



Garnkiem miodu w zombie

detekcja, analiza, dns-blackholing

Borys Łącki – Patryk Dawidziuk

<http://www.logicaltrust.net>



Podstawy teoretyczne

- botnet – informacje ogólne
 - armia komputerów zainfekowana trojanami (botami)
 - słucha rozkazów od C&C
 - wykonuje polecenia nie tylko polecenia legalnego właściciela
 - **rozprzestrzenia się**



Podstawy teoretyczne

- „poznacie ich po owocach (...)” Mat. 7:16
 - skanowanie po portach i exploitowanie ofiar
 - 135, 445, 139 i inne ogólnie znane
 - <http://dshield.org> prezentuje zestawienie najczęściej atakowanych portów:

Top 10 Ports

by Reports

Port	Reports
22	1844704
445	573405
1434	541200
25	486018
20940	396591
139	393529
1433	383181
1026	367506
41170	314922
135	259727

by Targets

Port	Targets
22	1561054
1434	117936
80	90991
135	88129
2967	79727
5900	77580
3389	66585
1026	62401
137	58676
1433	58179

by Sources

Port	Sources
27016	61698
41170	52878
1026	47093
6881	47034
1028	29844
20940	26816
48286	26074
1027	25835
25	21305
21411	18611

port report



Podstawy teoretyczne

– port 22

- ataki typu 'brute force', przeważnie 2 fazowe
 - 1) zdobycie lokalnego konta (niekoniecznie z uid=0)
 - boty ircowe
 - strony phishingowe
 - 2) jeżeli uid != 0, próba eskalacji uprawnień (exploitowanie, najczęściej błędów w kernelu)
 - DDoS,
 - sniffing ruchu sieciowego (hasła)

– port 445

- Microsoft Security Bulletin MS04-{011,012}
- dcom, lsass, itp.



Podstawy teoretyczne

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



Skuteczność wykrywania

Plik **mas.exe** otrzymany 2007.10.09 12:56:52 (CET)
Obecny status: **zakończono**
Wynik: **5/32 (15.63%)**

[Zwińź](#)

[Drukuj wyniki](#)

Antywirus	Wersja	Ostatnia aktualizacja	Wynik
AhnLab-V3	2007.10.9.1	2007.10.09	-
AntiVir	7.6.0.20	2007.10.09	-
Authentium	4.93.8	2007.10.08	-
Avast	4.7.1051.0	2007.10.08	-
AVG	7.5.0.488	2007.10.09	BackDoor.Generic8.UCK
BitDefender	7.2	2007.10.09	-
CAT-QuickHeal	9.00	2007.10.08	-
ClamAV	0.91.2	2007.10.09	-
DrWeb	4.44.0.09170	2007.10.09	-
eSafe	7.0.15.0	2007.10.08	-
eTrust-Vet	31.2.5198	2007.10.09	-
Ewido	4.0	2007.10.09	-
FileAdvisor	1	2007.10.09	-
Fortinet	3.11.0.0	2007.10.09	-
F-Prot	4.3.2.48	2007.10.08	-
F-Secure	6.70.13030.0	2007.10.09	-
Ikarus	T3.1.1.12	2007.10.09	Trojan-Downloader.Agent.YFZ
Kaspersky	7.0.0.125	2007.10.09	-
McAfee	5136	2007.10.08	-
Microsoft	1.2908	2007.10.09	-
NOD32v2	2579	2007.10.09	-
Norman	5.80.02	2007.10.09	-
Panda	9.0.0.4	2007.10.09	-
Prevx1	V2	2007.10.09	-
Rising	19.44.12.00	2007.10.09	-
Sophos	4.22.0	2007.10.09	Mal/Dropper-G

Wynik: **5/32 (15.63%)**

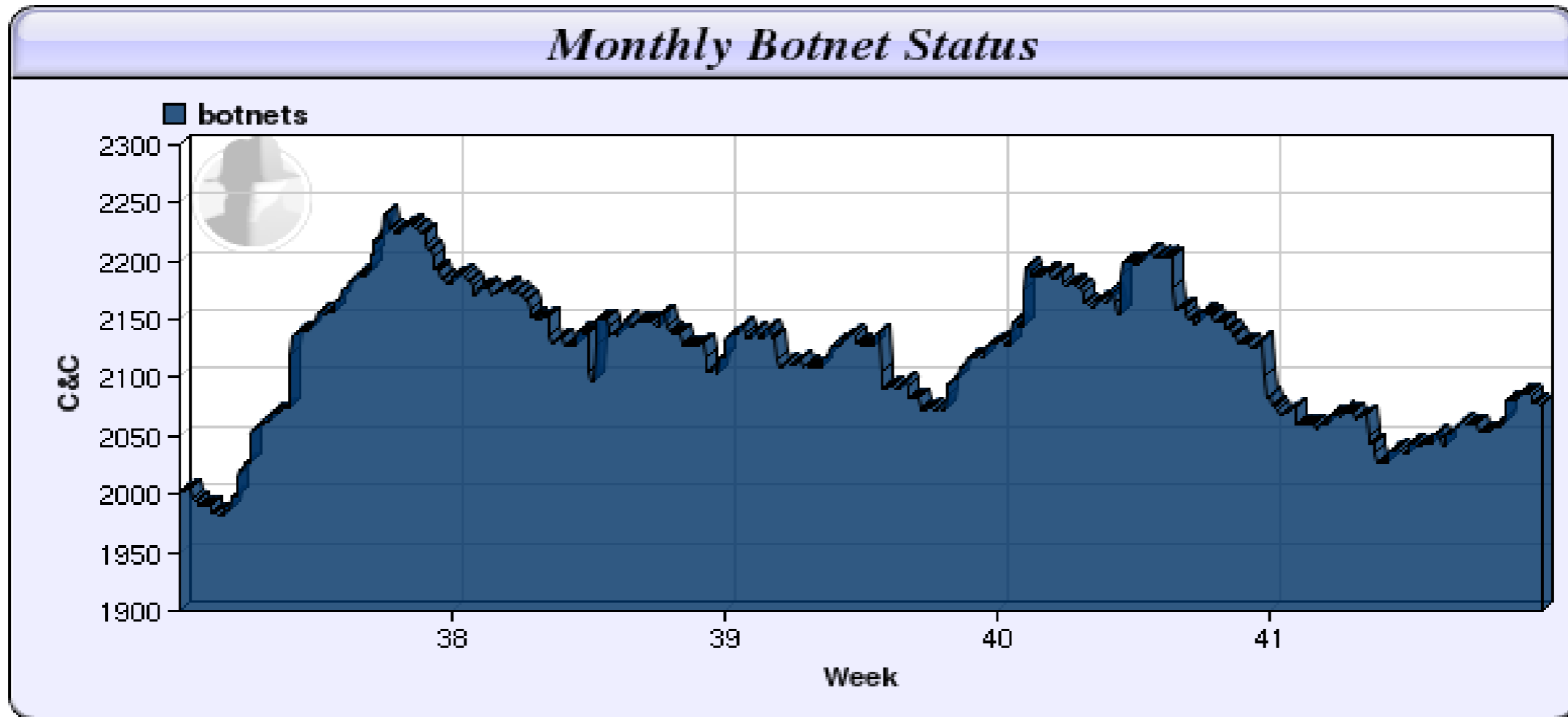


Fakty

- 2007.06 – operacja FBI „BOT ROAST”
 - ~1 milion zainfekowanych maszyn
- 2007.07 – Storm Botnet
 - ~1.7 miliona
- 2007.08 – Chiny
 - ~1 milion



Fakty

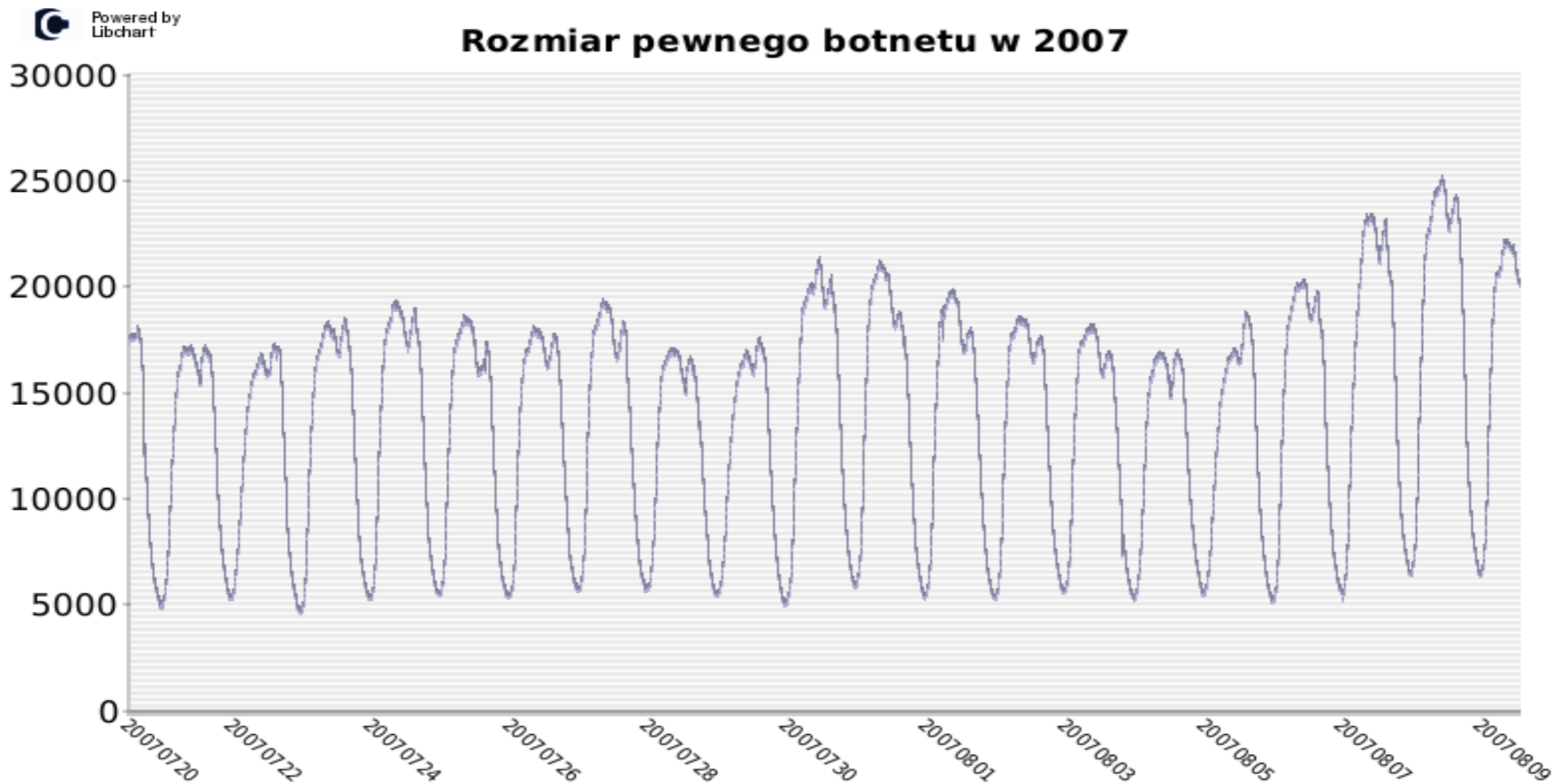


Źródło: www.shadowserver.org

1 000 000 botów / 2000 botnetów = 500 botów per botnet



Fakty





Spam

Upload: 256 Kb/s = 32 KB/s

1 spam = 11 KB

Srednia botów: 13862

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

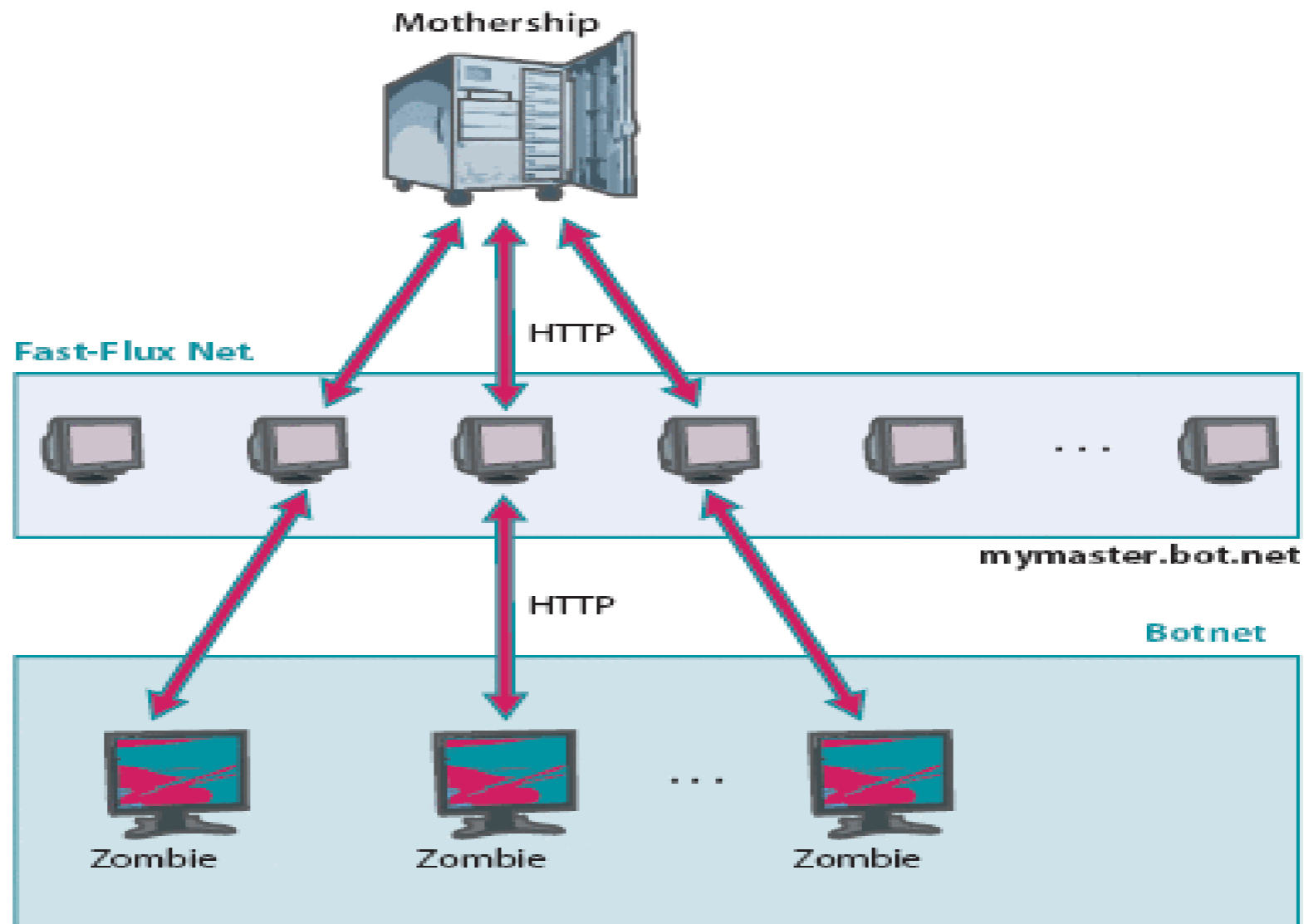
$159690240 / 11 = 14.517.294$ Wiadomosci typu spam / godzina

348.415.056 Wiadomosci typu spam / dziennie



Fakty

FastFlux



Źródło: <http://www.heise-online.pl>



Fakty

- **2007.02 Superbowl NHL:**
 - <http://www.miamidolphins.com>
 - <http://www.dolphinsstadium.com>
- **2007.06 „Italian Job”** - podmienione > 10.000 stron w ciągu 24 godzin
- **2007.09 Bank of India** - 31 unikalnych exploitów



Narzędzia

- **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 \$

http://www.iframedollars.com/?lang=en



JOIN US AND START MAKING MONEY TODAY!
DO YOU WANT TO EARN MUCH MONEY ON THE TRAFFIC?
SIGNUP TODAY!
WE HOPE TO HAVE A LONG-TERM COOPERATION WITH YOU!

LAST NEWS

04/09/07:
We Increased rates!:
We Increased rates for all countries! Now its for 20% MORE!

11/07/06:
Asia accept!:
Now we accept ASIA loads(China, India, Korea etc.)!

31/05/06:
New anti antivirus system:
From the 31th of May the new system of anti antivirus is started.

14/11/05:
CGPAY payments:
From the 14th of November we can pay with help of CGPAY

10/10/05:
New tariffs:
From the 10th of Octobre the new system of tariffing IS STARTED. From this moment we pay different \$\$ for different countries!

iframeCash.biz association is:

- Everyone is welcome to join the iframedollars.com partnership program
- Earn \$80/1000 installs) and more for each unique iframe installs
- You only put the short one line iframe code on your page(s) and start to MAKE MONEY
- WITHOUT any Active-X console or any pop-ups...It means that you will not lose your unique visitors with our iframe!
- The best percentage of installs (10-40% from the total traff or it's \$4-\$15 FOR 1000 UNIQUE VISITORS)
- DAILY updated soft
- We have 3 reliable servers with excellent speed
- Payments every Tuesday
- Real-time statistic of your work
- Payment via: Fethard, Webmoney, Wire, E-gold, Western Union (WU), MoneyGram, Anelik and Epassporte
- More than 300 webmasters work with us
- Friendly support service
- Everybody who works with us is satisfied.

HOME | TERMS | FAQ | SIGN UP | ABOUT US | RATES



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(B0A/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
```



Fakty

- Wywiady [1 osoba !!!]
 - **Phisher:** 30000 osób / 3000-4000 dolarów / dzień
 - **Spamer:** 10-15000 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 (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) 2004-2006 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) 2004-2006 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>**
 - 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:	2007-10-19 01:50:07
Wszystkich ataków:	1.542.714
Unikalnych źródłowych adresów IP:	85774
Unikalnych docelowych adresów IP:	1274
Unikalnych plików malware:	7326



Statystyki

- maksymalna ilość ataków ze źródłowego IP:
 - xxx.xxx.80.246 – **37542**
- minimalna ilość ataków ze źródłowego IP:
 - xxx.xxx.102.15 – **1**
- maksymalna ilość ataków do docelowego IP:
 - xxx.xxx.32.29 – **12281**
- minimalna ilość ataków do docelowego IP:
 - xxx.xxx.58.19 - **3**



Statystyki

Maksymalna ilość ataków dla malware:
7d99b0e9108065ad5700a899a1fe3441
[392 unikalne adresy URL]

87907

Ataków na minutę:
Ataków na godzinę:
Ataków na dzień:

4.38

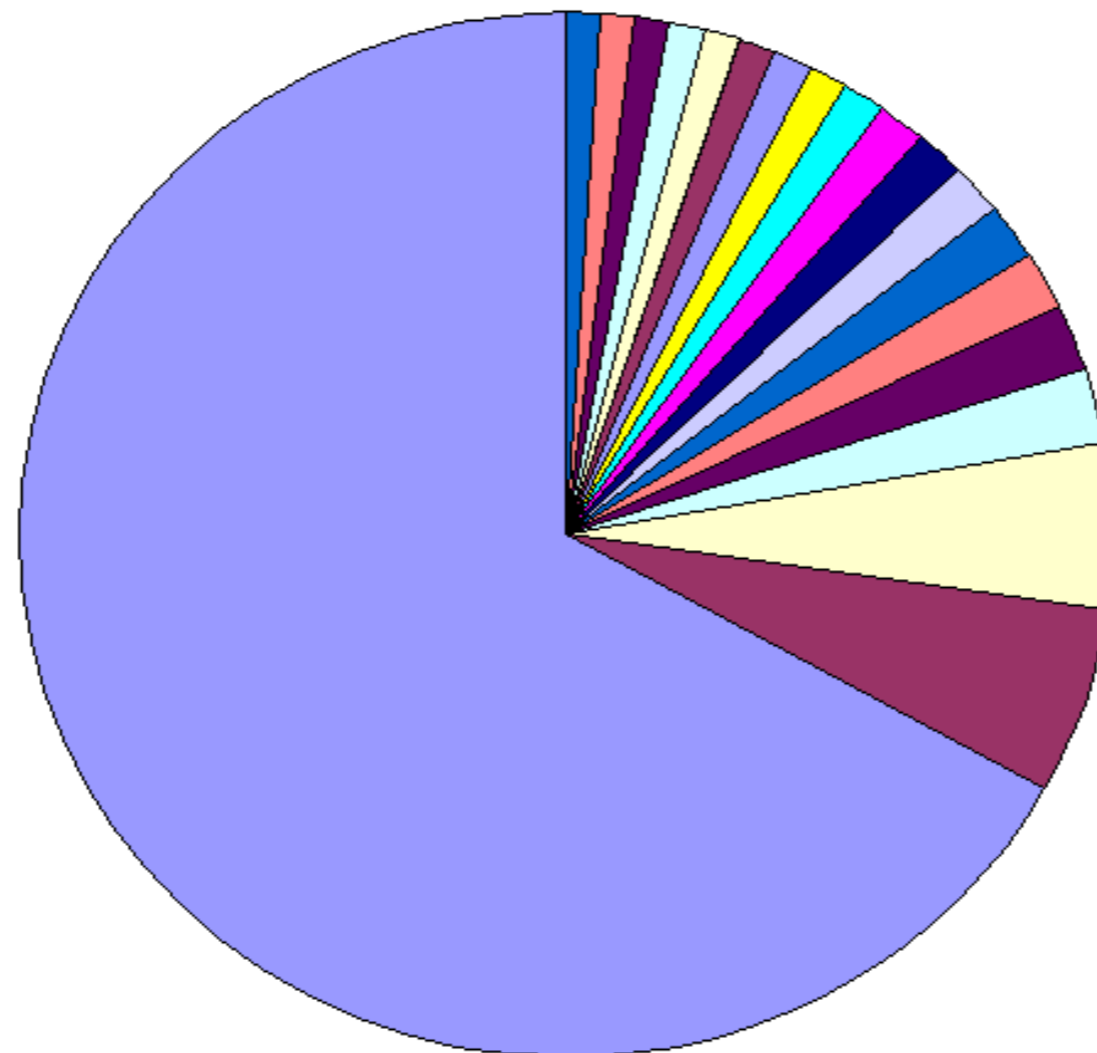
263.15

6315.77



Statystyki

SSH login

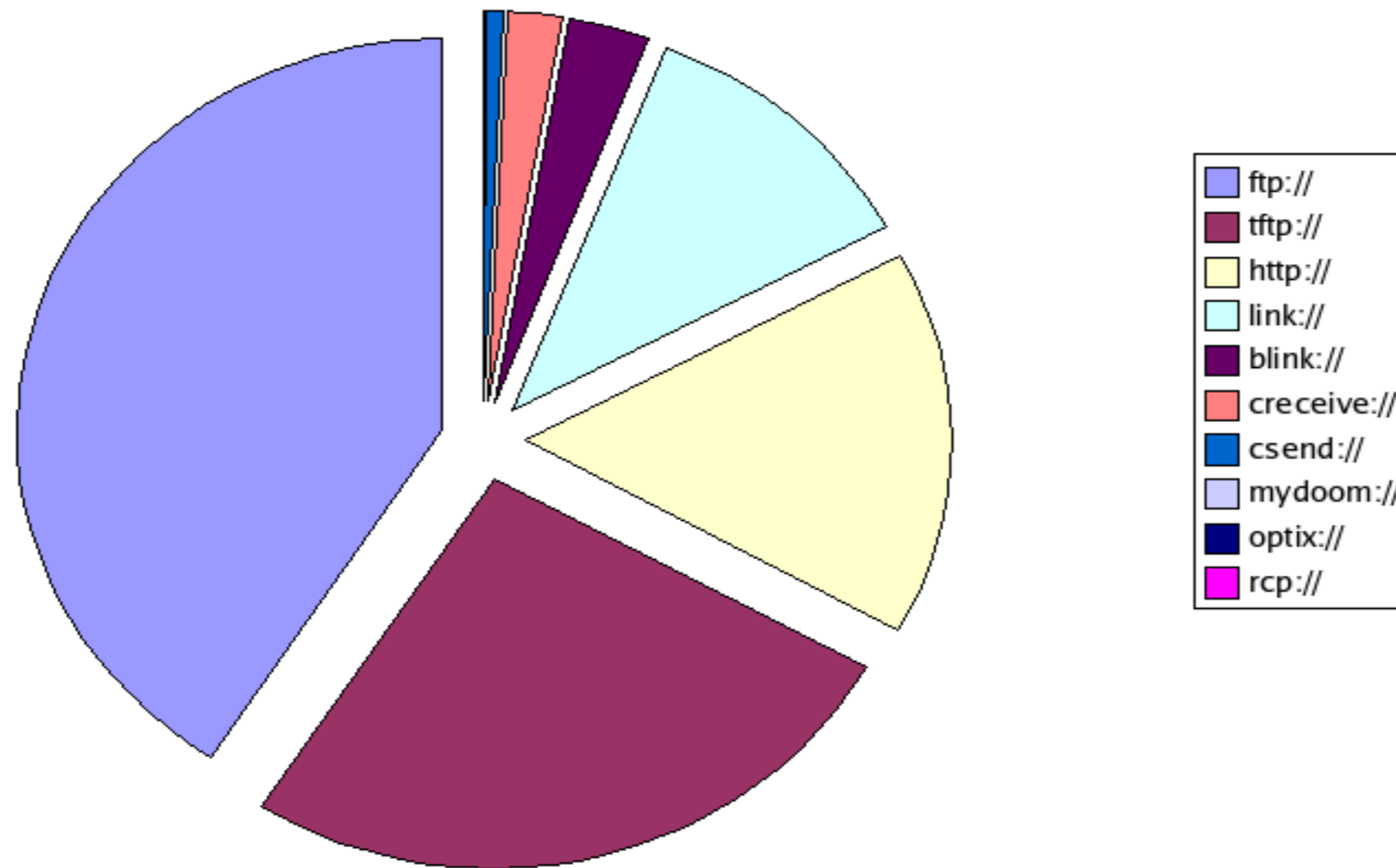


- root
- admin
- test
- guest
- user
- mysql
- www
- oracle
- webmaste
- info
- postgres
- apache
- ftp
- web
- tester
- student
- data
- sales
- testing



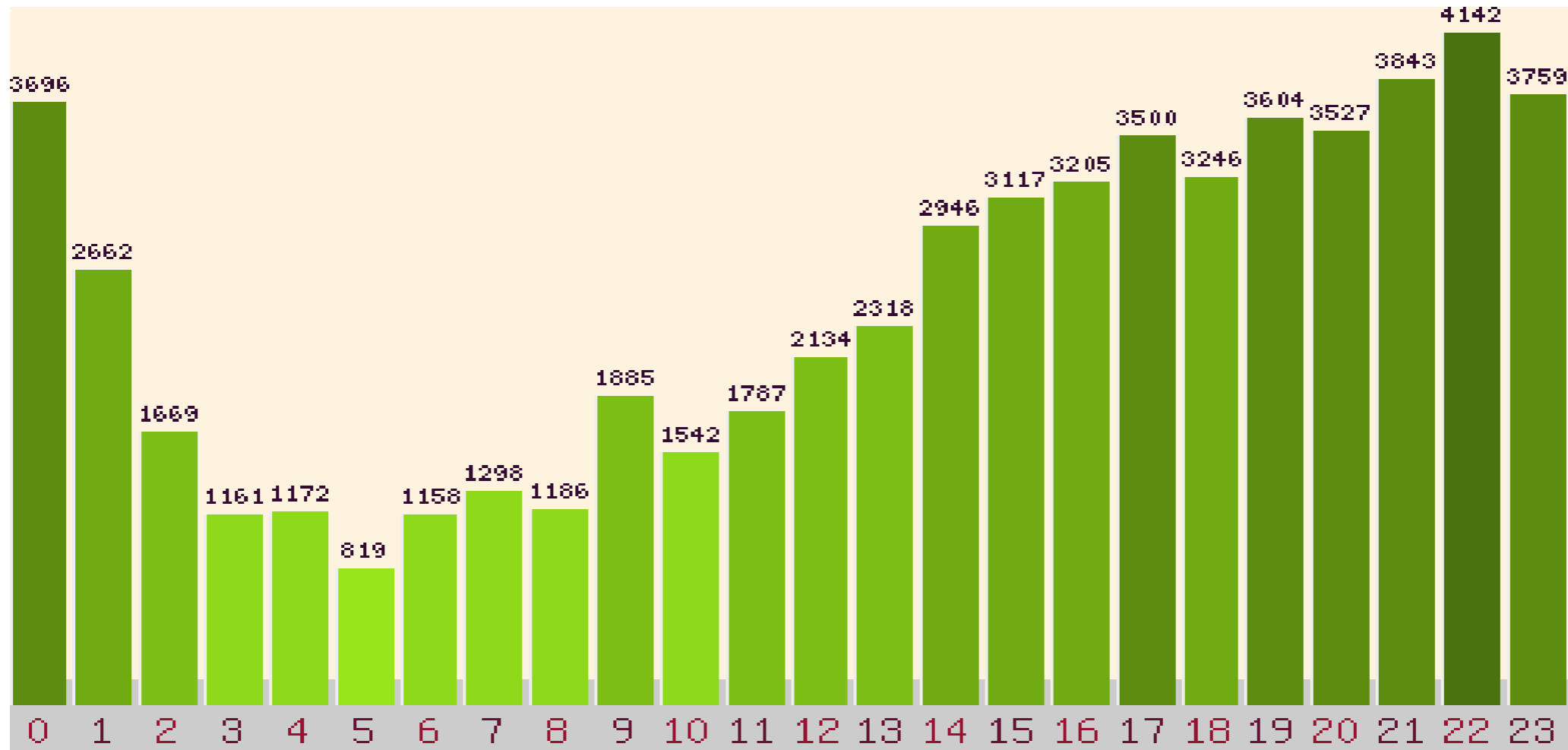
Statystyki

Malware Download Protocol





Statystyki



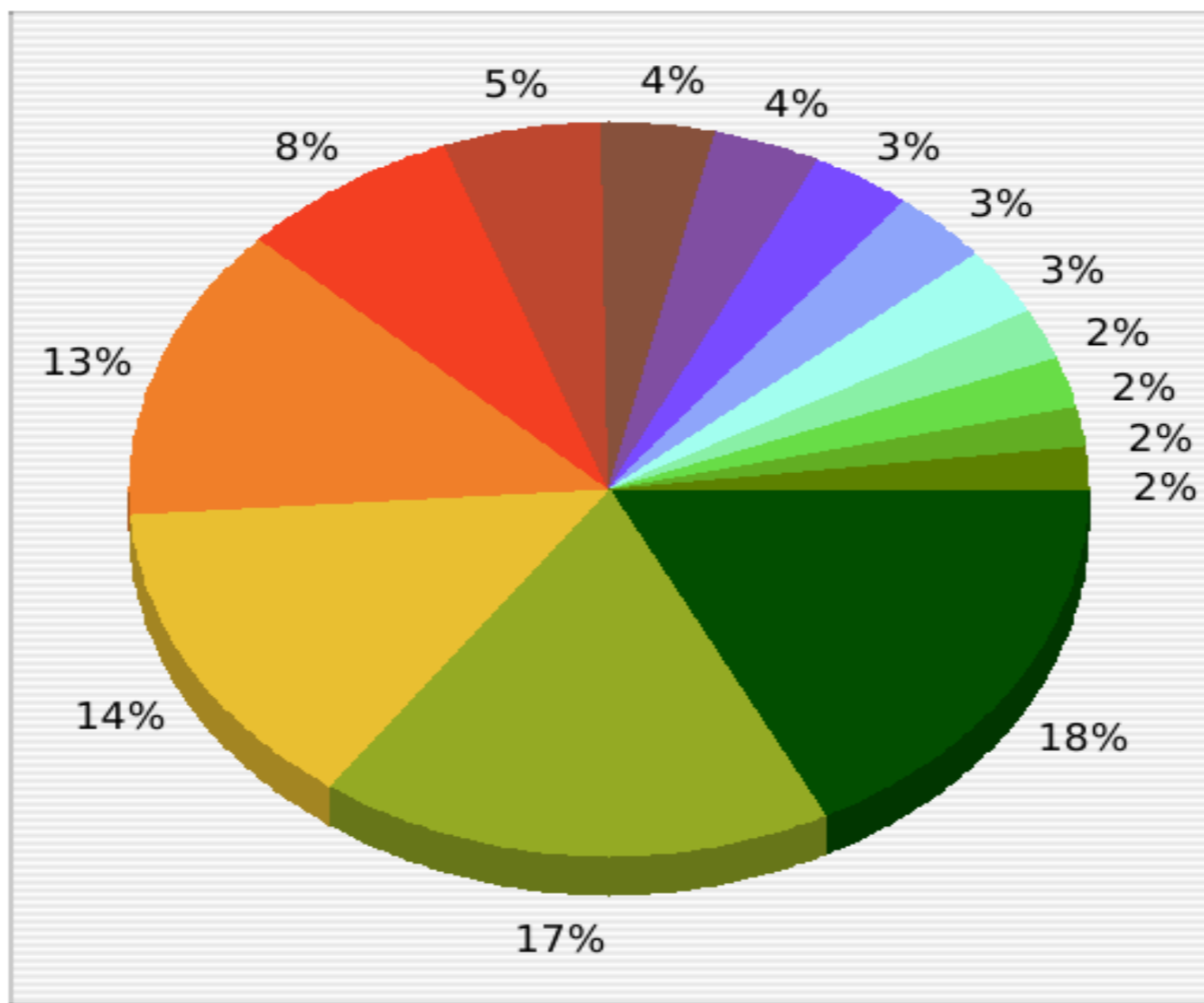
Ilość ataków / godzina
[2007.09] - maks: 4142 o 22.xx



Statystyki

Powered by Libchart

Atak / Source IP / Kraj



- 12602 (PL)
- 12420 (GB)
- 9964 (DE)
- 9298 (IT)
- 5387 (FR)
- 3790 (ES)
- 2645 (HU)
- 2590 (JP)
- 2474 (DK)
- 2353 (RO)
- 2228 (BE)
- 1548 (RU)
- 1476 (TW)
- 1327 (US)
- 1212 (BR)

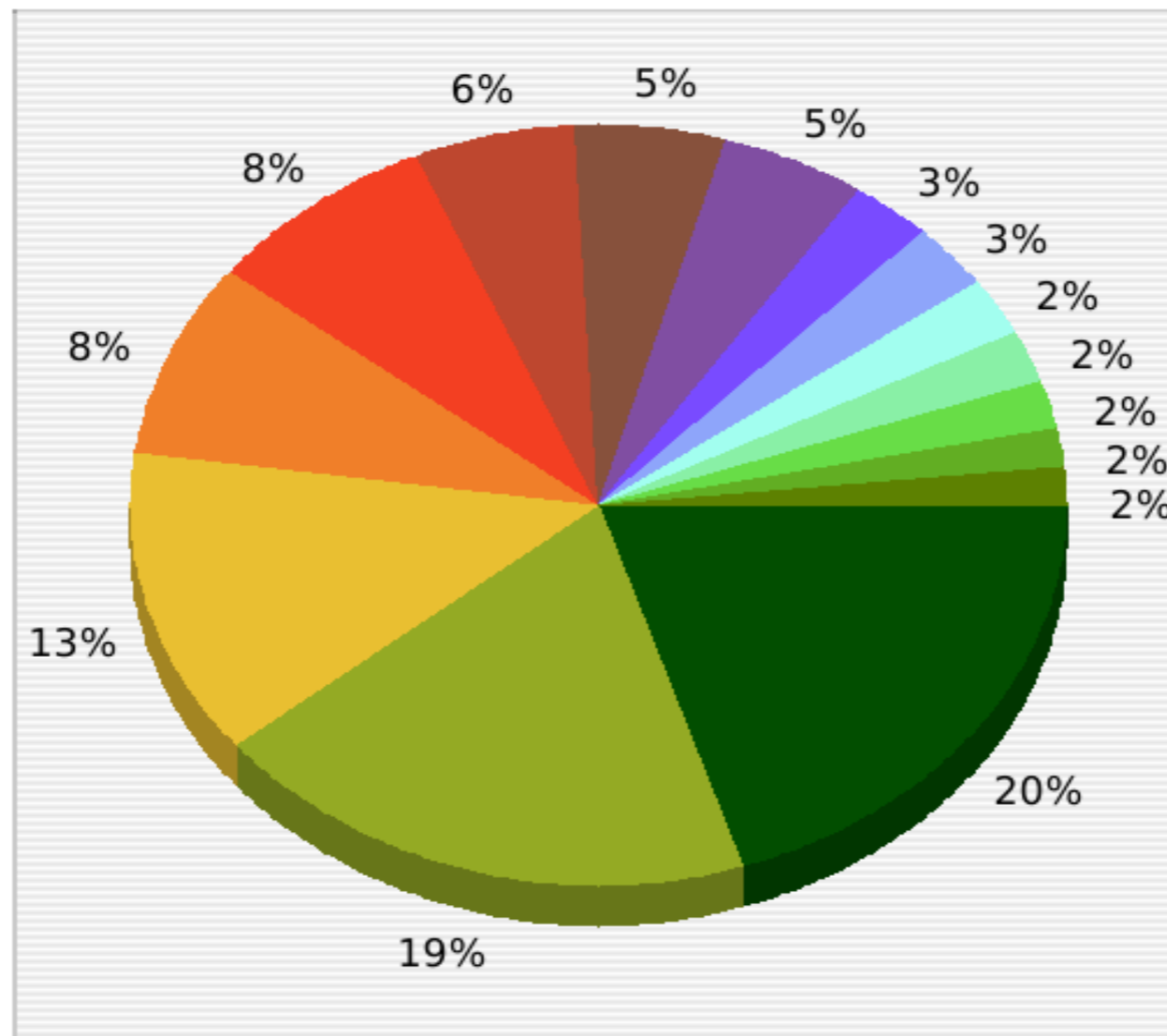
133 KRAJE



Statystyki

Powered by Libchart

Malware URL / IP / Kraj



- 6941 (DE)
- 6616 (GB)
- 4513 (IT)
- 2907 (PL)
- 2782 (FR)
- 1906 (JP)
- 1790 (DK)
- 1780 (HU)
- 966 (ES)
- 948 (RO)
- 825 (BE)
- 788 (US)
- 668 (RU)
- 570 (IL)
- 518 (JO)

40123 IP



Statystyki

384 domen serwerów C&C

244 has address xxx.xxx.xxx.xxx

62 not found

36 has no A record

29 connection timed out

9 has address 127.0.0.1

4 has address 0.0.0.0



Statystyki

384 domeny

Czas stałego dowiązania domeny do IP:

Najkrótszy: < 1 dzień

Najdłuższy: > 8 miesięcy

Maksymalna ilość wykorzystanych unikalnych IP: **9**

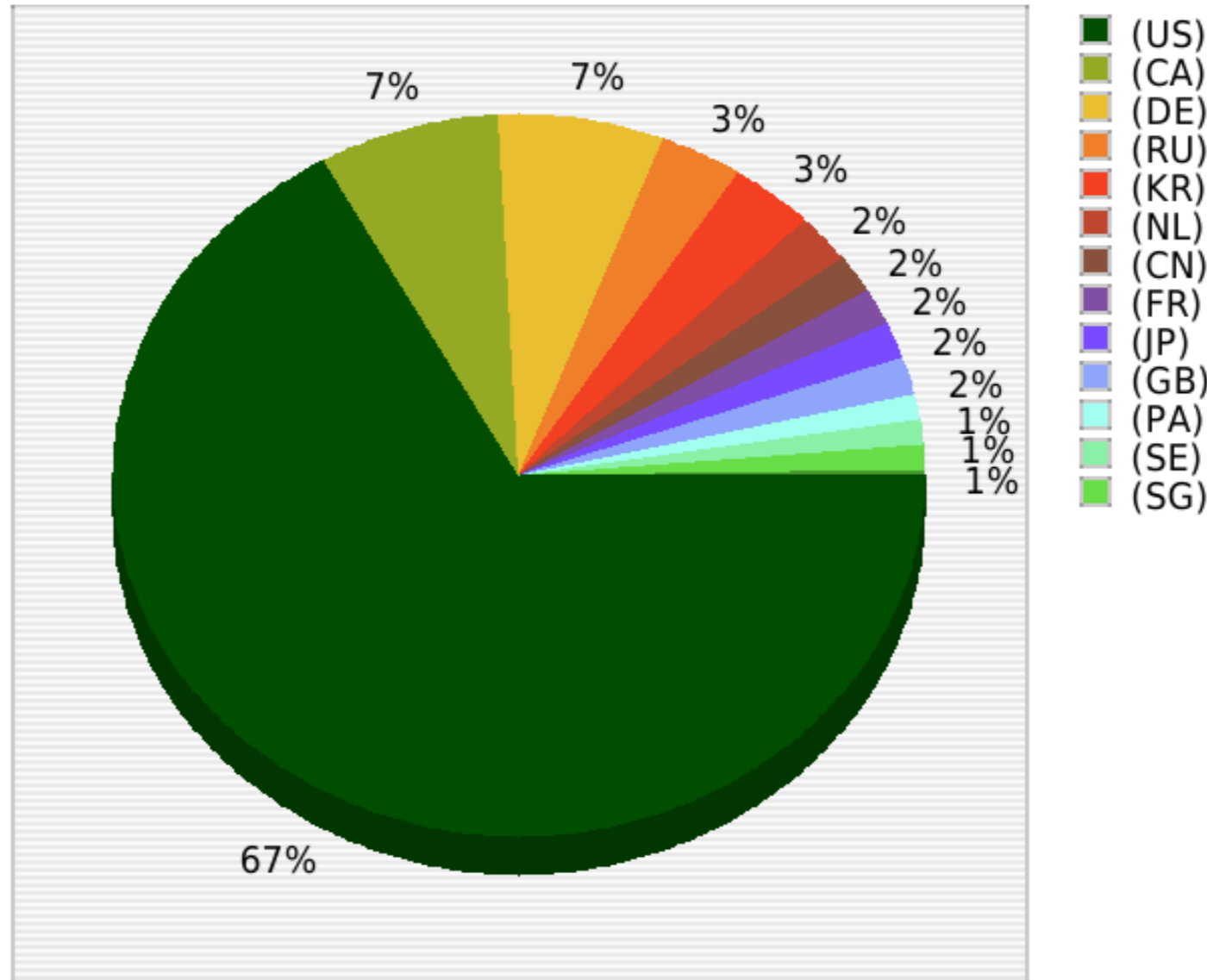
Maksymalna ilość jednoczesnych adresów IP do domeny: **8**



Statystyki

Powered by Libchart

C & C / Kraj





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
- 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'u – 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,
 - tak, zagłosowaliśmy już w wyborach,
 - projekt dns-blackholingu nie jest upubliczniony ze względu na brak odwaznych do jego hostowania,
 - ogólnodostępność projektu dns-blackholingu omawiamy po prezentacji



Linki

- <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



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/>