

Betabot retrospective

xylibox.com/2015/04/betabot-retrospective.html

General statistics

Botnet: **Net1**
 Created: **07/29/2013**
 Version: **1.0.2.5**
 Failed login attempts: **71**
 Gate status: **Enabled**

Connections

Total bots: **467**
 Total bots from USB: **13**
 Bots online: **79**
 Bots online (Past 3h): **166**
 Bots online (Past 24h): **295**
 Bots online (Past 3 days): **414**
 Bots online (Past 7 days): **542**
 New bots (Past 24h): **27**
 New bots from USB (Past 24h): **9**
 Bots offline: **388**
 Bots dead: **4130**
 Possible duplicate entries: **201**

Components

.NET Framework: **428 / 467**
 Has Admin. Rights: **263 / 467**
 UAC S.E. Success rate: **181 / 222**

Logs

Form captures to date: **107**
 Login captures to date: **716**

Operating Systems

Windows 8: **21**

Search Bots

[Click here to expand / collapse search options](#)

Machine ID	IP	Location	Operating System	Install date	AntiVirus	Killed
C8CA96C4B94F284382A239281C93FC4		United States (US)	Windows XP SP3 (x86)	09/23/2013 04:13:15 pm	N/A	0
D49F4AA10646E24CA5ACC01A2C24A049		France (FR)	Windows 7 SP1 (x86)	09/14/2013 09:53:57 am	N/A	0
F80138950F8D0043A88449C470A82C2A		France (FR)	Windows 7 SP1 (x64)	09/08/2013 04:41:21 am	Avira	0
ACCF57D39AE02441AA79DA5F39170776		France (FR)	Windows 7 SP1 (x86)	09/07/2013 05:05:26 pm	N/A	0
E2A685AA22CC7A4195E50A5695BD8297		United States (US)	Windows 7 SP1 (x64)	09/07/2013 11:58:37 am	United States (US)	0
697A43DF8F888447971A990ED84AE91F		France (FR)	Windows 7 SP1 (x86)	09/07/2013 08:43:59 am	Avira	0
F8B0FC4E5A34748D00FE3A1148B1F1F		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:43:38 am	Avast	0
06ABFD3678879540A447BE230832FA8		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:43:38 am	ESET	0
0E66915AD9466743A3A6CB9F36AEE00B		France (FR)	Windows Vista SP2 (x64)	09/07/2013 08:43:06 am	N/A	0
852BCA470146114887F6D9C5D06948D2		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:42:13 am	Avira	0
C40630A30AA1C846A865F70577ABFA94		France (FR)	Windows 7 (x86)	09/07/2013 08:41:36 am	N/A	0
09820C68EAE3D04A8AB1F8823C36165F		France (FR)	Windows 7 SP1 (x86)	09/07/2013 08:41:30 am	McAfee	0
248F1D86724D24F973BF4DF50576F48		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:40:09 am	N/A	0
F4026E0ECF6949A577036E53B4E199		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:40:04 am	N/A	0
ASD443EC740B6A4F831294798DE78A3D		France (FR)	Windows 7 SP1 (x86)	09/07/2013 08:39:34 am	Norton	0
CS20618DD2E592479ECC87F7E6137CD3		France (FR)	Windows 7 SP1 (x86)	09/07/2013 08:39:16 am	Avast	0
DDCSAC2948625C4CB84695248D2AD5AA		United States (US)	Windows 7 (x64)	09/07/2013 08:36:27 am	N/A	0

Some of you know Betabot.. if you don't: <http://www.ic3.gov/media/2013/130918.aspx>

1.0.2.5 panel:
Dashboard:

The screenshot shows the Betabot control panel interface. At the top, there are navigation tabs: Betabot, Clients, Tasks, Statistics, Logs, Settings, and Help. The main content area is divided into several sections:

- General statistics:** Botnet: Net1, Created: 07/29/2013, Version: 1.0.2.5, Failed login attempts: 71, Gate status: Enabled.
- Connections:** Total bots: 467, Total bots from USB: 13, Bots online: 79, Bots online (Past 3h): 166, Bots online (Past 24h): 295, Bots online (Past 3 days): 414, Bots online (Past 7 days): 542, New bots (Past 24h): 27, New bots from USB (Past 24h): 9, Bots offline: 388, Bots dead: 4130, Possible duplicate entries: 201.
- Components:** .NET Framework: 428 / 467, Has Admin. Rights: 263 / 467, UAC S.E. Success rate: 181 / 222.
- Logs:** Form captures to date: 107, Login captures to date: 716.
- Operating Systems:** Windows 8: 21, Windows 7: 285, Windows Vista: 17, Windows XP: 144, Windows Server 2008: 2, Windows Server 2003: 0.

Below these sections is a 'Search Bots' table with columns for Machine ID, IP, Location, Operating System, Install date, AntiVirus, and Killed. The table lists various bots with their details, including locations like United States (US), France (FR), and Ukraine (UA).

extended information:

Extended information for ██████████

Status:	Online
Bot GUID:	9CCF38332F12742989F29D7467878B
Source:	Spam / Exploit Pack
Install Path:	C:\ProgramData\Magic Services\oldtsandku.exe
Install Date:	09/22/2013 10:35:09 am
Last CheckIn:	09/23/2013 04:43:37 pm
Bot owned for:	1d 6h 7m 28s
Operating System:	Windows 7 SP1 (x64)
Local Time:	04:43:43 pm
IP:	██████████
Country:	France (FR)
SOCKS4 Port:	N/A
Bots killed since installed:	0
Default Browser:	torch.exe
Login Username:	patia-HP(AURELIEN ET OLIVIER
Detected Antivirus:	Norton
Exceptions Info:	0 (r) / 0 (w)
Running with Administrator privileges:	No
Has .NET Framework installed:	Yes
Has Steam installed:	Yes
Has Java installed:	Yes

Search options:

[Click here to expand / collapse search options](#)

Misc. Filters

- Online
- Has .NET Framework
- Has Steam
- Has administrative privileges
- Has used RDP at least once before
- Has individual comment

Operating Systems

- All Operating Systems
- Windows 8
- Windows 7
- Windows Vista
- Windows XP
- Windows Server 2008
- Windows Server 2003

IP Search (Only a single IP can be searched at a time)

Tasks:

Task Name - 25

Order of tasks | Delete all completed tasks | Suspend all active tasks | Export tasks table | Export tasks table (0/8-1/3)

Task Name	Type	Created	# Executed / Max	Status	Options
PlayStation	Site / Uninstall	06/27/2013 06:09:23 pm	1 / 1	Completed	New Task Info Details Back Resume
mp3tag	Build / operation	06/26/2013 06:20:26 pm	1 / 104	Completed	New Task Info Details Back Resume
MSI	Build / operation	06/26/2013 06:46:23 pm	60 / 107	Completed	New Task Info Details Back Resume
MSI	Download / Update file	06/26/2013 07:17:11 pm	0 / 106	Completed	New Task Info Details Back Resume
MSI	Site / Uninstall	06/26/2013 06:46:53 pm	1 / 1	Completed	New Task Info Details Back Resume
MSI	Site / Uninstall	06/26/2013 06:20:26 pm	1 / 1	Completed	New Task Info Details Back Resume
FourPattStarE	Download / Update file	06/26/2013 06:20:43 pm	20 / 206	Completed	New Task Info Details Back Resume
MSI-4	Build / operation	06/26/2013 06:40:26 pm	69 / 104	Completed	New Task Info Details Back Resume
SetBot	Site / Uninstall	06/27/2013 12:09:22 pm	1 / 1	Completed	New Task Info Details Back Resume
mp3tag-DownloadP32	Download / Update file	06/27/2013 07:28:44 pm	0 / 106	Completed	New Task Info Details Back Resume
MSI-4	Site / Uninstall	06/26/2013 06:20:49 pm	1 / 1	Completed	New Task Info Details Back Resume
mp3tag	Build / Attack	06/26/2013 06:27:46 pm	60 / 104	Completed	New Task Info Details Back Resume
DownloadP32	Download / Update file	06/26/2013 06:07:47 pm	1 / 1	Completed	New Task Info Details Back Resume
mp3tag	Download / Update file	06/26/2013 06:20:43 pm	22 / 104	Completed	New Task Info Details Back Resume
mp3tag	Download / Update file	06/26/2013 06:16:42 pm	42 / 103	Completed	New Task Info Details Back Resume

[1 / 1]

Remove bot:

General statistics

Bot ID: 140
Created: 1/19/2013
Version: 1.0.0.1

Configuration

Task ID: 140
Max retries: 24
Max offset: 300

Task Name

Task Name:

Maximum tasks to execute task:

Expiration date for task: 12/31/2013

Task status

Initial task status:
 Active
 Suspended

Excluded operating systems

Apply task only to these list OSes (Example: *Ubuntu, *Linux, *BSD, *...)

Apply task only to bots with these IDs (Example: 123456, 789012, ...)

Only execute on bots that ...

Have API Framework
 Have used Windows Family Desktop at some point
 Are running with administrative privileges
 Have no detectable anti-virus running
 Is a new bot

All bot systems
 All OS systems

[Click here to select filters based on specific installed software](#)

Operating Systems the task applies to ...

- Windows XP
- Windows 7
- Windows Vista
- Windows XP
- Windows Server 2008
- Windows Server 2003

Countries task applies to (Example: US, RU, ...)

Run Task

Terminate bot till next reboot:

General statistics

Bot ID: 140
Created: 1/19/2013
Version: 1.0.0.1

Configuration

Task ID: 140
Max retries: 24
Max offset: 300

Task Name

Task Name:

Maximum tasks to execute task:

Expiration date for task: 12/31/2013

Task status

Initial task status:
 Active
 Suspended

Excluded operating systems

Apply task only to these list OSes (Example: *Ubuntu, *Linux, *BSD, *...)

Apply task only to bots with these IDs (Example: 123456, 789012, ...)

Only execute on bots that ...

Have API Framework
 Have used Windows Family Desktop at some point
 Are running with administrative privileges
 Have no detectable anti-virus running
 Is a new bot

All bot systems
 All OS systems

[Click here to select filters based on specific installed software](#)

Operating Systems the task applies to ...

- Windows XP
- Windows 7
- Windows Vista
- Windows XP
- Windows Server 2008
- Windows Server 2003

Countries task applies to (Example: US, RU, ...)

Run Task

Botkill:

General installation

Release: 4.0.0 (beta)
Version: 4.0.0 (beta)

Dependencies

Full OS: Win
Min. version: Win
Max. version: Win

Non-Task Features

Win: Windows Firewall
Win: Windows Defender
Win: Windows Update
Win: Windows Defender
Win: Windows Defender
Win: Windows Defender

Install a task type

Install task: Socks4

General installation options

Task name:

Maximum tasks to execute task:

Expiration date for task:

Initial task status:
 Active
 Suspended

Excluded language

Apply task only to those that match language:

Apply task only to tasks with these PID (Example: 12345, 67890, ...):

Only execute on tasks that ...

From .NET Framework
 Has used Windows Firewall history at some point
 Has running with administrative privileges
 Has no Windows anti-virus running
 Is a new task

Citrix systems
 Citrix systems

[Click here to select filters based on specific installed software](#)

Operating Systems this task applies to ...

Windows 7
Windows 8
Windows 10
Windows XP
Windows Server 2008
Windows Server 2012

Countries task applies to (Example: US, RU, ...):

ADD TASK

Socks4:

General installation

Release: 4.0.0 (beta)
Version: 4.0.0 (beta)

Dependencies

Full OS: Win
Min. version: Win
Max. version: Win

Non-Task Features

Win: Windows Firewall
Win: Windows Defender
Win: Windows Update
Win: Windows Defender
Win: Windows Defender
Win: Windows Defender

Install a task type

Install task: Socks4

General installation options

Task name:

Server address: (Server - change if for no proxy)

Port: (Optional)

Use random port for each client
 Stop sending SOCKS error - (if false - field are ignored)

Task options

Task name:

Maximum tasks to execute task:

Expiration date for task:

Initial task status:
 Active
 Suspended

Excluded language

Apply task only to those that match language:

Apply task only to tasks with these PID (Example: 12345, 67890, ...):

Only execute on tasks that ...

From .NET Framework
 Has used Windows Firewall history at some point
 Has running with administrative privileges
 Has no Windows anti-virus running
 Is a new task

Citrix systems
 Citrix systems

[Click here to select filters based on specific installed software](#)

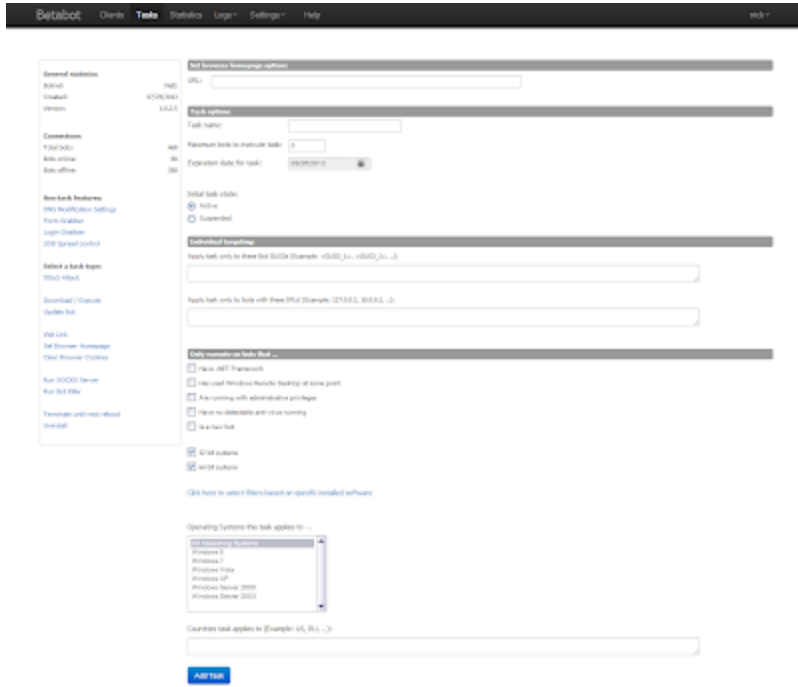
Operating Systems this task applies to ...

Windows 7
Windows 8
Windows 10
Windows XP
Windows Server 2008
Windows Server 2012

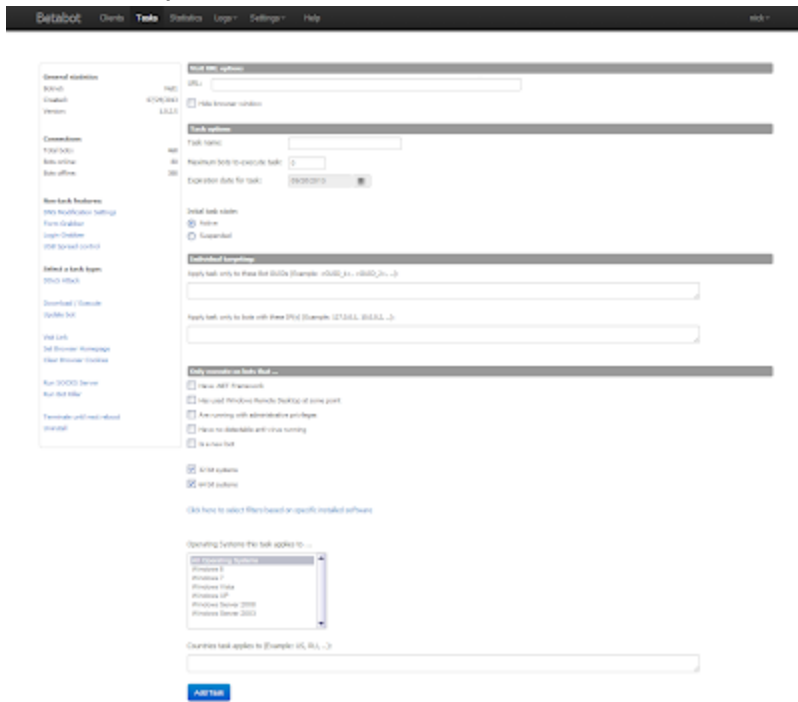
Countries task applies to (Example: US, RU, ...):

ADD TASK

Set browser homepage:



Visit URL option:



Update bot option:

Database Clients **Tasks** Statistics Logs Settings Help

General statistics

Users: 100

Threads: 412/1000

Version: 4.0.11.2

Connections

Total: 100

Idle: 100

Idle: 100

Idle: 100

Non-Task Features

SQL Replication Settings

Auto-kill User

Logon-Timeout

SQL Server-Timeout

Admin a Task type

SQL-Task

Download | Upgrade

Update list

SQL-Task

Set Browser Homepage

Clear Browser Cookies

Run SQL-Task Server

Run Task Client

Formulas and math about

General

Task type

File URL:

Random wait before download (Set of wait random 1-8 seconds before downloading to reduce stress on file host)

This update is a recursive version of **taskdef** (This is a feature update for your own task use this for a more reliable update)

Ignore if both task matches same as task update (Set of not match the update if another connection is used)

Task settings

Task name:

Maximum tasks to execute task:

Expiration date for task:

Initial task state:

Active

Suspended

Advanced configuration

Apply task only to these IP addresses (Example: 192.168.1.1 - 192.168.1.2)

Apply task only to tasks with these IDs (Example: 123456, 789012)

Only execute on task that

Have .NET Framework

Have used Windows Remote Desktop at some point

Are running with administrative privileges

Have no detectable anti-virus running

Is a local host

All task systems

All task systems

Click here to select files based on specific installed software

Operating Systems this task applies to ...

Operating Systems

Windows 8

Windows 7

Windows Vista

Windows XP

Windows Server 2008

Windows Server 2003

Countries task applies to (Example: US, RU, ...)

Add Task

Download file option:

Database Clients **Tasks** Statistics Logs Settings Help

General statistics

Users: 100

Threads: 412/1000

Version: 4.0.11.2

Connections

Total: 100

Idle: 100

Idle: 100

Idle: 100

Non-Task Features

SQL Replication Settings

Auto-kill User

Logon-Timeout

SQL Server-Timeout

Admin a Task type

SQL-Task

Download | Upgrade

Update list

SQL-Task

Set Browser Homepage

Clear Browser Cookies

Run SQL-Task Server

Run Task Client

Formulas and math about

General

Task type

File URL:

Random wait before download (Set of wait random 1-8 seconds before downloading to reduce stress on file host)

Hide application window

Automatically schedule downloaded file for deletion on release

Run program in console (Prevent program from making particular changes to system)

Enable process deletion for the new process (Disable deletion resources for the process and allow for access to system resources)

Task settings

Task name:

Maximum tasks to execute task:

Expiration date for task:

Initial task state:

Active

Suspended

Advanced configuration

Apply task only to these IP addresses (Example: 192.168.1.1 - 192.168.1.2)

Apply task only to tasks with these IDs (Example: 123456 & 789012)

Only execute on task that

Have .NET Framework

Have used Windows Remote Desktop at some point

Are running with administrative privileges

Have no detectable anti-virus running

Is a local host

All task systems

All task systems

Click here to select files based on specific installed software

Operating Systems this task applies to ...

Operating Systems

Windows 8

Windows 7

Windows Vista

Windows XP

Windows Server 2008

Windows Server 2003

Countries task applies to (Example: US, RU, ...)

Add Task

DDoS cmd option:

General settings

Language: English

Username:

Bot settings

of bots before bot is activated:

Bot mode interval (min):

Bot Instance (Global) [1] If you click on disabling bot mode it will not work unless you check this box and press it off.

Aggressive security and targeting [2]

Use DNS spoofing [2]

Redirect to fake website [2]

Reduced functionality mode

Enabling reduced functionality mode will improve bot stability, but also disable certain functionality, as well as custom configuration. Features disabled are:

1. DNS
2. Forwarder (Only if reduced functionality option is checked)
3. Use FTP type mode (Does not work in reduced mode)
4. Hosts configuration
5. Proxy to fake website

If you encounter a problem with the bot, try using reduced functionality mode and please post your logs to our support forum if you are stuck.

Enable reduced functionality mode. No options

Enable reduced functionality mode. With custom options (longer support only)

Disable custom site path.

Security settings

General bot aggressivity with (Global):

Hosts or hosts

Redirect from existing suspicious source

Check for communication pattern. (Checking for patterns will prevent you from communicating with the panel and it will not work.)

Bot DNS Modification List

IP blacklist:

IP Blacklist

Enter blacklisted IPs in the following format:

```
127.0.0.1:<reason ID>
10.1.1.255:1
169.168.1.2:5
```

IDs: **1** = Suspicious Behavior, **2** = Honeypot, **3** = Other, **4** = SQLi Attempt(s), **5** = Login Page Attack(s), **6 and up** = User-defined

85.156.5.53:4
88.172.66.132:4

List of dns record to modify:

List of DNS records to modify

Enter domain entries in this format:

```
domain.com 127.0.0.1
sub.blah.com 10.0.0.1
*symantec.* 127.0.0.1
```

And so on. Wildcards are accepted. Failure to abide precisely by this format could result in unknown errors. Maximum of **1024** entries are allowed.

Save list
Close

Help:

Help contents

What type of bot is this?
This is an all purpose HTTP based bot with some information gathering properties for no way of advertising but and not will it ever be developed into one.

How do I update the IP list?
In order of first time you may need to add the IP list information into writing script as there is no start button yet sometimes you do it or more that all others. Since IP is always configured for this case you should go to the database you created for the bot then "update ip list" "yes" - Click "yes" and on the page what type "CSV" - Simply select and continue handling with it's fully supported.

Do we get any form reports, what?
In order to receive form reports, you need to add your own site files to the page. In menu, that at the bottom right of the site panel select "manage website grab files" - Once you have done this, enter the URL of the page that handles the form you want to capture data from, and surround it with asterisks (*) - Because forms are grabbed based on URL/Wildcard rules, you must always surround with asterisks.

What should I see (sensitive data) from panel settings?
The below prevents other programs (mainly other malware) from starting, cookies, scripts, and any links some attempt it makes installation. This is useful when you do not want other bots reading or writing property on the same system. However, if you plan on downloading other components, you should keep the database as well because with anything you may download (pdf for ex. etc).

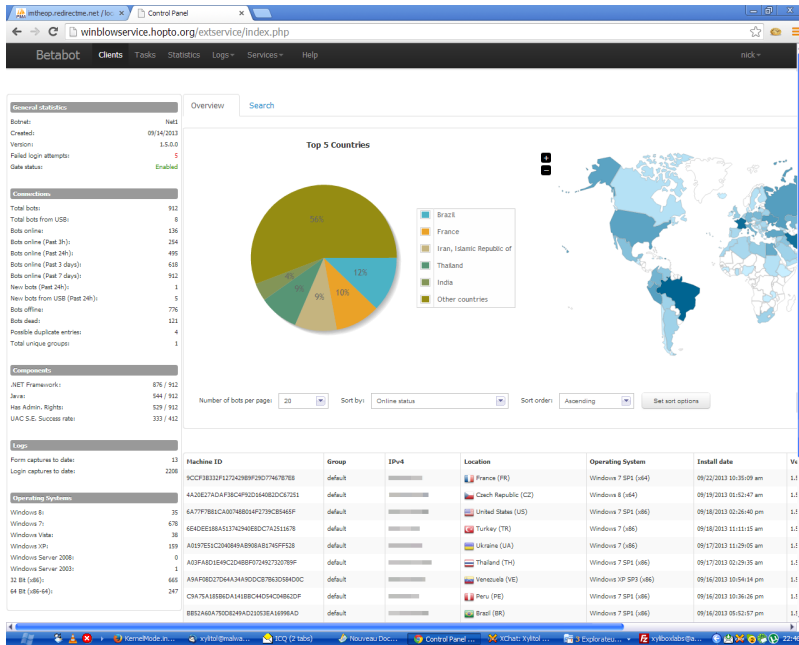
Trying to export data from the panel says unable to write / cannot download. What?
A few places in the panel need write access. The panel.php script need write access to the following directories:

- 1. database
- 2. reports
- 3. settings.php (during who-who)

Please CHMOD these areas with correct permissions (or write access) if you have not already.

Sometimes error dialogs are not properly executed. It says completed but?
If the script is done by "done" of task) and it will be back to execute.

1.5.0.0:



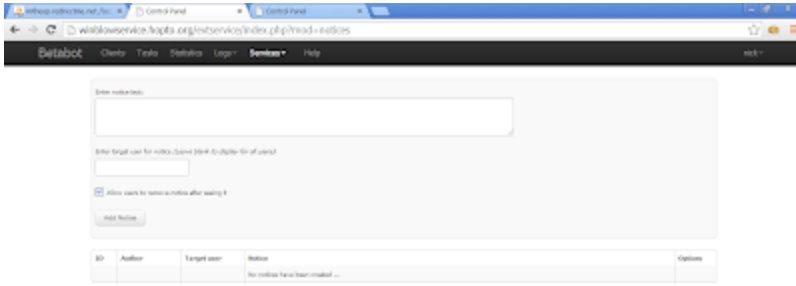
Tasks:

Total tasks: 2

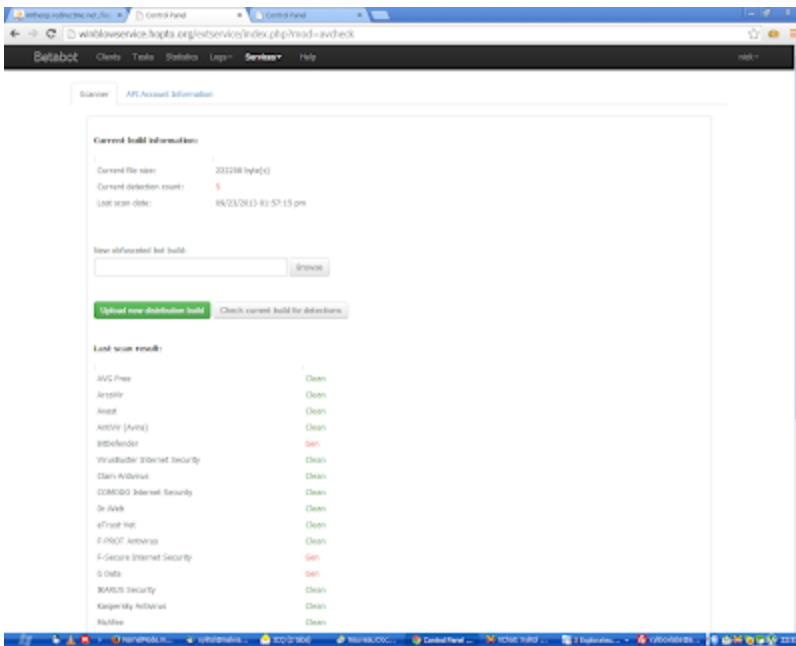
Filter: all tasks | Details of completed tasks | Suspend all active tasks | Export tasks from | Export tasks from CSV

Task Name	Type	Created	Executed / Miss / Failed	Status	Options
BotB operation	BotB operation	09/16/2013 02:26:35 am	4/3 / 286 / 16	Completed	View Task Info Details Edit Remove
BotB offline	BotB offline	09/16/2013 02:26:35 am	0/0 / 16 / 16	Suspended	View Task Info Details Edit Remove

Statistics:



AV Checker:



1.7.0.1:


```














1308 jabberid      : siricilly@limun.org
1309 topic         : AssisSense
1310 question_data : [16:57:35] siricilly: Can you please respond back, involving my issue with "Services and logs" tab
1311 [16:58:01] siricilly: I'm currently using latest jQuery
1312 [17:00:07] siricilly: I've added the geopip.csv via phpMyAdmin but it doesn't want it to load.
1313 The page loads but it's white and I did increase the limits on the maximum file size etc. so it could upload
1314 Thanks in advance.
1315 -siricilly
1316 creation_date : 1391629725
1317 num_views     : 0
1318 user_ip       : 5.254.112.2
1319 reserved0    : 0
1320 -----
1321 id            : 122
1322 jabberid     : firef4rt@default.cs
1323 topic        : Problems with connect bots
1324 question_data : Hi,
1325 have been got my files, installed and looks good. After installation a cracked bin file - nothing happened. Testtest with disabled A
1326 creation_date : 1391632652
1327 num_views     : 0
1328 user_ip       : 46.115.39.87
1329 reserved0    : 0
1330 -----
1331 id            : 123
1332 jabberid     : gh87893@exploit.im
1333 topic         : Received wrong update from you
1334 question_data : A few days ago I purchased the upgrade from 1.0.2.5 to 1.7.0.1
1335 When running update.php it states that the update is for 1.5+ to 1.7.0.1 and I am getting a bunch of mysql errors.
1336 Please contact me on jabber when you have a moment.
1337 Thanks!
1338 GeorgeH
1339 creation_date : 1391760175
1340 num_views     : 0
1341 user_ip       : 116.231.117.117
1342 reserved0    : 0
1343 -----
1344 id            : 124
1345 jabberid     : volay@im.asins.org
1346 topic         : Update
1347 question_data : Hello,
1348 Can i get latest update for BetaBot.
1349 In volay from HF.
1350 creation_date : 1391788941
1351 num_views     : 0
1352 user_ip       : 88.227.146.231
1353 reserved0    : 0
1354 -----
1355 id            : 125
1356 jabberid     : BETASELL@EXPLOIT.IM
1357 topic         : I want to buy this program

```

Site structure:

 b	01/02/2014 17:33	Dossier de fichiers	
 dist	01/02/2014 17:34	Dossier de fichiers	
 docs-assets	01/02/2014 17:34	Dossier de fichiers	
 fonts	01/02/2014 17:34	Dossier de fichiers	
 img	01/02/2014 17:34	Dossier de fichiers	
 js	01/02/2014 17:34	Dossier de fichiers	
 less	01/02/2014 17:34	Dossier de fichiers	
 pma2	01/02/2014 17:34	Dossier de fichiers	
 buy.php	05/12/2013 21:07	Fichier PHP	5 Ko
 contact.php	20/01/2014 03:48	Fichier PHP	8 Ko
 dbi.php	05/12/2013 02:27	Fichier PHP	3 Ko
 index.php	20/01/2014 03:48	Fichier PHP	10 Ko
 question.php	05/12/2013 02:09	Fichier PHP	4 Ko
 screenshots.php	05/12/2013 02:09	Fichier PHP	5 Ko
 site.php	05/12/2013 02:09	Fichier PHP	10 Ko
 updates.php	20/01/2014 03:48	Fichier PHP	15 Ko
 viewquestions.php	05/12/2013 02:09	Fichier PHP	7 Ko

Some clients kits:

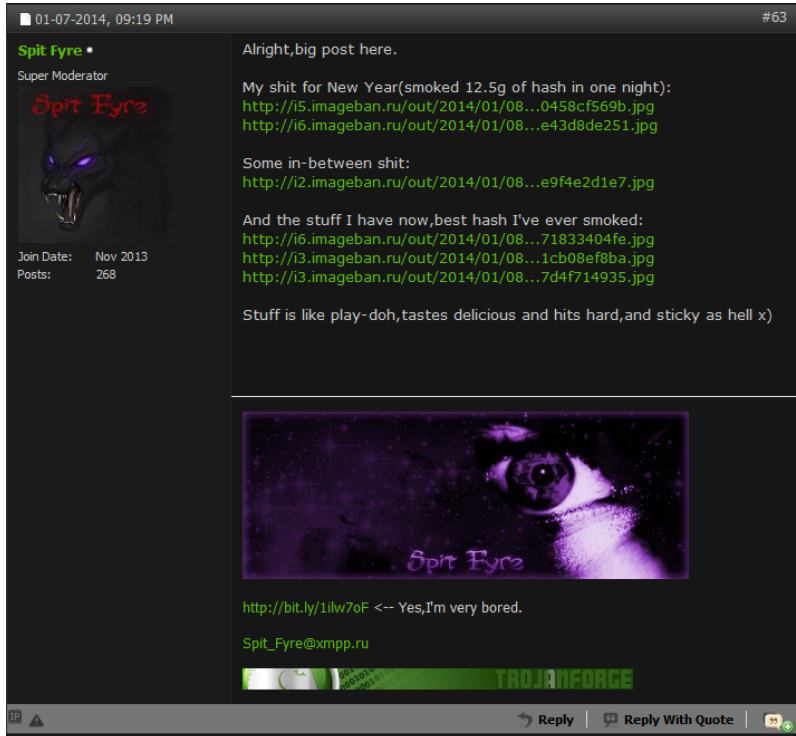
 2335ftbt 1.7.rar	11/05/2014 19:40	Archive WinRAR	5 946 Ko
 ahmedxo 1.7.rar	17/03/2014 12:38	Archive WinRAR	5 945 Ko
 bd 1.7.rar	19/04/2014 15:38	Archive WinRAR	5 943 Ko
 bitman 1.7.rar	28/02/2014 18:06	Archive WinRAR	5 945 Ko
 Blue Shark.rar	19/04/2014 15:38	Archive WinRAR	5 945 Ko
 changeme.rar	19/04/2014 15:37	Archive WinRAR	5 944 Ko
 Honey Singh 1.7.rar	14/03/2014 13:52	Archive WinRAR	5 947 Ko
 jamey 1.6.rar	14/01/2014 13:52	Archive WinRAR	4 015 Ko
 ninja12345 1.7.rar	11/04/2014 14:35	Archive WinRAR	5 946 Ko
 ofc 1.7.rar	11/04/2014 14:32	Archive WinRAR	5 943 Ko
 rebuild_4_10_2014_id21207.zip	11/04/2014 14:43	Archive WinRAR ZIP	135 Ko
 rebuild_4_17_2014_id1678.rar	19/04/2014 15:44	Archive WinRAR	136 Ko
 s1r1c1ly.rar	07/05/2014 00:54	Archive WinRAR	3 543 Ko

Finally some people got busted using these informations..

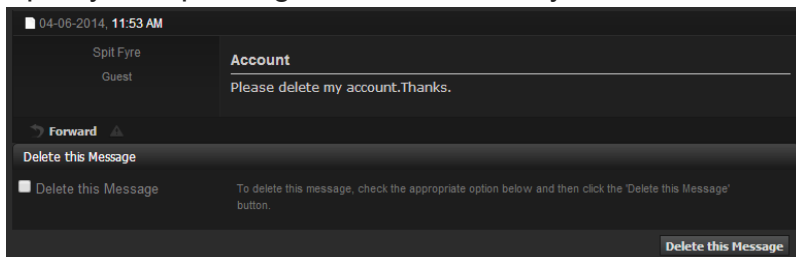
If you want an example.. 'Spit Fyre' ex super moderator at Trojanforge who reside in the

same country as me.

If you wonder why he disappeared you know why now.



Spit Fyre requesting an admin of Hackyard to delete his account after he got cops at door:



Some of his domains:

- dns: 1 » ip: 124.248.205.104 - adress: DARKNESS.SU
 - dns: 1 » ip: 124.248.205.104 - adress: WEED.SU
 - dns: 1 » ip: 124.248.205.104 - adress: MEZIAMUSSUCEMAQUEUE.SU
 - dns: 1 » ip: 124.248.205.104 - adress: UMBXD15896.SU
 - dns: 1 » ip: 124.248.205.135 - adress: STYXB1TCH35.SU
 - dns: 1 » ip: 124.248.205.135 - adress: J1NXFYR3.SU
- Anyway it's useless to talk about him and others betabot clients who had visits, the current status of betabot is stalled now and someone even made a builder for the 1.7.0.1 version. Betabot was a creative malware, plagued by bugs though.