Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

Breaking into a computer : attack techniques and tools

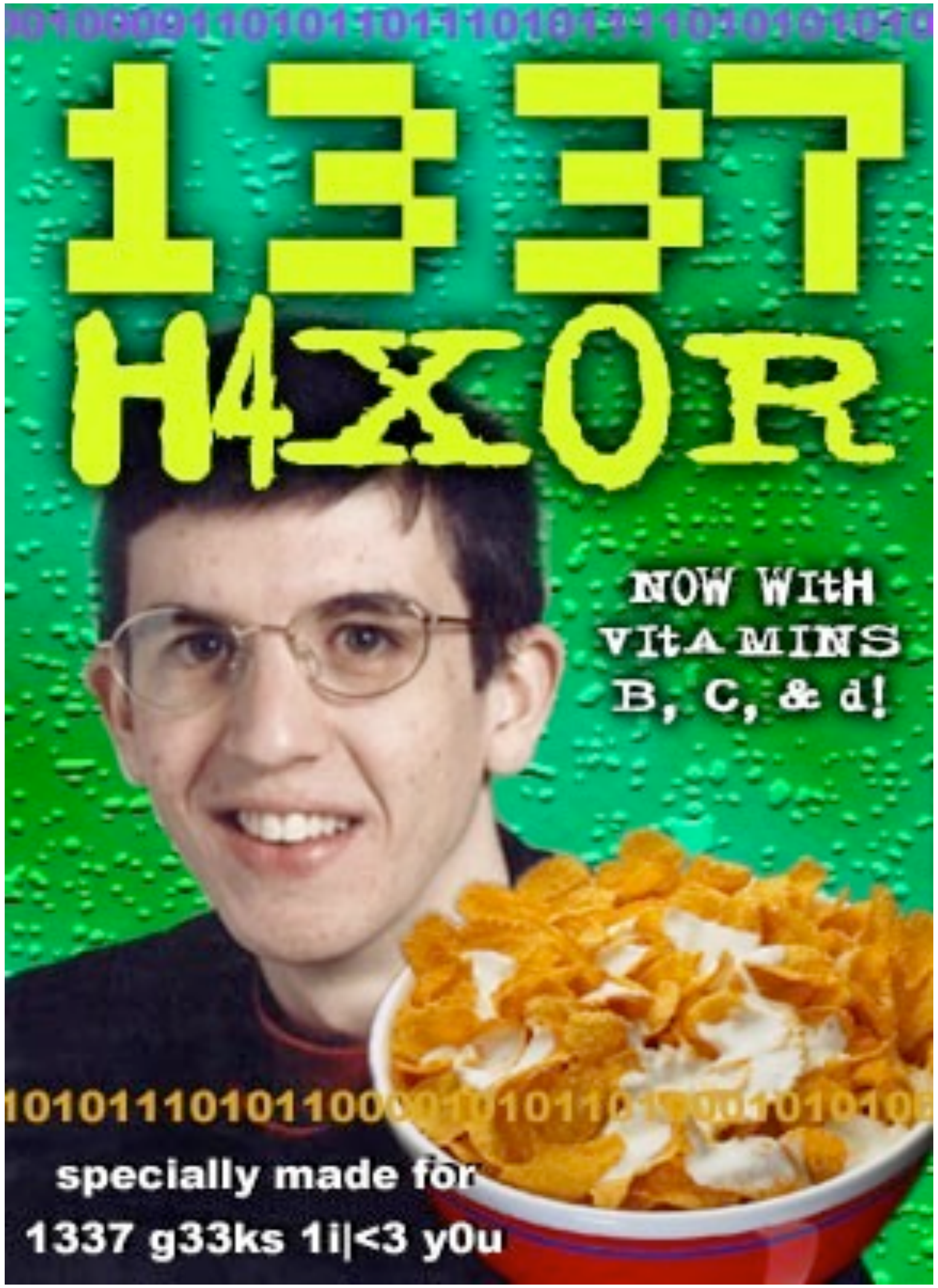
Romain Wartel
CERN Security Team - http://cern.ch/security
Worldwide LHC Computing Grid - http://cern.ch/LCG

Outline

- ►Underground market
- ►Exploits and payloads
- ►Propagation infrastructures
- ►Popular for-profit malware
- ►Malware: interfaces and functionalities
- ►Linux rootkits

Perception

- ►Common perception of a "hacker"

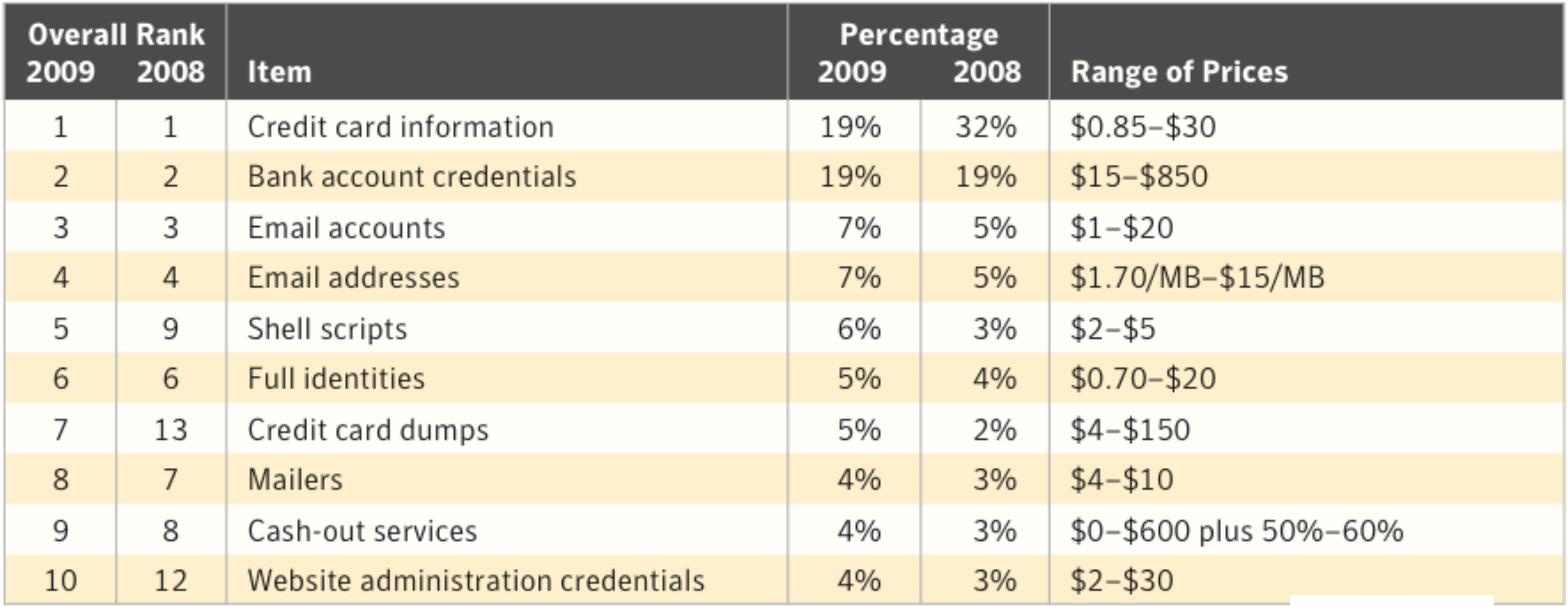


Reality

- In reality, attackers may rather look like:

Underground Market

- ► Main motive behind most security attacks is money



Overall Rank		Item	Percentage		Range of Prices
2009	2008		2009	2008	
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Goods and services advertised on underground economy servers

Source: Symantec

- ► Objective: collect marketable information
- ► Needs: exploits + payloads, propagation infrastructure

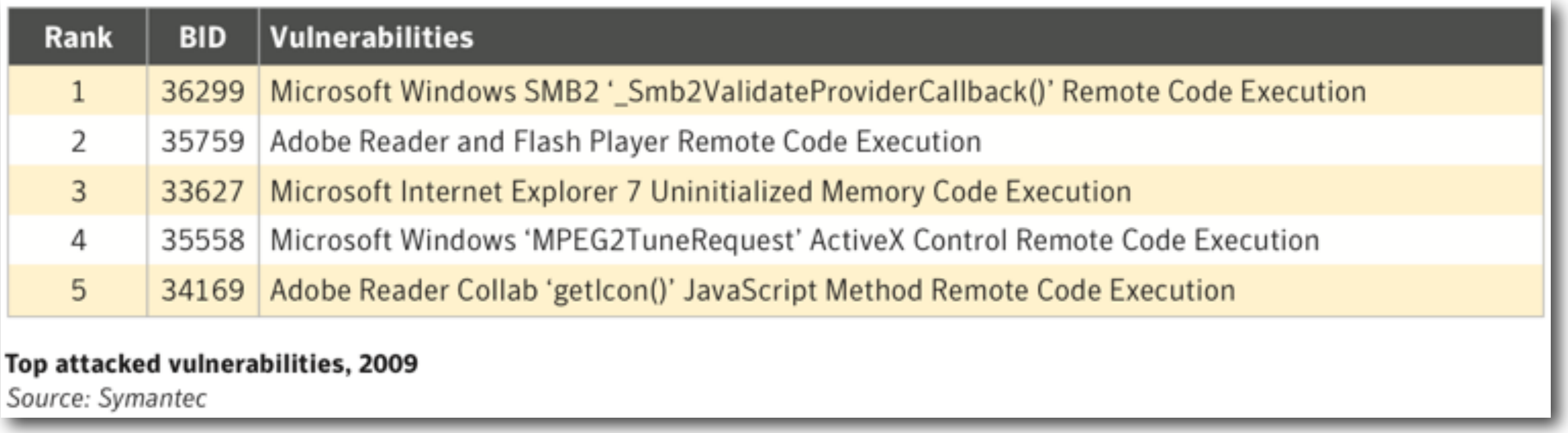
Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

Exploits, payload and propagation infrastructure

Exploits

► Exploit: software exploiting a security vulnerability

- ► Objective: gain (some) remote control over the victim’s host
- ► Exploits can be purchased on the underground markets
  - ▪ Public/private vulnerabilities
    - “0 day exploits” are best but most expensive
    - Some claim there are governments willing to pay as high as $1 million for a single vulnerability
  - ▪ Potential impact, privileges gained, portability, ease of use



Rank	BID	Vulnerabilities
1	36299	Microsoft Windows SMB2 ‘_Smb2ValidateProviderCallback()’ Remote Code Execution
2	35759	Adobe Reader and Flash Player Remote Code Execution
3	33627	Microsoft Internet Explorer 7 Uninitialized Memory Code Execution
4	35558	Microsoft Windows ‘MPEG2TuneRequest’ ActiveX Control Remote Code Execution
5	34169	Adobe Reader Collab ‘getIcon()’ JavaScript Method Remote Code Execution

Top attacked vulnerabilities, 2009
Source: Symantec

- ► Once the attacker has an exploit, a payload needs to be added

Malicious Payload

The payload performs the malicious work

- Objectives:
  - Alter system's behavior
    - e.g. add popups, fake search bars, send spam with host is idle, etc.
  - Collect data without the consent of the victim
    - e.g. keylogger

- The payload may be a framework multiple purposes:
  - Dynamically pull payload on demand
  - Auto update mechanisms built-in
  - Eliminate competitors' "products"
  - Patch the system to protect it from competitors

Propagation Infrastructure

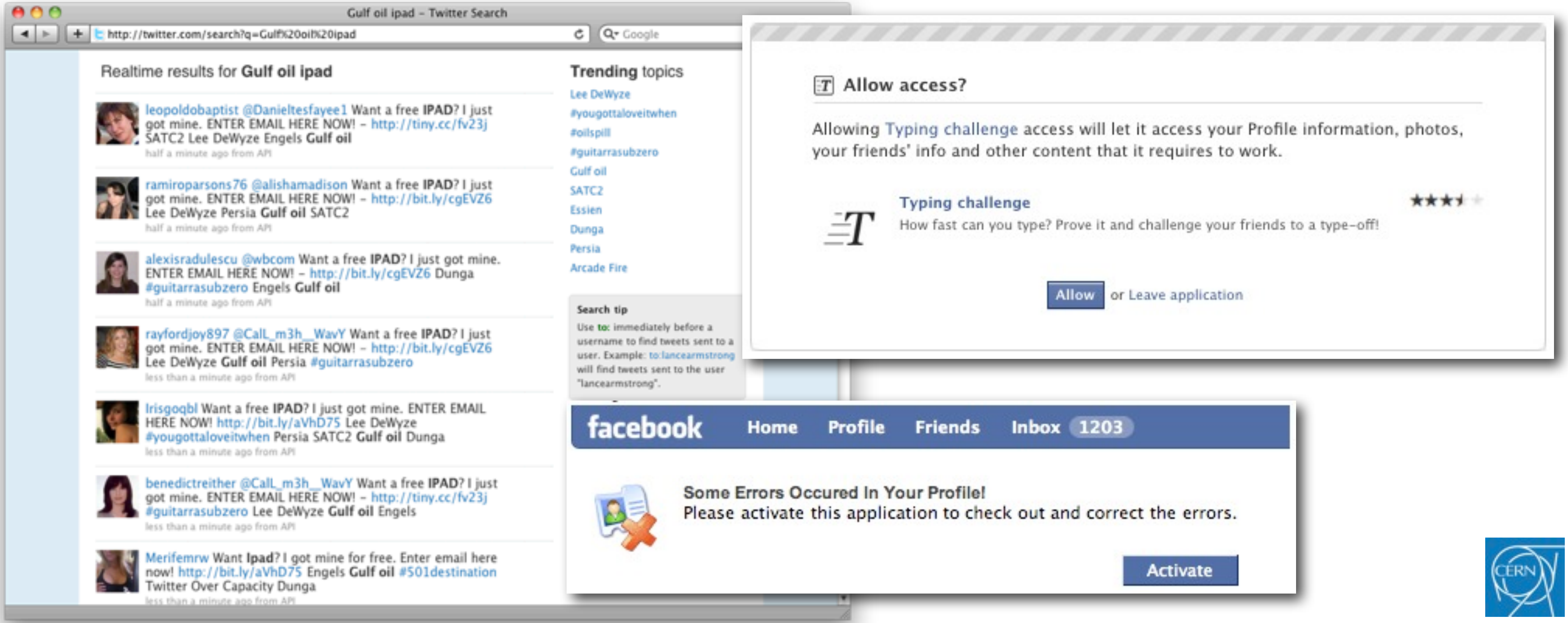
- **To propagate the malware to more victims, a strong computing infrastructure is need:**
  - Hosting for the malicious payloads, rogue websites, etc.
  - Bandwidth to send spam, etc.

- **Significant challenges**
  - Must be very resilient!
  - Must scale to the number of victims
  - Must be customisable to adapt to the needs of customers
  - Must be cheap, to maximise profit

Propagation Infrastructure

► Solution 1

- ► Enjoy existing services widely used by the victims:
  - P2P networks (“Bond_23_Unreleased_2011_[HDRips.4.iPod]”)
  - Social networks: Facebook, Twitter, MySpace, etc.
  - Inject malware via ads on large websites (BBC, etc.)


Gulf oil ipad – Twitter Search
http://twitter.com/search?q=Gulf%20oil%20ipad
Google

Realtime results for **Gulf oil ipad**

leopoldobaptist @Danieltesfayee1 Want a free **IPAD**? I just got mine. ENTER EMAIL HERE NOW! – http://tiny.cc/fv23j SATC2 Lee DeWyze Engels **Gulf oil**
half a minute ago from API

ramiroparsons76 @alishamadison Want a free **IPAD**? I just got mine. ENTER EMAIL HERE NOW! – http://bit.ly/cgEVZ6 Lee DeWyze Persia **Gulf oil** SATC2
half a minute ago from API

alexisradulescu @wbcom Want a free **IPAD**? I just got mine. ENTER EMAIL HERE NOW! – http://bit.ly/cgEVZ6 Dunga #guitarrasubzero Engels **Gulf oil**
half a minute ago from API

rayfordjoy897 @CalL_m3h__WavY Want a free **IPAD**? I just got mine. ENTER EMAIL HERE NOW! – http://bit.ly/cgEVZ6 Lee DeWyze **Gulf oil** Persia #guitarrasubzero
less than a minute ago from API

Irisgoqbl Want a free **IPAD**? I just got mine. ENTER EMAIL HERE NOW! http://bit.ly/aVhD75 Lee DeWyze #yougottaloveitwhen Persia SATC2 **Gulf oil** Dunga
less than a minute ago from API

benedictreither @CalL_m3h__WavY Want a free **IPAD**? I just got mine. ENTER EMAIL HERE NOW! – http://tiny.cc/fv23j #guitarrasubzero Lee DeWyze **Gulf oil** Engels
less than a minute ago from API

Merifemrw Want **Ipad**? I got mine for free. Enter email here now! http://bit.ly/aVhD75 Engels **Gulf oil** #501destination Twitter Over Capacity Dunga
less than a minute ago from API

Trending topics

- Lee DeWyze
- #yougottaloveitwhen
- #oilspill
- #guitarrasubzero
- Gulf oil
- SATC2
- Essien
- Dunga
- Persia
- Arcade Fire

Search tip
Use to: immediately before a username to find tweets sent to a user. Example: to:lancearmstrong will find tweets sent to the user "lancearmstrong".

Allow access?

Allowing Typing challenge access will let it access your Profile information, photos, your friends' info and other content that it requires to work.

Typing challenge
How fast can you type? Prove it and challenge your friends to a type-off!

Some Errors Occured In Your Profile!
Please activate this application to check out and correct the errors.

Propagation Infrastructure

►Solution 2

- Become the Internet Service Provider:
  - Much more difficult to be taken off line, "bulletproof hosting"
  - Manage its own pool of IP addresses
  - Accreditation removal may be complex and time consuming
- Legal complexity ensures stable operations (for a while)
  - ISP may be settled in countries with relaxed Internet laws
  - International ramification does help
  - Sell the service to other underground companies
    - Actual crime is not committed by the ISP itself
- Popular examples:
  - http://en.wikipedia.org/wiki/Intercage
  - http://en.wikipedia.org/wiki/Russian_Business_Network

Propagation Infrastructure

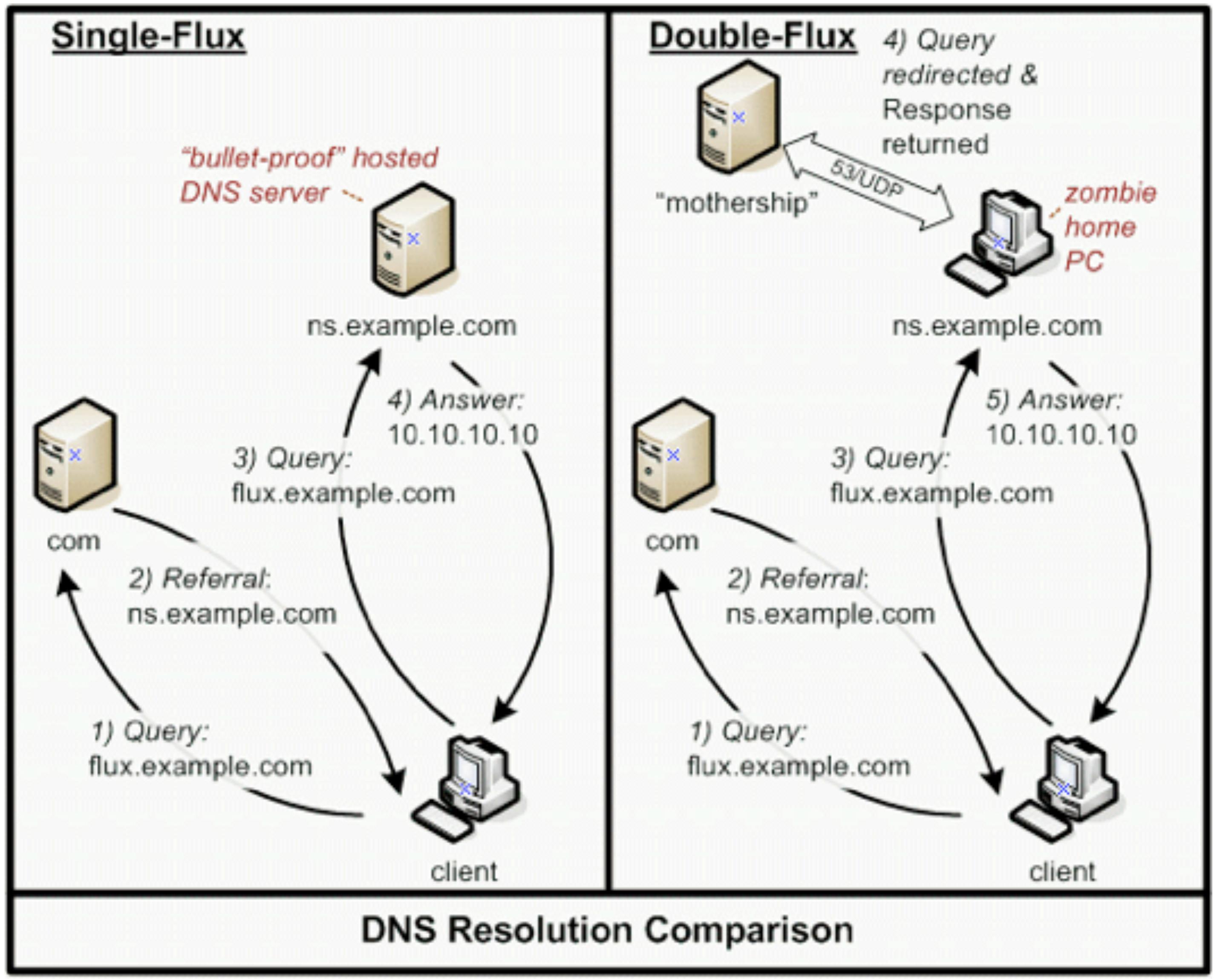
►Solution 3

- Get the victims to host and spread the malware!
  - Cheap, highly distributed and resilient
  - Build a own network of robots, a so-called "botnet"
    - The victim hosts are controls by malware and turned into "bots"
    - Payload and malicious services are distributed across the botnet
    - Control via IRC, P2P, etc.
- "Fast Flux" is a common design to turn bots (victims) into:
  - Rogue DNS servers
  - Reverse proxies for rogue websites
  - Malicious domains needed to run the infrastructure
- Bots are "selected" to offer a load-balanced + resilient service:
  - Selection based on availability, bandwidth, performance, etc.
  - Short time-to-live, rapid turn over of the bots

Propagation Infrastructure

►Solution 3

- ►Fast Flux:
  - "Both the DNS A record sets and the authoritative NS records for a malicious domain are continually changed in a round robin manner"


Single-Flux
"bullet-proof" hosted DNS server
ns.example.com
com
1) Query: flux.example.com
2) Referral: ns.example.com
3) Query: flux.example.com
4) Answer: 10.10.10.10
client
Double-Flux
4) Query redirected & Response returned
"mothership"
53/UDP
zombie home PC
ns.example.com
com
1) Query: flux.example.com
2) Referral: ns.example.com
3) Query: flux.example.com
5) Answer: 10.10.10.10
client

DNS Resolution Comparison

http://www.honeynet.org/papers/ff/

Propagation Infrastructure

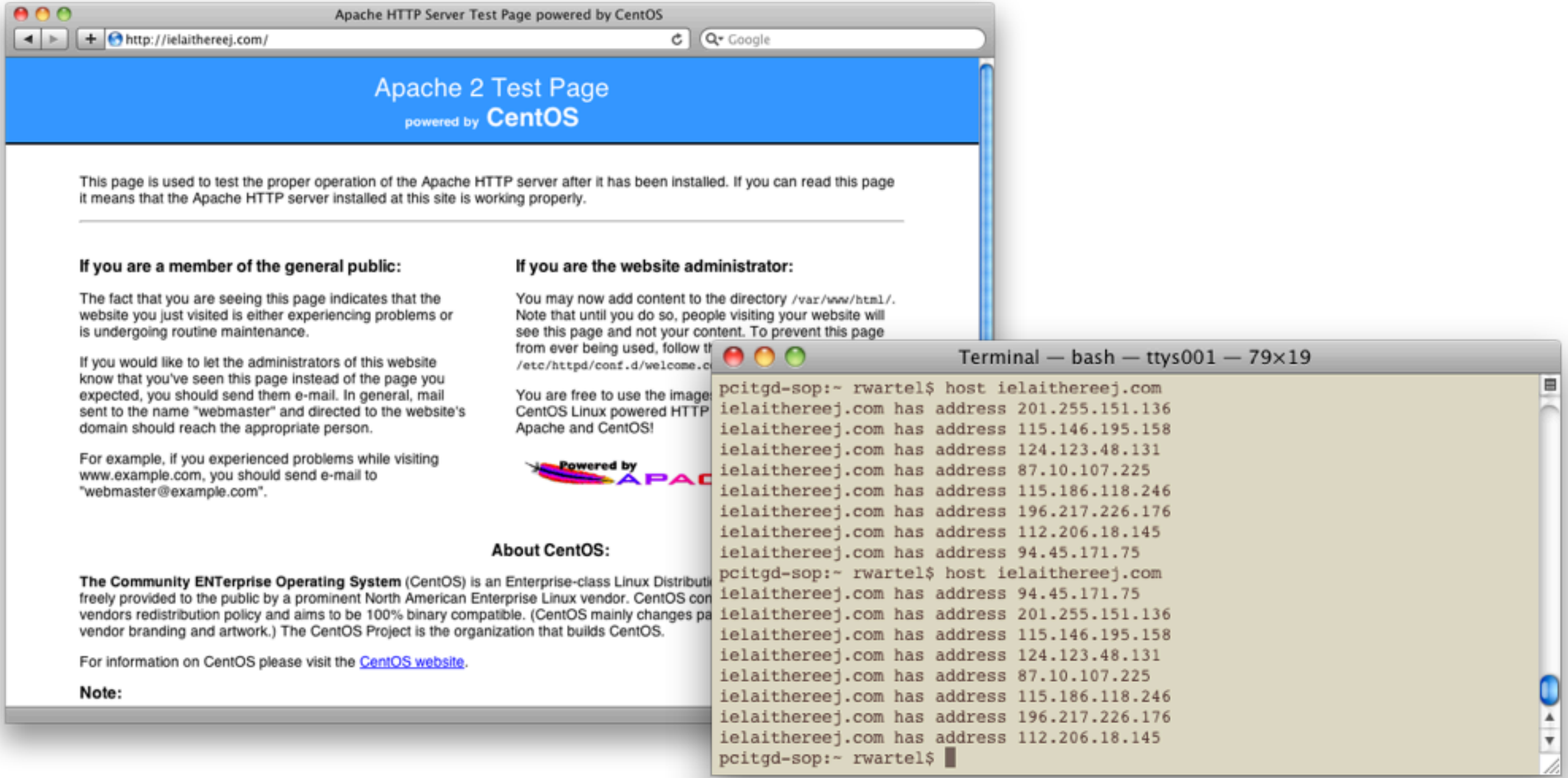
► Solution 3

- ► Example of Fast Flux tracking with Zeus:
  - http://en.wikipedia.org/wiki/Zeus_%28trojan_horse%29
  - The Zeus botnet is targeting login credentials
    - Facebook, Yahoo, Hi5, Metroflog, Sonico and Netlog etc.
    - Targeting banking sites as well
  - The botnet is estimated to include millions of compromised computers
  - As of October 28, 2009 Zeus has sent out over 1.5 million phishing messages on Facebook.

Propagation Infrastructure

▶ Solution 3

- ▶ Example malicious URLs:
  - http://ielaithereej.com/bin/aiphaipi.bin (Zeus v2 + config file)



Apache HTTP Server Test Page powered by CentOS
http://ielaithereej.com/
Google
Terminal — bash — ttys001 — 79×19

Apache 2 Test Page
powered by CentOS

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page and not your content. To prevent this page from ever being used, follow th `/etc/httpd/conf.d/welcome.c`

You are free to use the image CentOS Linux powered HTTP Apache and CentOS!

Powered by APAC

About CentOS:

The Community ENTerprise Operating System (CentOS) is an Enterprise-class Linux Distributi freely provided to the public by a prominent North American Enterprise Linux vendor. CentOS con vendors redistribution policy and aims to be 100% binary compatible. (CentOS mainly changes pa vendor branding and artwork.) The CentOS Project is the organization that builds CentOS.

For information on CentOS please visit the CentOS website.

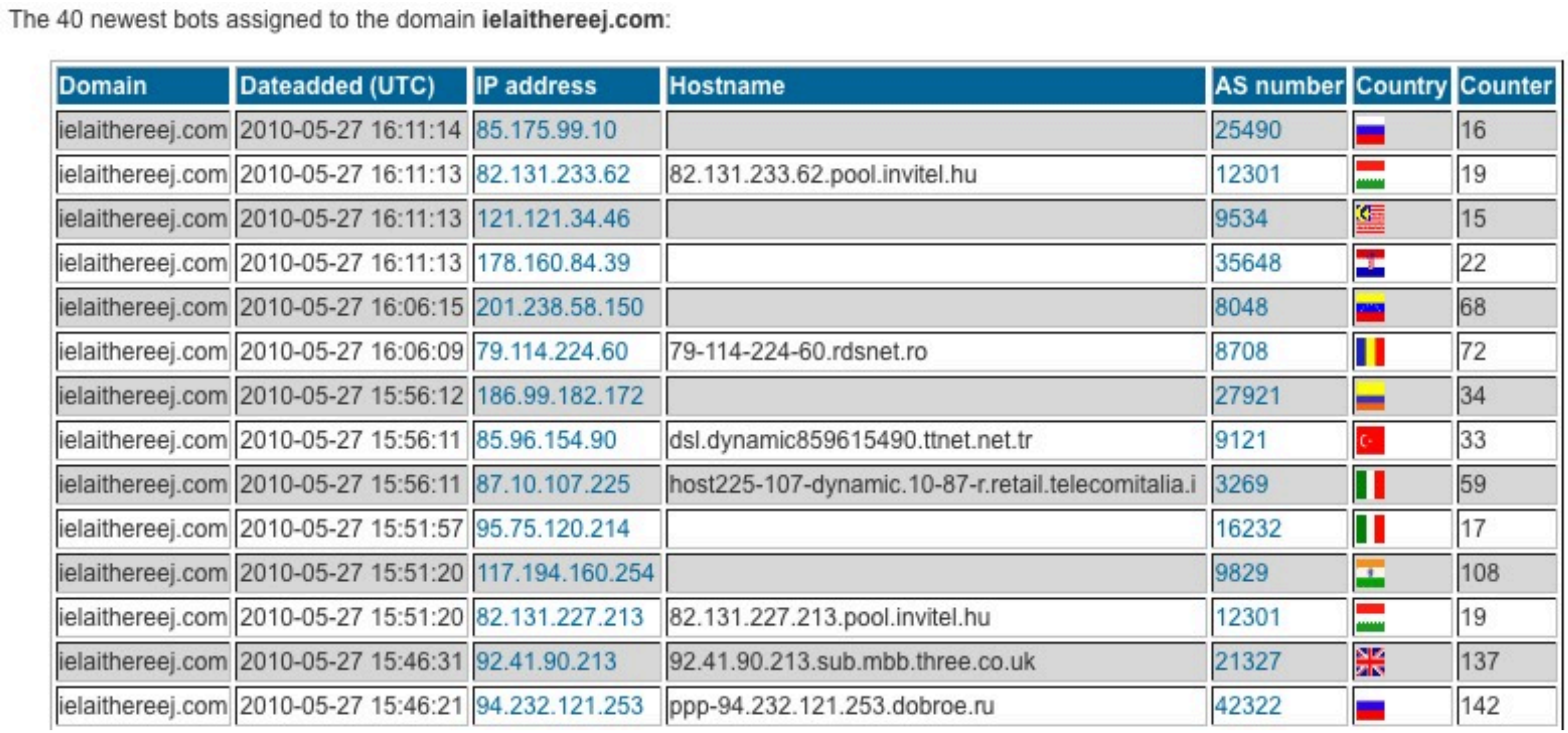
Note:

```
pcitgd-sop:~ rwartel$ host ielaithereej.com
ielaithereej.com has address 201.255.151.136
ielaithereej.com has address 115.146.195.158
ielaithereej.com has address 124.123.48.131
ielaithereej.com has address 87.10.107.225
ielaithereej.com has address 115.186.118.246
ielaithereej.com has address 196.217.226.176
ielaithereej.com has address 112.206.18.145
ielaithereej.com has address 94.45.171.75
pcitgd-sop:~ rwartel$ host ielaithereej.com
ielaithereej.com has address 94.45.171.75
ielaithereej.com has address 201.255.151.136
ielaithereej.com has address 115.146.195.158
ielaithereej.com has address 124.123.48.131
ielaithereej.com has address 87.10.107.225
ielaithereej.com has address 115.186.118.246
ielaithereej.com has address 196.217.226.176
ielaithereej.com has address 112.206.18.145
pcitgd-sop:~ rwartel$ █
```

Propagation Infrastructure

►Solution 3

- Example of Fast Flux tracking:



The 40 newest bots assigned to the domain **ielaithereej.com**:

Domain	Dateadded (UTC)	IP address	Hostname	AS number	Country	Counter
ielaithereej.com	2010-05-27 16:11:14	85.175.99.10		25490	🇷🇺	16
ielaithereej.com	2010-05-27 16:11:13	82.131.233.62	82.131.233.62.pool.invitel.hu	12301	🇭🇺	19
ielaithereej.com	2010-05-27 16:11:13	121.121.34.46		9534	🇲🇾	15
ielaithereej.com	2010-05-27 16:11:13	178.160.84.39		35648	🇭🇷	22
ielaithereej.com	2010-05-27 16:06:15	201.238.58.150		8048	🇻🇪	68
ielaithereej.com	2010-05-27 16:06:09	79.114.224.60	79-114-224-60.rdsnet.ro	8708	🇷🇴	72
ielaithereej.com	2010-05-27 15:56:12	186.99.182.172		27921	🇨🇴	34
ielaithereej.com	2010-05-27 15:56:11	85.96.154.90	dsl.dynamic859615490.ttnet.net.tr	9121	🇹🇷	33
ielaithereej.com	2010-05-27 15:56:11	87.10.107.225	host225-107-dynamic.10-87-r.retail.telecomitalia.i	3269	🇮🇹	59
ielaithereej.com	2010-05-27 15:51:57	95.75.120.214		16232	🇮🇹	17
ielaithereej.com	2010-05-27 15:51:20	117.194.160.254		9829	🇮🇳	108
ielaithereej.com	2010-05-27 15:51:20	82.131.227.213	82.131.227.213.pool.invitel.hu	12301	🇭🇺	19
ielaithereej.com	2010-05-27 15:46:31	92.41.90.213	92.41.90.213.sub.mbb.three.co.uk	21327	🇬🇧	137
ielaithereej.com	2010-05-27 15:46:21	94.232.121.253	ppp-94.232.121.253.dobroe.ru	42322	🇷🇺	142

http://dnsbl.abuse.ch/fastfluxtracker.php

Popular for-profit malware

Malware business

►Malware infrastructure has become more sophisticated:

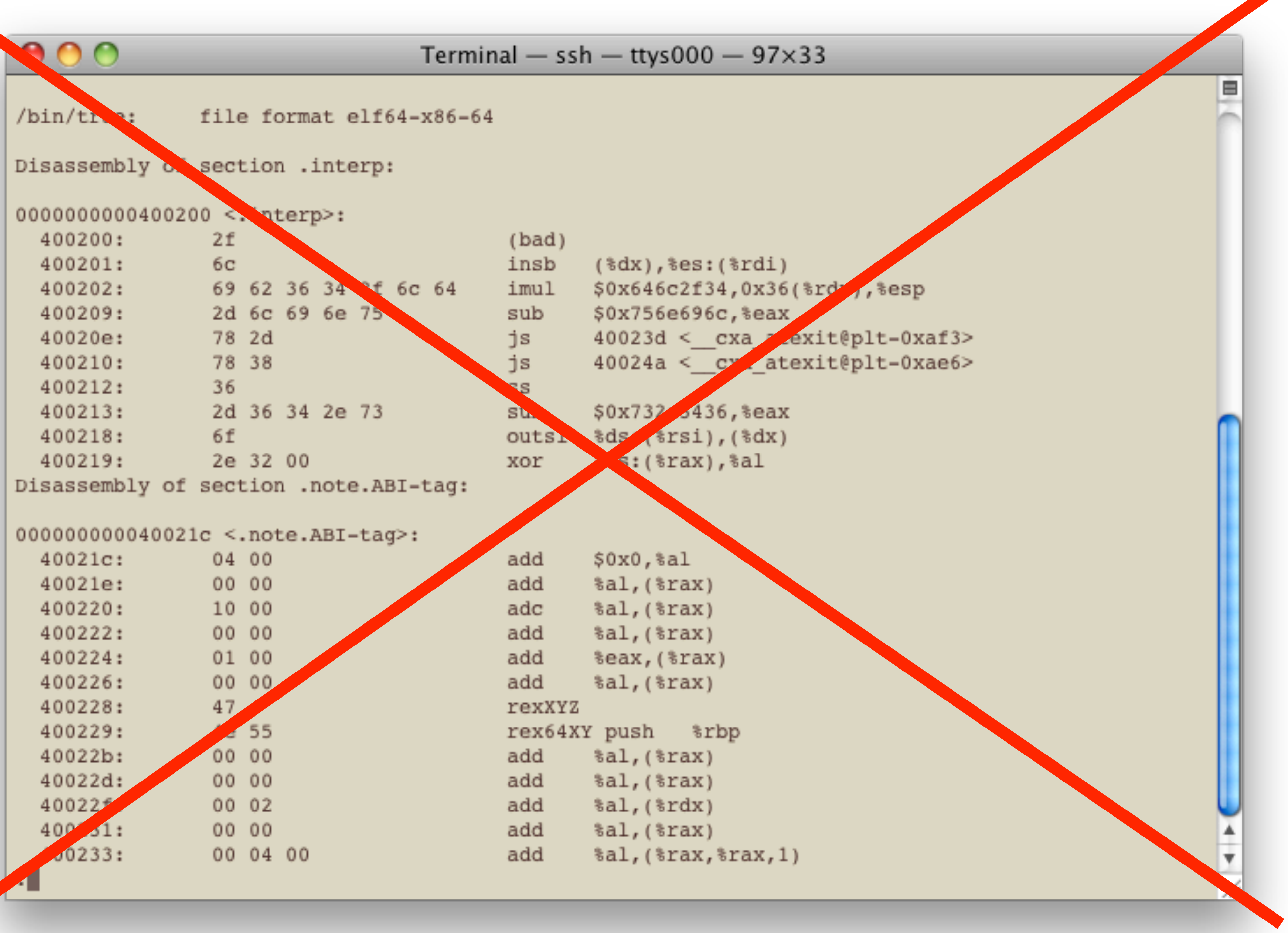
- ►Malicious software developers: provide exploits and tools
- ►Bot herders: maintain and rent the bot infrastructure
- ►Money mules: turn "dirty" money into real currencies
- ►Malware hosting, etc.
- ►Coordination via Internet forums, IRC, IM, etc.

►A closer look on the actual tools

- ►Easy to use
- ►Enable automated attacks
- ►Very sophisticated

Malware Interfaces

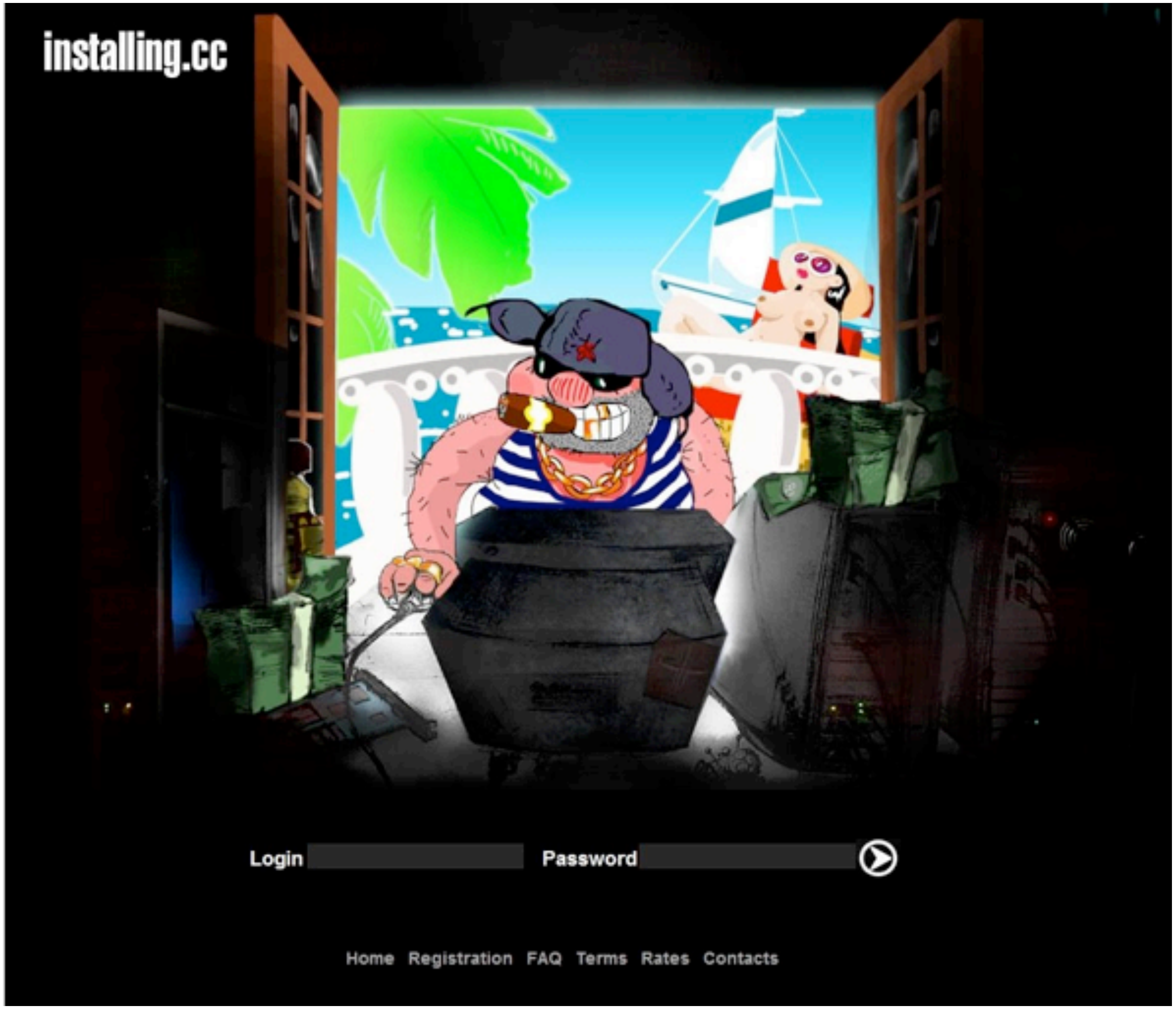
► Modern malware can be convenient and easy to use



```
/bin/true:     file format elf64-x86-64

Disassembly of section .interp:

0000000000400200 <.interp>:
  400200:       2f                      (bad)
  400201:       6c                      insb   (%dx),%es:(%rdi)
  400202:       69 62 36 34 2f 6c 64    imul   $0x646c2f34,0x36(%rdx),%esp
  400209:       2d 6c 69 6e 75          sub    $0x756e696c,%eax
  40020e:       78 2d                   js     40023d <__cxa_atexit@plt-0xaf3>
  400210:       78 38                   js     40024a <__cxa_atexit@plt-0xae6>
  400212:       36                      ss
  400213:       2d 36 34 2e 73          sub    $0x732e3436,%eax
  400218:       6f                      outsl  %ds:(%rsi),(%dx)
  400219:       2e 32 00                xor    %cs:(%rax),%al
Disassembly of section .note.ABI-tag:

000000000040021c <.note.ABI-tag>:
  40021c:       04 00                   add    $0x0,%al
  40021e:       00 00                   add    %al,(%rax)
  400220:       10 00                   adc    %al,(%rax)
  400222:       00 00                   add    %al,(%rax)
  400224:       01 00                   add    %eax,(%rax)
  400226:       00 00                   add    %al,(%rax)
  400228:       47                      rexXYZ
  400229:       4e 55                   rex64XY push   %rbp
  40022b:       00 00                   add    %al,(%rax)
  40022d:       00 00                   add    %al,(%rax)
  40022f:       00 02                   add    %al,(%rdx)
  400231:       00 00                   add    %al,(%rax)
  400233:       00 04 00                add    %al,(%rax,%rax,1)
:
```

Malware Interfaces

- ►Modern malware can be convenient and easy to use



installing.cc

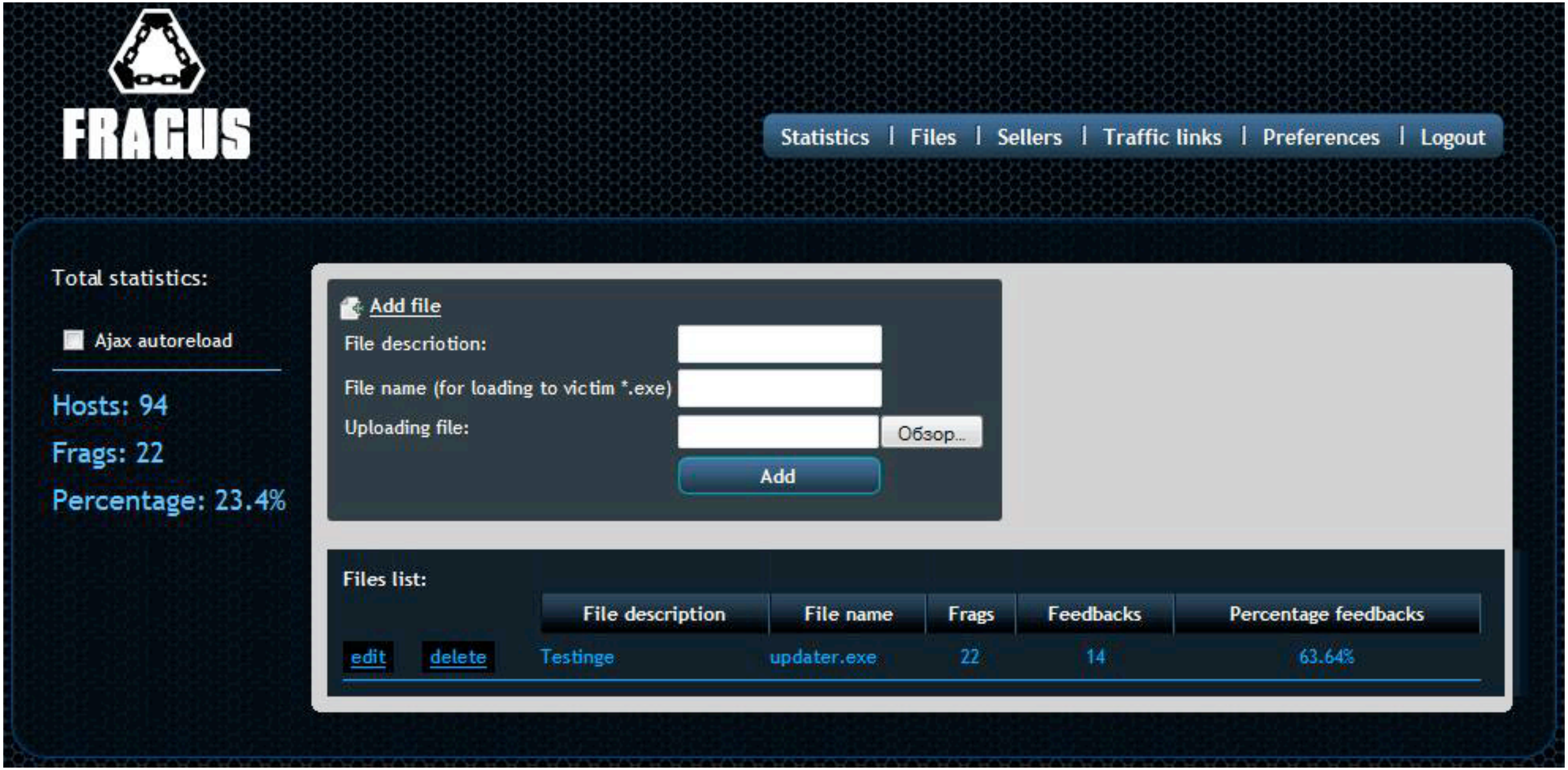
Login

Password

Zeus botnet rental and loading

Malware Interfaces

►Modern malware can be convenient and easy to use



FRAGUS
Statistics | Files | Sellers | Traffic links | Preferences | Logout

Total statistics:

□ Ajax autoreload

Hosts: 94

Frags: 22

Percentage: 23.4%

Add file

File desсriotion:

File name (for loading to victim *.exe)

Uploading file:

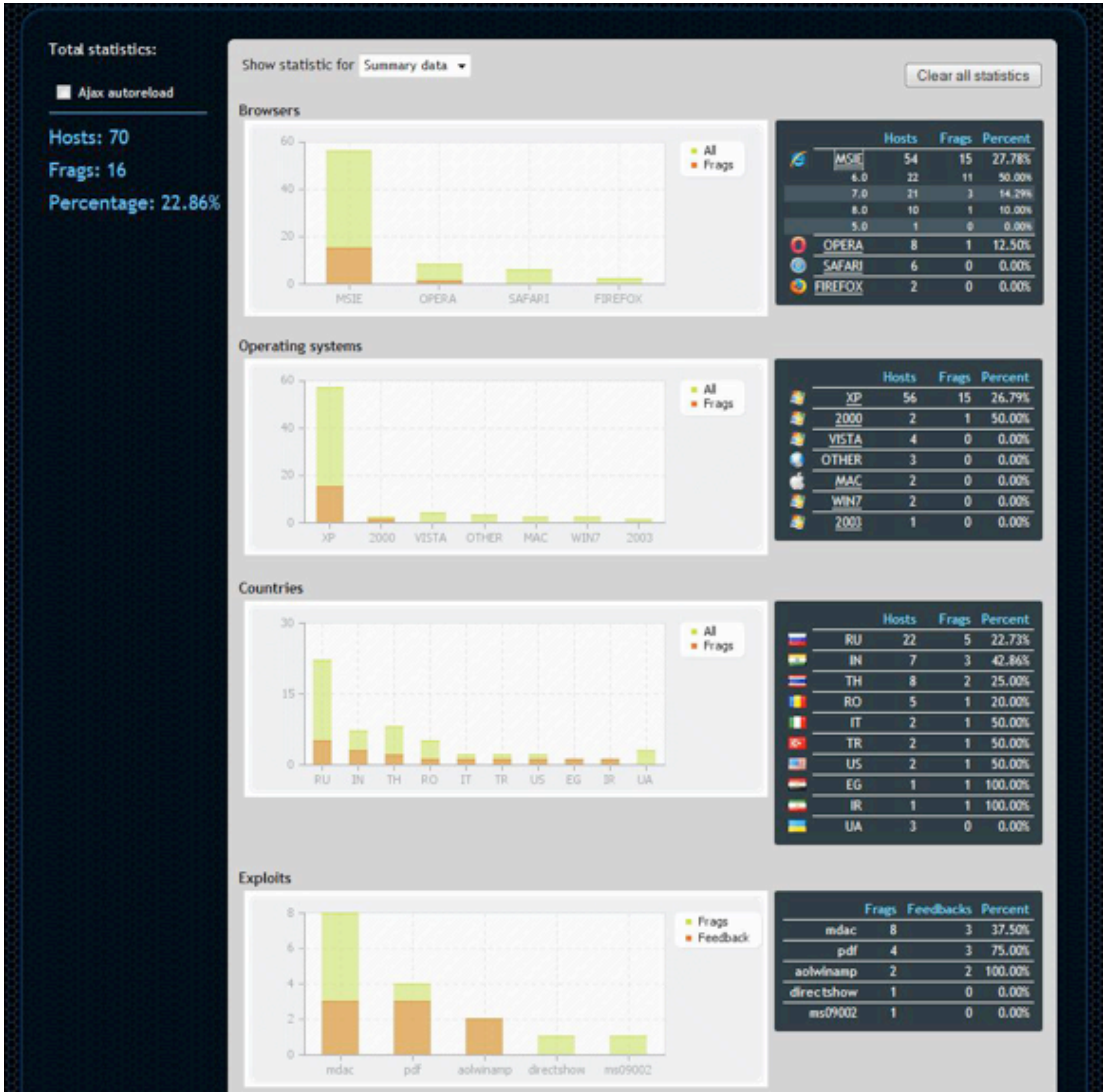
Files list:

		File description	File name	Frags	Feedbacks	Percentage feedbacks
edit	delete	Testinge	updater.exe	22	14	63.64%

Fragus botnet rental and loading

Malware Interfaces

►Modern malware can be convenient and easy to use



Hosts: 70

Frags: 16

Percentage: 22.86%

	Hosts	Frags	Percent
MSIE	54	15	27.78%
6.0	22	11	50.00%
7.0	21	3	14.29%
8.0	10	1	10.00%
5.0	1	0	0.00%
OPERA	8	1	12.50%
SAFARI	6	0	0.00%
FIREFOX	2	0	0.00%

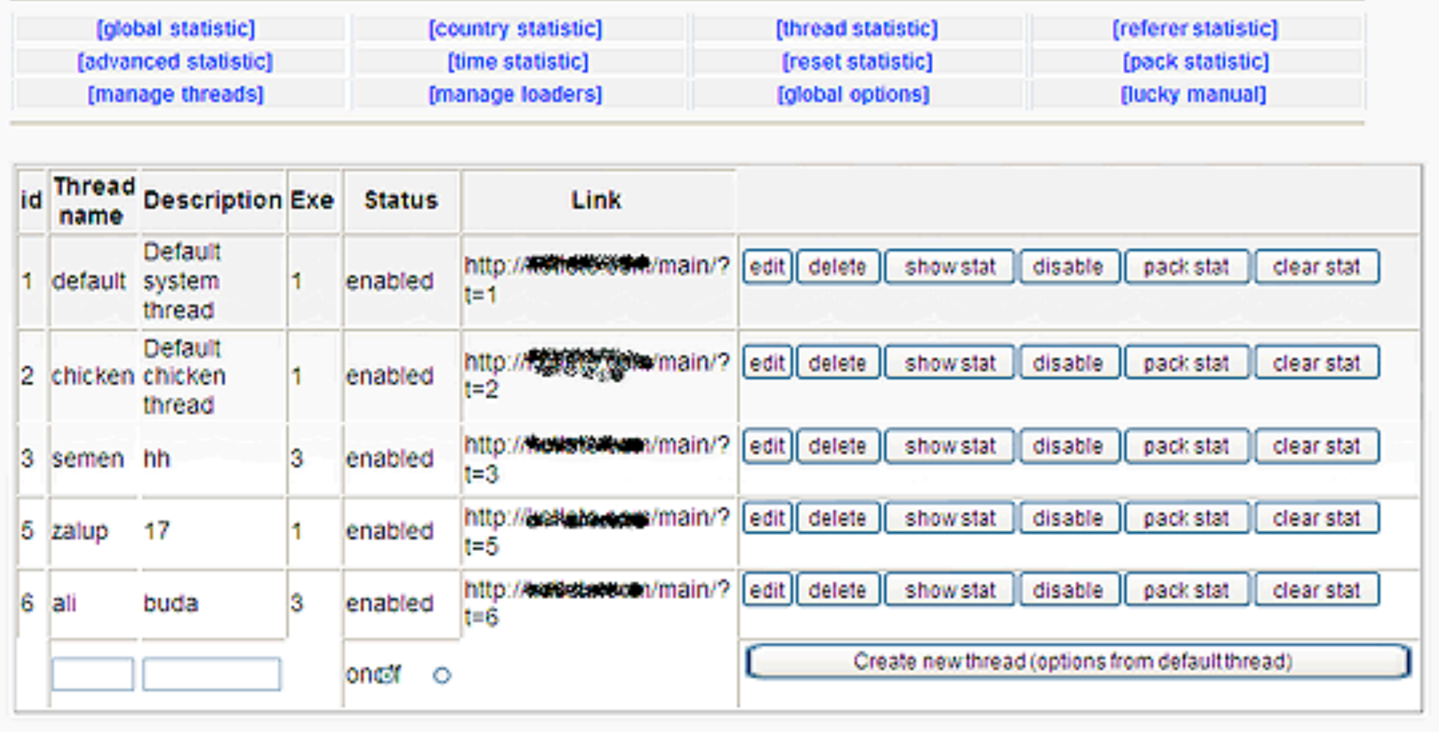
	Hosts	Frags	Percent
XP	56	15	26.79%
2000	2	1	50.00%
VISTA	4	0	0.00%
OTHER	3	0	0.00%
MAC	2	0	0.00%
WIN7	2	0	0.00%
2003	1	0	0.00%

	Hosts	Frags	Percent
RU	22	5	22.73%
IN	7	3	42.86%
TH	8	2	25.00%
RO	5	1	20.00%
IT	2	1	50.00%
TR	2	1	50.00%
US	2	1	50.00%
EG	1	1	100.00%
IR	1	1	100.00%
UA	3	0	0.00%

	Frags	Feedbacks	Percent
mdac	8	3	37.50%
pdf	4	3	75.00%
aolwinamp	2	2	100.00%
directshow	1	0	0.00%
ms09002	1	0	0.00%

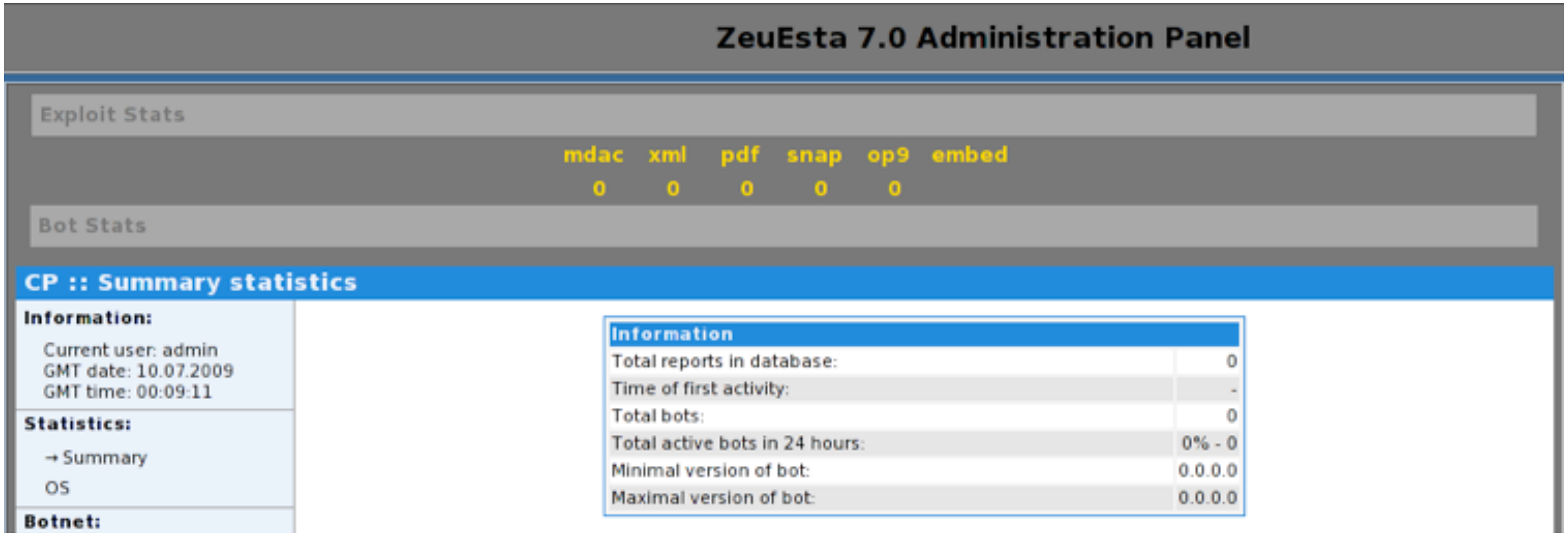
Malware Interfaces

►Modern malware can be convenient and easy to use



[global statistic]	[country statistic]	[thread statistic]	[referer statistic]
[advanced statistic]	[time statistic]	[reset statistic]	[pack statistic]
[manage threads]	[manage loaders]	[global options]	[lucky manual]

id	Thread name	Description	Exe	Status	Link	
1	default	Default system thread	1	enabled	http://[redacted]/main/?t=1	edit delete show stat disable pack stat clear stat
2	chicken	Default chicken thread	1	enabled	http://[redacted]/main/?t=2	edit delete show stat disable pack stat clear stat
3	semen	hh	3	enabled	http://[redacted]/main/?t=3	edit delete show stat disable pack stat clear stat
5	zalup	17	1	enabled	http://[redacted]/main/?t=5	edit delete show stat disable pack stat clear stat
6	ali	buda	3	enabled	http://[redacted]/main/?t=6	edit delete show stat disable pack stat clear stat
				on ● off ○		Create new thread (options from default thread)



ZeuEsta 7.0 Administration Panel

Exploit Stats

mdac	xml	pdf	snap	op9	embed
0	0	0	0	0	

Bot Stats

CP :: Summary statistics

Information:

Current user: admin
GMT date: 10.07.2009
GMT time: 00:09:11

Statistics:

→ Summary
OS

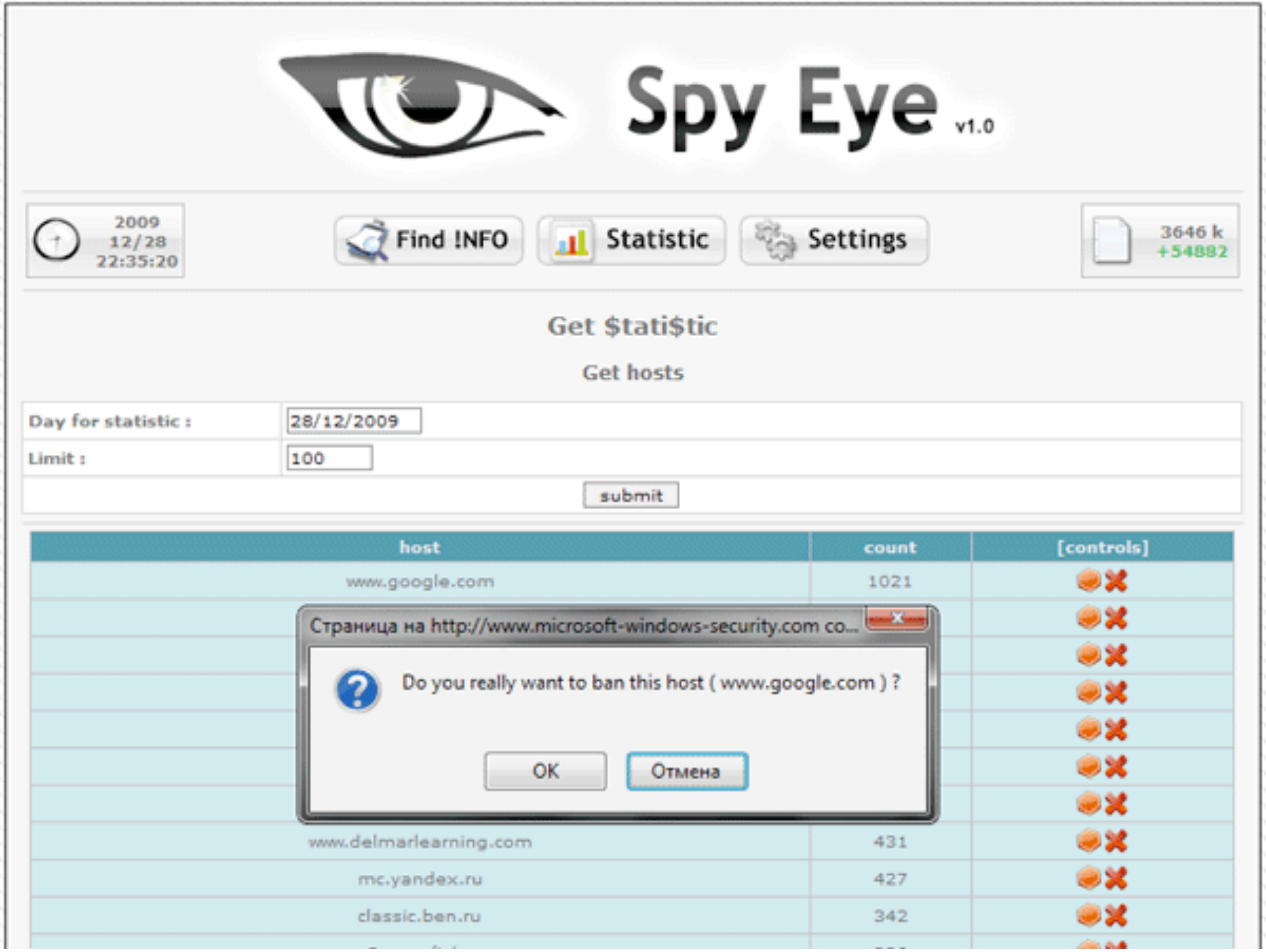
Botnet:

Information	
Total reports in database:	0
Time of first activity:	-
Total bots:	0
Total active bots in 24 hours:	0% - 0
Minimal version of bot:	0.0.0.0
Maximal version of bot:	0.0.0.0

LuckySploit and ZeuEsta Exploit Kit

Malware Interfaces

►Modern malware can be convenient and easy to use



Get $tati$tic

Get hosts

Day for statistic :	28/12/2009
Limit :	100

host	count	[controls]
www.google.com	1021	● ✗
		● ✗
		● ✗
		● ✗
		● ✗
		● ✗
		● ✗
		● ✗
www.delmarlearning.com	431	● ✗
mc.yandex.ru	427	● ✗
classic.ben.ru	342	● ✗

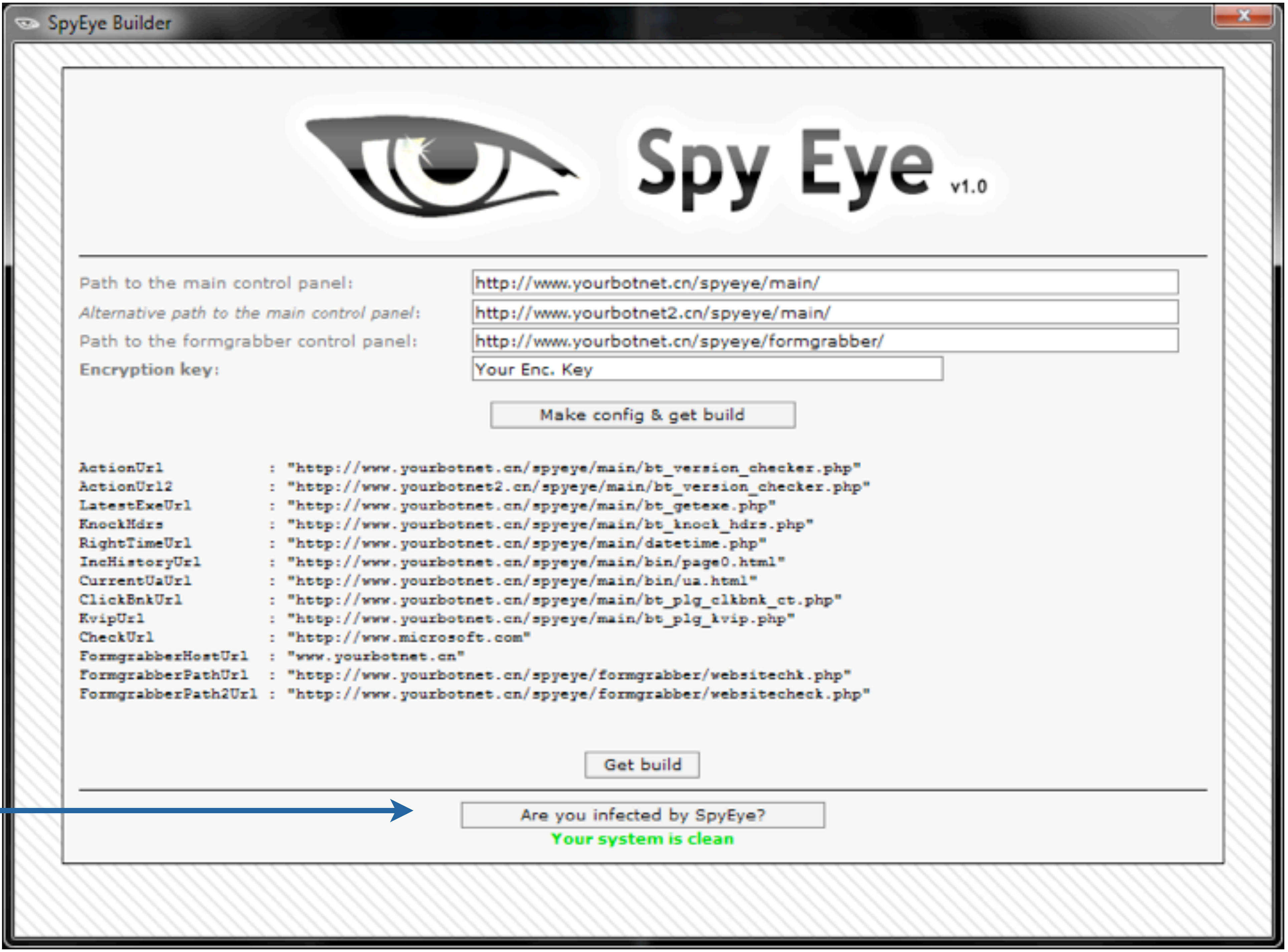
Страница на http://www.microsoft-windows-security.com co...

Do you really want to ban this host (www.google.com) ?

Spy Eye botnet control

Malware Interfaces

►Modern malware can be convenient and easy to use



Path to the main control panel: http://www.yourbotnet.cn/spyeye/main/

Alternative path to the main control panel: http://www.yourbotnet2.cn/spyeye/main/

Path to the formgrabber control panel: http://www.yourbotnet.cn/spyeye/formgrabber/

Encryption key: Your Enc. Key

```
ActionUrl           : "http://www.yourbotnet.cn/spyeye/main/bt_version_checker.php"
ActionUrl2          : "http://www.yourbotnet2.cn/spyeye/main/bt_version_checker.php"
LatestExeUrl        : "http://www.yourbotnet.cn/spyeye/main/bt_getexe.php"
KnockHdrs           : "http://www.yourbotnet.cn/spyeye/main/bt_knock_hdrs.php"
RightTimeUrl        : "http://www.yourbotnet.cn/spyeye/main/datetime.php"
IncHistoryUrl       : "http://www.yourbotnet.cn/spyeye/main/bin/page0.html"
CurrentUaUrl        : "http://www.yourbotnet.cn/spyeye/main/bin/ua.html"
ClickBnkUrl         : "http://www.yourbotnet.cn/spyeye/main/bt_plg_clkbnk_ct.php"
KvipUrl             : "http://www.yourbotnet.cn/spyeye/main/bt_plg_kvip.php"
CheckUrl            : "http://www.microsoft.com"
FormgrabberHostUrl  : "www.yourbotnet.cn"
FormgrabberPathUrl  : "http://www.yourbotnet.cn/spyeye/formgrabber/websitechk.php"
FormgrabberPath2Url : "http://www.yourbotnet.cn/spyeye/formgrabber/websitecheck.php"
```

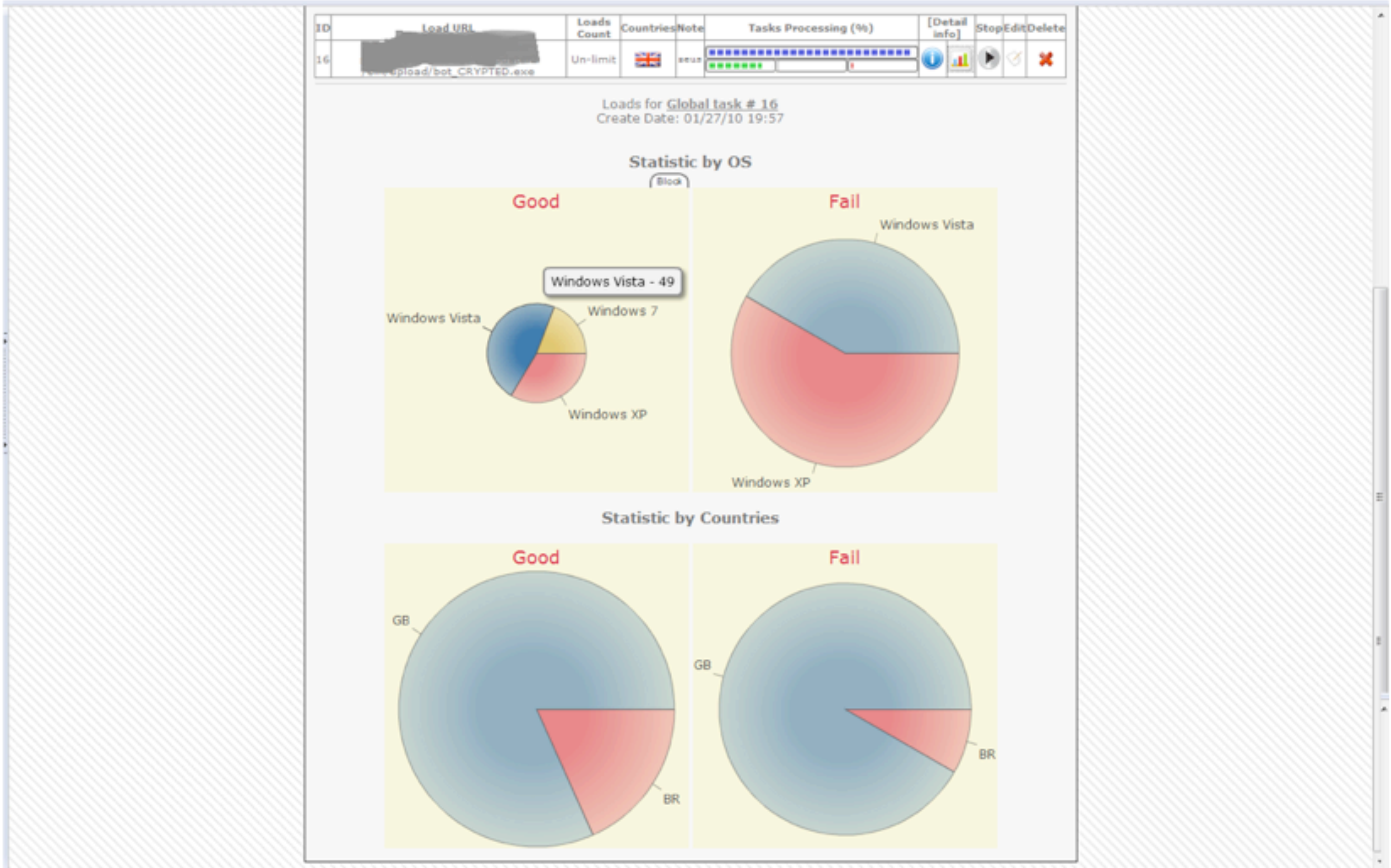
Your system is clean

Don’t get infected by your own malware

Spy Eye botnet control

Malware Interfaces

►Modern malware can be convenient and easy to use



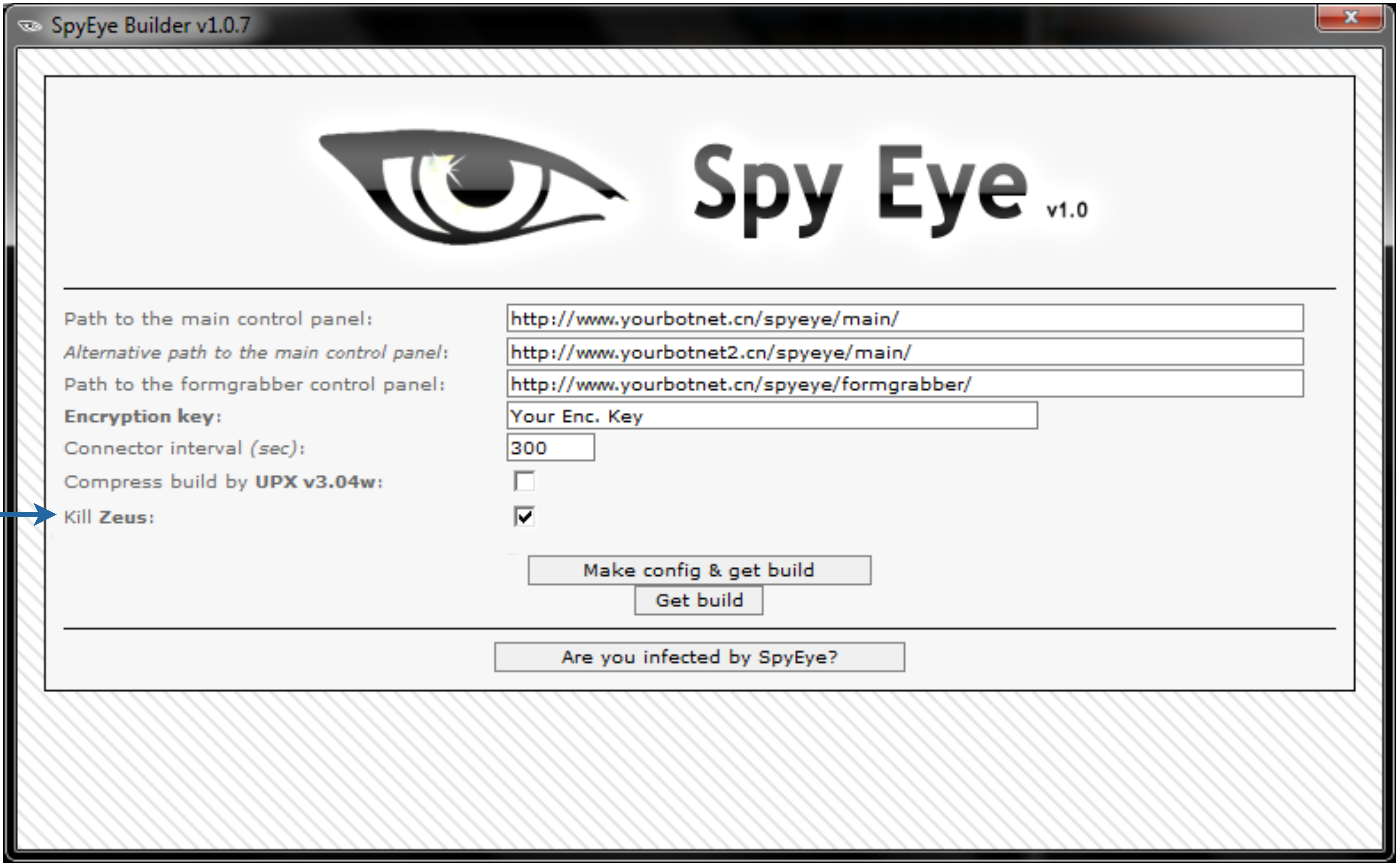
ID	Load URL	Loads Count	Countries	Note	Tasks Processing (%)	[Detail info]	Stop	Edit	Delete
16	[redacted]	Un-limit	🇬🇧	zeus		ⓘ	▶		✖

Loads for Global task # 16
Create Date: 01/27/10 19:57

Spy Eye botnet control

Malware Interfaces

- ►Modern malware can be convenient and easy to use



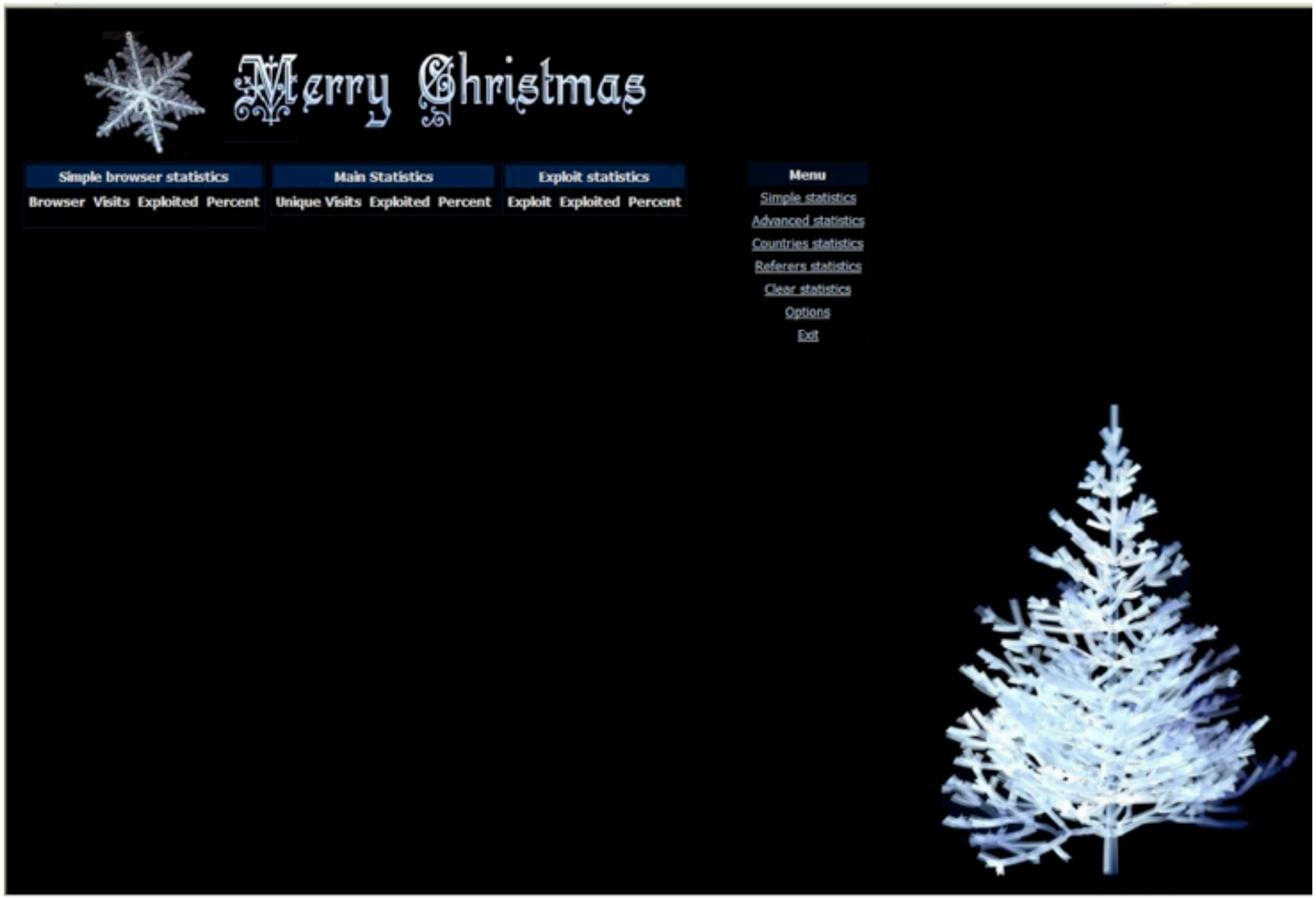
Path to the main control panel: http://www.yourbotnet.cn/spyeye/main/
Alternative path to the main control panel: http://www.yourbotnet2.cn/spyeye/main/
Path to the formgrabber control panel: http://www.yourbotnet.cn/spyeye/formgrabber/
Encryption key: Your Enc. Key
Connector interval *(sec)*: 300
Compress build by **UPX v3.04w**: □
Kill **Zeus**: ☑

Kill competitors easily

Spy Eye botnet control

Malware Interfaces

►Modern malware can be convenient and easy to use



Simple browser statistics				Main Statistics			Exploit statistics		
Browser	Visits	Exploited	Percent	Unique Visits	Exploited	Percent	Exploit	Exploited	Percent

A botnet control screen featuring a Christmas theme

Malware Interfaces

►Modern malware can be convenient and easy to use

- ►Neon Exploit System v2.0.5 ($ 400)
  - "Among the modules of exploits that are preinstalled and preconfigured include: IE7 MC, PDF collab, PDF util.printf, PDF foxit reader, MDAC, Snapshot and Flash 9."
- ►Eleonore Exploits Pack v1.2 ($ 700 - $ 1500)
  - "MDAC, MS009-02, Telnet - Opera, Font tags - FireFox, PDF collab.getIcon, PDF Util.Printf, PDF collab.collectEmailInfo, DirectX DirectShow and Spreadsheet."
- ►Limbo Trojan Kit ($ 300)
- ►ElFiesta v3 ($ 800)
- ►Unique Sploits Pack v2.1 ($ 750)
- ►YES Exploit System v2.0.1 ($800)

etc.

Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

Linux rootkits

Rootkits

►A lookout at the state of Linux rootkits

- ►Rootkit: "Designed to hide or obscure the fact that a system has been compromised." (Wikipedia)
- ►Set of software to maintain malicious access to a compromised host

►Rootkit: first generation

- ►Change binaries (ps, ls, netstat, lsof, ssh) or libraries (ld.so.preload, etc.)
- ►*Pros*: kernel independent
- ►*Cons*: need to be compiled for the target platform, easy to detect
- ►*How to detect*: check system binaries against trusted instances
  - ▪ Tripwire, rpm -V, etc.

Rootkits

Rootkit: second generation

- Kernel level rootkits
  - Modify kernel structures (syscall table, IDT, etc.)
- Malicious codes is loaded directly in the kernel
  - Loadable Kernel Modules
  - Direct /dev/mem access (patch kernel on-the-fly)

- *Pros*: difficult to detect, usually includes backdoor features
- *Cons*: LKM can be disabled, /dev/{k,}mem access now restricted
- *How to detect*: search for known patterns, or known bugs.
  - rkhunter, chkrootkit, Samhain, etc.

Rootkits

▶ Rootkit: new trends

- ▶ Filesystem, network stack level rootkits
  - Often used as additional features
- ▶ Hypervisor rootkit
- ▶ Debug register based rootkit
  - Seen in the wild early 2010...

▶ Conclusion: Root account compromised == "game over"

SEC_RITY is not complete without U

Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

What to do when it is too late?

Dealing with a security incident

Procedure to deal with a compromised system

- Contact the CERN security team at Computer.Security@cern.ch
- Don't panic:
- Disconnect, but leave "on" (if applicable):
- Contact the Security Team at Computer.Security@cern.ch
- Don't touch anymore: wait for instructions

The response will be commensurate to the risk, e.g.:

- Compromised Windows laptop
  - Data will be backed up
  - Upon system reinstallation, auto-update + antivirus installed
- Multi-users Linux system
  - The cause of the problem must be understood to prevent reoccurrence
  - Dedicated incident response procedure followed
  - System reinstalled from scratch

Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

Thank you

"Just because you can, does not mean you should."

Computer Security Day
10 June 2010, Council Chamber and http://cern.ch/SecDay

Questions and discussion