

Betabot retrospective

Archived: 2026-04-05 14:23:52 UTC

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 dashboard interface. On the left, there are sections for 'General statistics' and 'Connections'. The main area is titled 'Search Bots' and contains a table with columns: Machine ID, IP, Location, Operating System, Install date, AntiVirus, and Killed. The table lists various bots with their respective details. Below the table, there are sections for 'Components' and 'Logs'.

Machine ID	IP	Location	Operating System	Install date	AntiVirus	Killed
C8C49C89F2381A23281C3FC04		United States (US)	Windows XP SP3 (x86)	09/22/2013 04:13:15 pm	N/A	0
D9F64A1D564E2C45AC3C3A1C2C4049		France (FR)	Windows 7 SP1 (x86)	09/14/2013 09:51:57 am	N/A	0
F0318F50F0D0043A8849C450A2C2A		France (FR)	Windows 7 SP1 (x64)	09/04/2013 04:41:21 am	Avira	0
ACCF37D304E024A1A70D4F3917076		France (FR)	Windows 7 SP1 (x86)	09/07/2013 05:05:26 pm	N/A	0
E2A8EA232C774939E05A5995C0297		United States (US)	Windows 7 SP1 (x64)	09/07/2013 11:58:37 am	N/A	0
57474DFF9984797499608A8E9F		France (FR)	Windows 7 SP1 (x86)	09/07/2013 08:43:59 am	Avira	0
F8BFCF4E5A3474E02CF6A11801F4F		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:43:59 am	Avast	0
0A8F02078276904478CC3C03F48		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:43:59 am	ESET	0
06281A026767033AC9F9364EE008		France (FR)	Windows Vista SP2 (x64)	09/07/2013 08:43:59 am	N/A	0
8528CA7041861740C7C0A06902		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:42:13 am	Avira	0
C0630A3A1C0648B3F70577A8FA4		France (FR)	Windows 7 (x86)	09/07/2013 08:41:36 am	N/A	0
9620C08EA2D04A848F823C74164F		France (FR)	Windows 7 SP1 (x86)	09/07/2013 08:41:30 am	McAfee	0
24F1D5870240F978F4D9F9576F46		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:40:09 am	N/A	0
F4028B0C0F6948A1773063384E199		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:40:04 am	N/A	0
A3DA43E7C028A4F932139478D7E3D		France (FR)	Windows 7 SP1 (x86)	09/07/2013 08:39:34 am	Norton	0
C32648D02592A796C0C87781317C03		France (FR)	Windows 7 SP1 (x86)	09/07/2013 08:39:34 am	Avast	0
DDC34C29825C484953A8D2A2A5A		United States (US)	Windows 7 (x64)	09/07/2013 08:36:27 am	N/A	0
BAA4A5F8483C4D45574F9F7958153		France (FR)	Windows 7 SP1 (x86)	09/07/2013 08:36:24 am	Norton	0
06B8EED83868F83C0C1D07C0A02		France (FR)	Windows 7 SP1 (x64)	09/07/2013 08:36:03 am	N/A	0
18507704B45C9C3C1C30636F6F		Ukraine (UA)	Windows 7 SP1 (x86)	09/04/2013 05:59:24 am	Avast	0

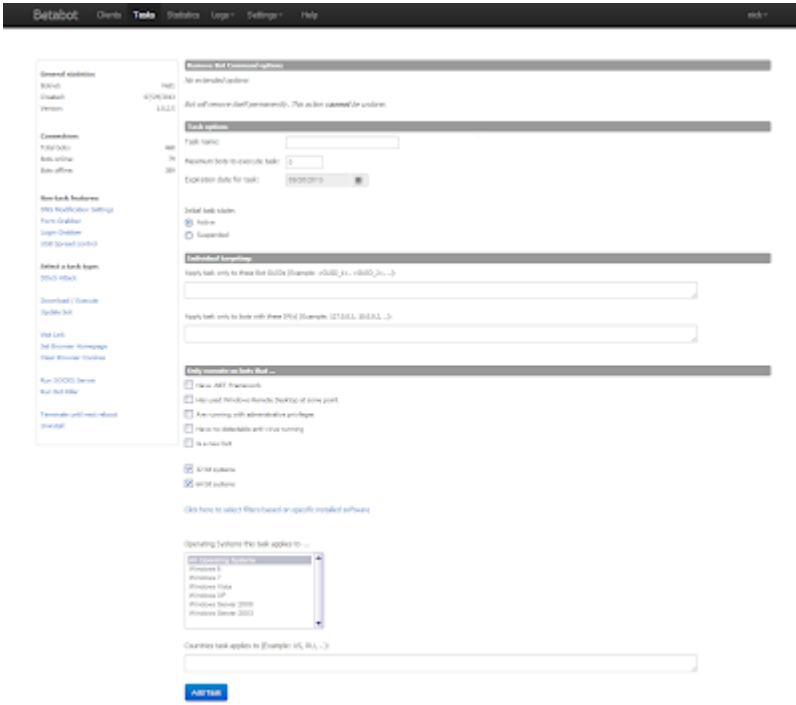
extended information:

The screenshot shows a window titled 'Extended information for' with a close button. It displays detailed information about a specific bot, including its status, GUID, source, install path, dates, and system details.

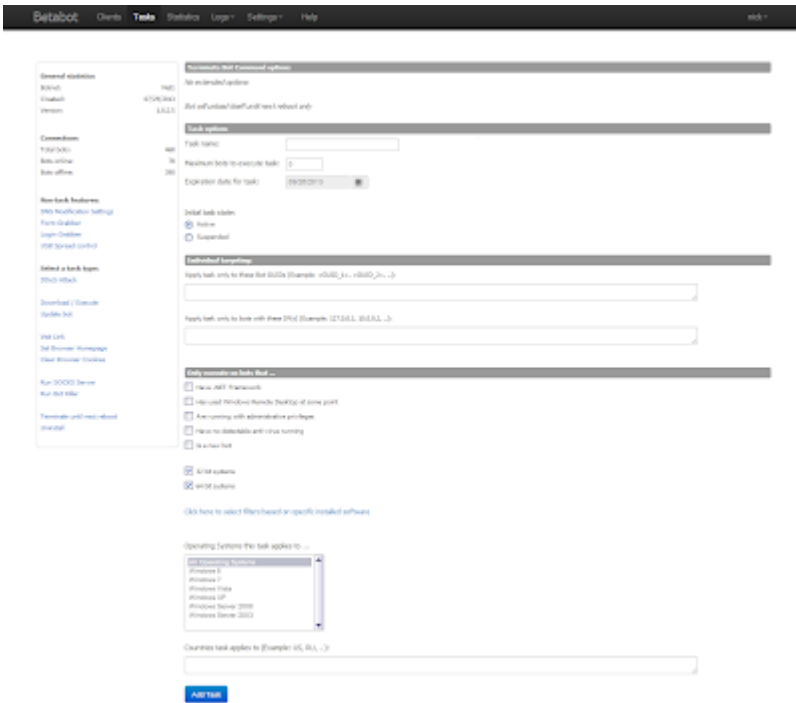
```

Status: Online
Bot GUID: 9CCF38332F127242989F29D746787E8
Source: Spam / Exploit Pack
Install Path: C:\ProgramData\Magic Services\0\dtidasndku.exe
Install Date: 09/22/2013 10:35:09 am
Last CheckIn: 09/23/2013 04:42:37 pm
Bot owned for: 1d 6h 7m 28s
Operating System: Windows 7 SP1 (x64)
Local Time: 04:41:43 pm
IP:
Country: France (FR)
SOCKS4 Port: N/A
Bots killed since installed: 0
Default Browser: torch.exe
Login Username: patisa-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
  
```

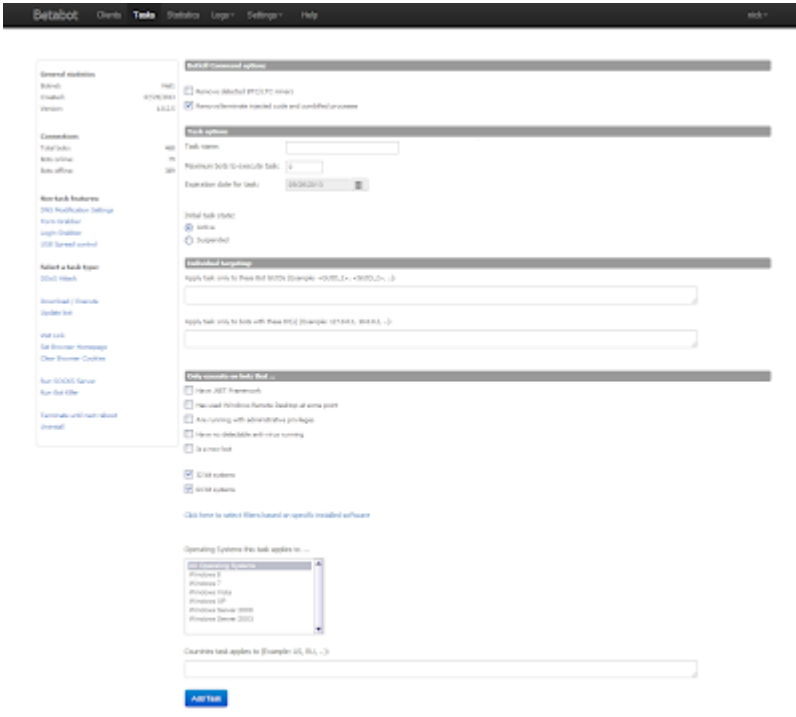
Search options:



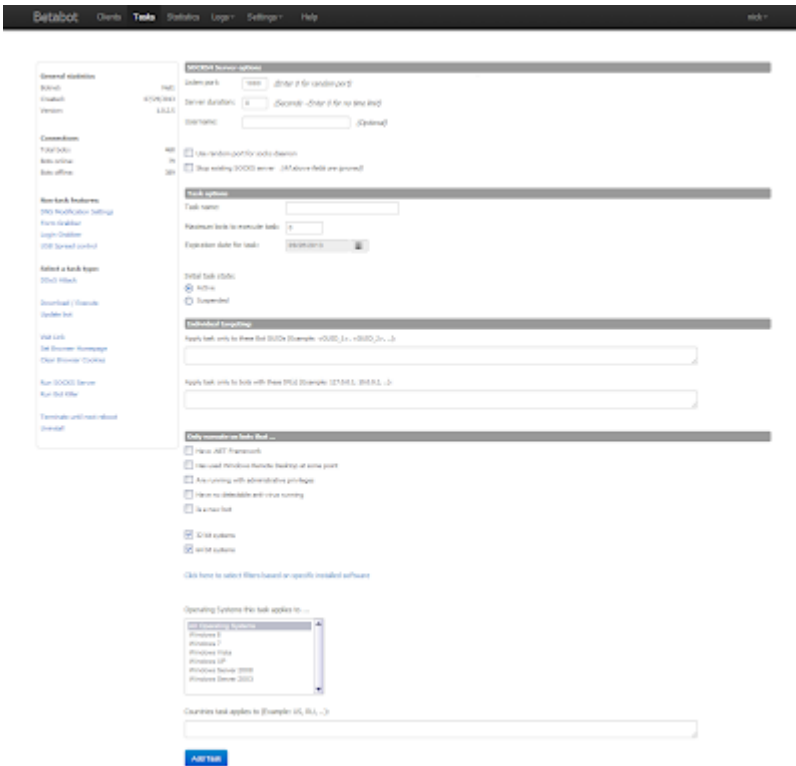
Terminate bot till next reboot:



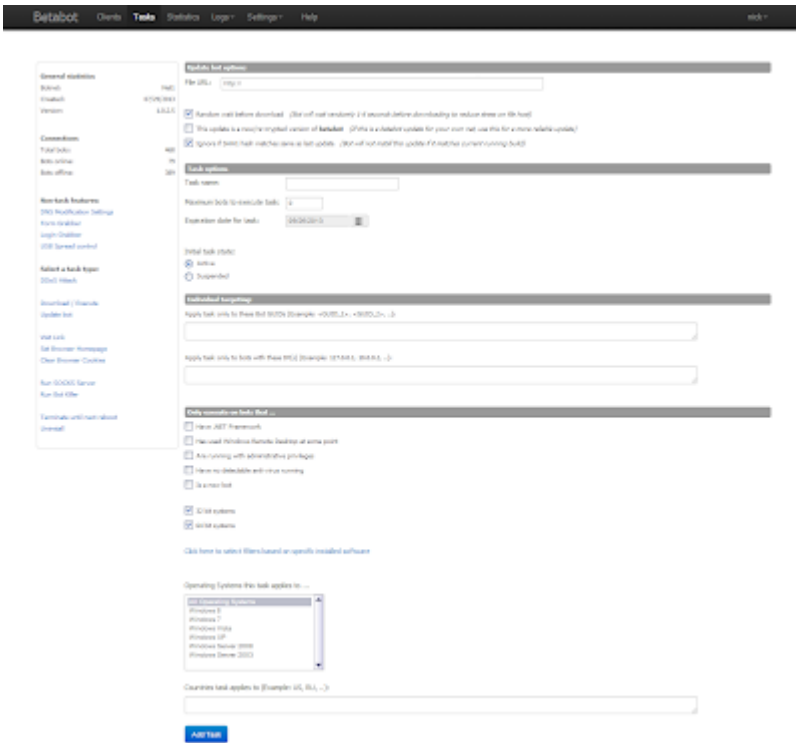
Botkill:



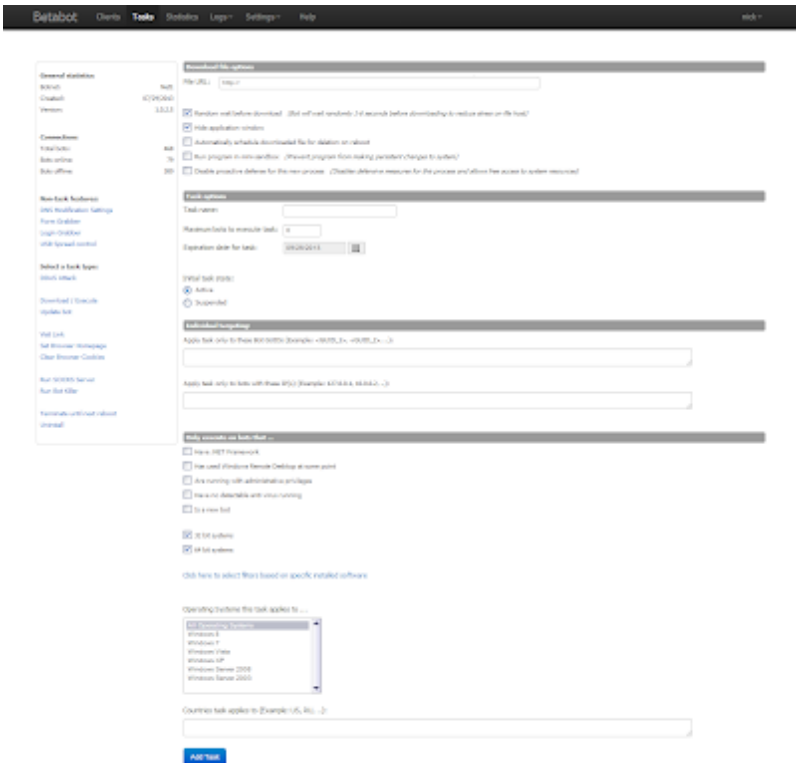
Socks4:



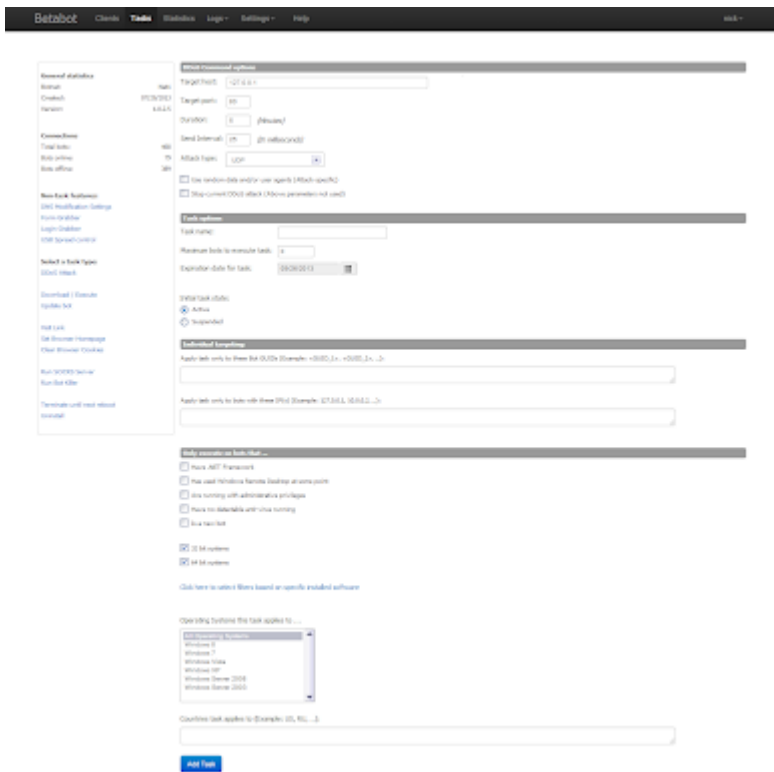
Set browser homepage:



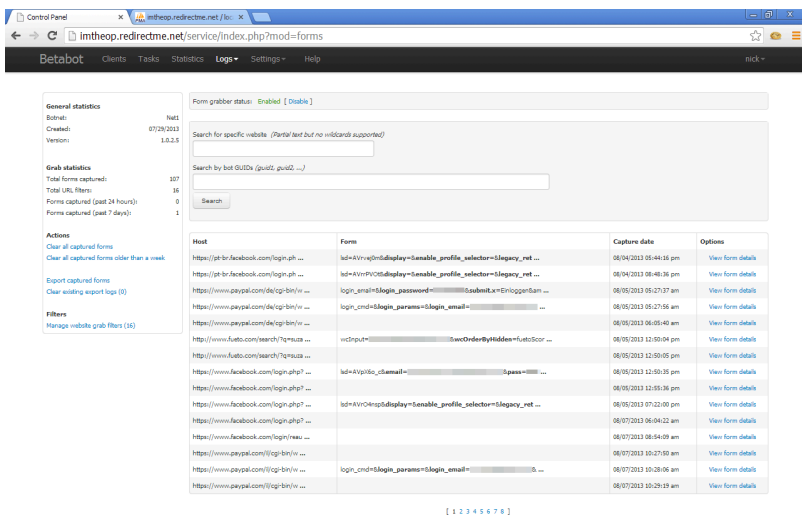
Download file option:



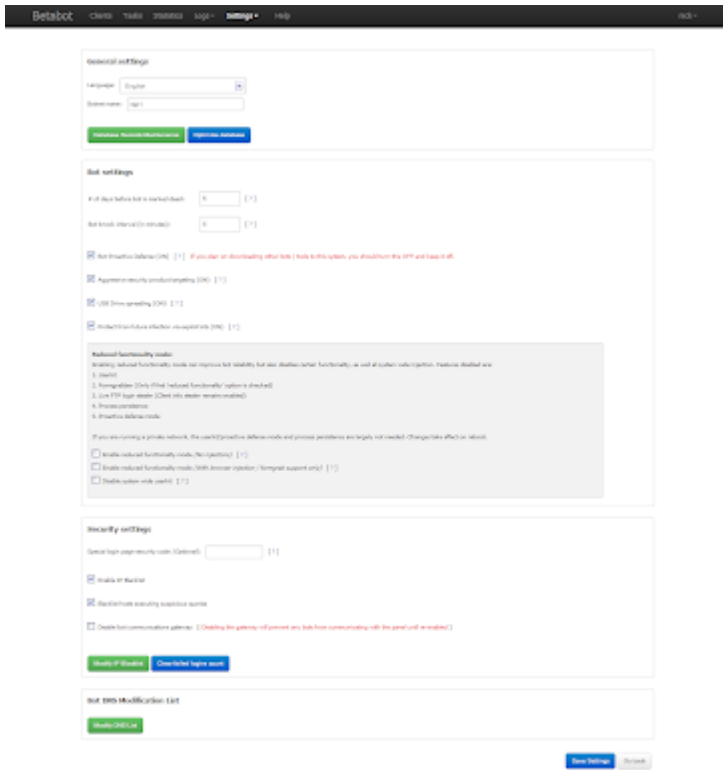
DDoS cmd option:



Formgrabber logs:



logins:



IP blacklist:



List of dns recod to modify:

List of DNS records to modify

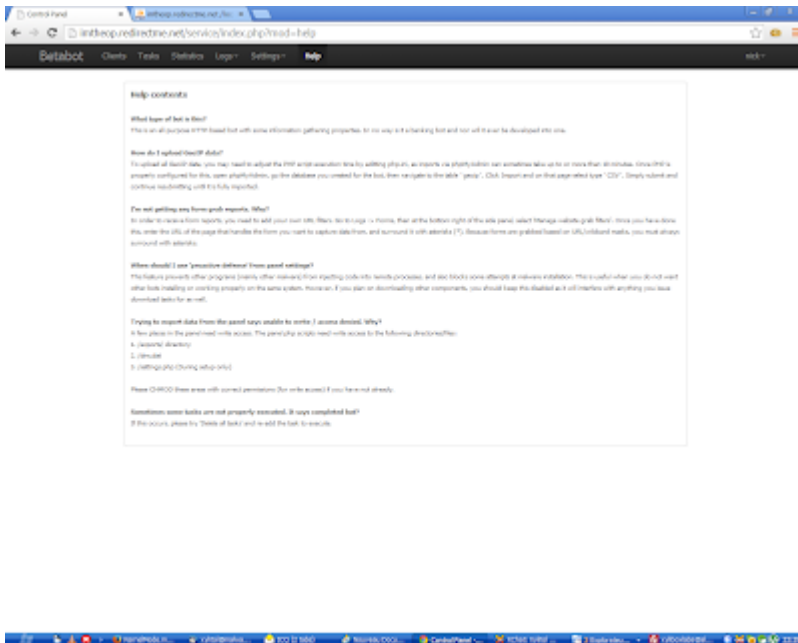
Enter domain entries in this format:

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

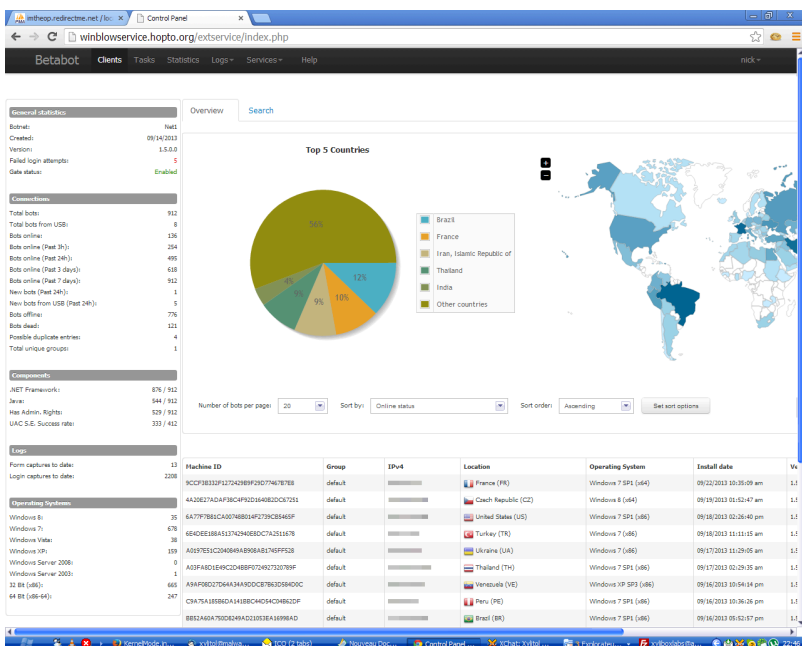
And so on. Wildcards are accepted. Failure to abide precisely by this format could result in unknown errors. Maximum of **1024** entries are allowed.

Save list Close

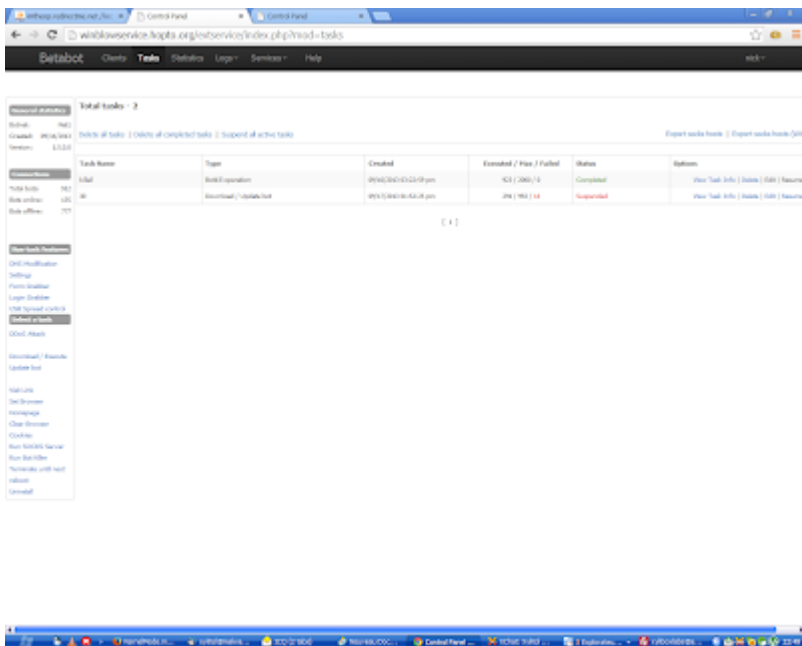
Help:



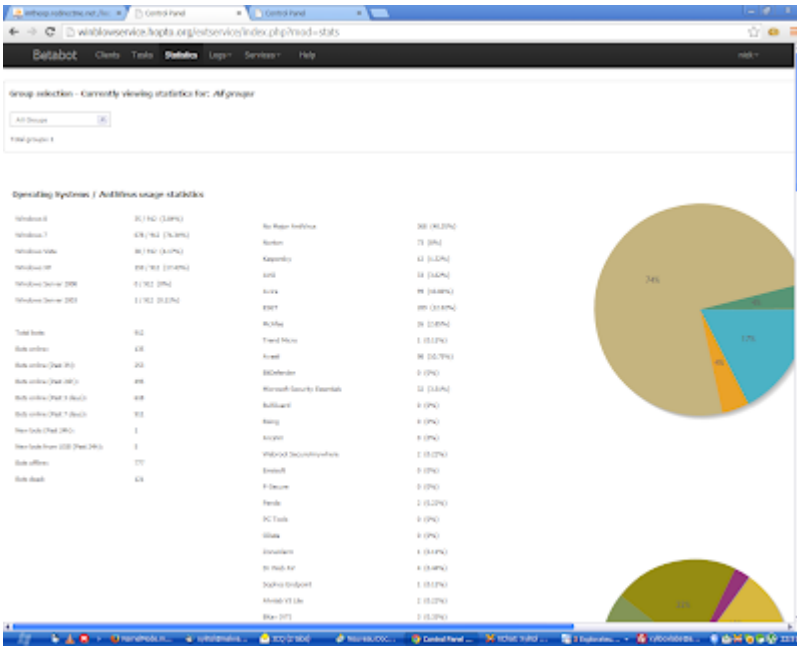
1.5.0.0:



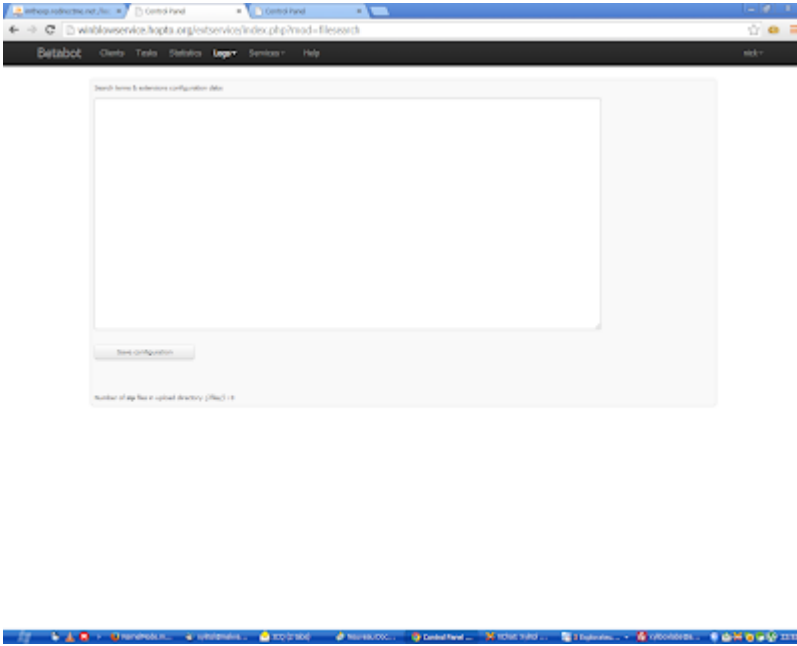
Tasks:



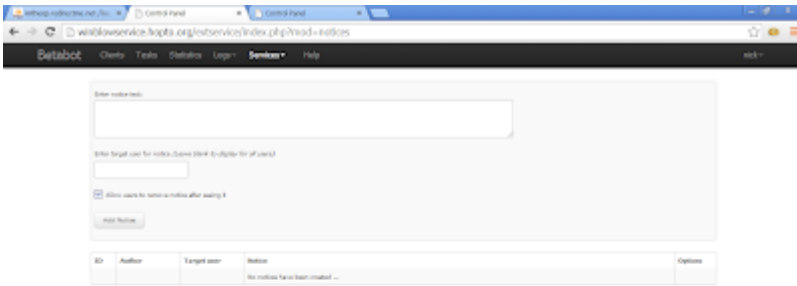
Statistics:



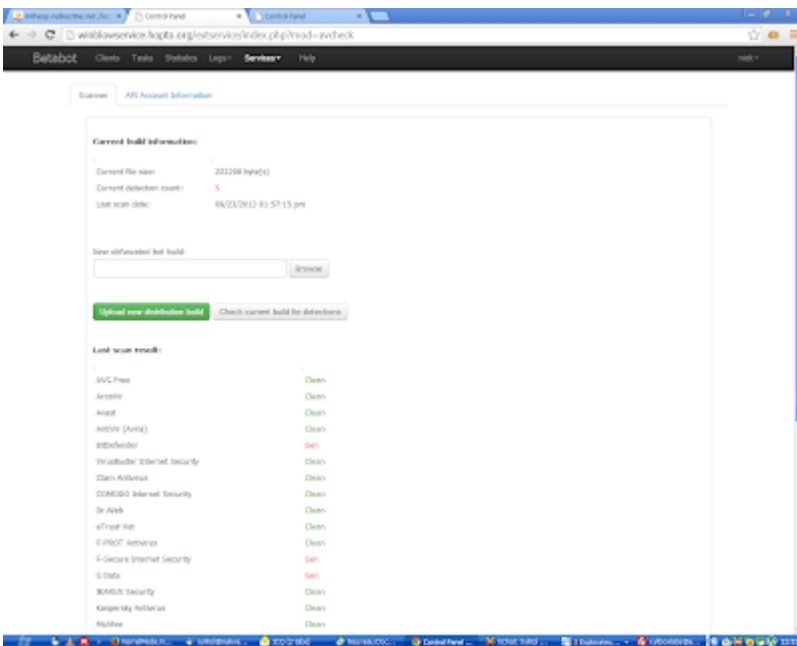
Files:



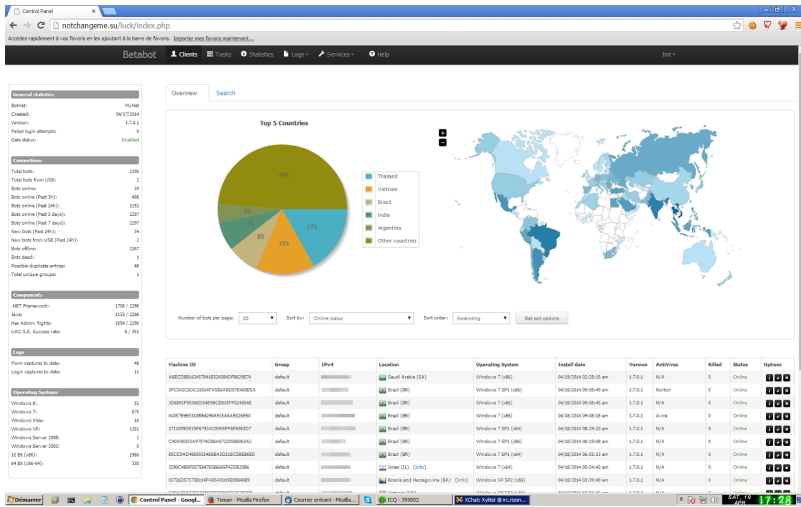
Users notice:



AV Checker:



1.7.0.1:



The botmaster was running a support site at the url betabot.ru that i've monitored since... i don't know almost the beginning till the end.

I've really collected a lot of datas and was constantly flagging new C&C urls even before they was active.

home	01/02/2014 17:33	Dossier de fichiers	
Neurevt clients build	11/05/2014 23:36	Dossier de fichiers	
usr	14/02/2014 13:21	Dossier de fichiers	
var	14/02/2014 13:26	Dossier de fichiers	
Beta Issues.mp4	27/01/2014 12:50	VLC media file (.mp4)	21 616 Ko
betabot_dump_big_7z	21/05/2014 13:49	Archive WinRAR	1 078 762 Ko
betabot.ru.7z	21/05/2014 13:42	Archive WinRAR	43 675 Ko
crap.txt	01/02/2014 15:26	Document texte	1 Ko
decode.php	29/12/2013 14:02	Fichier PHP	2 Ko
decode.txt	13/02/2014 20:35	Document texte	53 Ko
forum.tar.gz	01/02/2014 17:01	Archive WinRAR	1 107 946 Ko
hosts.txt	10/12/2013 20:22	Document texte	1 Ko
localhost.sql	21/05/2014 12:17	Fichier SQL	2 041 Ko
myquestions.sql	13/02/2014 20:34	Fichier SQL	70 Ko
nginx.conf.txt	10/12/2013 15:37	Document texte	3 Ko
nginx.txt	10/12/2013 15:36	Document texte	2 Ko
passwd.txt	10/12/2013 15:35	Document texte	1 Ko
Proof_of_payment.png	19/01/2014 23:25	Image PNG	15 Ko
viewquestions.php	05/12/2013 02:09	Fichier PHP	7 Ko
wtmp	14/01/2014 21:08	Fichier	67 Ko

Inquiries sent to the betabot team (before they started the support forum):

```














1308 jabberid      : s1r1c1ly@l1mun.org
1309 topic        : Assistance
1310 question_data : [16157:35] s1r1c1ly: Can you please respond back, involving my issue with "Services and logs" tab
1311 [16158:0] s1r1c1ly: I'm currently using latest jQuery
1312 [17100:0] s1r1c1ly: I've added the geoip.css 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 -s1r1c1ly
1316 creation_date : 1391629725
1317 num_views     : 0
1318 user_ip       : 5.254.112.2
1319 reserved0     : 0
1320 -----
1321 id            : 122
1322 jabberid      : f1ref4rt@default.rs
1323 topic        : Problems with connect bots
1324 question_data : Hi,
1325 have been got my files, installed and looks good. After installation a crashed bin file - nothing happened. Tested 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.in
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      : volvy@im-apsinc.org
1346 topic        : Update
1347 question_data : Hello,
1348 Can I get latest update for BetaBot.
1349 Im volvy from HF.
1350 creation_date : 1391788841
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

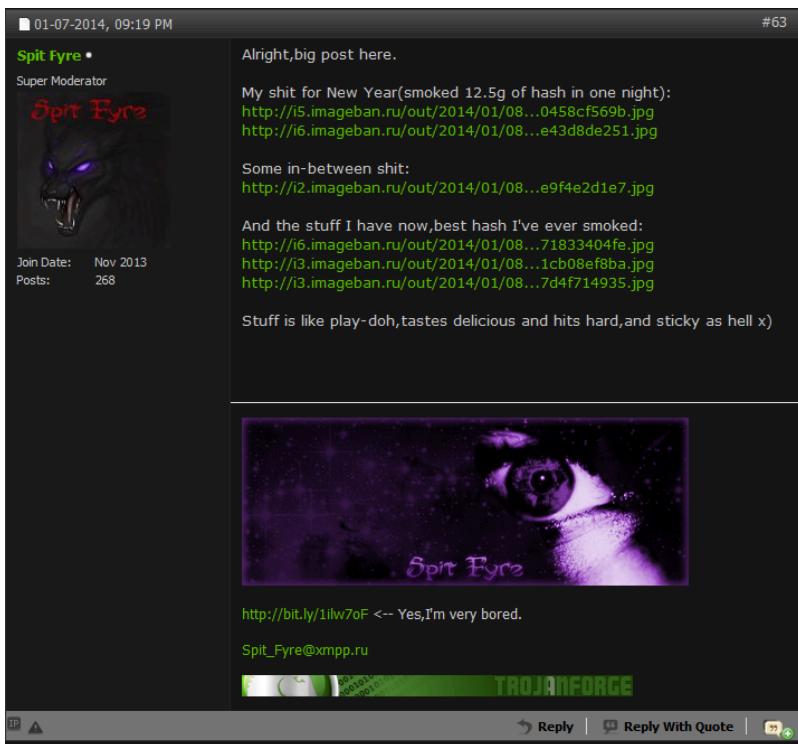
Some clients kits:

 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

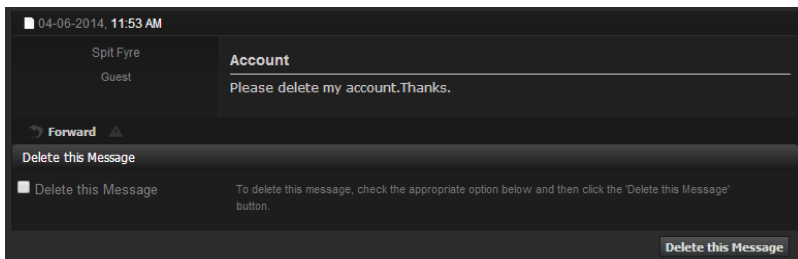
Finally some people got busted using these informations..

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.