

Garnkiem miodu w zombie

Detekcja, analiza, dns-blackholing sieci botnet.

Borys Łącki – Patryk Dawidziuk

<http://www.logicaltrust.net>

SekIT – Opole 2008

CONFID

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**

Podstawy teoretyczne

- botnety występują w domu, w ogrodzie a nawet w kosmosie
 - w domu wiadomo - komputery w domu zainfekowane malware
 - w ogrodzie - ledwo wyjdziemy do ogródka, boty (specjalny rodzaj, dresoboty) przejmują nasz komputer
 - w kosmosie - ostatnio wykryte trojany na komputerach astronautów, które nie mają oprogramowania AV (“bo po co tam”)

Podstawy teoretyczne

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

CONFID

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/aplikacji (injections)

Podstawy teoretyczne

- coraz rzadziej wysyłają maile ze złośliwymi załącznikami
- coraz częściej wysyłają linki do stron z fałszywymi kodekami
 - próbując zmanipulować użytkownika do zainstalowania najnowszej wersji Flasha wysyłając informacje o np. wybuchu w elektrowni atomowej koło Londynu
 - lub po prostu nakłonić do kliknięcia w infekującego linka
- ... lub do kartek okolicznościowych z okazji różnych

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 (gnutella) lub własnych
 - fast-flux
 - hydraflux

Topologie sieci botnet

- przypadkowa (random) – jest to topologia przyszłości, którą badacze postrzegają jako następny krok w ewolucji botnetów
 - komunikacja w oparciu o JeszczeNieWiadomoCo(tm)
 - serwer C&C ciężki do wykrycia
 - długi czas życia bota

Podstawy teoretyczne

- możliwości wykorzystania botnetu
 - spam, phishing, fraud
 - terroryzm (“podobno macie problem z dostępem do sieci”, patrz dowcip o skinheadach, którzy uratowali staruszkę) czyli DDoS, DoS i inne ataki
 - kradzież tożsamości, danych osobowych, numerów kart kredytowych, dokumentów, paszportów, legitymacji
 - środki wspomaganie przy akcjach o podłożu politycznym

Bezpieczeństwo użytkowników



CONFID

„Spokojnie, jesteśmy bezpieczni.
Mamy antywirusa...”

88 % internautów posiada regularnie **aktualizowany** program antywirusowy.

Badanie CBOS / 2008.06

CONFID



Bezpieczeństwo użytkowników, NOT!



CONFID

http://www.virustotal.com/analysis/105e31182db3d6472fb3746dffe551fc

File **Setup_ver1.113.0.exe** received on 09.08.2008 12:55:35 (CET)

Current status: **finished**

Result: **5/36 (13.89%)**

 [Compact](#)

[Print results](#) 

Antivirus	Version	Last Update	Result
AhnLab-V3	2008.9.6.0	2008.09.08	-
AntiVir	7.8.1.28	2008.09.08	TR/Dldr.Zlob.Gen
Authentium	5.1.0.4	2008.09.07	-
Avast	4.8.1195.0	2008.09.07	-
AVG	8.0.0.161	2008.09.08	-
BitDefender	7.2	2008.09.08	-

- **Race To Zero** - 2 i pół godziny
- F-Secure – 25 000 próbek / dzień

CONFID



LogicalTrust

www.logicaltrust.net



BUSINESS CONSULTING EXPERTS

Fakty



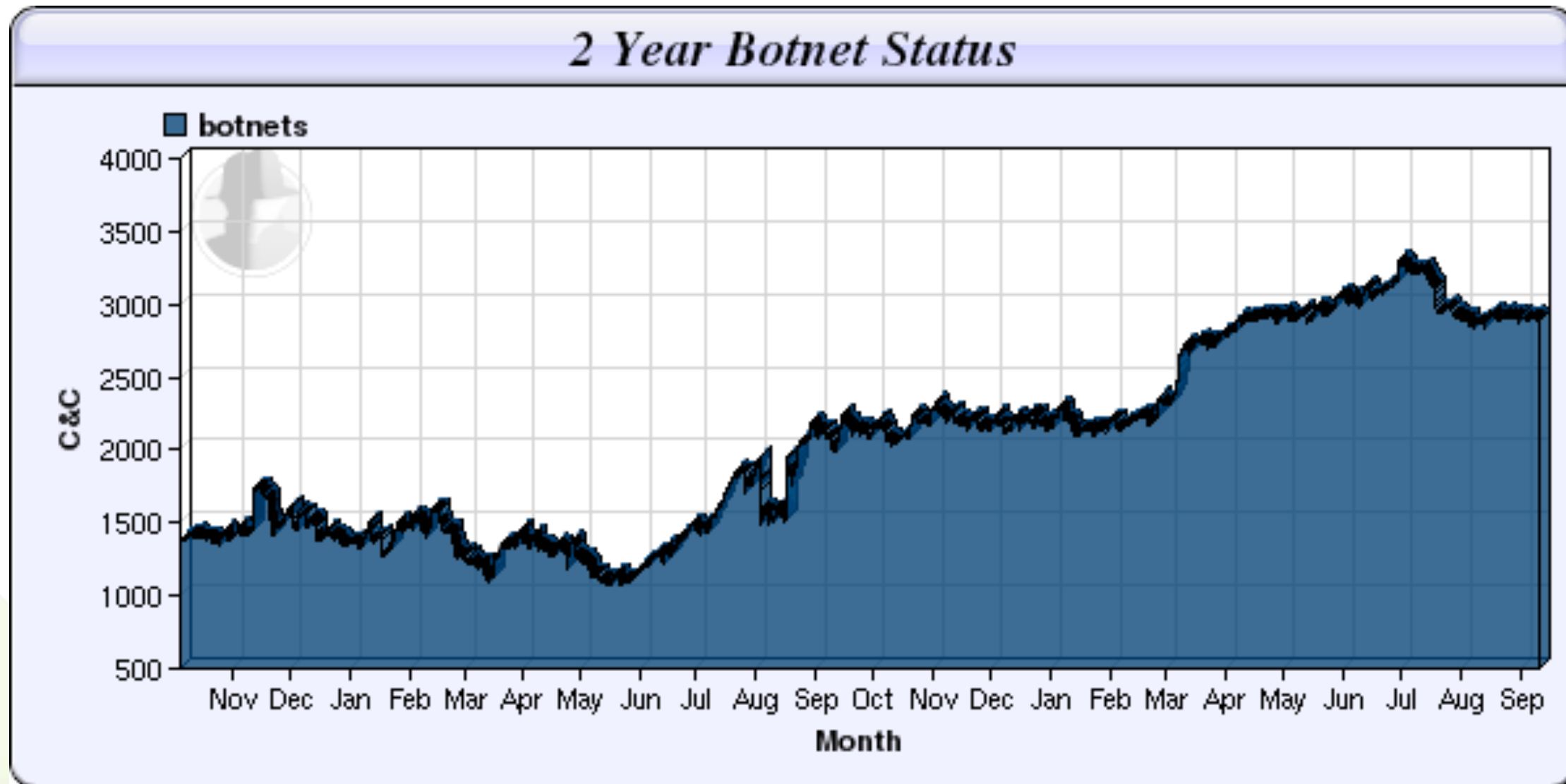
CONFID



- 2007.11 – Owen Thor Walker (18-latek)
~ 1 300 000
- 2008.03 – Kraken/Bobax botnet
~ 400 000 zainfekowanych maszyn
- 2008.04
~ 1 000 000 - Konferencja RSA (SecureWorks)
~ 350 000 - Srizbi botnet
- 2008.06 - Malicious Software Removal Tool
~ 700 000 – Taterf (1 dzień!)
- 2008.07 - Pat Peterson (Cisco Systems)
~ 1 400 000
- 2008.08 - Holandia
~ 100 000



Fakty

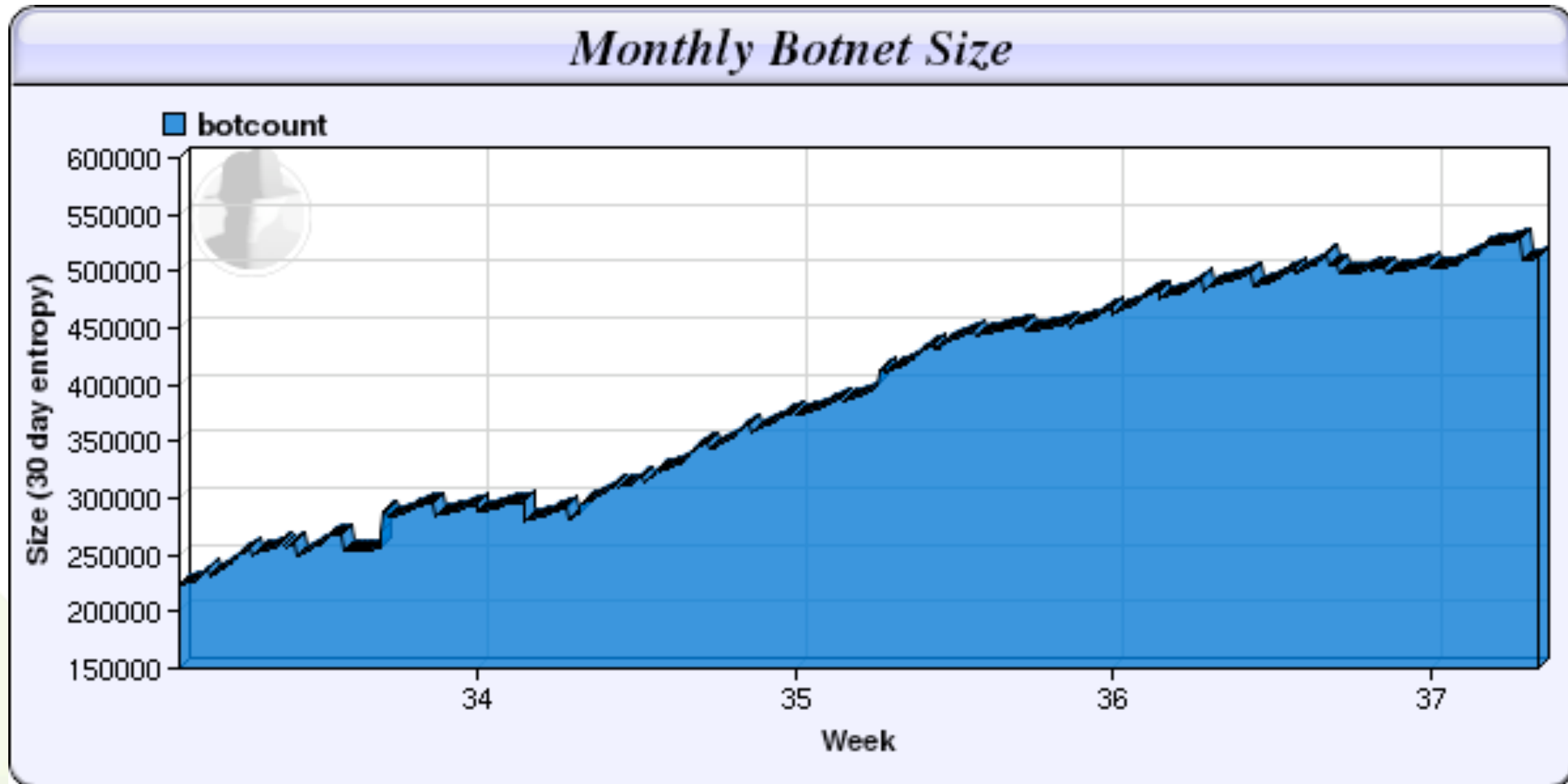


Źródło: www.shadowserver.org

CONFID

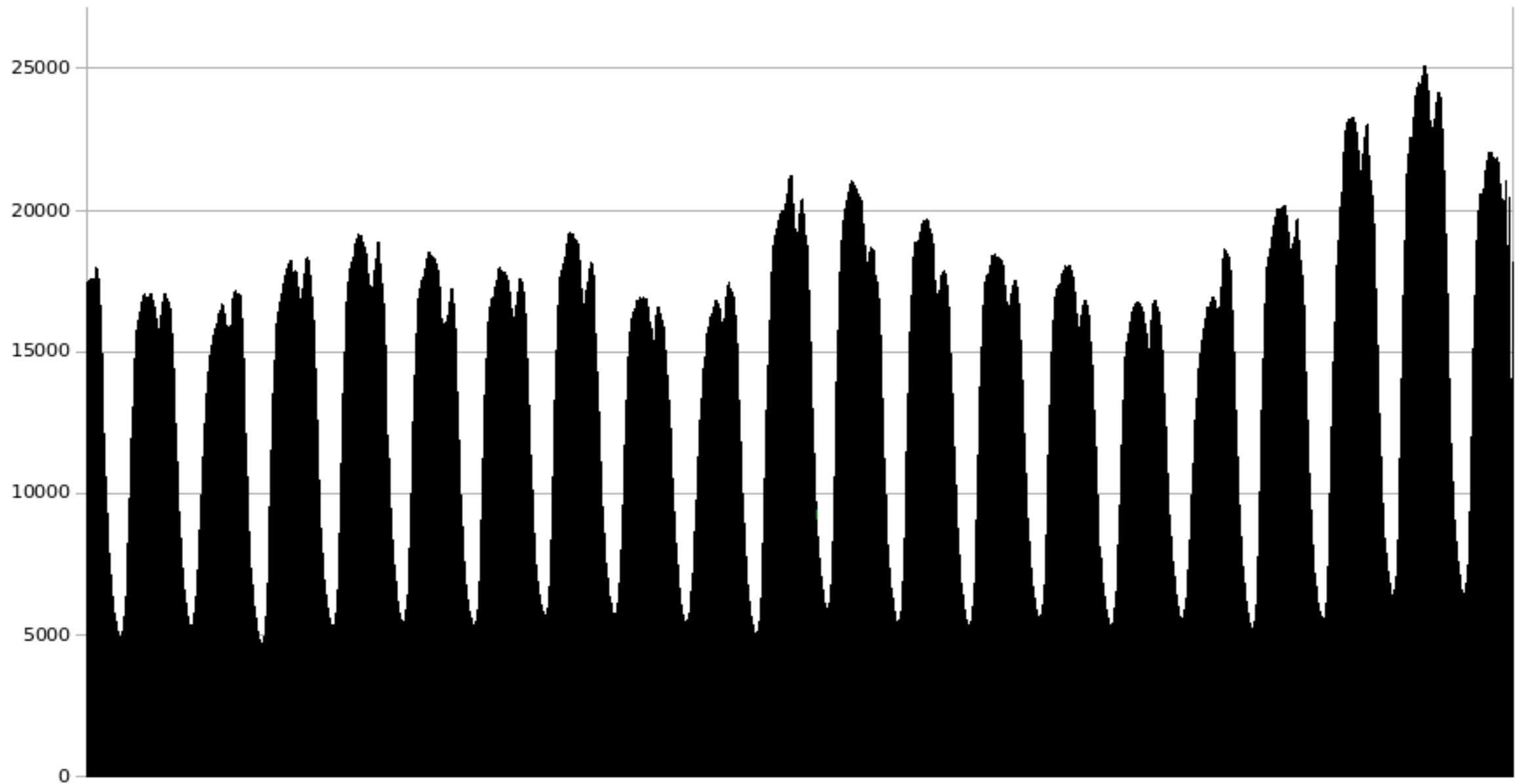


Fakty



Źródło: www.shadowserver.org

CONFID



2007.07.20

Rozmiar pewnego botnetu

2007.08.14



CONFID



SPAM

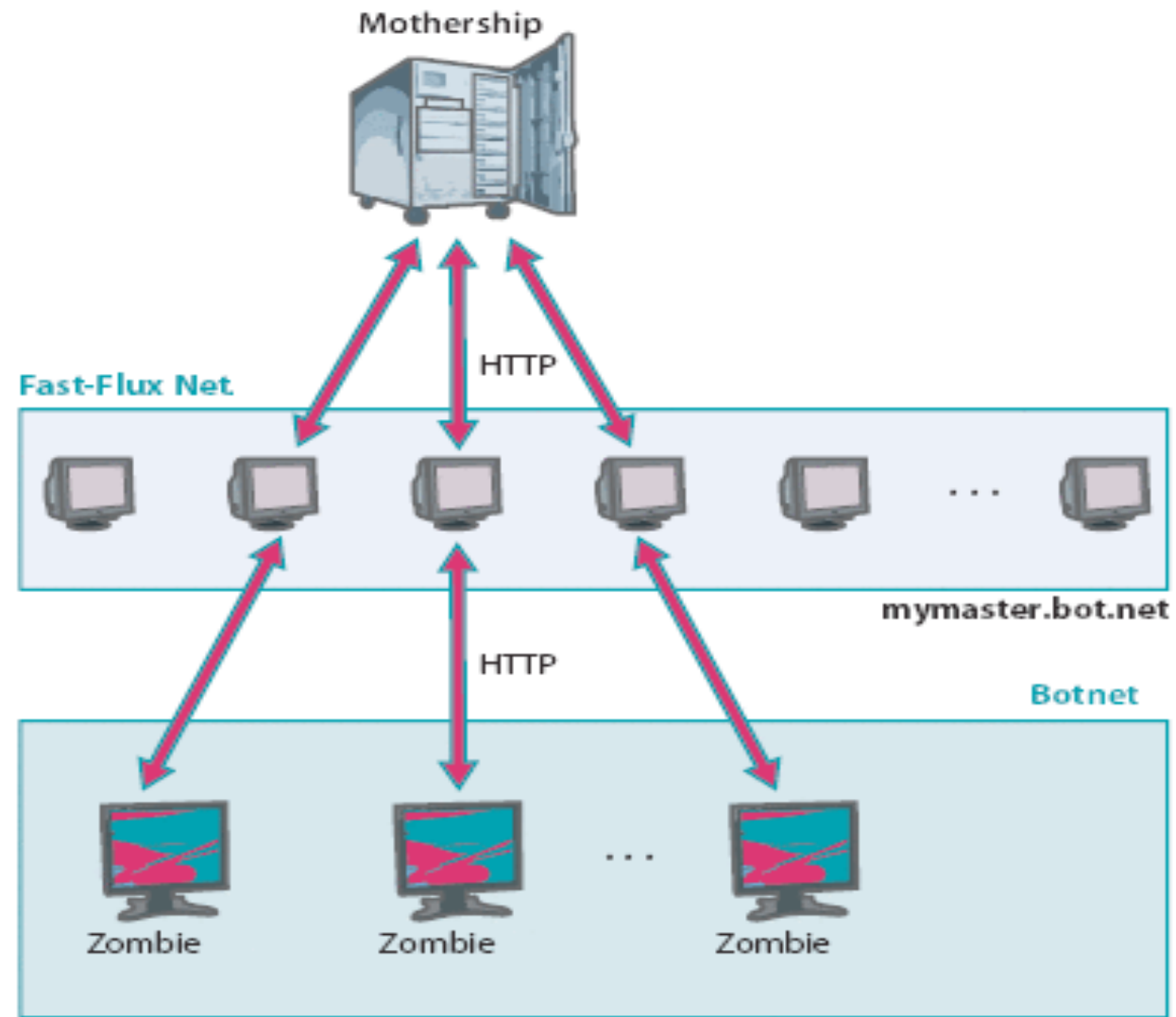
Upload: 256 Kb/s =	32 KB/s
1 spam =	11 KB
Średnia ilość botów:	13.862

$32 * 13.862 * 3.600 = 159.690.240$ KB /h = 156 GB /h
 $159.690.240 / 11 = 14.517.294$ wiadomości typu spam /h

348.415.056 wiadomości typu spam / dziennie

Fakty

- FastFlux
- Hydra



+ P2P

Źródło: <http://www.heise-online.pl>

CONFID

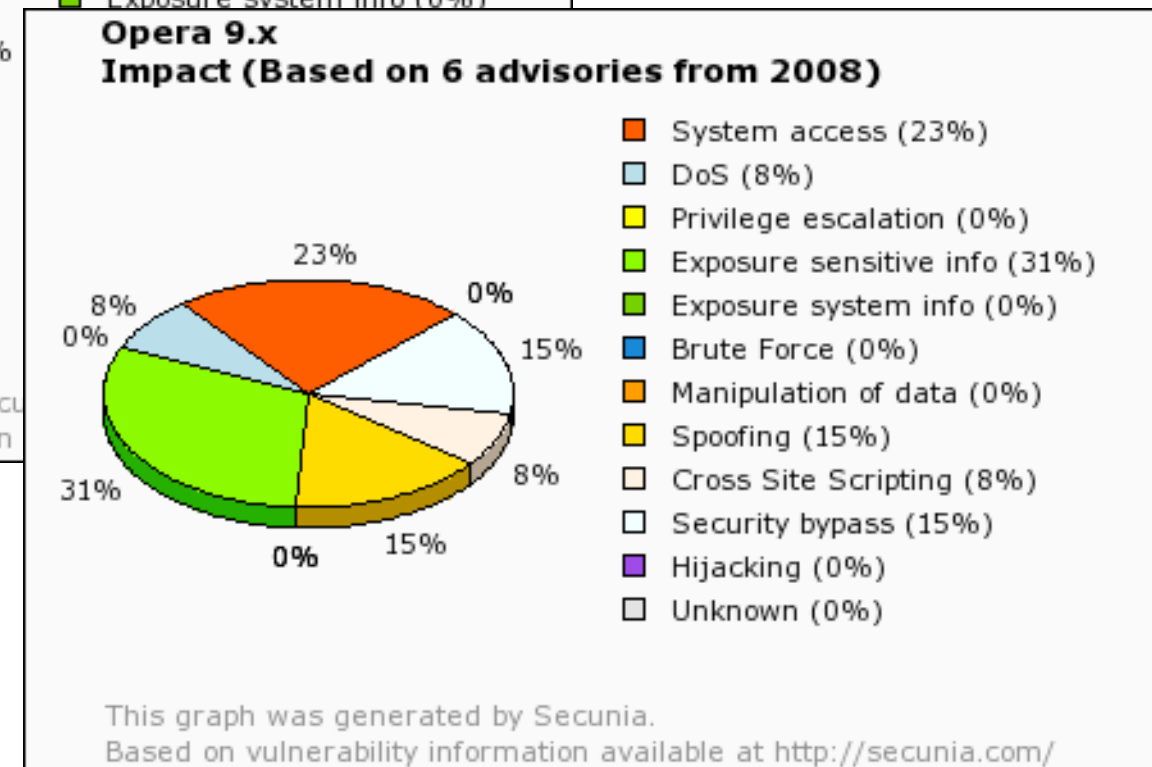
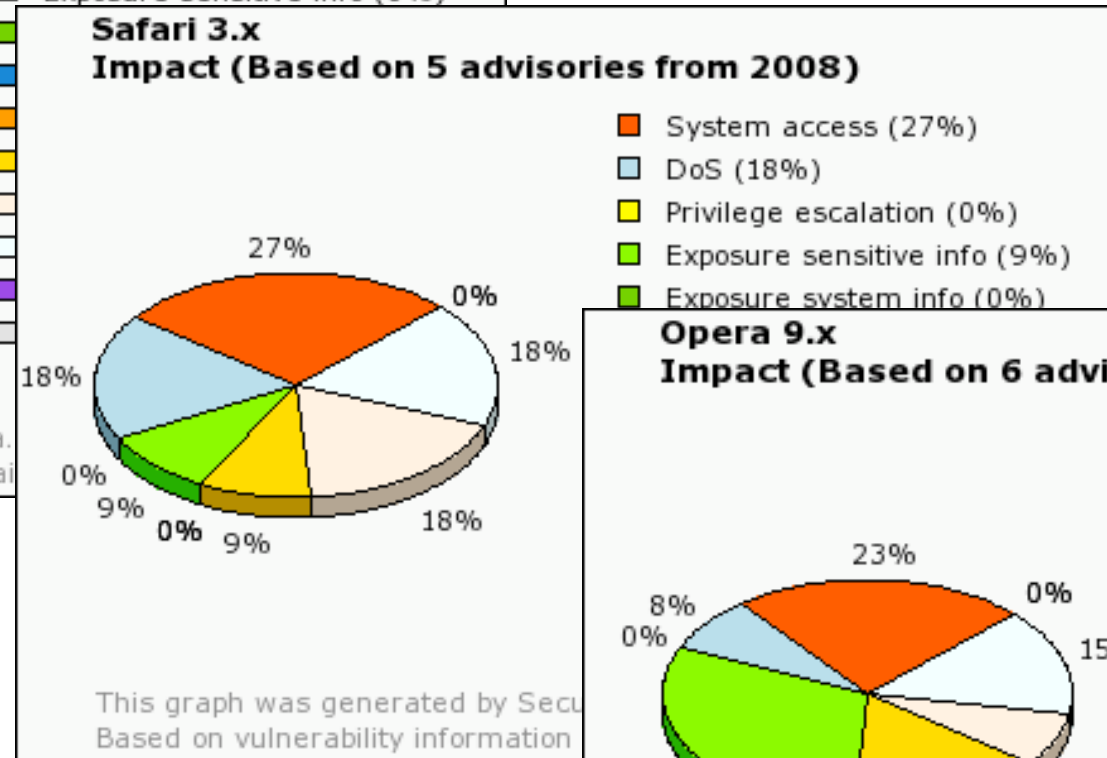
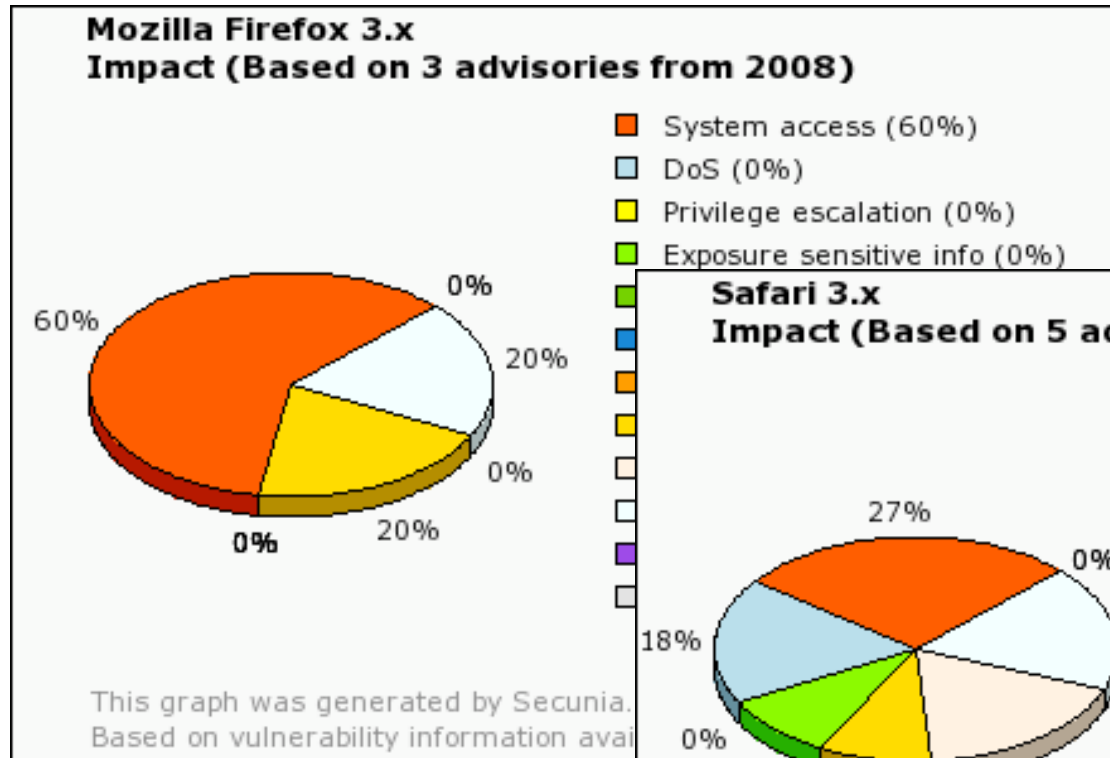
Fakty - WWW



„Alternatywy 4”



Fakty - WWW



- URL Handler Crash
- "SaveAs" stack-based overflow
- Automatic File Download
- Malicious link DoS
- Inspect Element DoS

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)

CONFID



„Botnet FastFluxowy każdy z nas ma... Mam i ja...”



Narzędzia

- **cuteQQ** - multi rootkit (400 – 3000 Juanów | 120 – 900 zł)
- **Zeus** - multigenerator
- **MPack** - Malware Kit [PHP]
- **DreamSystem** - zarządzanie sieciami botnet [WWW]
- **Xrumer** – Forum Spam

„Best price my friend, best price...” 50 – 1000 \$

- Icepack, Firepack, Neosploit, Pinch, Tornado, Ultra Lite Pack, G-Pack, Exploit Multipackage, Death-Pack, Apophis, DoS 5.0, BlackEnergy, Fishing Bait, Limbo 2, MicroJoiner, My Poly Sploits, PhpSpy, Ring 0, Shark 2, Turkojan 4.0, WOW Loader, Zunker.....

Narzędzia

Site:	ajcjobs.com
Login:	ajcjobs.com aol
Password:	careerbuilder.com-proxy careerbuilder.com-socks careermag.com computerjobs.com hotjobs.com jobcontrolcenter.c jobvertise.com militaryhire.com monster.com newmonster.com newmonster.com2 seek.com.au
Date (mm/dd/yy):	
Job Location:	-- All --
Parse pages:	10000
Target email:	
<input type="button" value="Start"/>	

Pinch 2 PRO builder
File About Build 2.60

Default

SMTP | HTTP | FILE | Protocol

str:

IRC-bot

Values

KEY:

DLL:

EXE:

SVC:

DIS:

Windows Firewall (SP2)

暗黑工作组

购买咨询QQ: 784378237 (仅此一位, 提防被骗)

会员验证

机器码 注册码

用户 密码

功能选项

智能性分析 延时性运行

智能化统计 破主动防御

破瑞星卡卡 破杀软拦截

破 IE 拦截 破 IE 监控

禁源码查看 禁右键点击

智能化检测 智能化除错

配置地址

木马地址:

存放地址:

统计地址:

生成选项

Ms Access Ms06014 Ms07004 Ms07055 Ms08011 Realplay11
 Yahoo Exp Google Exp 暴风影音 联众0day 迅雷网马 Realplayer

生成模式

.Gif模式

.Htm模式

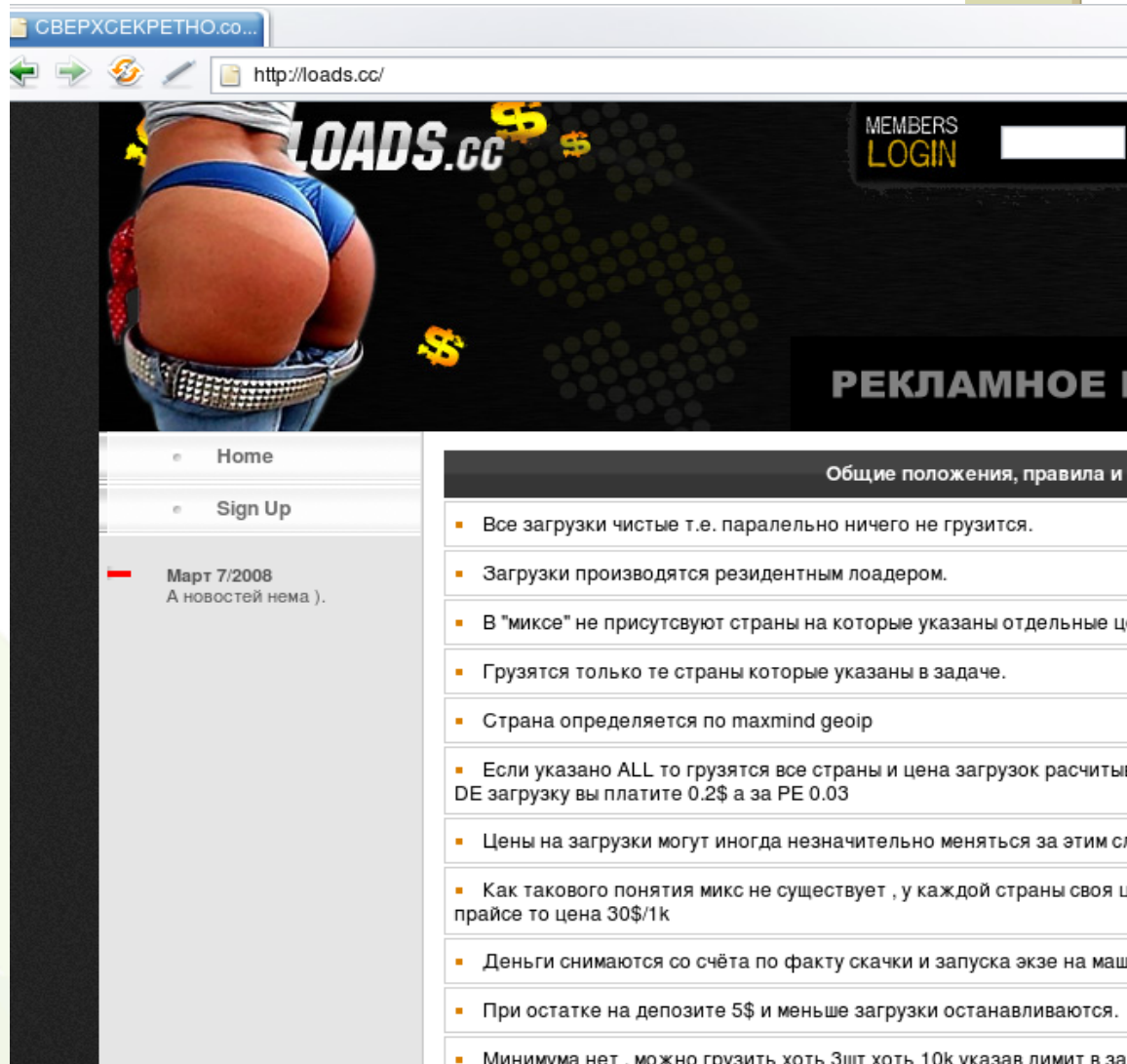
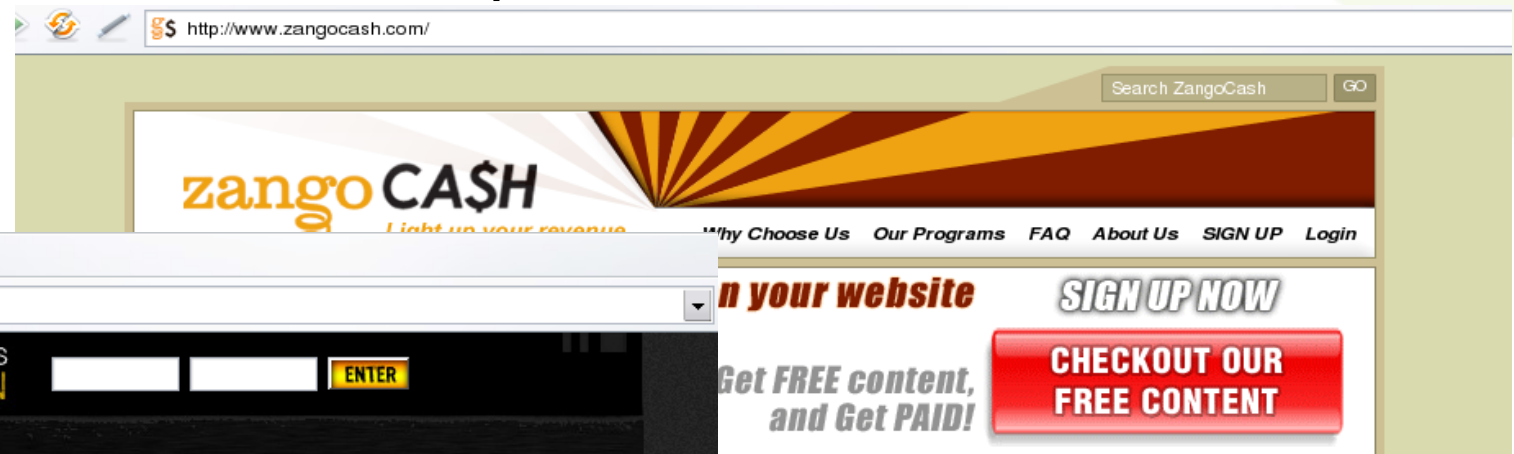
服务状态

其它

暗黑网马者 [Vip2008 Standard VerSion 3] Copyright (C) 2008 www.CuteQq.cn All Rights Reserved .

CONFID

Adware \$



CONFID



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
```

CONFID

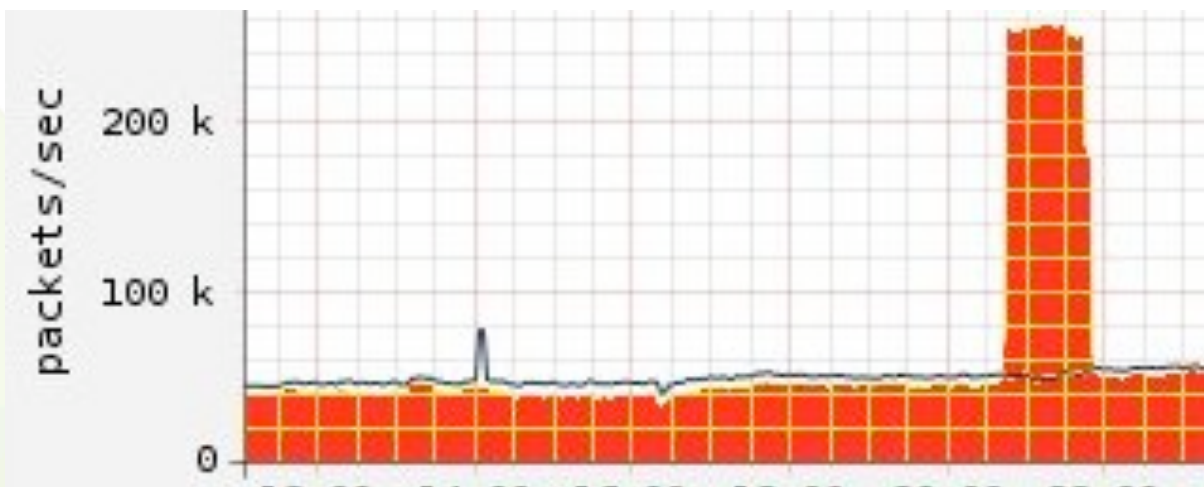
Czarny rynek \$\$\$

2004 – Forrester - **20 %**
2008 – Marshal - **29 %**

... uczestników badania przyznało, że dokonało zakupów ze spamu

Ile kosztuje SPAM

1.000.000 wiadomości E-mail	-	5 – 10 \$
10.000.000 wiadomości dziennie	-	600 \$
1.000.000 wiadomości ICQ	-	150 \$
1 wiadomość SMS	-	0.2 \$



...a ile kosztuje DDoS

1 godzina	-	10 \$ - 20\$
1 dzień	-	100 \$
> 1 dzień	-	> 200 \$
10 minut	-	free

CONFID

Czarny rynek \$\$\$

BOTNET

400 000 maszyn - 300 - 700 \$

ADRESY E-mail

1.000.000 - 100 \$
 3.000.000 - 200 \$
 5.000.000 - 300 \$
 8.000.000 - 500 \$
 16.000.000 - 900 \$
 32.000.000 - 1500 \$

ICQ 1 numer - 1 - 10 \$

FTP 1 konto - 1 \$

CAPTCHA

500 - 0.025 \$ - 12.50 \$
 5.000 - 0.020 \$ - 100 \$
 50.000 - 0.015 \$ - 750 \$
 500.000 - 0.010 \$ - 5.000 \$

AntiAntiVirus

1.exe - 1 - 5 \$

Limbo Trojan Logi

50 MB - 30 \$

CONFID

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

> 30.000 (PC i Mac)
Wygenerowało ruch na
poziomie **10 Gb/s.**



Serwery są przeciążone...

Wystap błą z powo zagrożeń przeciąż, pros ni próbow ponown.

zepsól.nasza-klapa.pl

CONFID

Zarobki \$\$\$

Król wysyłania spamu - Scott Richter

- 2004 – 50.000 \$ grzywny na rzecz stanu - > Nowy Jork
- 2006 - zapłacił już 6.000.000 \$ -> Microsoft
- 2008 – **6.000.000 \$** -> MySpace

150 000 000 \$ - przychody MyCanadianPharmacy.com
Pat Peterson (Cisco Systems)

- 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
 - boty skanują sieć, lokalną i każdą inną, w poszukiwaniu nowych ofiar
 - wykrycie (w dowolny sposób) skanowania sieci, najczęściej oznacza towarzystwo
 - można próbować w wyższych warstwach sieci (http, smtp)
 - a może po sygnaturach ruchu?
- wykrycie dużej ilości wysyłanego spamu także oznacza „towarzystwo”

Detekcja

- analiza ruchu na porty IRC
 - była skuteczna jeszcze dwa lata temu
 - czarny rynek powoli odchodzi w kierunku protokołów trudniejszych do namierzenia i komunikacji w oparciu o sieć p2p
 - oczywiście dalej można kupić starsze typy botów komunikujące się właśnie tą metodą (botnet dla ubogich)

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:
 - 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



LogicalTrust

www.logicaltrust.net



IT BCE BUSINESS CONSULTING EXPERTS

Nepenthes

przykładowe analizy

CONFID

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.

CONFID

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.

CONFID

Nepenthes

boty patchujące system, żeby nikt nie wykorzystał tej samej luki drugi raz istnieją (serio serio)

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.EXE>

as C:\WINDOWS\TEMP\patch.exe.

- * Connects to "download.microsoft.com" on port 80 (TCP).
- * Opens URL:

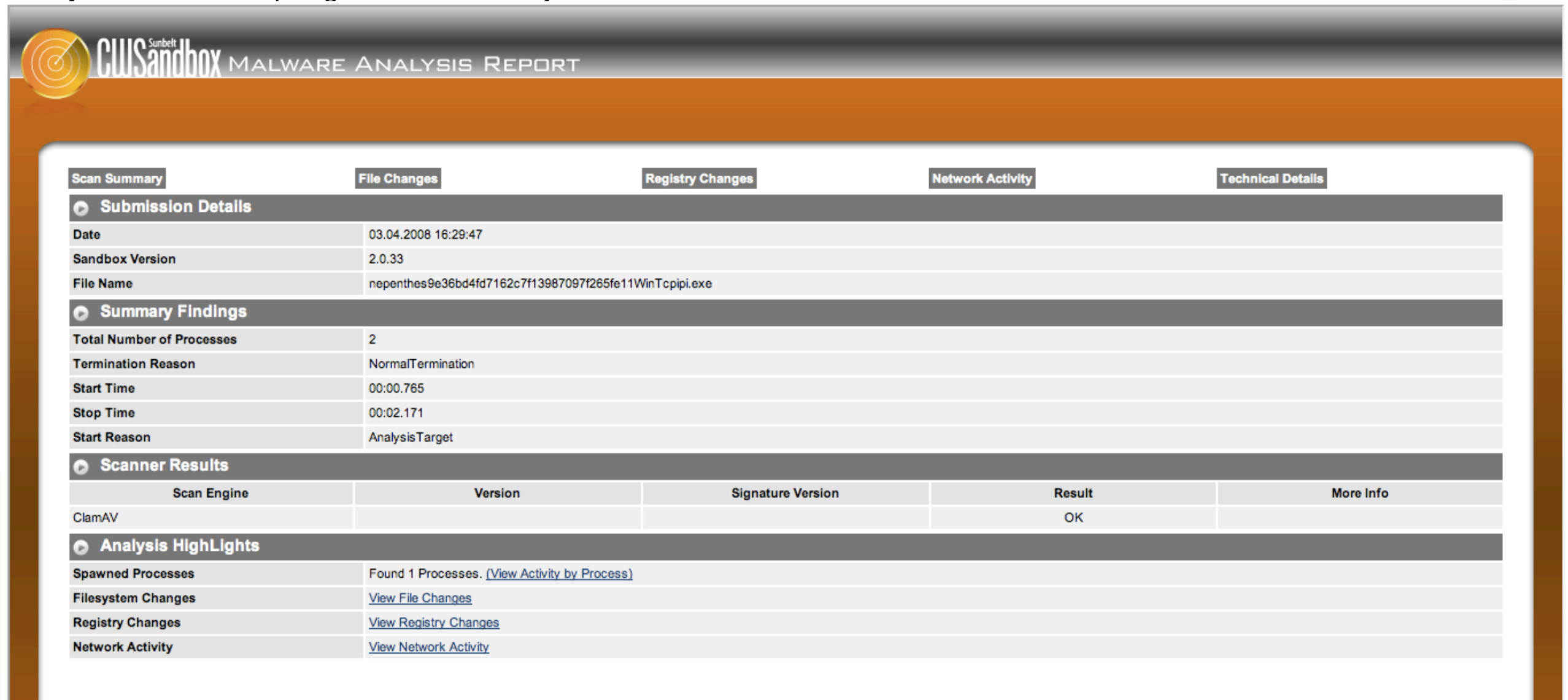
download.microsoft.com/download/6/1/5/615a50e9-a508-4d67-b53c-3a43455761bf/WindowsXP-KB835732-x86-ENU.EXE.

[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.**

Nepenthes

Przykład botnetu o topologii scentralizowanej:



CWSSandbox MALWARE ANALYSIS REPORT

Navigation tabs: Scan Summary | File Changes | Registry Changes | Network Activity | Technical Details

Submission Details

Date	03.04.2008 16:29:47
Sandbox Version	2.0.33
File Name	nepenthes9e36bd4fd7162c7f13987097f265fe11WinTcpi.exe

Summary Findings

Total Number of Processes	2
Termination Reason	NormalTermination
Start Time	00:00.765
Stop Time	00:02.171
Start Reason	AnalysisTarget

Scanner Results

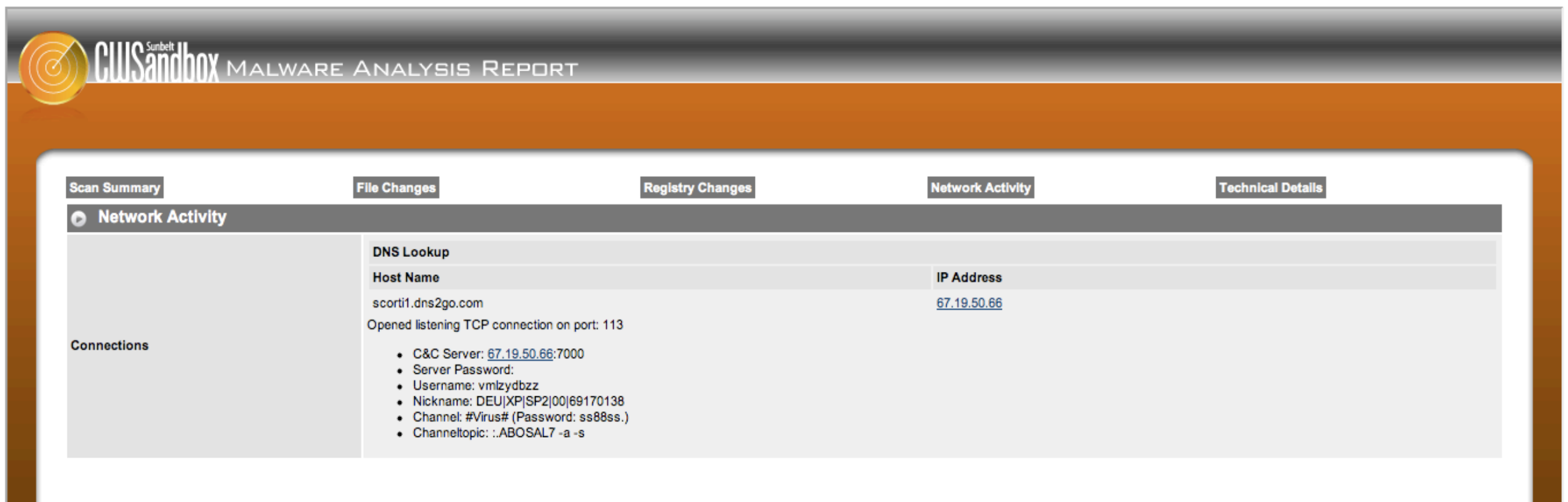
Scan Engine	Version	Signature Version	Result	More Info
ClamAV			OK	

Analysis HighLights

Spawned Processes	Found 1 Processes. (View Activity by Process)
Filesystem Changes	View File Changes
Registry Changes	View Registry Changes
Network Activity	View Network Activity

Nepenthes

... i jego aktywności sieciowych



CWSandbox Sunbelt MALWARE ANALYSIS REPORT

Scan Summary | File Changes | Registry Changes | **Network Activity** | Technical Details

Network Activity

DNS Lookup	
Host Name	IP Address
scort1.dns2go.com	67.19.50.66

Opened listening TCP connection on port: 113

Connections

- C&C Server: [67.19.50.66:7000](#)
- Server Password:
- Username: vmlzydbzz
- Nickname: DEU|XP|SP2|00|69170138
- Channel: #Virus# (Password: ss88ss.)
- Channeltopic: :.ABOSAL7 -a -s

CONFID



Nepenthes

Przykładowa analiza jest dostępna w linkach

CONFID

Statystyki

Data pierwszego ataku: 2007-02-16 18:34:23
Data ostatniego ataku: 2008-09-10 14:47:43

Wszystkich ataków: **3.377.155**

Unikalnych źródłowych adresów IP: 129.452

Unikalnych docelowych adresów IP: 5.876

Unikalnych plików malware: 13.088

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:

4,10

Ataków na godzinę:

246,04

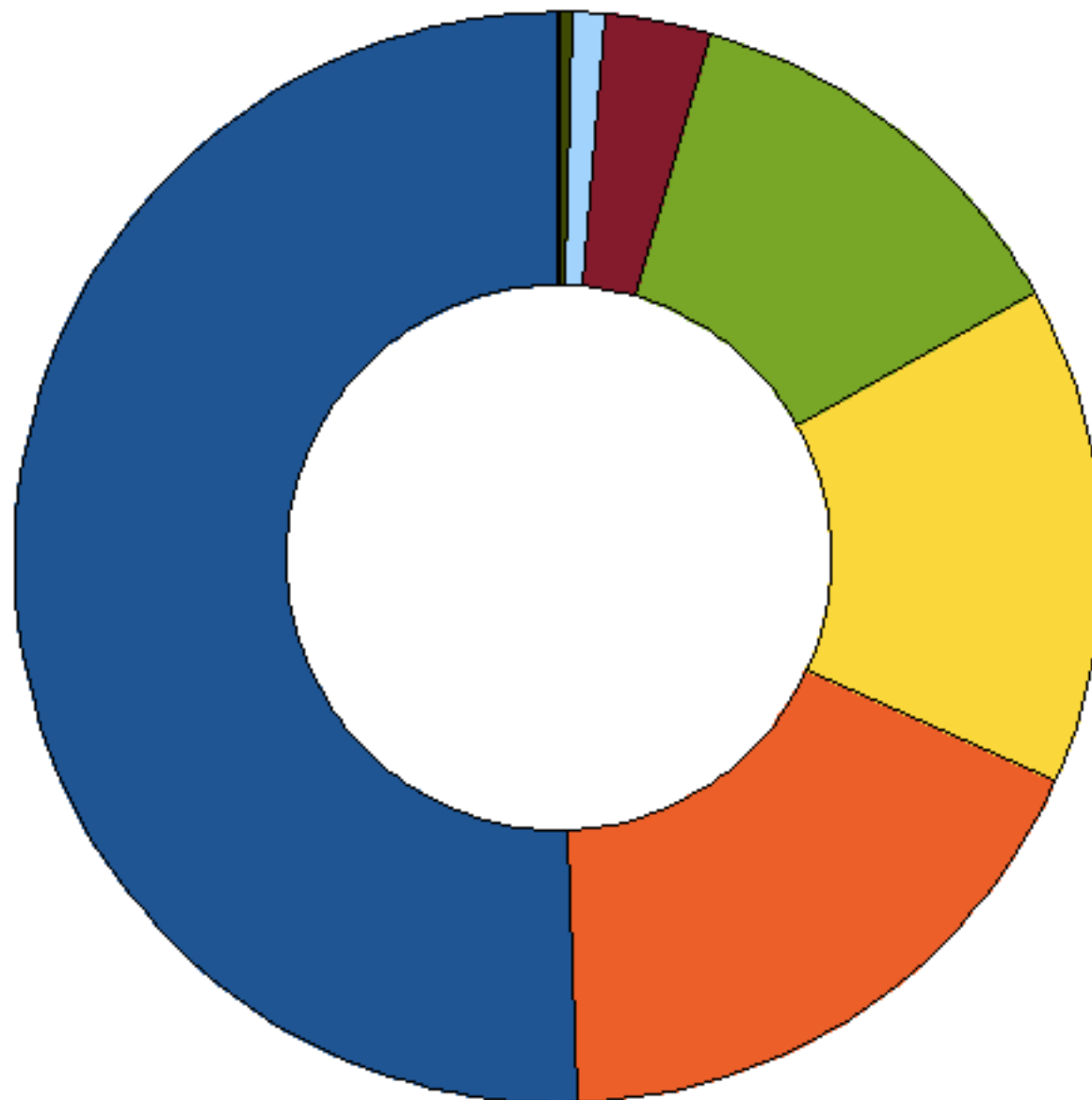
Ataków na dzień:

5905,06

CONFID

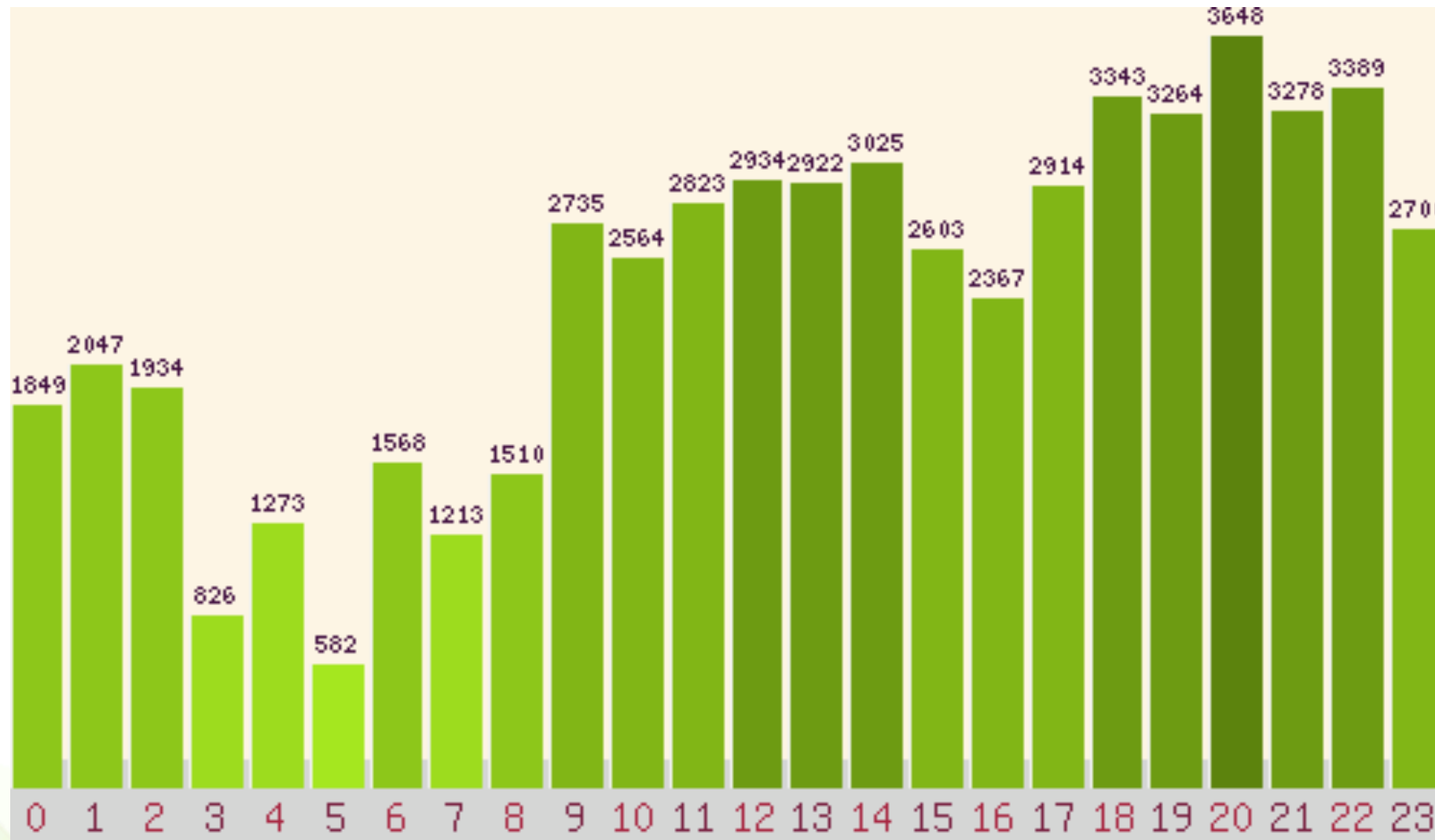


Statystyki



- ftp://
- link://
- tftp://
- http://
- blink://
- creceive://
- csend://
- mydoom://
- optix://
- rcp://

Statystyki

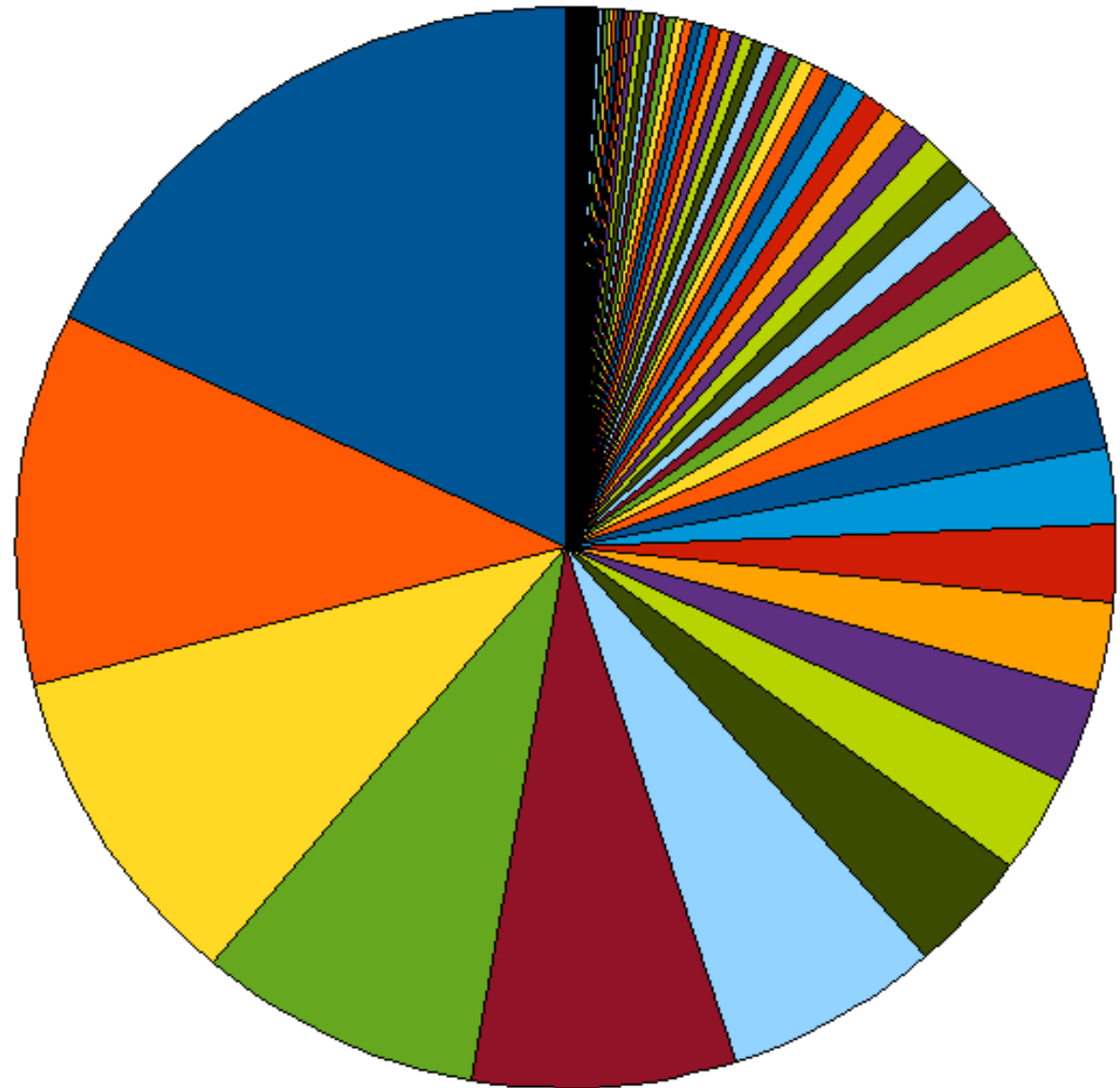


Ilość ataków na godzinę 2008.07, maks: 3.648 o 20.XX

CONFID



Statystyki

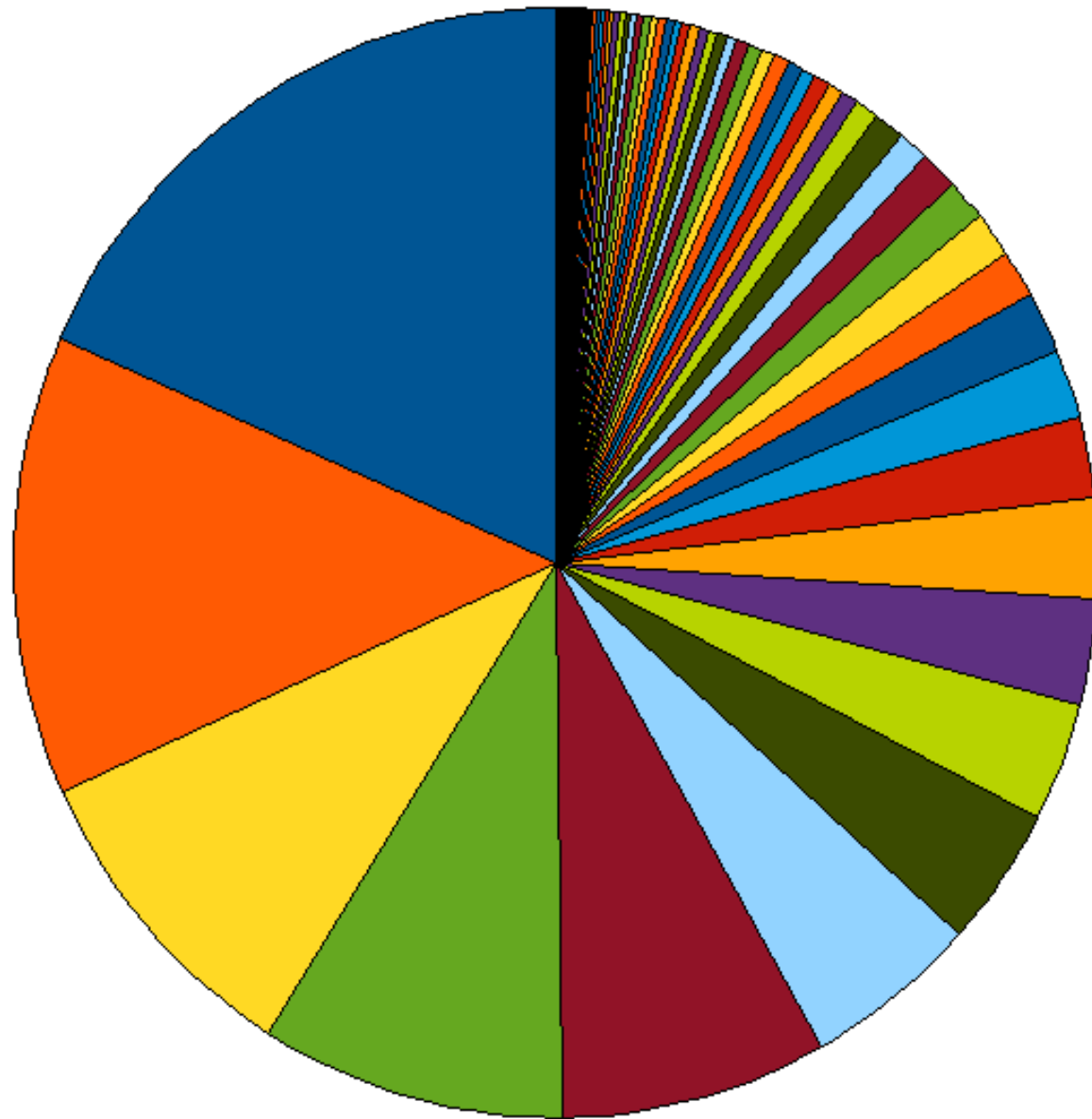


- GBR (17.99%)
- POL (11.08%)
- DEU (9.83%)
- ITA (8.34%)
- FRA (7.74%)
- RUS (6.38%)
- ESP (3.59%)
- ROM (2.91%)
- JPN (2.85%)
- HUN (2.63%)
- USA (2.36%)
- DNK (2.22%)
- BEL (2.15%)
- TWN (2.02%)
- KOR (1.54%)
- BRA (1.25%)
- PRT (0.98%)
- CHN (0.98%)
- JOR (0.88%)
- SWE (0.83%)

Źródło
ataku
137 krajów !

CONFID

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

61.083 IP

CONFID

Statystyki

485 domen

19 miesięcy

Czas stałego dowiązania domeny do IP:

Najkrótszy: < 1 dzień

Najdłuższy: > 11 miesięcy

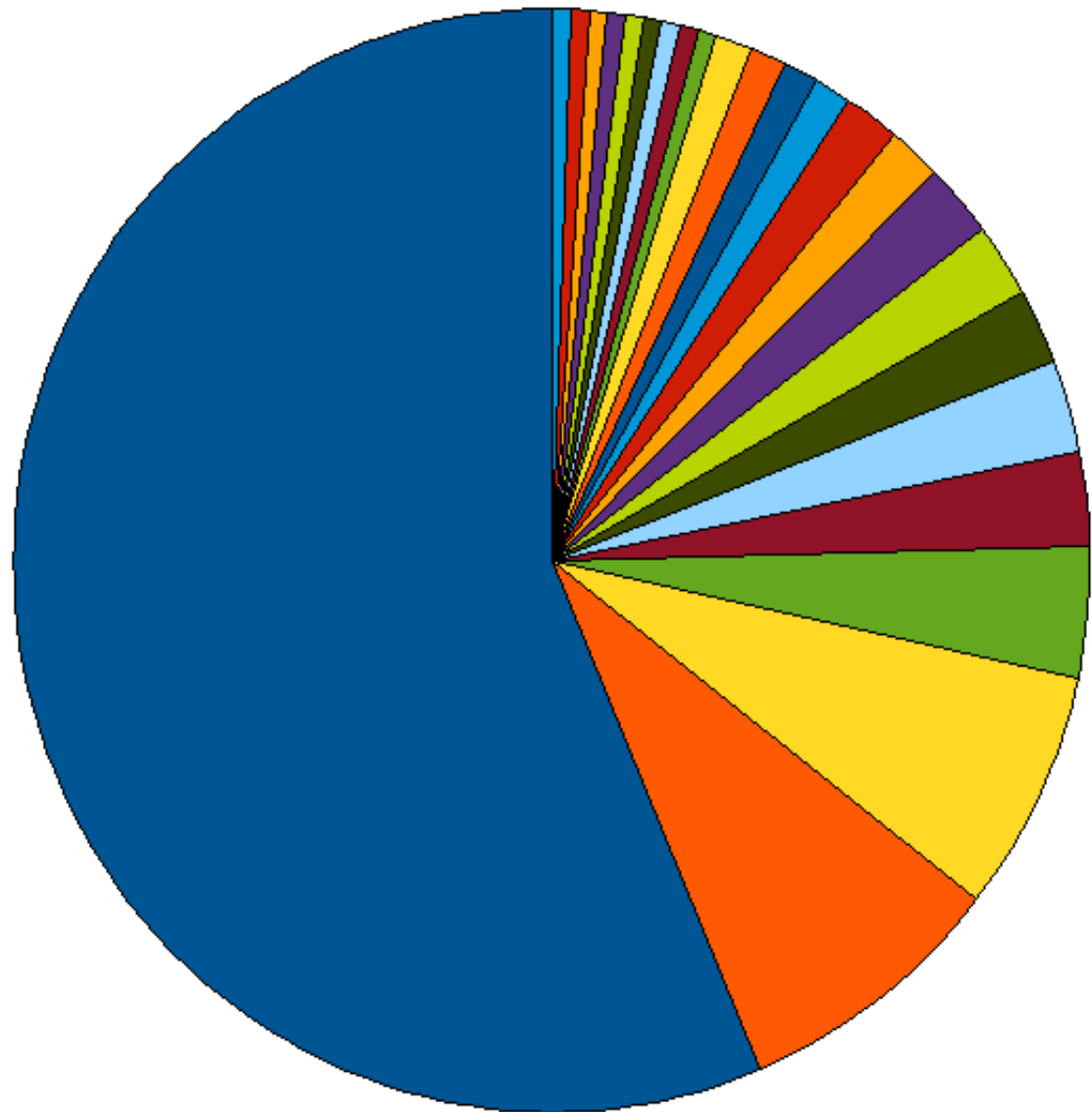
Maksymalna ilość wykorzystanych unikalnych IP: 57

Maksymalna ilość jednoczesnych adresów IP do domeny: 8

CONFID



Statystyki



- USA (55.08%)
- DEU (8.02%)
- CAN (6.95%)
- GBR (3.74%)
- FRA (2.67%)
- CHN (2.67%)
- SVK (2.14%)
- NLD (2.14%)
- RUS (2.14%)
- KOR (1.60%)
- LUX (1.60%)
- TWN (1.07%)
- FIN (1.07%)
- POL (1.07%)
- JPN (1.07%)
- CYP (0.53%)
- MOZ (0.53%)
- BEL (0.53%)
- PRY (0.53%)
- CHE (0.53%)

C & C

CONFID

DNS blackholing

- teoria działania
 - konfiguracja serwera DNS tak, żeby działał jako master dla konkretnej domeny
 - udajemy legalny serwer DNS obsługujący domenę
 - boty pytają o domenę, boty dostają adres IP inny, niż by tego chciał właściciel domeny, boty łączą się nie tam gdzie powinny, boty nie działają
- założenia
 - komputer musi korzystać z naszych dnsów
 - powyższy punkt można wymusić filtrami

DNS blackholing

- możliwości wykorzystania
 - przekierowanie zainfekowanych zombie na własny system, na którym można je dalej badać
 - dezaktywacja bota bez ingerencji w komputer klienta (załatwiamy kwestię etyczną)

CONFID

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 w inny sposób

DNS blackholing

- pozytywne efekty wdrożenia
 - boty nie działają bez głowy
 - nie ma spamu
 - nie ma ataków DDoS lub są one niezauważalne w skali sieci,
 - nie będzie niczego, wszystko zlikwidowane
- a wszystko to bez jakiegokolwiek ingerencji w komputer klienta

DNS blackholing

- skuteczność z życia wzięta
 - przejęta sieć na 1.2k userów
 - od 150 do 200 osób zainfekowanych (skanujących i komunikujących się z różnymi serwerami C&C [w sumie 4 różne botnety], niektóre hosty były zainfekowane kilkoma różnymi botami jednocześnie
 - po włączeniu dns-blackholingu (w wariancie twardym z wymuszeniem korzystania z naszych dnsów) po dwóch dobach zostało 3 skanujących, ale nie łączyli się oni do żadnego serwera C&C (raczej wormy, bo nie stwierdzono żadnego “podejrzanego” ruchu)
 - w sieci same z siebie zaczęły działać telefony VoIP, które wcześniej wykazywały zastanawiającą zbieżność ze stanem plam na Słońcu ;-)



LogicalTrust

www.logicaltrust.net



IT BCE

BUSINESS CONSULTING EXPERTS

Konfiguracja - przykłady

CONFID

Bind 9

/etc/bind/named.conf – główny konfig

```
zone "powiekszwojinteres.pl" IN {  
    type master;  
    file „dnsblackholing.conf”  
};
```

dnsblackholing.conf – plik domeny

```
$TTL 15m  
@           IN      SOA    ns1.domena.pl.    admin.domena.pl. (  
            2006112402 ; serial  
            4h ; refresh  
            30m ; retry  
            14d ; expire  
            15m ; negative_ttl
```

```
↑  
@           IN      NS     ns1.domena.pl.  
@           IN      NS     ns2.domena.pl.  
@           IN      A      127.0.0.1  
*           IN      A      127.0.0.1
```


Nepenthes

konfiguracja pod bazę PostgreSQL

```
submit-postgres
{
server "1.2.3.4"; // use ips,domains/hostnames won't work!
user "user"; // db user
pass "hasłord"; // db pass
db "mwcollect"; // which database to use
options ""; // not sure if options already work
spooldir "/var/spool/nepenthes/submitpostgres/";
};
```

wysyłanie wyników do Sandboxa Normana

```
submit-norman
{
// this is the adress where norman sandbox reports will be sent
email "dsfsdfsdfs@no-mail.pl";
urls ("http://www.norman.com/microsites/nsic/Submit/Special/45773/",
"http://luigi.informatik.uni-mannheim.de/submit.php?action=verify"); };
```

Pytania

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

Linki

- <http://bothunters.pl> - nasz blog tropicieli botów,
- <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.malwaredomains.com> - jak sama nazwa wskazuje
- <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
- <https://cwsandbox.org/?page=samdet&id=80496&password=hkgyy> - przykładowa analiza z sandboxa Sunbeltu



Zdjęcia

- http://www.hyscience.com/archives/Lane-Iran_Nuclear_Po.jpg
- <http://flickr.com/photos/angelillo182/170068133/>
- <http://files.myopera.com/Numen/blog/browsers-logos.png>
- <http://flickr.com/photos/jnatividad/2566951902/>
- <http://flickr.com/photos/laloyd/801634032/>
- <http://flickr.com/photos/edglazar/460186475/>
- <http://flickr.com/photos/seanrayford/482058734/>

Dziękujemy za uwagę

Logicaltrust – IT Security Solutions

IT BCE sp. z o.o.

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



CONFID