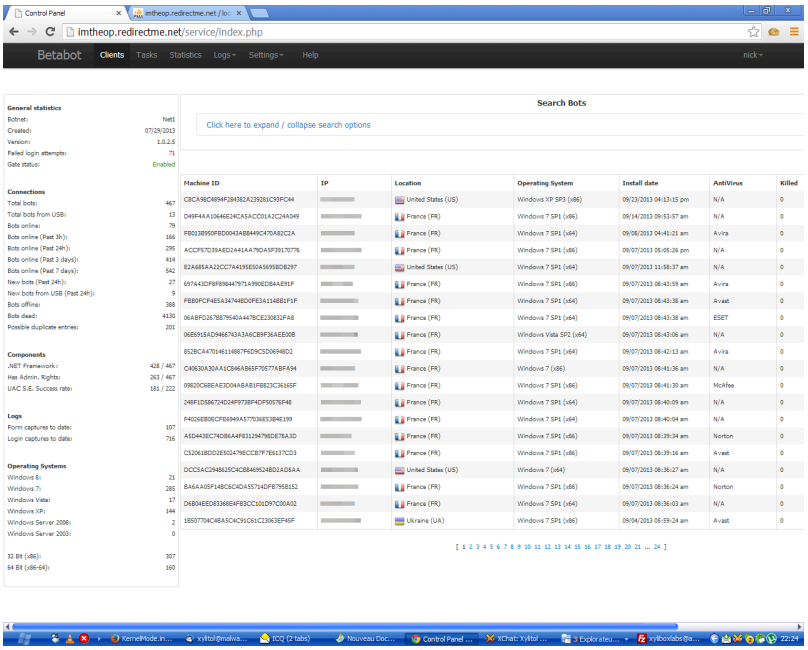
Betabot retrospective

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

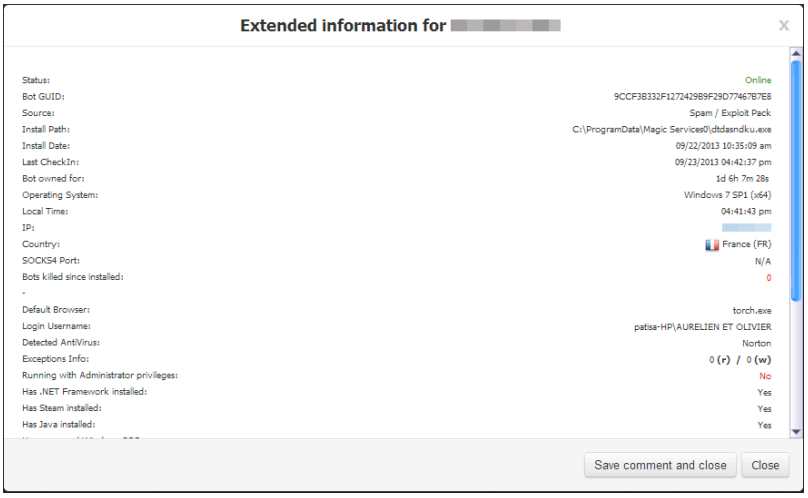
Some of you know Betabot.. if you don't: http://www.ic3.gov/media/2013/130918.aspx

1.0.2.5 panel:

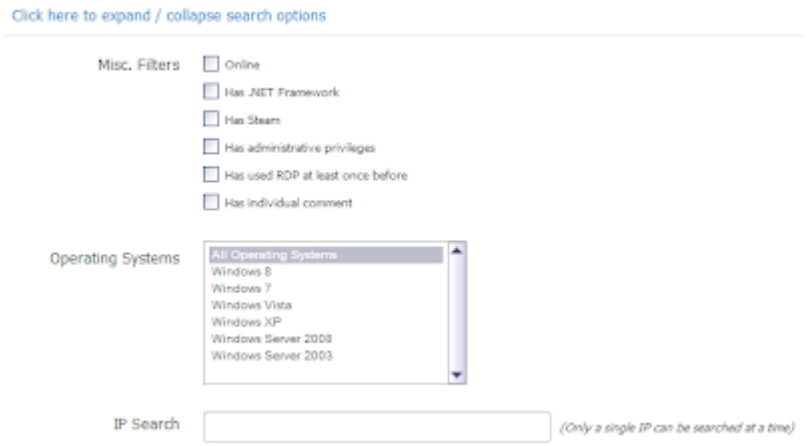
Dashboard:



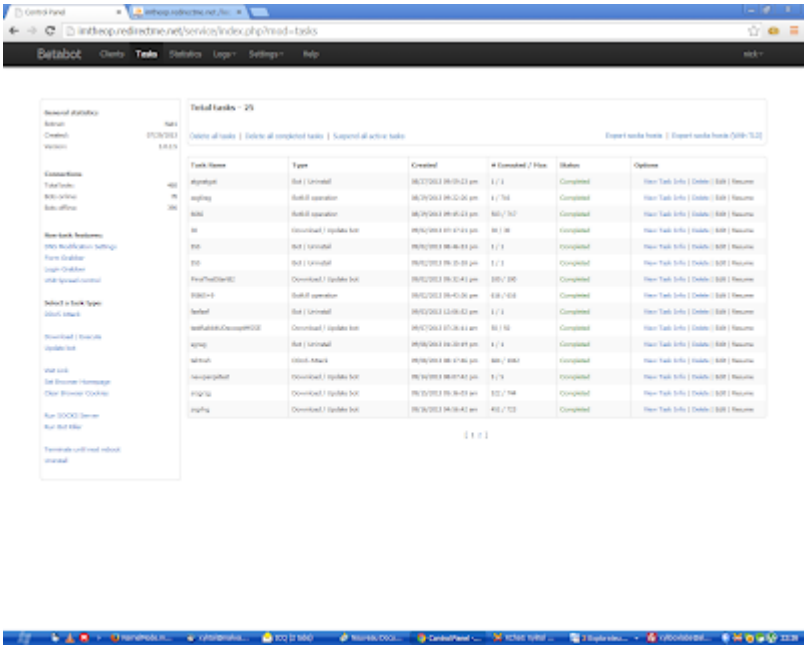
extended information:



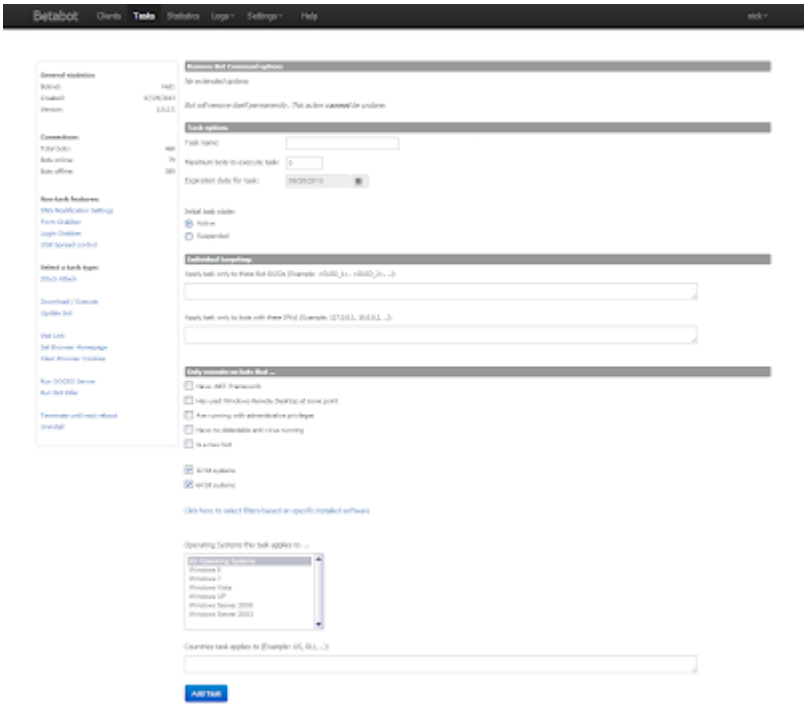
Search options:



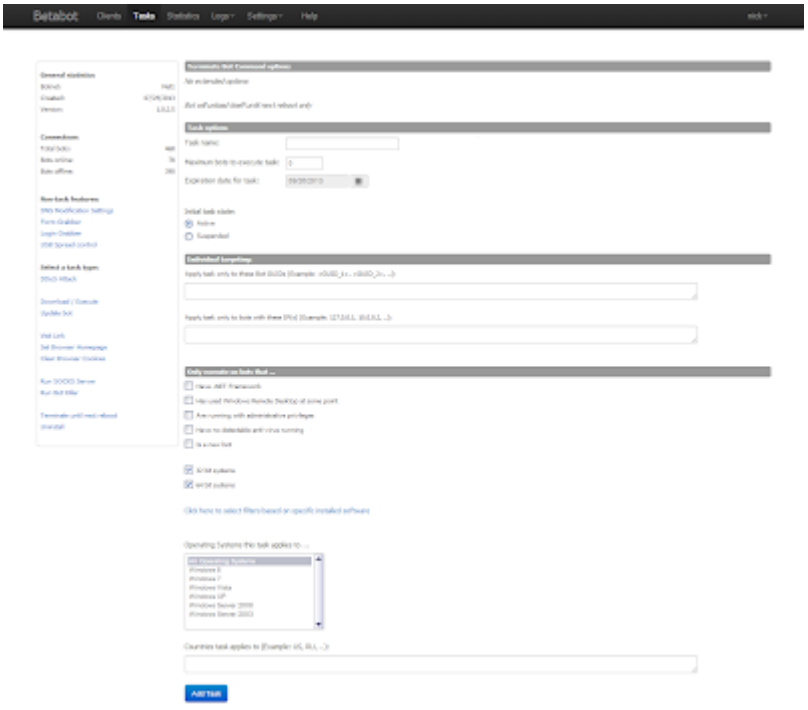
Tasks:



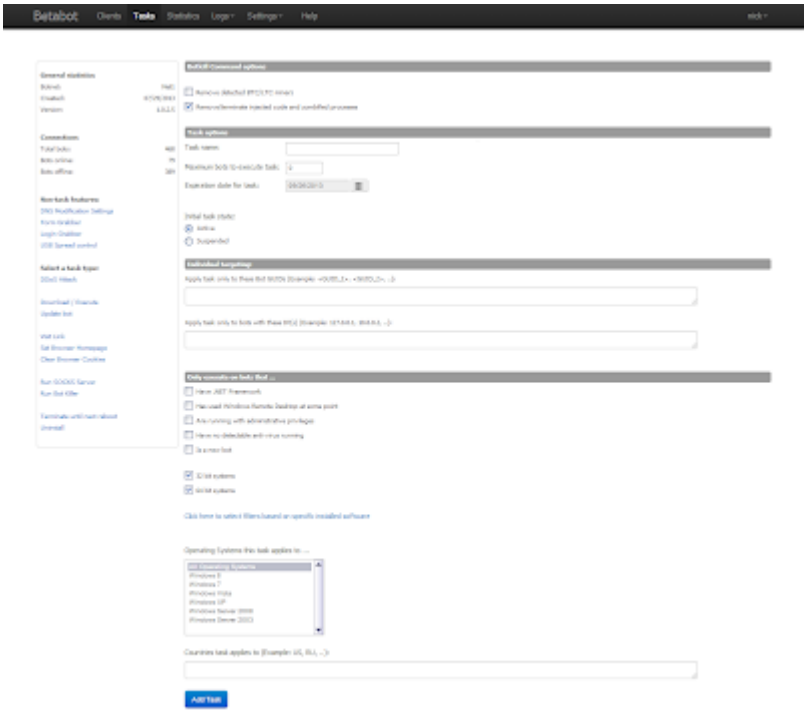
Remove bot:



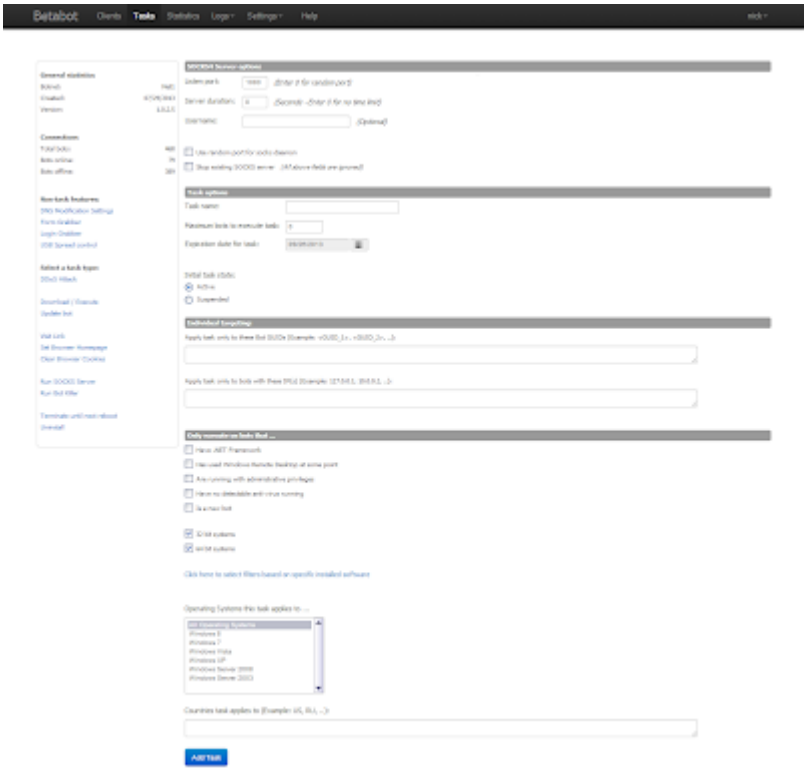
Terminate bot till next reboot:



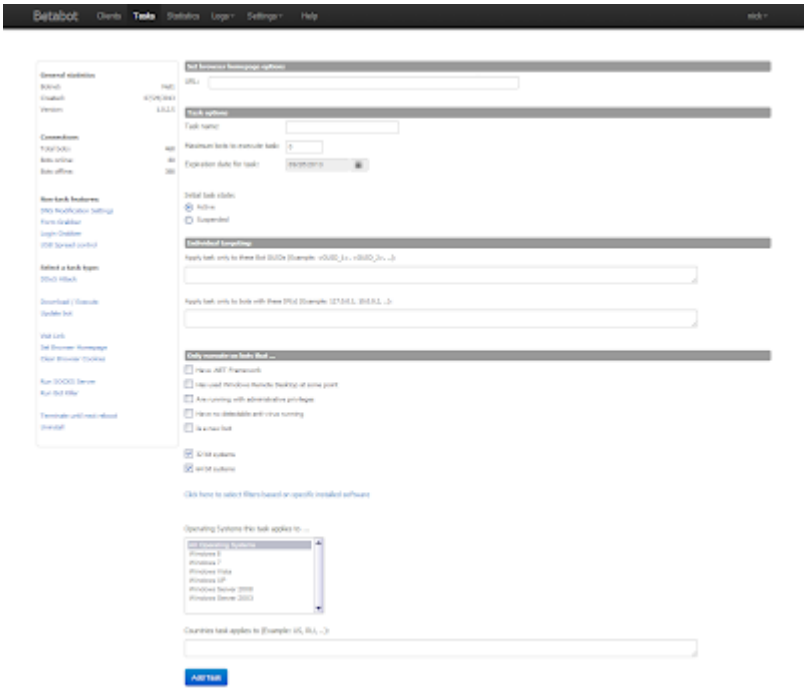
Botkill:



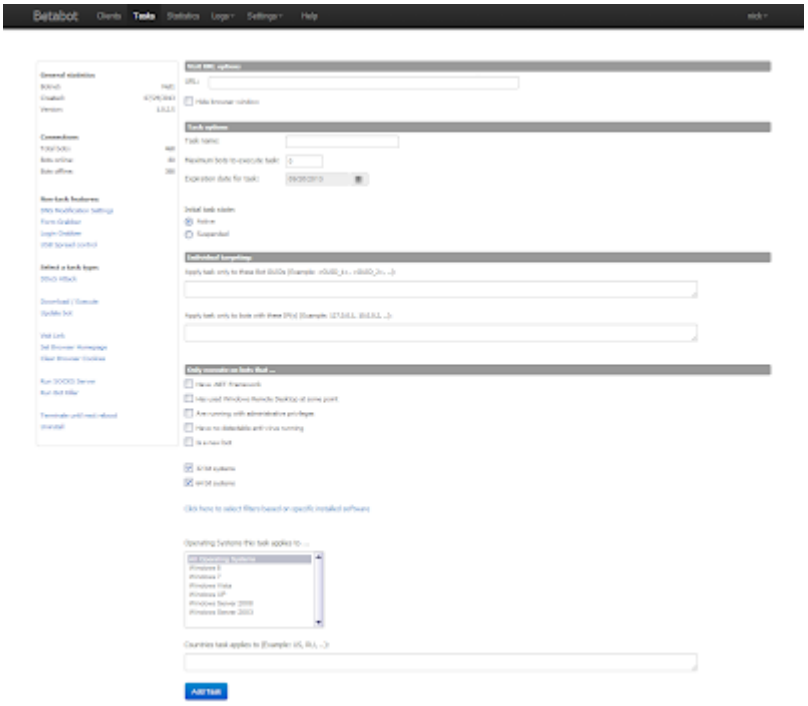
Socks4:



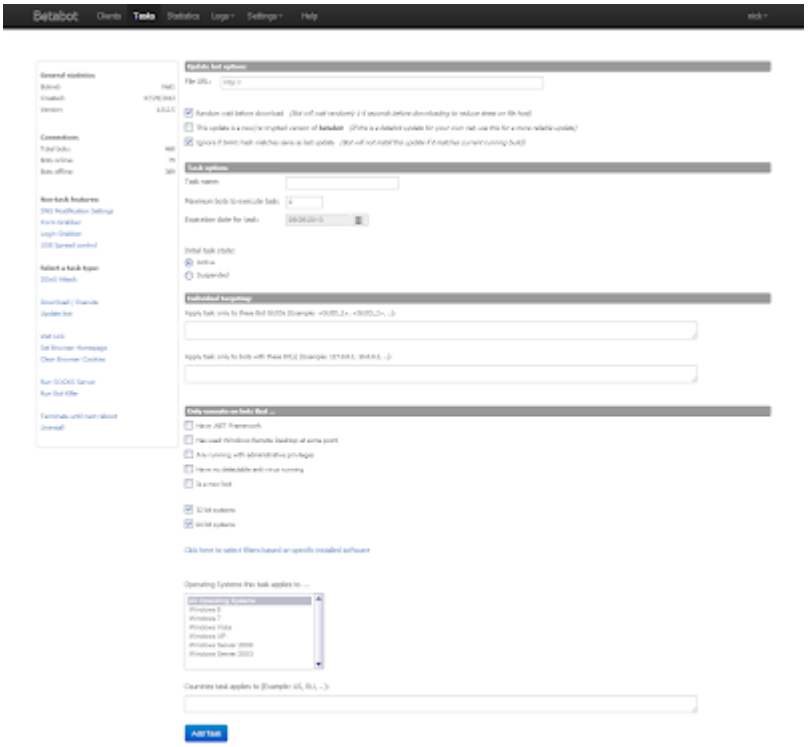
Set browser homepage:



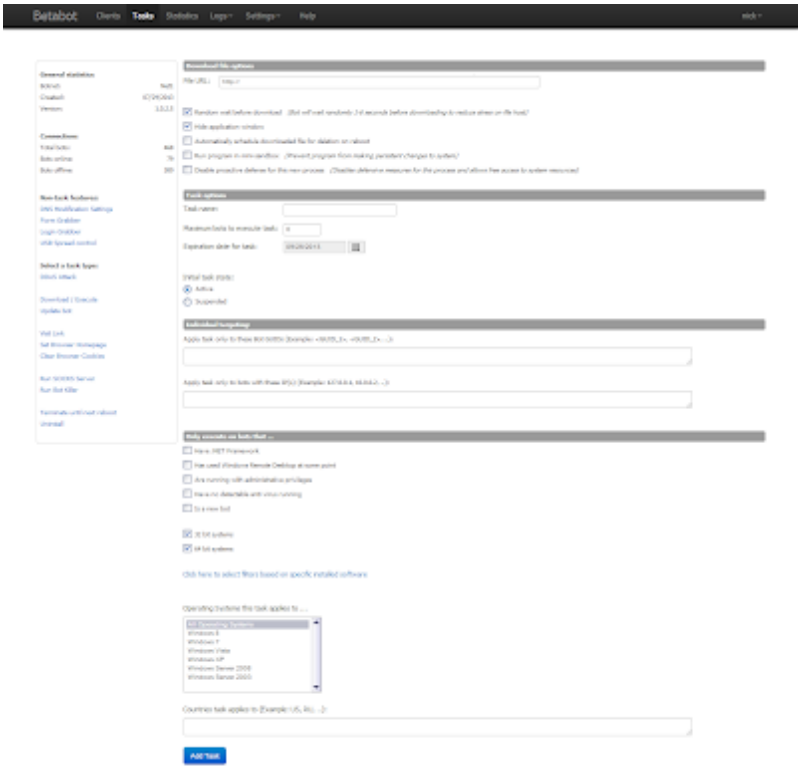
Visit URL option:



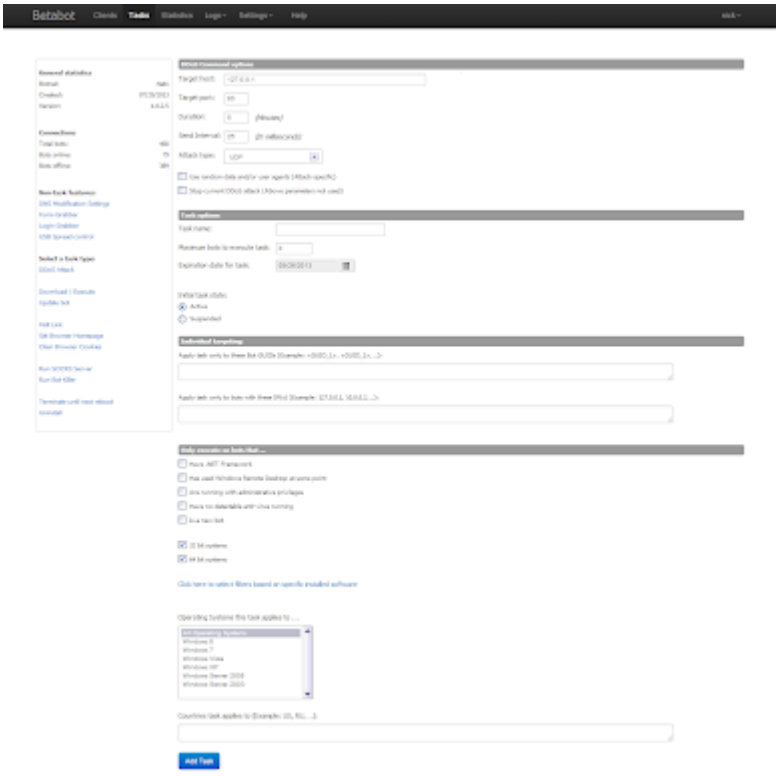
Update bot option:



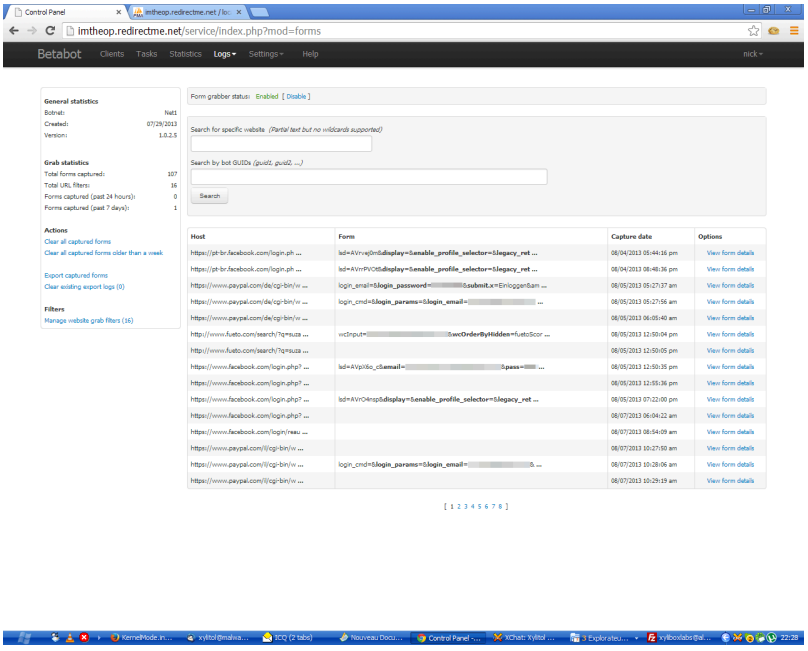
Download file option:



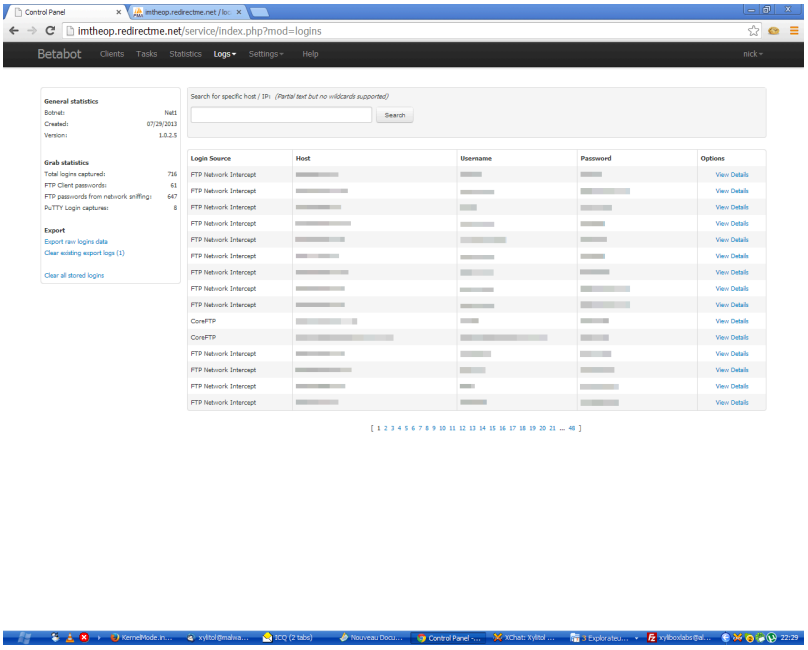
DDoS cmd option:



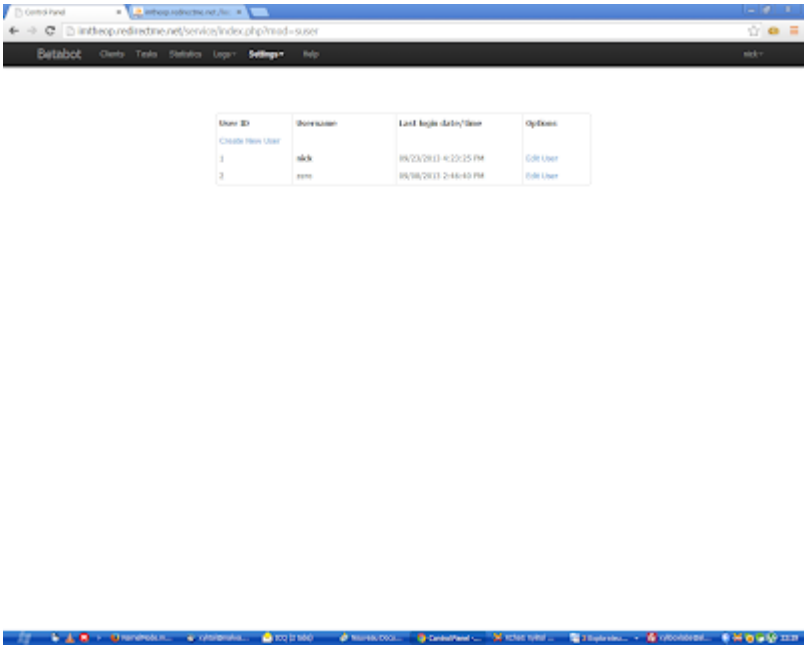
Formgrabber logs:



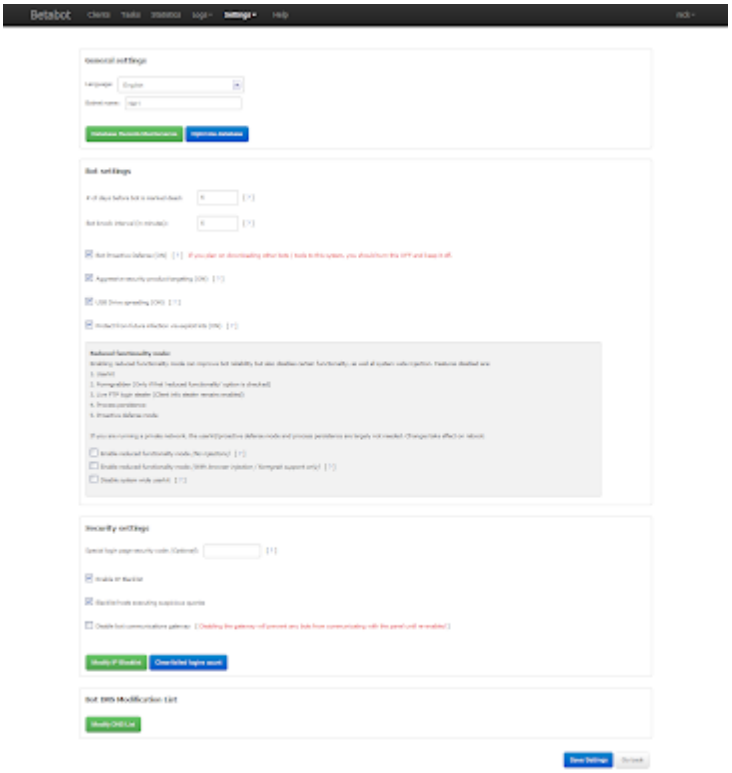
logins:



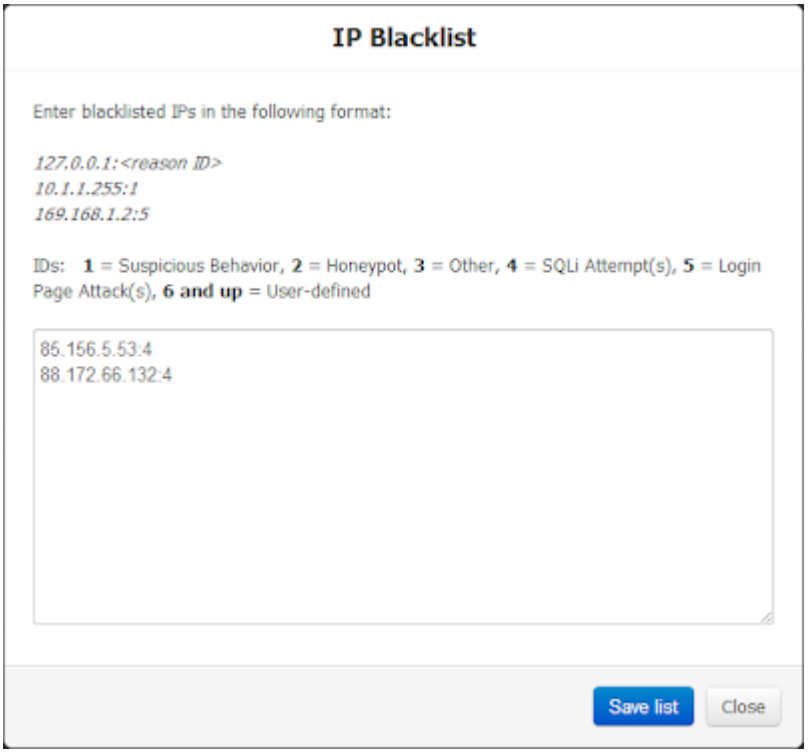
users:



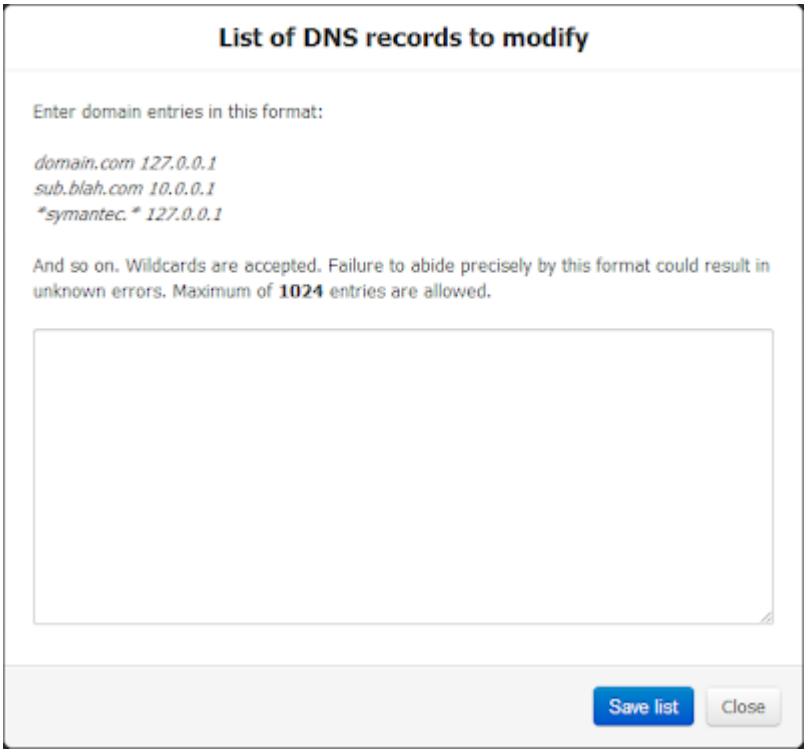
Settings:



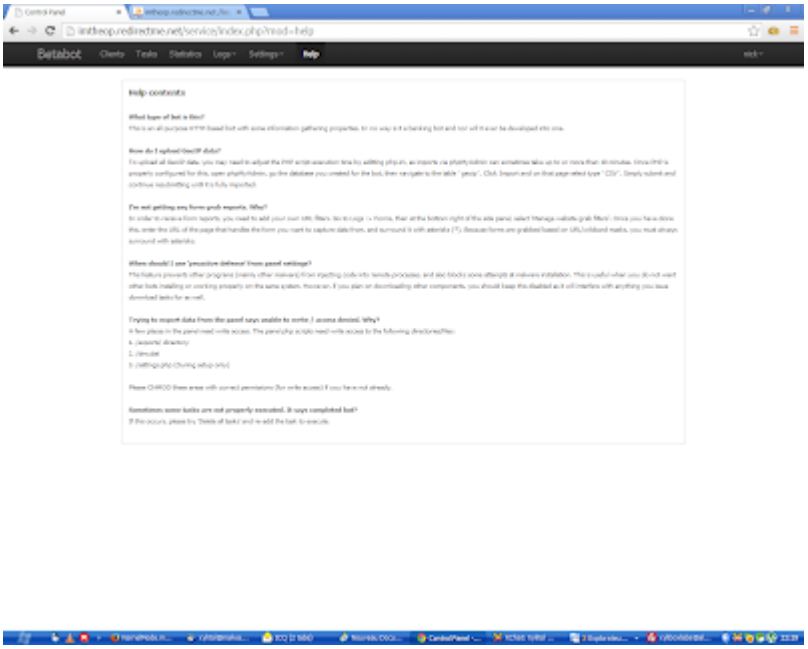
IP blacklist:



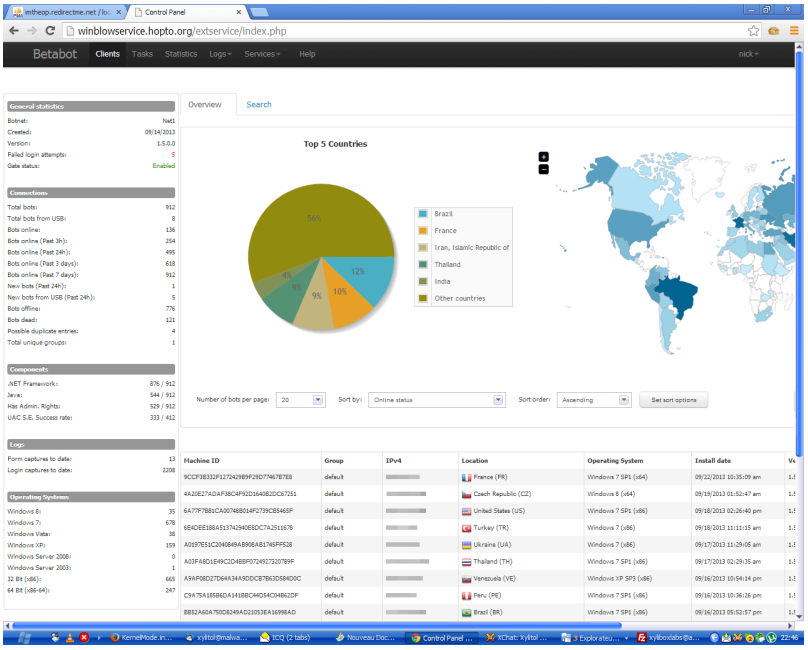
List of dns recod to modify:


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

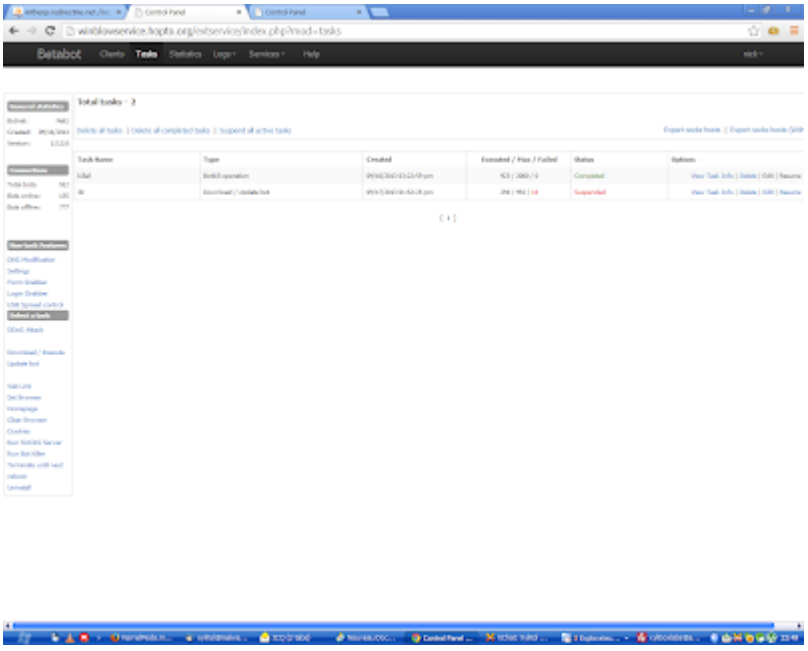
Help:


Betabot
Help contents

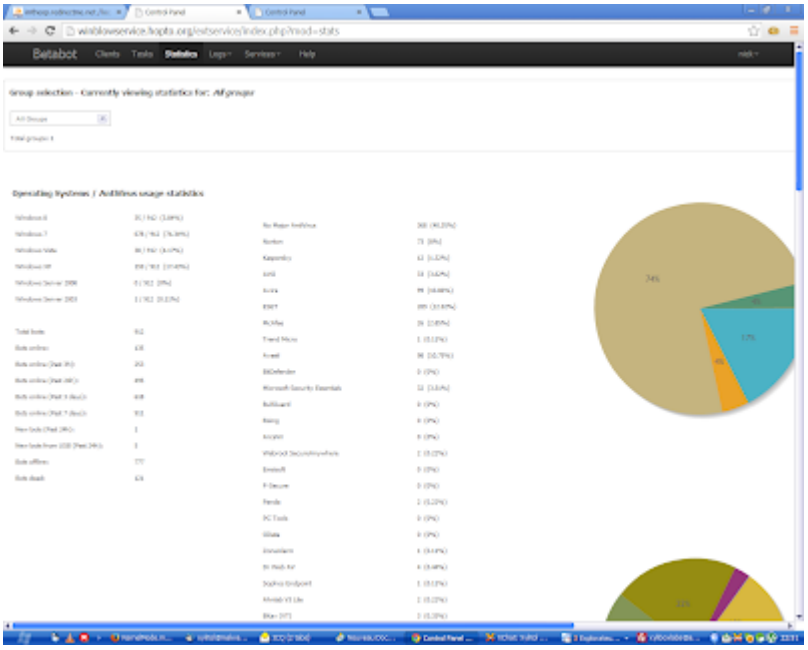
1.5.0.0:



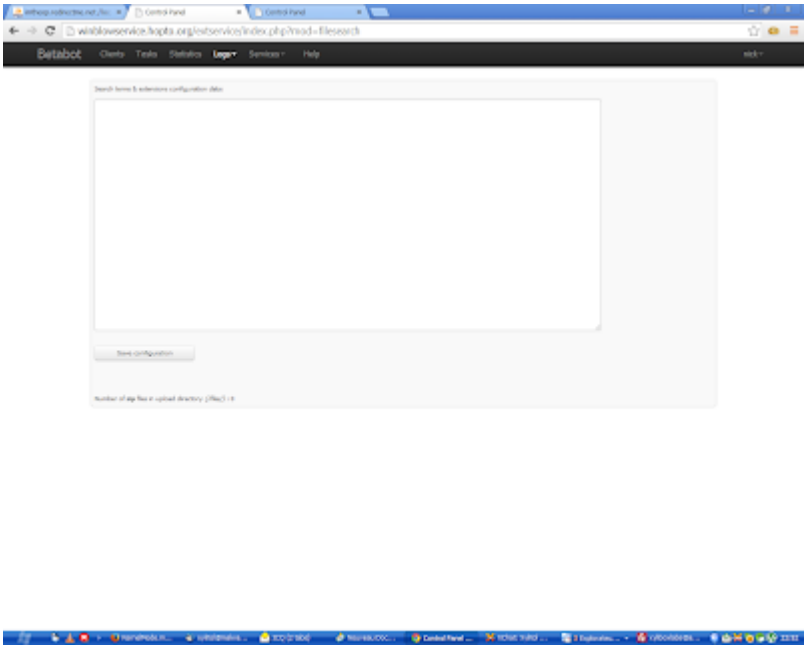
Tasks:



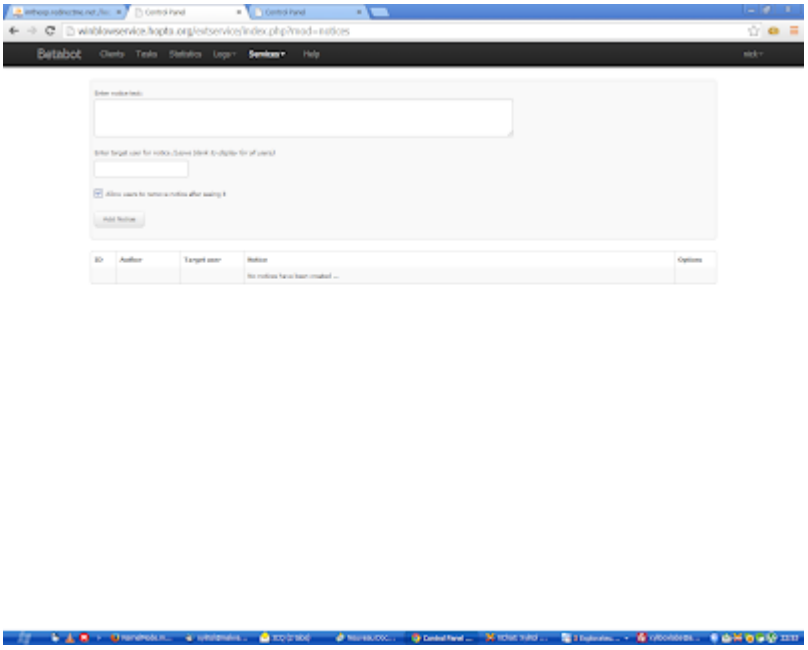
Statistics:



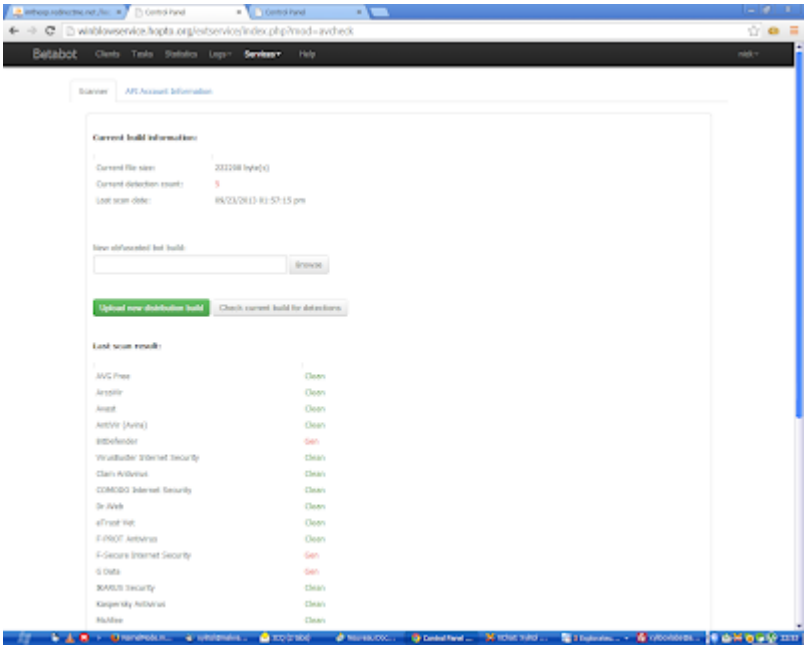
Files:



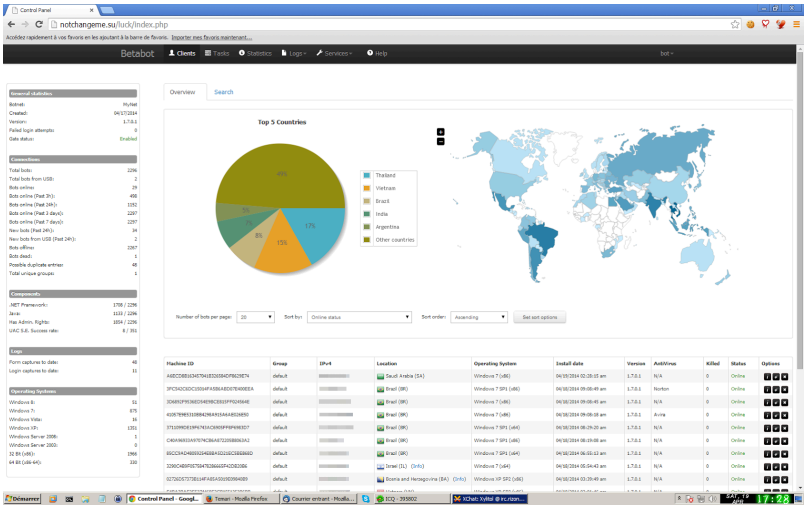
Users notice:



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 begining 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):

```
jabberid      : s1r1c1ly@limun.org
topic         : Assistence
question_data : [16:57:35] s1r1c1ly: Can you please respond back, involving my issue with "Services and logs" tab
[16:58:01] s1r1c1ly: I'm currently using latest jQuery
[17:00:07] s1r1c1ly: I've added the geoip.csv via phpMyAdmin but it doesn't want it to load.
The page loads but it's white and I did increase the limits on the maximum file size etc. so it could upload
Thanks in advance.
-s1r1c1ly
creation_date : 1391629725
num_views     : 0
user_ip       : 5.254.112.2
reserved0     : 0
---------------
id            : 122
jabberid      : flref4rt@default.rs
topic         : Problems with connect bots
question_data : Hi,
have been got my files, installed and looks good. After installation a crypted bin file  - nothing happened. Testest with disabled A
creation_date : 1391632652
num_views     : 0
user_ip       : 46.115.39.87
reserved0     : 0
---------------
id            : 123
jabberid      : gh87893@exploit.im
topic         : Received wrong update from you
question_data : A few days ago I purchased the upgrade from 1.0.2.5 to 1.7.0.1
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.
Please contact me on jabber when you have a moment.
Thanks!
GeorgeH
creation_date : 1391760175
num_views     : 0
user_ip       : 116.231.117.117
reserved0     : 0
---------------
id            : 124
jabberid      : volwy@im.apinc.org
topic         : Update
question_data : Hello,
Can I get lastest update for BetaBot.
Im volwy from HF.
creation_date : 1391788941
num_views     : 0
user_ip       : 88.227.146.231
reserved0     : 0
---------------
id            : 125
jabberid      : BETASELL@EXPLOIT.IM
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

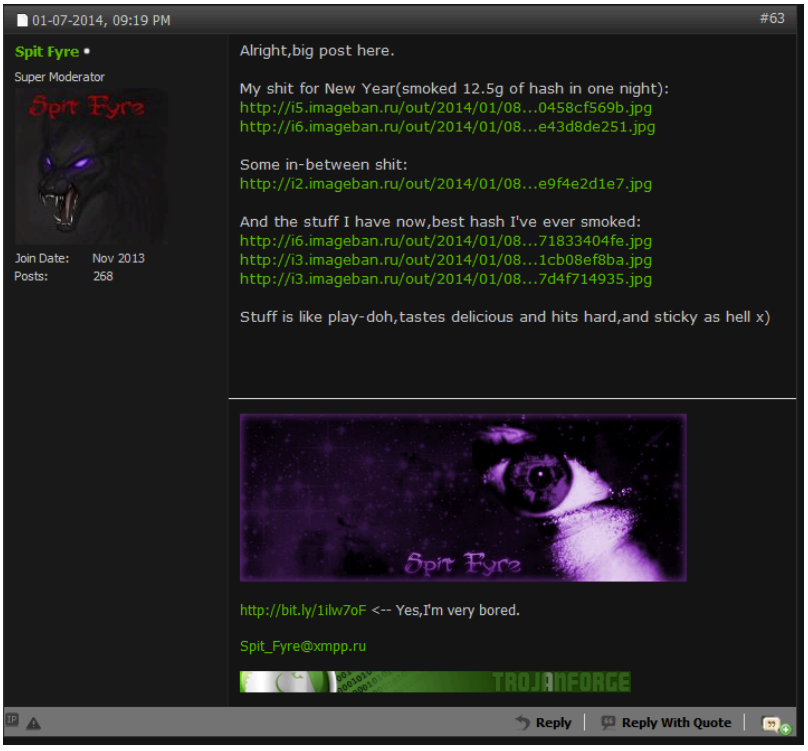
Some clients kits:

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

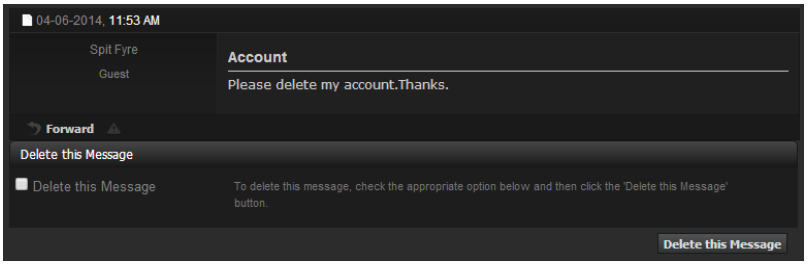
Finally some people got busted using these informations..

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.

Source: http://www.xylibox.com/2015/04/betabot-retrospective.html