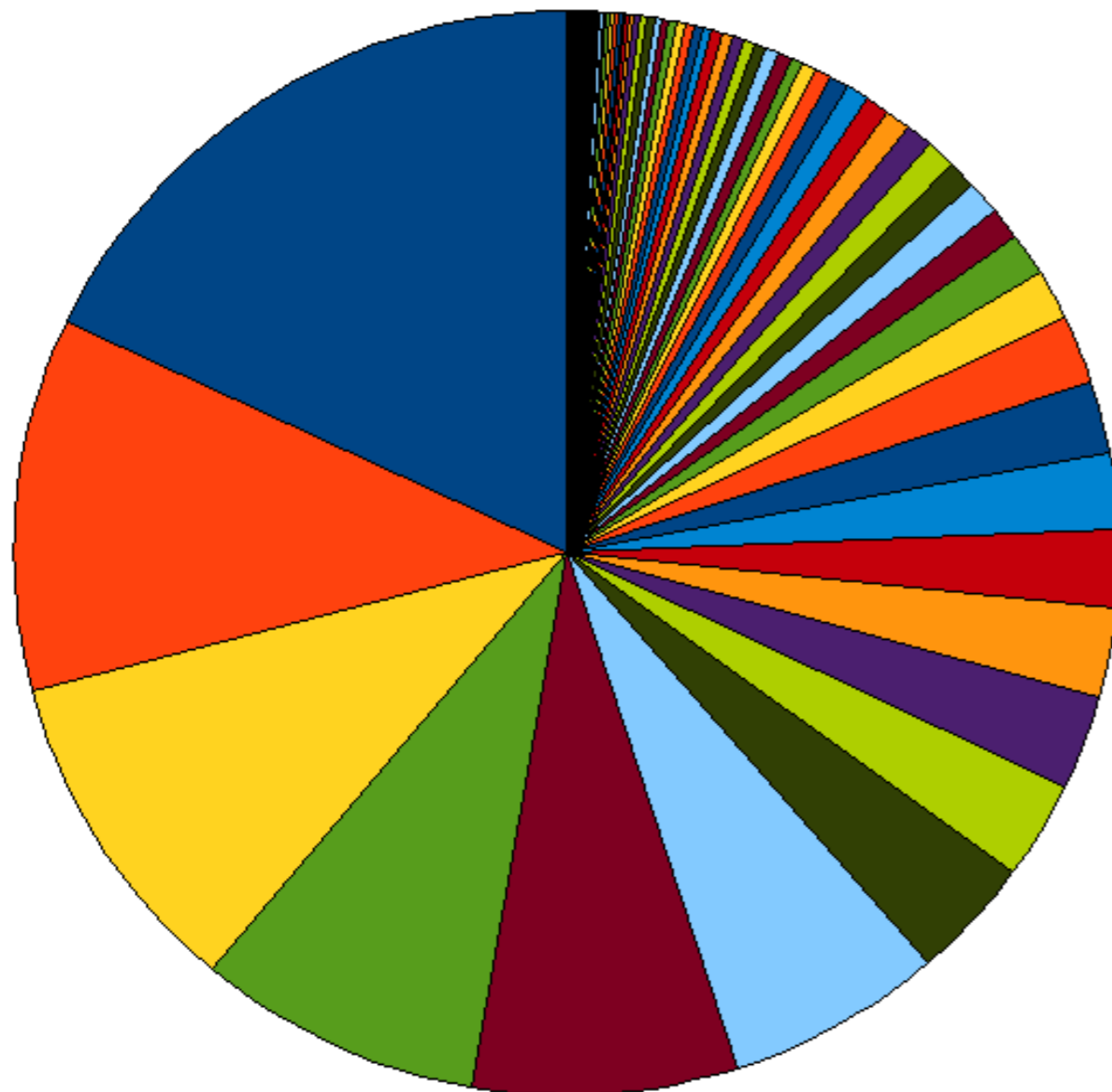
Statystyki



Ilość ataków na godzinę 2008.05, maks: 1.623 o 16.XX



Statystyki



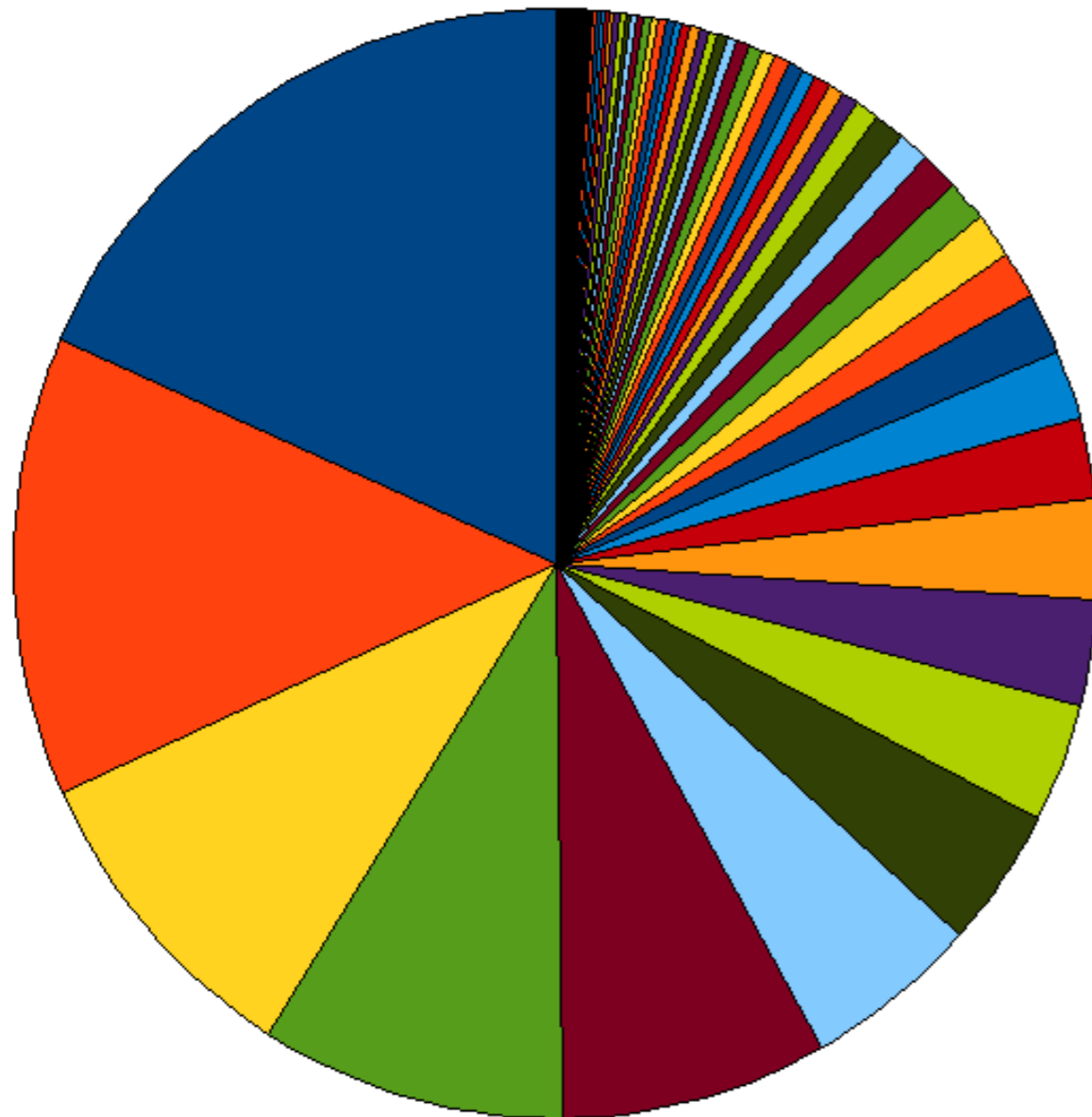
- GBR (17.99%)
- POL (11.08%)
- DEU (9.83%)
- ITA (8.34%)
- FRA (7.74%)
- RUS (6.38%)
- ESP (3.59%)
- ROM (2.91%)
- JPN (2.85%)
- HUN (2.63%)
- USA (2.36%)
- DNK (2.22%)
- BEL (2.15%)
- TWN (2.02%)
- KOR (1.54%)
- BRA (1.25%)
- PRT (0.98%)
- CHN (0.98%)
- JOR (0.88%)
- SWE (0.83%)

Źródło ataku

137 krajów !



Statystyki



- GBR (18.35%)
- DEU (13.40%)
- FRA (9.32%)
- RUS (9.12%)
- ITA (7.91%)
- POL (5.21%)
- JPN (4.11%)
- HUN (3.43%)
- DNK (3.11%)
- USA (2.88%)
- ROM (2.39%)
- ESP (2.00%)
- BEL (1.82%)
- JOR (1.36%)
- TWN (1.34%)
- ISR (1.17%)
- SWE (1.15%)
- PRT (0.95%)
- CHN (0.89%)
- GRC (0.71%)

Malware URL

60.775 IP



Statystyki

483 domeny

Czas stałego dowiązania domeny do IP:

Najkrótszy: < 1 dzień

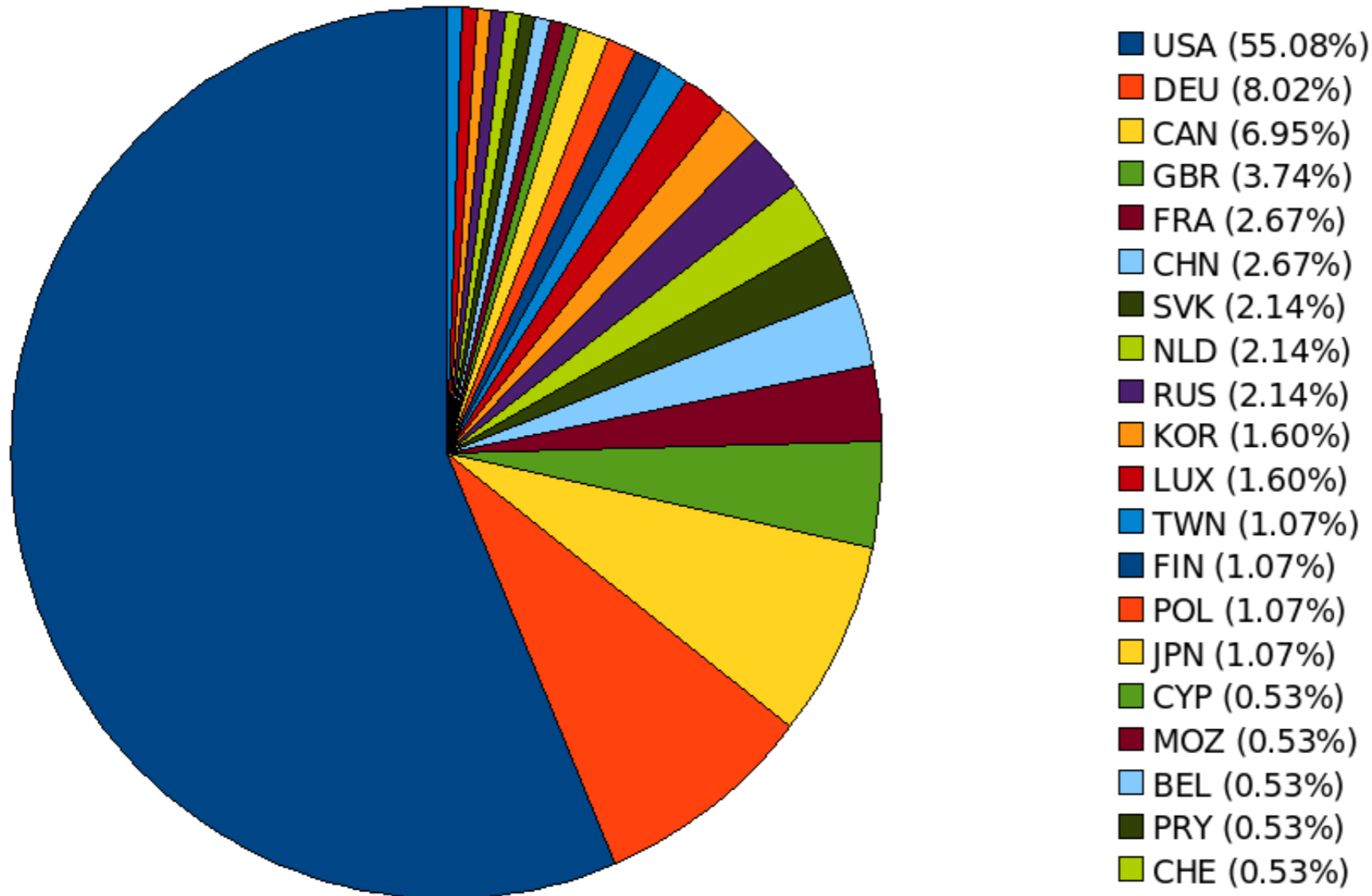
Najdłuższy: > 11 miesięcy

Maksymalna ilość wykorzystanych unikalnych IP: **57**

Maksymalna ilość jednoczesnych adresów IP do domeny: **8**



Statystyki



C & C



DNS blackholing

- teoria działania
 - konfiguracja serwera DNS tak, żeby działał jako master dla konkretnej domeny
 - udajemy legalny serwer DNS obsługujący domenę
- założenia
 - komputer musi korzystać z naszych dnsów
 - powyższy punkt można wymusić filtrami



DNS blackholing

- możliwości wykorzystania
 - przekierowanie blackholowanych domen na dowolny adres IP w celu dalszej analizy
 - dezaktywacja bota bez ingerencji w komputer klienta (kwestia etyczna)
- konfiguracja
 - (w linkach)



DNS blackholing

- skuteczniejszy od firewalli
 - adresy IP serwerów C&C w ramach domeny zmieniają się często
 - oprogramowanie AV nie nadąża za botami
 - wyłączenie domeny usuwa zagrożenie nawet dla nowo zainfekowanych hostów
 - bot nie działa nawet, jeżeli uda mu się zaktualizować



DNS blackholing

- podnosi ogólny standard bezpieczeństwa w sieci
- mniej malware – mniejsze lub słabsze ataki DDoS przeciwko innym sieciom/systemom
- pozwala na zmniejszenie ilości komputerów wysyłających spam



Pytania

- Często Zadawane Pytania - odpowiedzi
 - nie posiadamy własnego botnetu
 - prowadzimy na własne potrzeby projekt dns-blackholingu
 - projekt dns-blackholingu nie jest upubliczniony ze względu na brak odwaznych do jego hostowania
 - dostępność projektu dns-blackholingu omawiamy po prezentacji



Linki

- <http://bothunters.pl> - botnet blog,
- <http://nepenthes.mwcollect.org> - HomePage Nepenthesa,
- <http://www.honeynet.org> - strona projektu 'Honeynet',
- <http://www.mwcollect.org> - statystyki z ataków,
- <http://honeynet.org/tools/index.html> - alternatywne narzędzia do łapania malware'u
- <http://dshield.org> - statystyki dotyczące ilości ataków w sieci
- <http://www.virustotal.com> - strona zapewniająca skan pliku wieloma silnikami av
- <http://www.bleedingsnort.com/blackhole-dns/files/> - zestaw domen spyware'u do zablokowania
- <http://doc.bleedingthreats.net/bin/view/Main/BlackHoleDNS> - jak skonfigurować serwer DNS Microsoftu i nie tylko do DNS blackholingu
- <http://www.norman.com/microsites/nsic/Submit/en> - Norman Sandbox



Linki

- <http://ircproxy.packetconsulting.pl> - ircproxy do badania konwersacji irca
- <http://kaneda.bohater.net/files/spamdetector.sh> - spamdetector
- <http://www.spywareguide.com/> - Spyware Guide
- <http://research.sunbelt-software.com/Submit.aspx> - Sunbelt Sandbox
- <http://dshield.org> - statystyki
- <http://damballa.com/> - Front Line Against BotArmies



LogicalTrust IT Security Solutions



Dziękujemy za uwagę

Logicaltrust - IT Security Solutions

IT BCE sp. z o.o.

Borys Łacki - b.lacki@itbce.com
Patryk Dawidziuk - p.dawidziuk@itbce.com

LogicalTrust

IT Business Consulting Experts Sp. z o.o.
50-453 Wrocław, ul. Hercena 3-5

office@logicaltrust.net
<http://www.logicaltrust.net/>