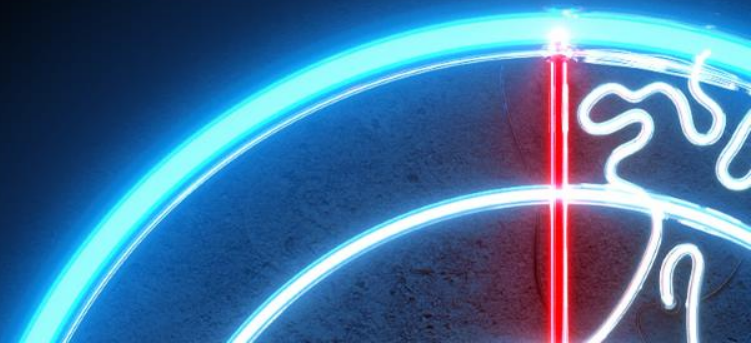
Dreambot
Business overview
2019

THE SAAS CON

CSIS

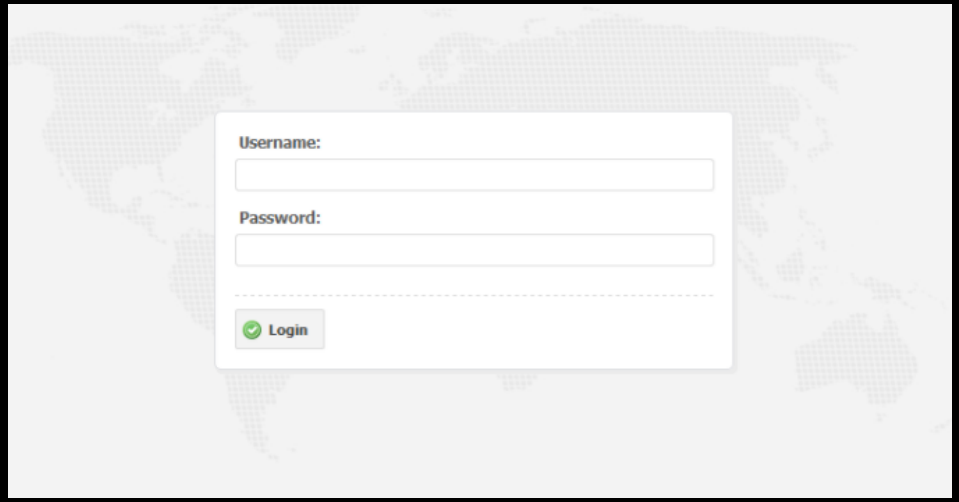


Who’s who

Benoît ANCEL
@benkow_

Peter KRUSE
@peterkruse

Dreambot



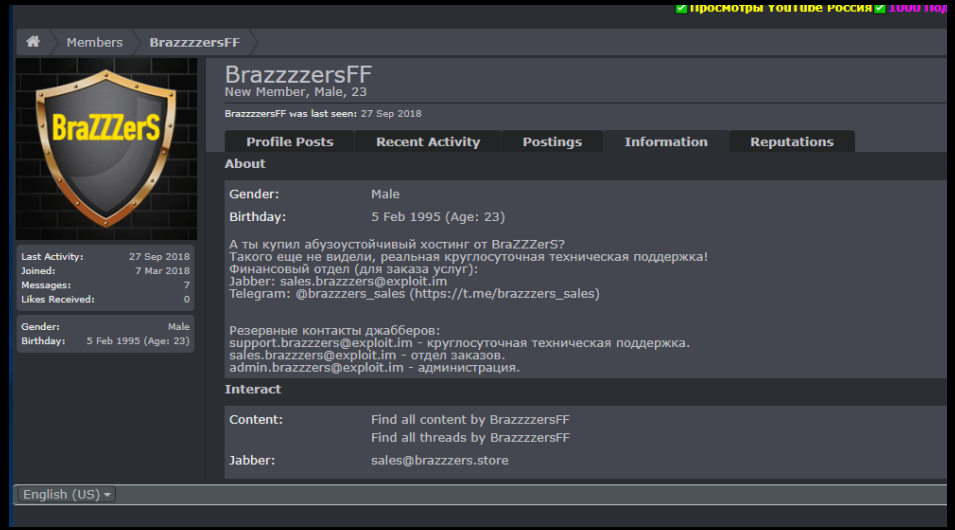
- Crime as a service
  - Based on Gozi2 (ISFB) + TOR + Bootkit
  - Around since 2015
  - ~ 450 000 bots (Oct-Dec 2018)
  - ~ 250 000 bots (Jan-March 18)
  - JP/DE/BG/PL/IT/US/CA/ES/AU/IN

- Business model:
  - You rent access to Dreambot
  - You obtain a non packed binary + the source code of the panel.

Dreambot

Under the hood

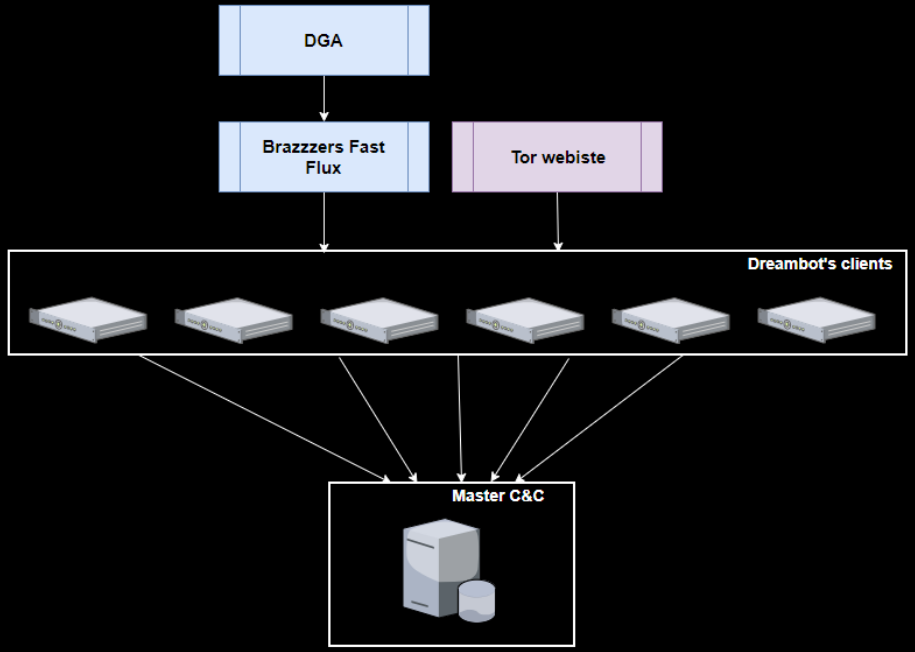
Dreambot



- 3 different ways to communicate:
  - Hard coded domains (BrazzzzersFF)
  - DGA (BrazzzzersFF)
  - Onion website

- Gozi features:
  - Webinjects
  - Keylogger
  - FormGrabber
  - email grabber
  - Screenshots
  - Socks
  - VNC

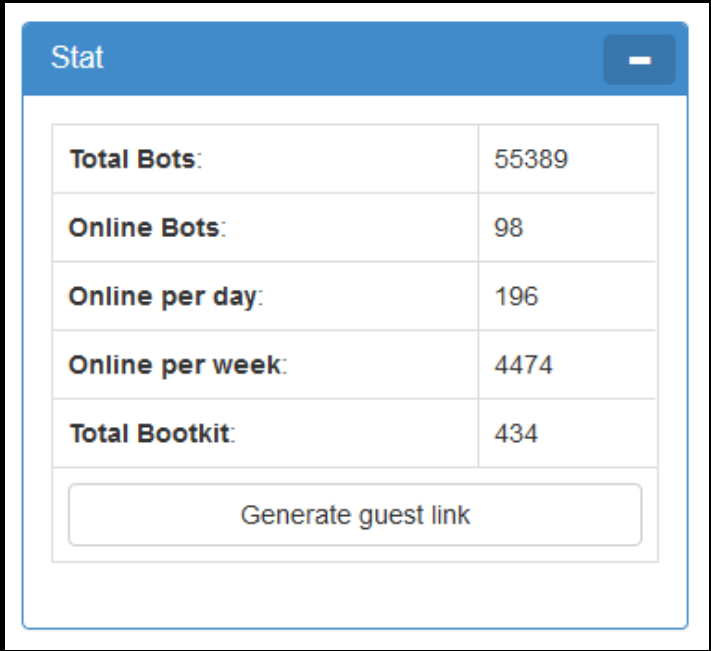
Dreambot



- 2 kinds of C&C:
  - Dreambot client's C&C
  - "Master" C&C

- "Master" is used for:
  - Bots storage
  - Banks frauds
  - Targeted attacks

Dreambot's client

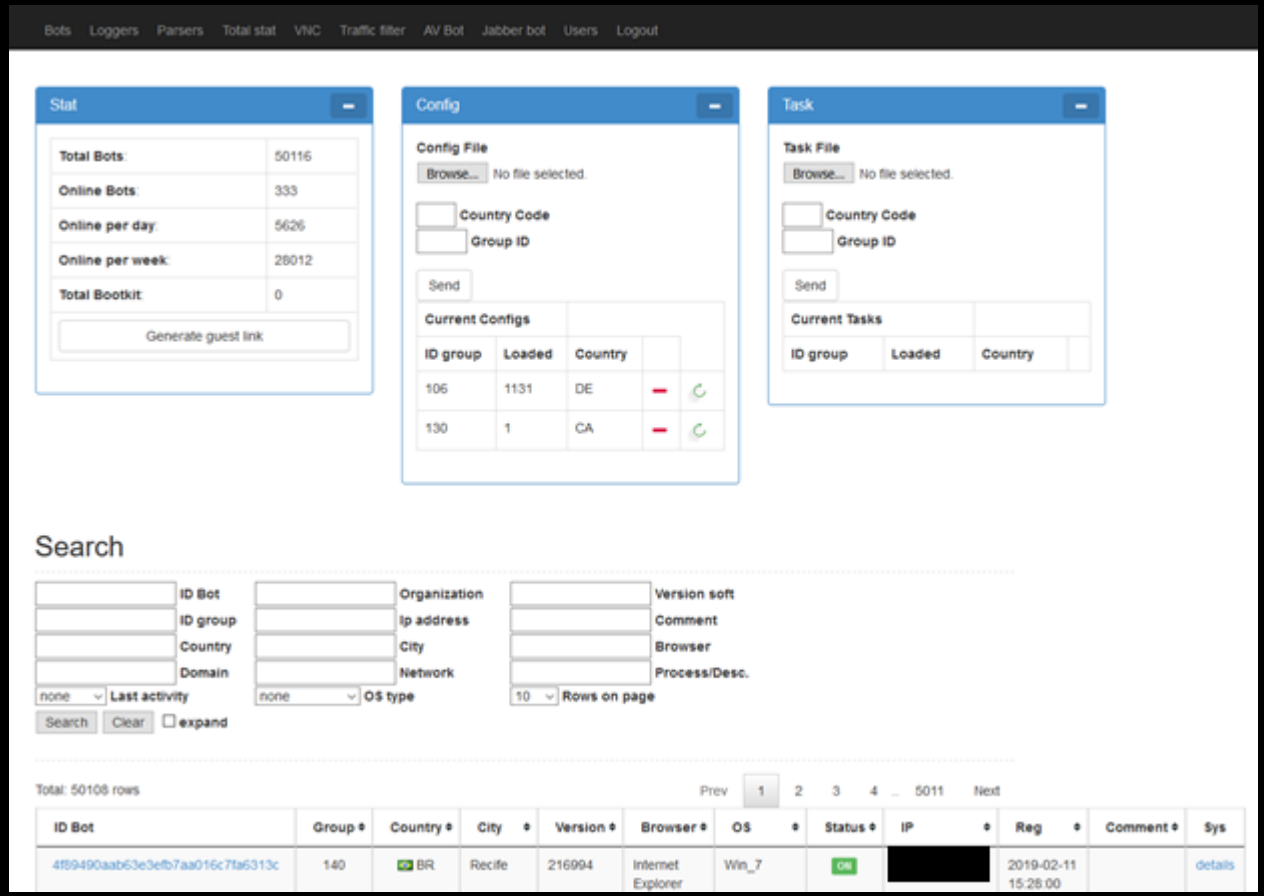


- Servers used for a defined period of time (subscription based)
- The client can:
  - Distribute Dreambot code
  - Access harvested drop data
  - Configure own webinjects
  - Configure a stage 2
- 3 different panels are available

~ 15 different customers between 2018 and yesterday

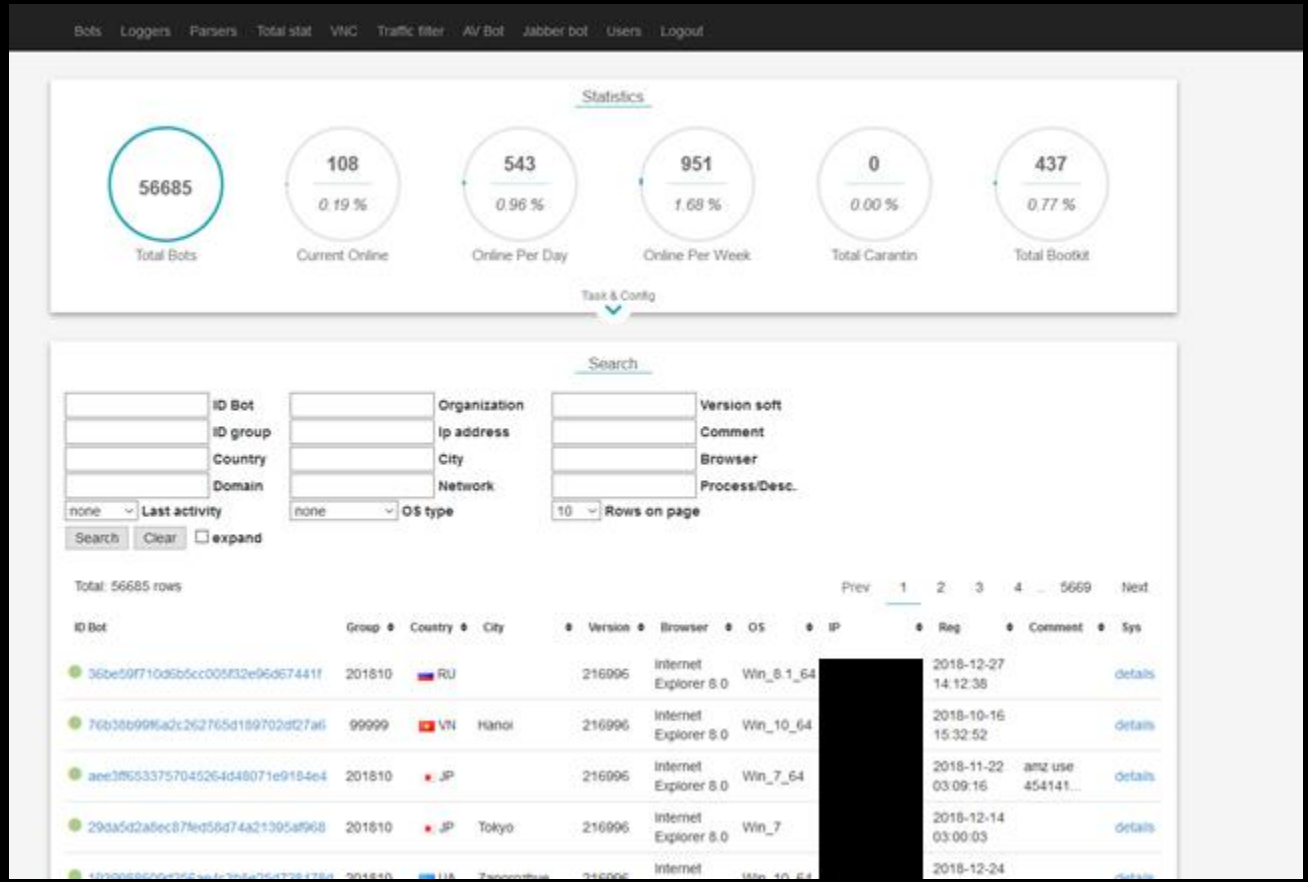
Dreambot

Panel 1



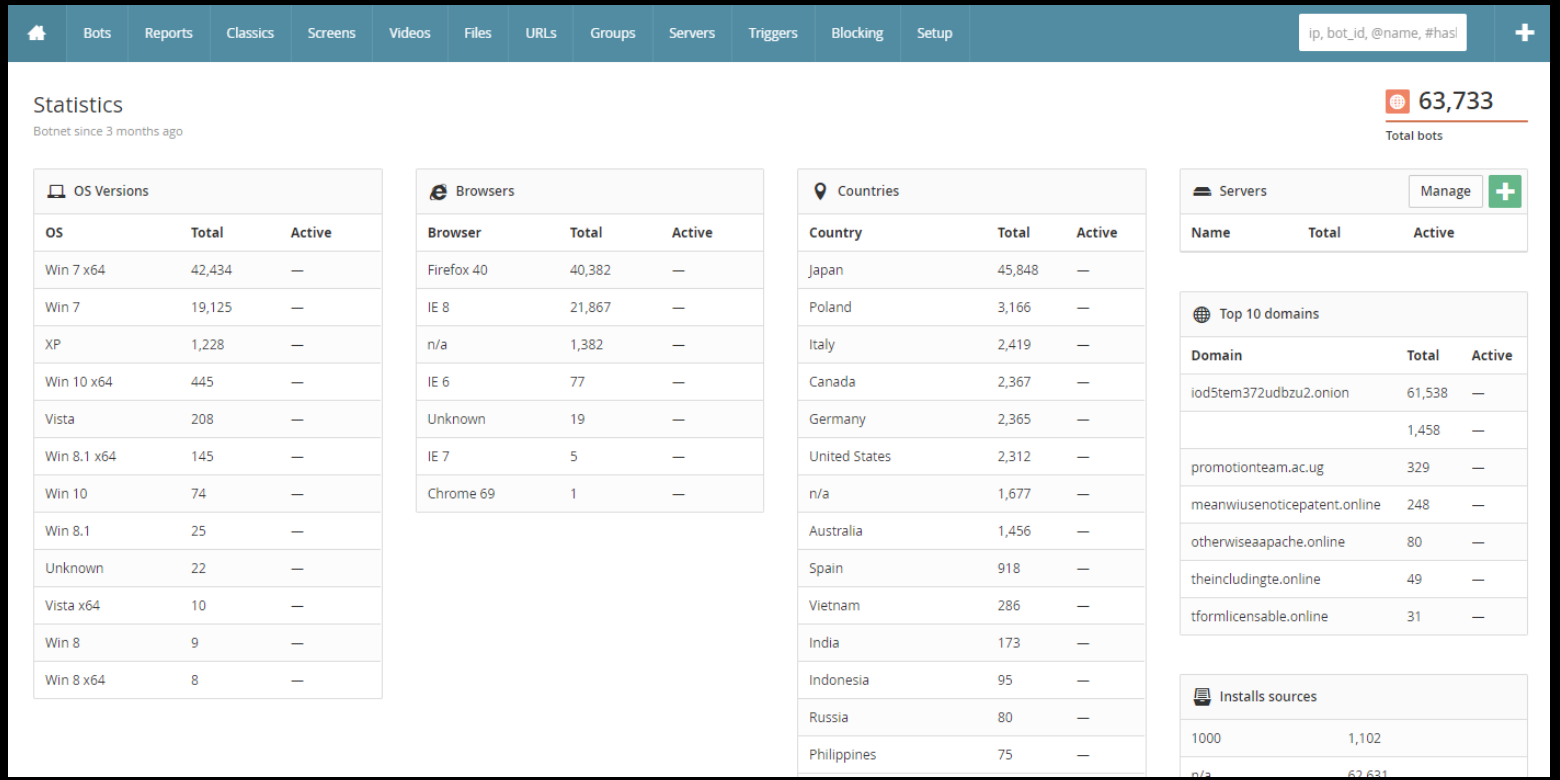
Dreambot

Panel 2

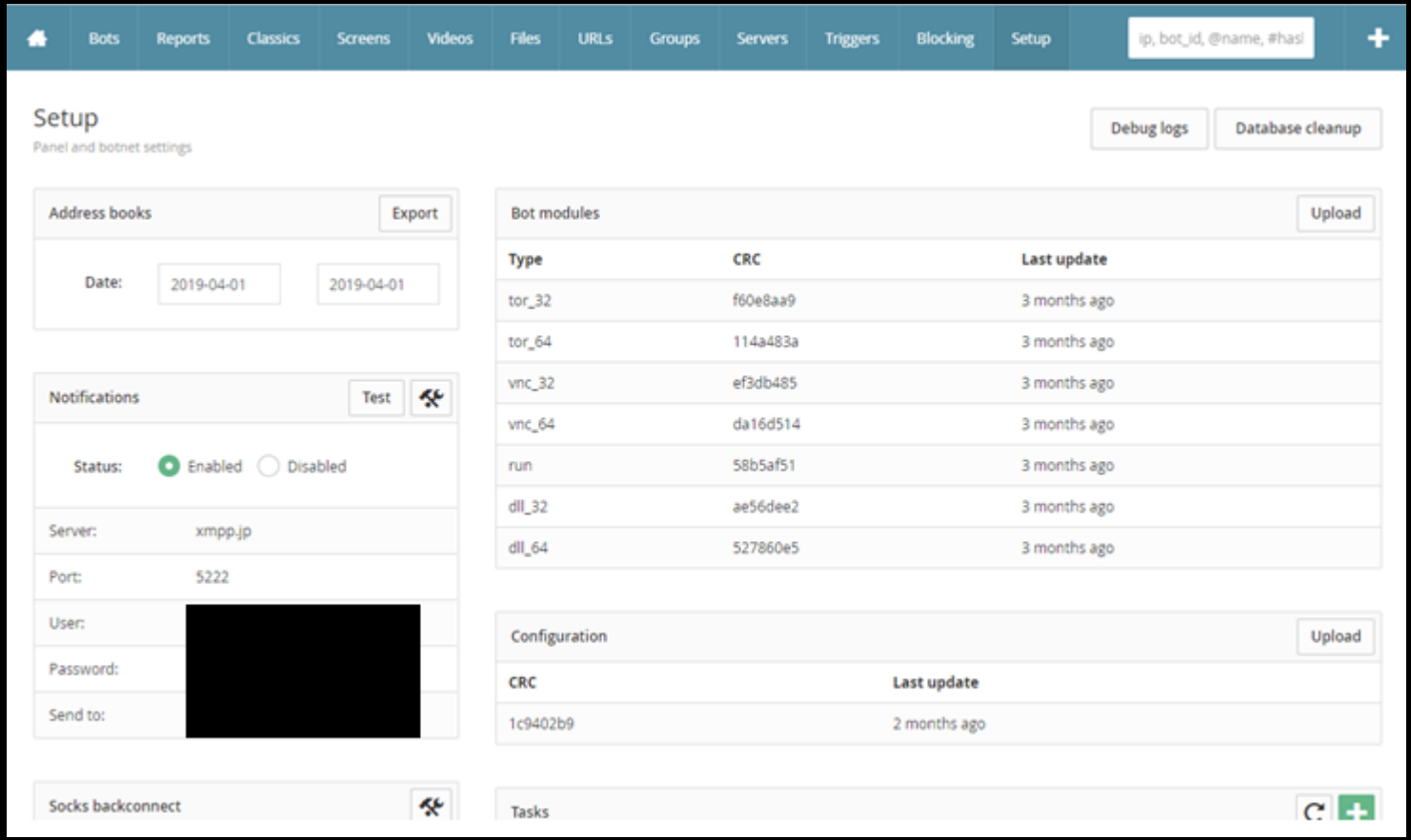


Dreambot

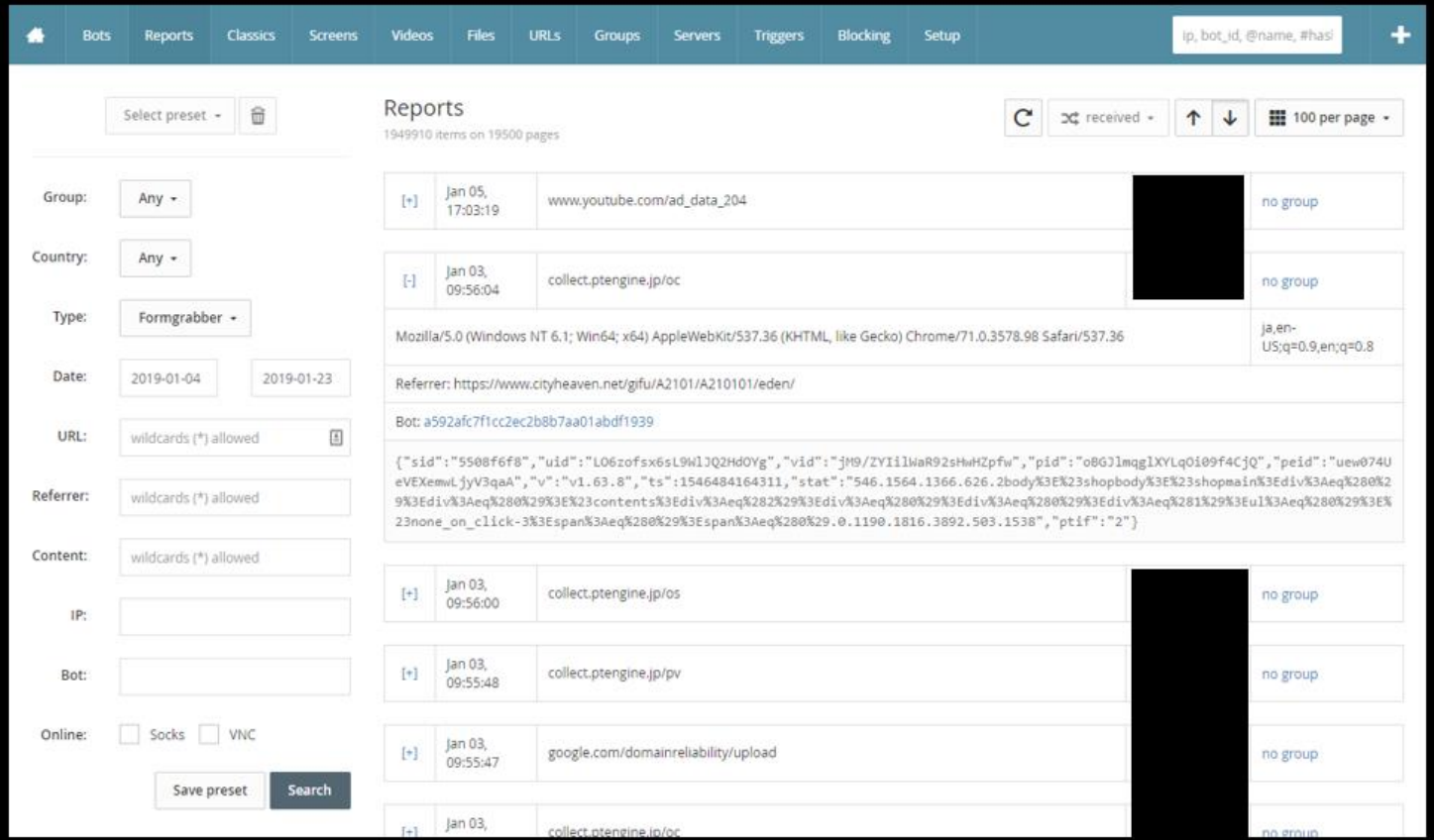
Panel 3



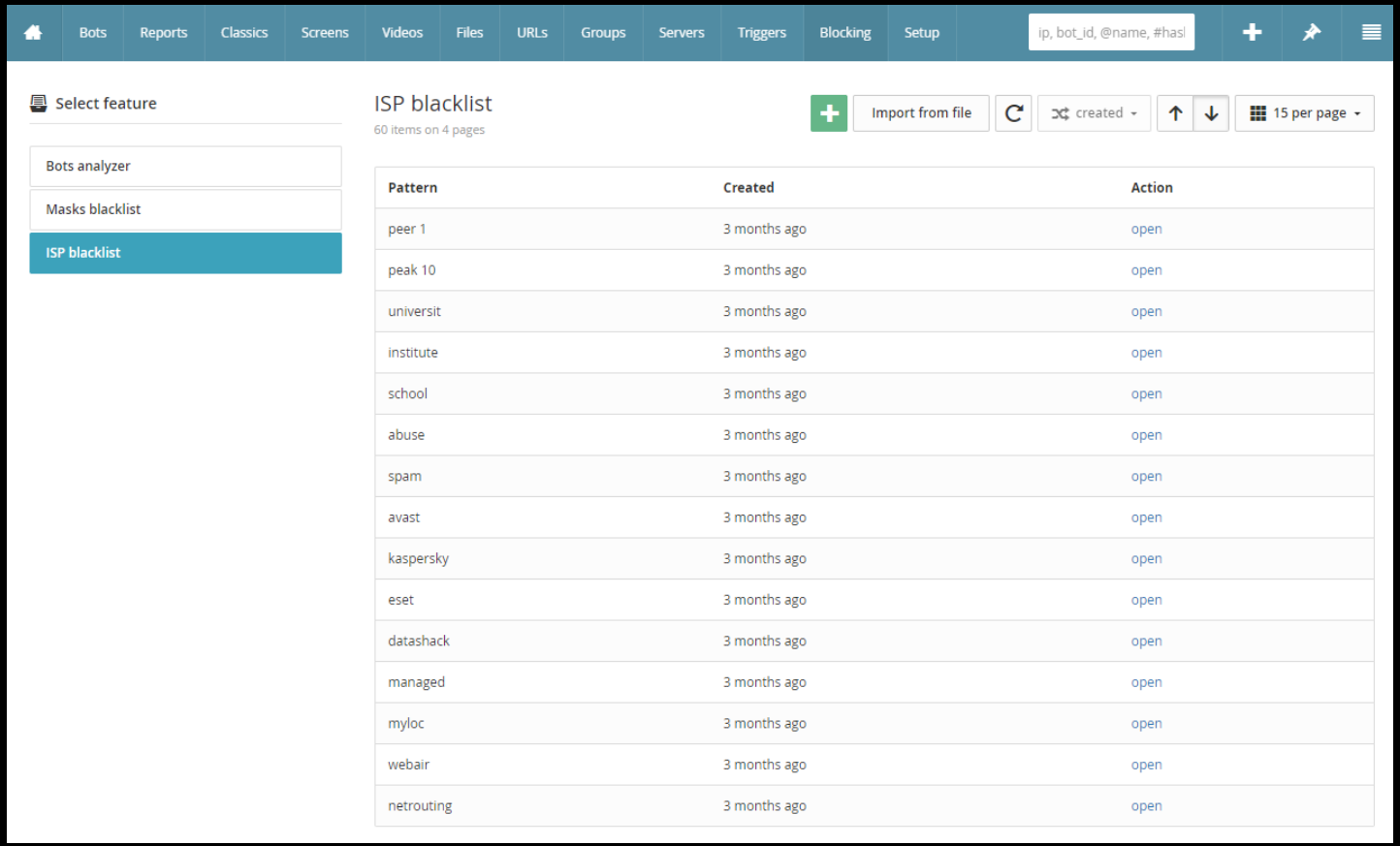
Dreambot


Bots
Reports
Classics
Screens
Videos
Files
URLs
Groups
Servers
Triggers
Blocking
Setup
ip, bot_id, @name, #hasl
Setup
Panel and botnet settings
Debug logs
Database cleanup
Address books
Export
Date:
2019-04-01
2019-04-01
Bot modules
Upload
Type
CRC
Last update
tor_32
f60e8aa9
3 months ago
tor_64
114a483a
3 months ago
vnc_32
ef3db485
3 months ago
vnc_64
da16d514
3 months ago
run
58b5af51
3 months ago
dll_32
ae56dee2
3 months ago
dll_64
527860e5
3 months ago
Notifications
Test
Status:
Enabled
Disabled
Server:
xmpp.jp
Port:
5222
User:
Password:
Send to:
Configuration
Upload
CRC
Last update
1c9402b9
2 months ago
Socks backconnect
Tasks

Dreambot


Bots
Reports
Classics
Screens
Videos
Files
URLs
Groups
Servers
Triggers
Blocking
Setup
ip, bot_id, @name, #hasi
Select preset
Group:
Any
Country:
Any
Type:
Formgrabber
Date:
2019-01-04
2019-01-23
URL:
wildcards (*) allowed
Referrer:
wildcards (*) allowed
Content:
wildcards (*) allowed
IP:
Bot:
Online:
Socks
VNC
Save preset
Search
Reports
1949910 items on 19500 pages
received
100 per page
[+] Jan 05, 17:03:19 www.youtube.com/ad_data_204 no group
[-] Jan 03, 09:56:04 collect.ptengine.jp/oc no group
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
ja,en-US;q=0.9,en;q=0.8
Referrer: https://www.cityheaven.net/gifu/A2101/A210101/eden/
Bot: a592afc7f1cc2ec2b8b7aa01abdf1939
{"sid":"5508f6f8","uid":"LO6zofsx6sL9WlJQ2HdOYg","vid":"jM9/ZYIilWaR92sHwHZpfw","pid":"oBGJlmqglXYLqOi09f4CjQ","peid":"uew074UeVEXemwLjyV3qaA","v":"v1.63.8","ts":1546484164311,"stat":"546.1564.1366.626.2body%3E%23shopbody%3E%23shopmain%3Ediv%3Aeq%280%29%3Ediv%3Aeq%280%29%3E%23contents%3Ediv%3Aeq%282%29%3Ediv%3Aeq%280%29%3Ediv%3Aeq%280%29%3Ediv%3Aeq%281%29%3Eul%3Aeq%280%29%3E%23none_on_click-3%3Espan%3Aeq%280%29%3Espan%3Aeq%280%29.0.1190.1816.3892.503.1538","ptif":"2"}
[+] Jan 03, 09:56:00 collect.ptengine.jp/os no group
[+] Jan 03, 09:55:48 collect.ptengine.jp/pv no group
[+] Jan 03, 09:55:47 google.com/domainreliability/upload no group
[+] Jan 03, collect.ptengine.jp/oc no group

Dreambot


Bots
Reports
Classics
Screens
Videos
Files
URLs
Groups
Servers
Triggers
Blocking
Setup
ip, bot_id, @name, #hasl
Select feature
Bots analyzer
Masks blacklist
ISP blacklist
ISP blacklist
60 items on 4 pages
Import from file
created
15 per page
Pattern
Created
Action
peer 1
3 months ago
open
peak 10
3 months ago
open
universit
3 months ago
open
institute
3 months ago
open
school
3 months ago
open
abuse
3 months ago
open
spam
3 months ago
open
avast
3 months ago
open
kaspersky
3 months ago
open
eset
3 months ago
open
datashack
3 months ago
open
managed
3 months ago
open
myloc
3 months ago
open
webair
3 months ago
open
netrouting
3 months ago
open

Dreambot

```
const DEBUG_MODE = 0;

const DB_NAME
const ENCRYPTI
const DECRYPT_
const USE_ZIP

const VIDEOS_P
const ONLINE_T

const PARSE_AC

// common depe
require_once('

// connect to
$mongo = new M
$db = $mongo->

// CLI MODE (W
if (php_sapi_n
{
    require_on
    require_on

    // route a
    $route = isset($argv[1]) ? $argv[1] : null;
```

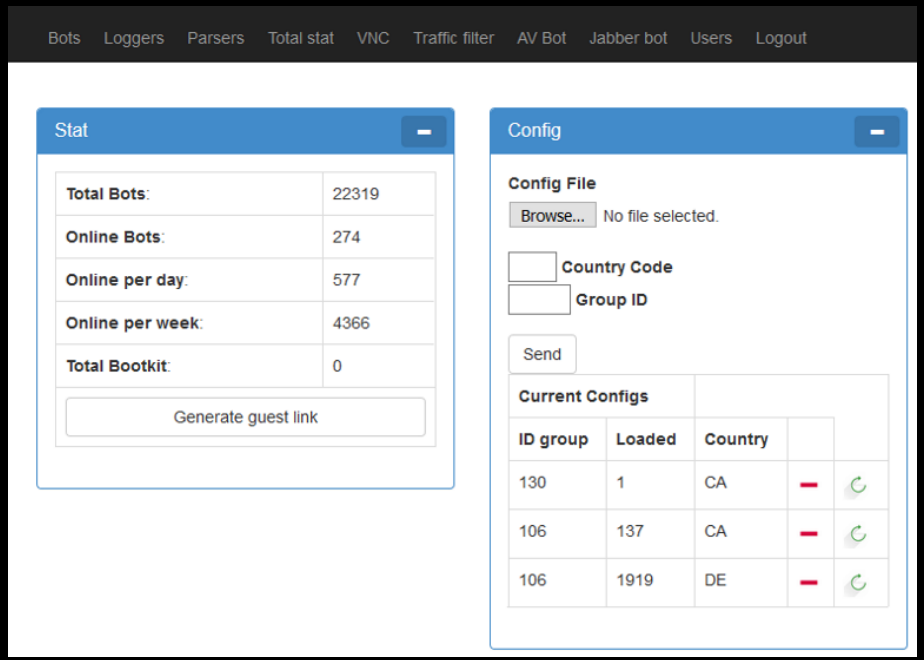
```
// route extensions
const ExtConfig = 'jpeg';
const ExtTask = 'gif';
const ExtData = 'bmp';
// route extentions for download files
const ExtBinary = 'ttf';
// bot writer decided to add vali is for tor only,
// url is generated automatically, so i also need
// to check for OS version, thank you author...
const ExtTor = 'avi';

if( strstr($_SERVER['REQUEST_URI'], ".avi") ){
    error_log("Got our request now.");
}
```

```
const DB_NAME = 'standard';
const ONLINE_TIMEOUT = 1800;
const ACTIVE_TIMEOUT = 86400;

                                    ;
                                    nstall.txt';

                                    /server.conf';
                                    penssl-1.0.0.cnf';

                                    key.exe';
                                    ;
                                    ate.key';

                                    os';
                                    os';

// injects support
const ACCOUNTS_ENABLED = false;
const ENGINES_LIST = 'bofa,chase,citi,schwab,usaa,wells';
```

Dreambot

Customer use case

Dreambot customer in Germany



- The example:

The German customer:

- New client since October 2018
- ~ 210 000 infections in Germany/US/CA

(October 18 – March 19)

(EK and targeted emails)

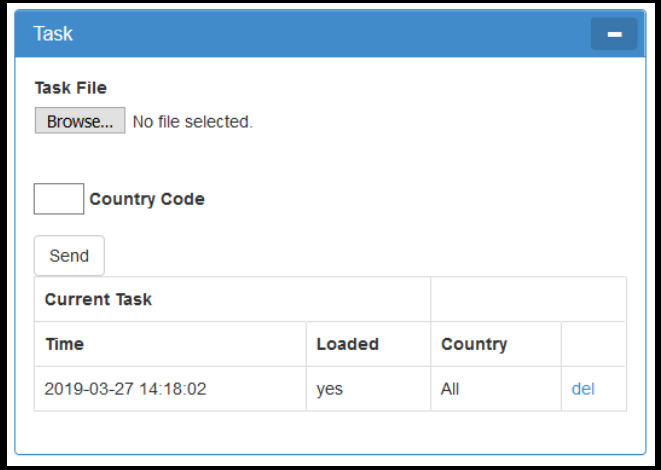
- This client (known as Bagsu) is only interested in baning fraud and targeting 725 unique banks in Germany

Dreambot's client - Germany

ID Bot	Group	Country	City	Version	Browser	OS	Status	IP	Reg	Comment	Sys
ff06ae1581ff2eac5396fd38504be17b	10	DE	Salzwedel	216998	Internet Explorer 8.0	Win_7_64	OFF	[redacted]	2019-03-19 20:53:18	pp inc pass, gp used, amz decl	details
d2b2bddb2118d53b3a517cabce337032	10	DE		216998	Internet Explorer 8.0	Win_8.1_64	ON		2019-03-18 22:17:37	pp inc pass	details
fcfa1b7abeab77bfb9c45396a0e3b90a	10	DE	Mainz	216998	Internet Explorer 8.0	Win_8.1_64	OFF		2019-03-18 23:51:04	pp cant pay	details
cfef1acfeb9288751ee5005f59aa6363	10	DE	Wuppertal	216998	Internet Explorer 8.0	Win_7_64	ON		2019-03-19 09:06:33	pp cant pay	details
78da5561e86751a119a4b376ba8e6508	10	DE	Stollberg	216998	Internet Explorer 8.0	Win_7_64	OFF		2019-03-18 20:37:39	pp 2nd fact, amz skinny	details
ec9741c6e18e5537bad1fc2bd9ebe6cf	10	DE		216998	Internet Explorer 8.0	Win_7_64	ON		2019-03-19 08:51:34	gp, amz used, pp used	details
ad69f14fdfda710d6cdb7ec5ebf37cfb	10	DE	Ennepetal	216998	Internet Explorer 8.0	Win_10_64	OFF		2019-03-18 20:40:48	gp cant pay thru pp	details
122a3b0e00f3a067ef82f90422982f49	10	DE		216998	Internet Explorer 8.0	Win_8.1_64	OFF		2019-03-18 20:36:08	chrome untouch	details

Dreambot's client - Germany

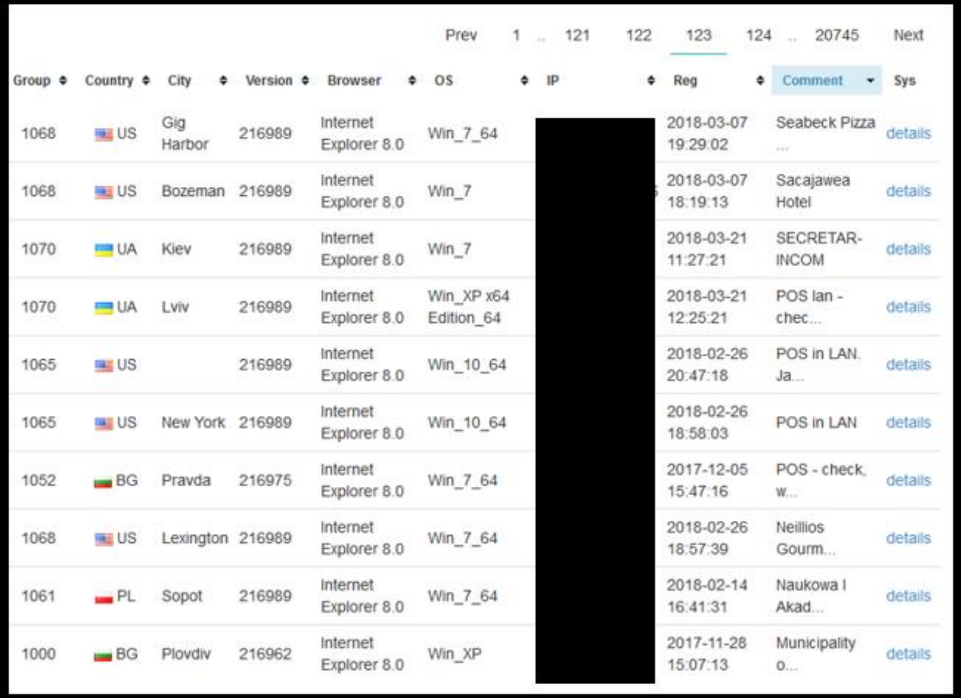
Files:	No. Use "GET_FILES=*"
Cookies:	No. Use "GET_COOKIES"
Video	No.
Certificates:	No. Use "GET_CERTS"
Screenshots	No. Use "GET_SCRSHOT"
Mail accounts	No. Use "GET_MAIL"
Address book	0
Cards	0
System Info	No. Use "GET_SYSINFO"
FormGrabber	List / Table (3118 reports)
ContentGrabber	0
KeyLogger	List / Table (1318 reports)
Last Online	2019-04-01 14:57:58
Registration	2019-03-19 08:35:51



Dreambot

“Master” C&C

Dreambot

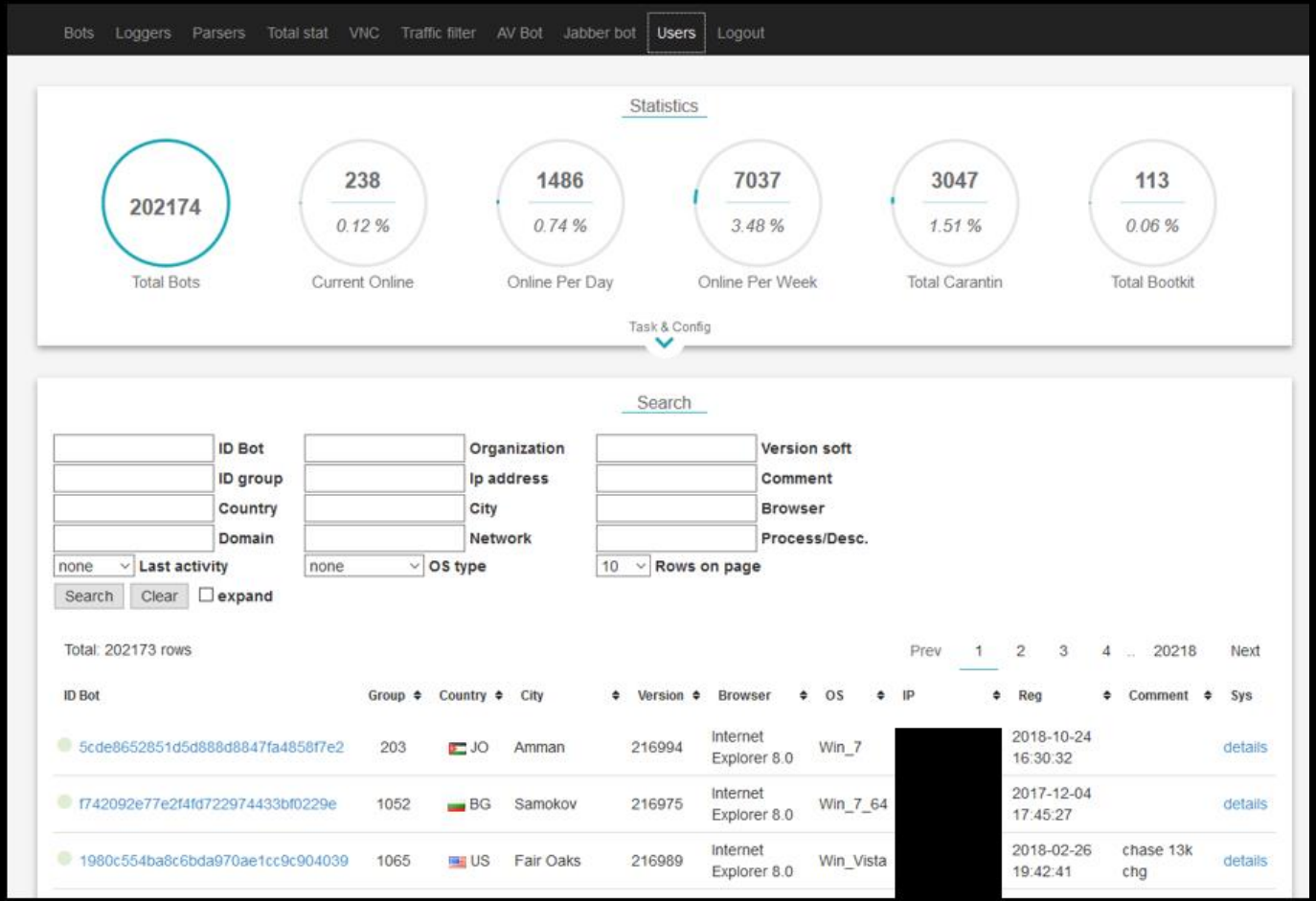


Prev 1 .. 121 122 123 124 .. 20745 Next

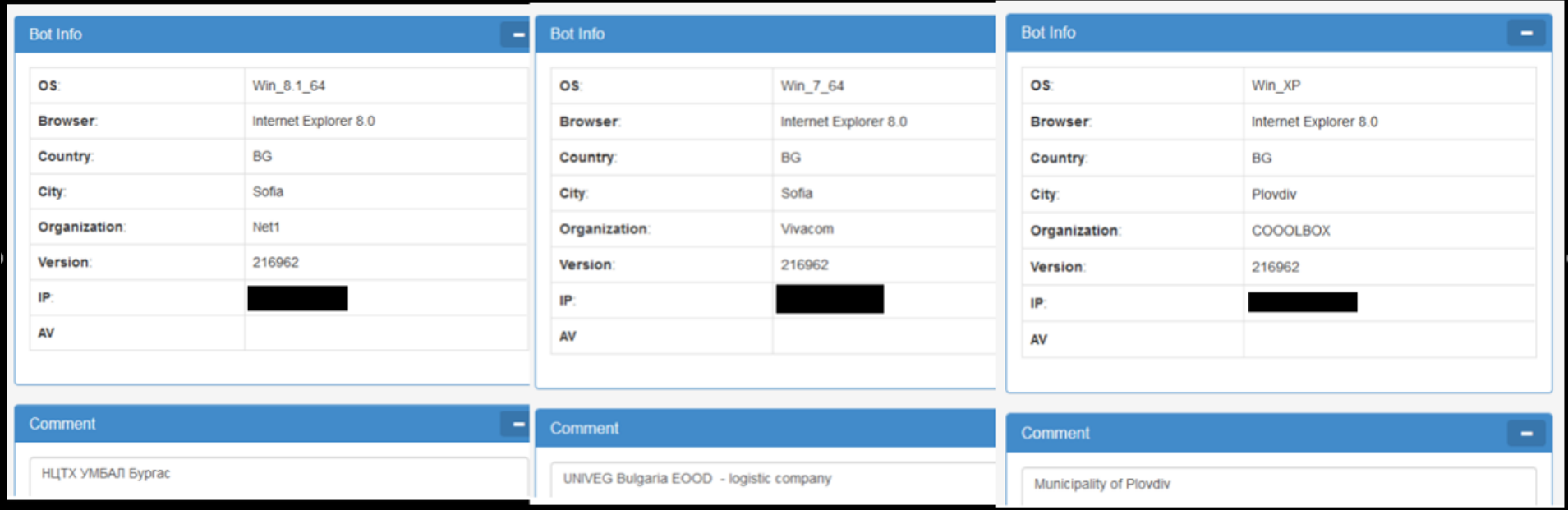
Group	Country	City	Version	Browser	OS	IP	Reg	Comment	Sys
1068	US	Gig Harbor	216989	Internet Explorer 8.0	Win_7_64	[redacted]	2018-03-07 19:29:02	Seabeck Pizza ...	details
1068	US	Bozeman	216989	Internet Explorer 8.0	Win_7		2018-03-07 18:19:13	Sacajawea Hotel	details
1070	UA	Kiev	216989	Internet Explorer 8.0	Win_7		2018-03-21 11:27:21	SECRETAR-INCOM	details
1070	UA	Lviv	216989	Internet Explorer 8.0	Win_XP x64 Edition_64		2018-03-21 12:25:21	POS lan - chec...	details
1065	US		216989	Internet Explorer 8.0	Win_10_64		2018-02-26 20:47:18	POS in LAN. Ja...	details
1065	US	New York	216989	Internet Explorer 8.0	Win_10_64		2018-02-26 18:58:03	POS in LAN	details
1052	BG	Pravda	216975	Internet Explorer 8.0	Win_7_64		2017-12-05 15:47:16	POS - check, w...	details
1068	US	Lexington	216989	Internet Explorer 8.0	Win_7_64		2018-02-26 18:57:39	Neillios Gourm...	details
1061	PL	Sopot	216989	Internet Explorer 8.0	Win_7_64		2018-02-14 16:41:31	Naukowa I Akad...	details
1000	BG	Plovdiv	216962	Internet Explorer 8.0	Win_XP		2017-11-28 15:07:13	Municipality o...	details

- “Master” C&C
    - Used to store bots after the expiration of a custumer subscription periode
    - Likely controlled by the Dreambot operators
    - Involved in targeted attacks
    - Involved in frauds in BG in 2018-2019

Dreambot


Bots
Loggers
Parsers
Total stat
VNC
Traffic filter
AV Bot
Jabber bot
Users
Logout
Statistics
202174
Total Bots
238
0.12 %
Current Online
1486
0.74 %
Online Per Day
7037
3.48 %
Online Per Week
3047
1.51 %
Total Carantin
113
0.06 %
Total Bootkit
Task & Config
Search
ID Bot
Organization
Version soft
ID group
Ip address
Comment
Country
City
Browser
Domain
Network
Process/Desc.
none
Last activity
none
OS type
10
Rows on page
Search
Clear
expand
Total: 202173 rows
Prev
1
2
3
4
..
20218
Next
ID Bot
Group
Country
City
Version
Browser
OS
IP
Reg
Comment
Sys
5cde8652851d5d888d8847fa4858f7e2
203
JO
Amman
216994
Internet Explorer 8.0
Win_7
2018-10-24 16:30:32
details
f742092e77e2f4fd722974433bf0229e
1052
BG
Samokov
216975
Internet Explorer 8.0
Win_7_64
2017-12-04 17:45:27
details
1980c554ba8c6bda970ae1cc9c904039
1065
US
Fair Oaks
216989
Internet Explorer 8.0
Win_Vista
2018-02-26 19:42:41
chase 13k chg
details

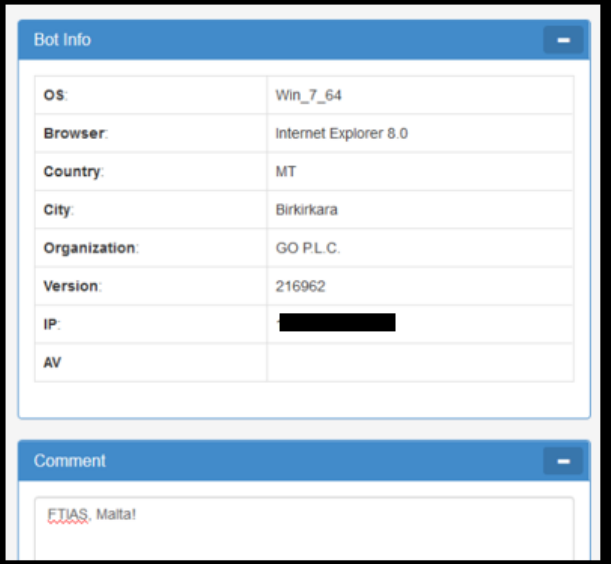
Dreambot


Bot Info
OS: Win_8.1_64
Browser: Internet Explorer 8.0
Country: BG
City: Sofia
Organization: Net1
Version: 216962
IP: [redacted]
AV
Comment
НЦТХ УМБАЛ Бургас
Bot Info
OS: Win_7_64
Browser: Internet Explorer 8.0
Country: BG
City: Sofia
Organization: Vivacom
Version: 216962
IP: [redacted]
AV
Comment
UNIVEG Bulgaria EOOD - logistic company
Bot Info
OS: Win_XP
Browser: Internet Explorer 8.0
Country: BG
City: Plovdiv
Organization: COOOLBOX
Version: 216962
IP: [redacted]
AV
Comment
Municipality of Plovdiv

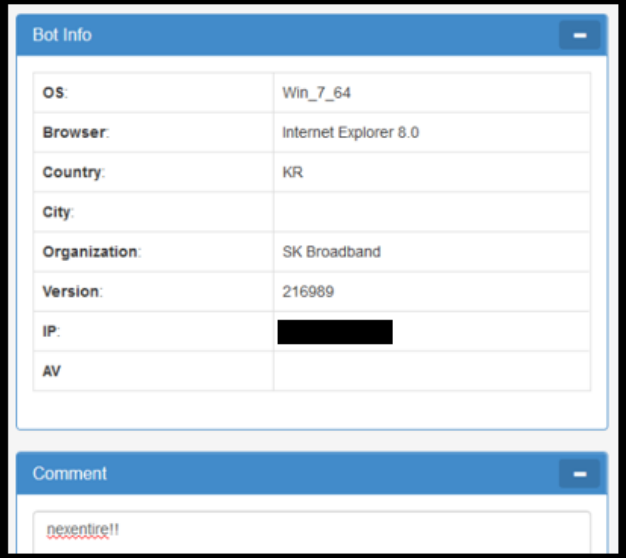
Dreambot

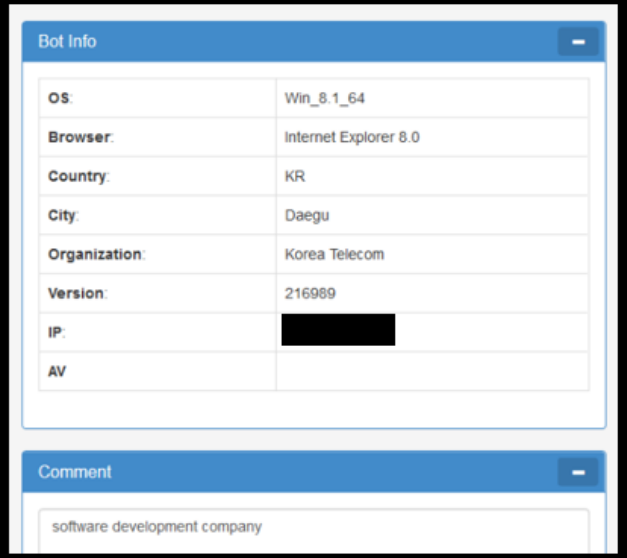

Bot Info
OS: Win_7_64
Browser: Internet Explorer 8.0
Country: DE
City: Ratingen
Organization: Vodafone GmbH
Version: 216994
IP: [redacted]
AV:
Comment
WORK DONT USE Vodafone adminka O2 adminka

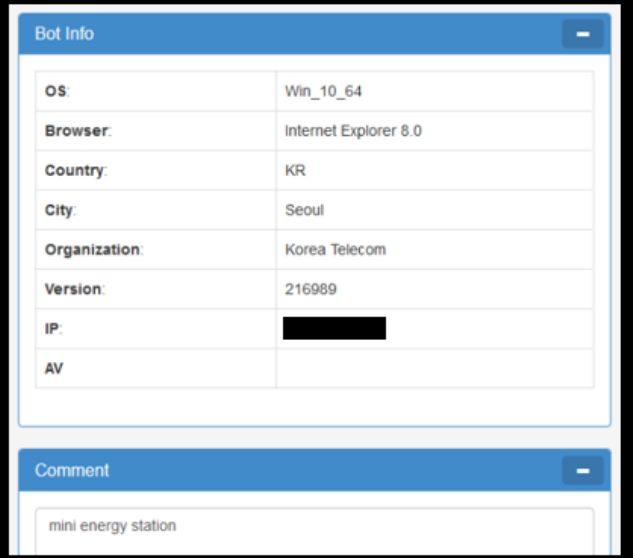

Bot Info
OS: Win_7_64
Browser: Internet Explorer 8.0
Country: BG
City: Sofia
Organization: COOOLBOX
Version: 216975
IP: [redacted]
AV:
Comment
honda Pwn3d
dsk checked


Bot Info
OS: Win_7_64
Browser: Internet Explorer 8.0
Country: MT
City: Birkirkara
Organization: GO P.L.C.
Version: 216962
IP: [redacted]
AV:
Comment
FTIAS, Malta!

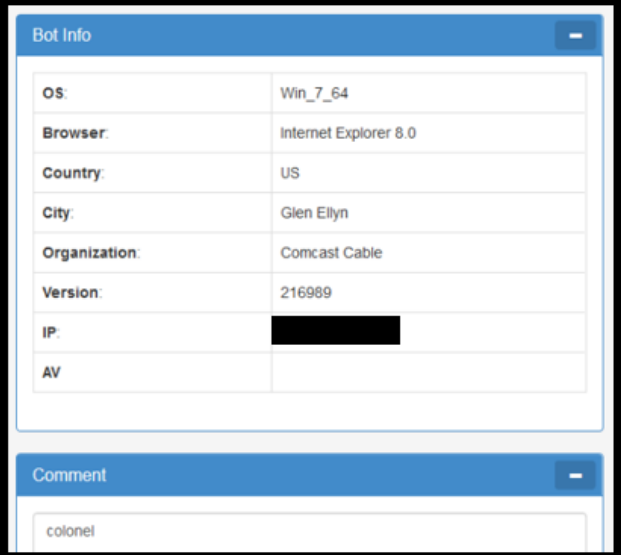
Dreambot

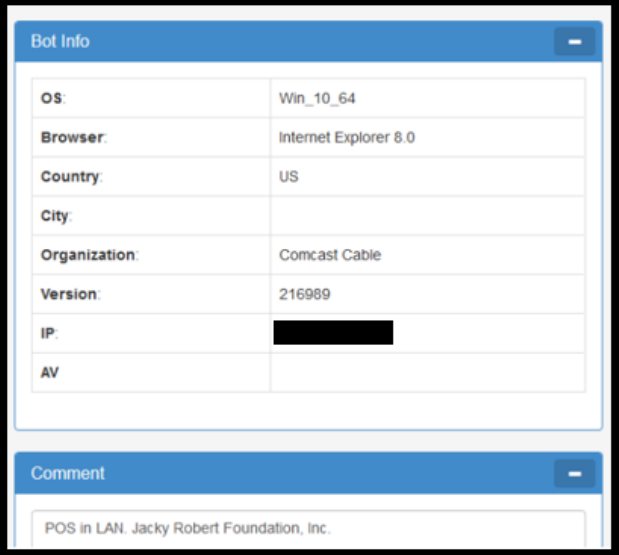

Bot Info
OS: Win_7_64
Browser: Internet Explorer 8.0
Country: KR
City:
Organization: SK Broadband
Version: 216989
IP: [redacted]
AV
Comment
nexentire!!

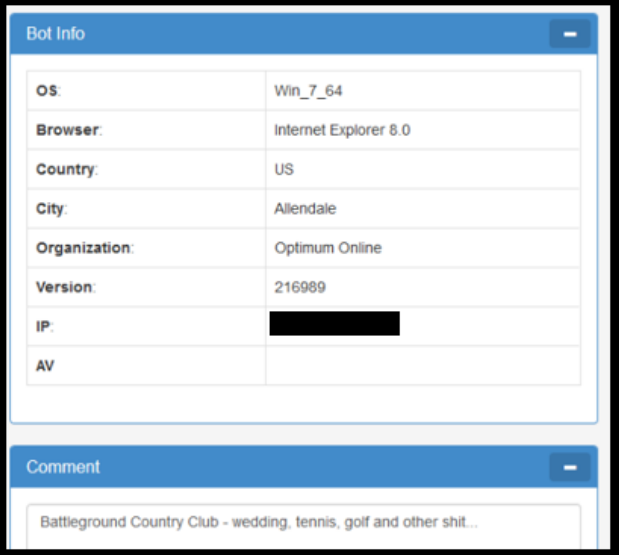

Bot Info
OS: Win_8.1_64
Browser: Internet Explorer 8.0
Country: KR
City: Daegu
Organization: Korea Telecom
Version: 216989
IP: [redacted]
AV
Comment
software development company


Bot Info
OS: Win_10_64
Browser: Internet Explorer 8.0
Country: KR
City: Seoul
Organization: Korea Telecom
Version: 216989
IP: [redacted]
AV
Comment
mini energy station

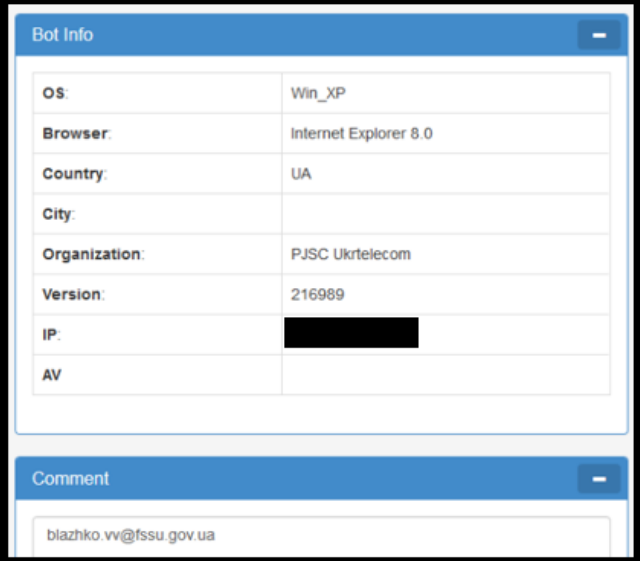
Dreambot

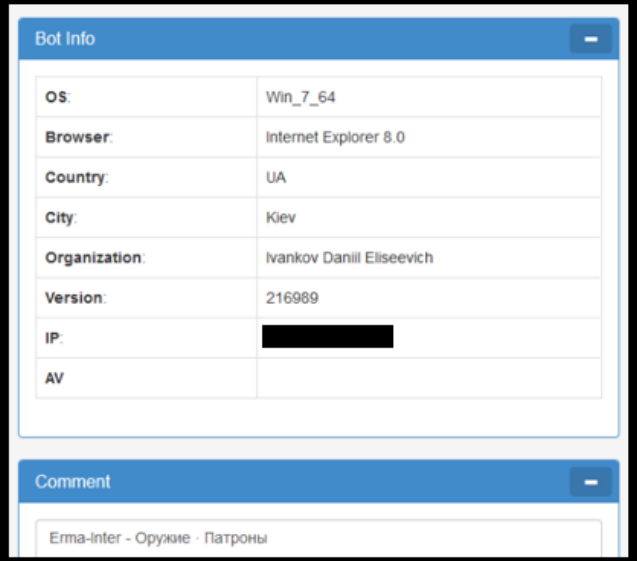

Bot Info
OS: Win_7_64
Browser: Internet Explorer 8.0
Country: US
City: Glen Ellyn
Organization: Comcast Cable
Version: 216989
IP: [redacted]
AV
Comment
colonel

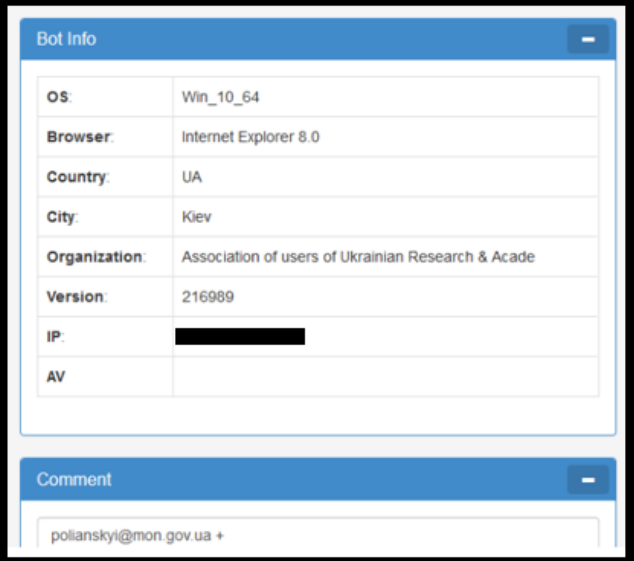

Bot Info
OS: Win_10_64
Browser: Internet Explorer 8.0
Country: US
City:
Organization: Comcast Cable
Version: 216989
IP: [redacted]
AV
Comment
POS in LAN. Jacky Robert Foundation, Inc.


Bot Info
OS: Win_7_64
Browser: Internet Explorer 8.0
Country: US
City: Allendale
Organization: Optimum Online
Version: 216989
IP: [redacted]
AV
Comment
Battleground Country Club - wedding, tennis, golf and other shit...

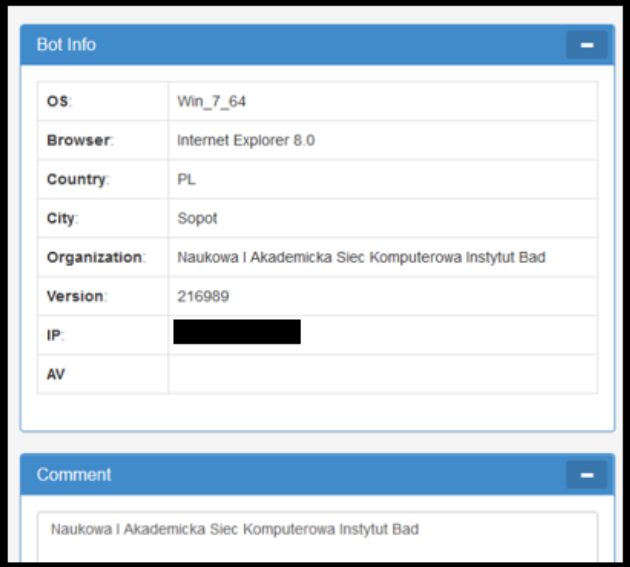
Dreambot

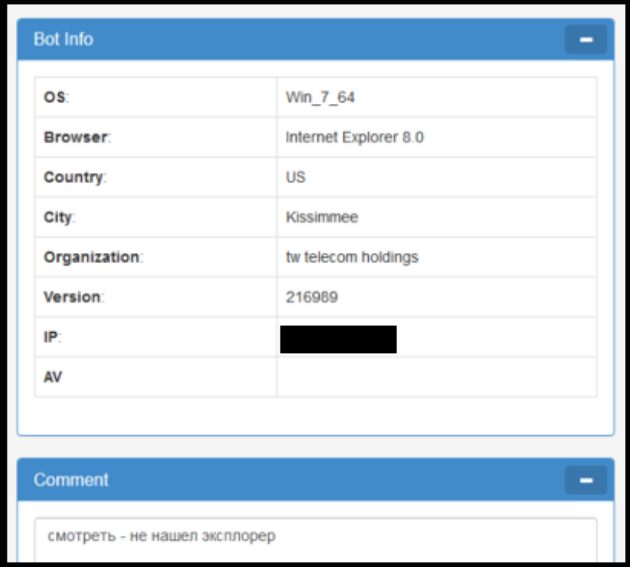

Bot Info
OS: Win_XP
Browser: Internet Explorer 8.0
Country: UA
City:
Organization: PJSC Ukrtelecom
Version: 216989
IP: [redacted]
AV:
Comment
blazhko.vv@fssu.gov.ua

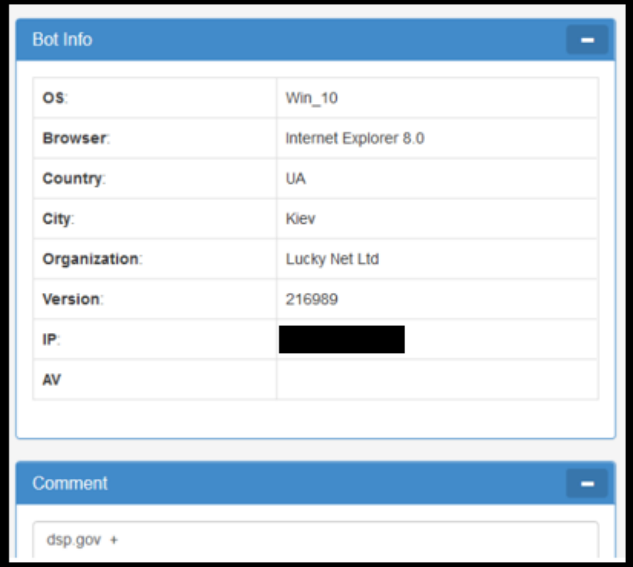

Bot Info
OS: Win_7_64
Browser: Internet Explorer 8.0
Country: UA
City: Kiev
Organization: Ivankov Daniil Eliseevich
Version: 216989
IP: [redacted]
AV:
Comment
Erma-Inter - Оружие · Патроны


Bot Info
OS: Win_10_64
Browser: Internet Explorer 8.0
Country: UA
City: Kiev
Organization: Association of users of Ukrainian Research & Acade
Version: 216989
IP: [redacted]
AV:
Comment
polianskyi@mon.gov.ua +

Dreambot


Bot Info
OS: Win_7_64
Browser: Internet Explorer 8.0
Country: PL
City: Sopot
Organization: Naukowa I Akademicka Siec Komputerowa Instytut Bad
Version: 216989
IP: [redacted]
AV
Comment
Naukowa I Akademicka Siec Komputerowa Instytut Bad


Bot Info
OS: Win_7_64
Browser: Internet Explorer 8.0
Country: US
City: Kissimmee
Organization: tw telecom holdings
Version: 216989
IP: [redacted]
AV
Comment
смотреть - не нашел эксплорер


Bot Info
OS: Win_10
Browser: Internet Explorer 8.0
Country: UA
City: Kiev
Organization: Lucky Net Ltd
Version: 216989
IP: [redacted]
AV
Comment
dsp.gov +

Conclusion

Conclusion

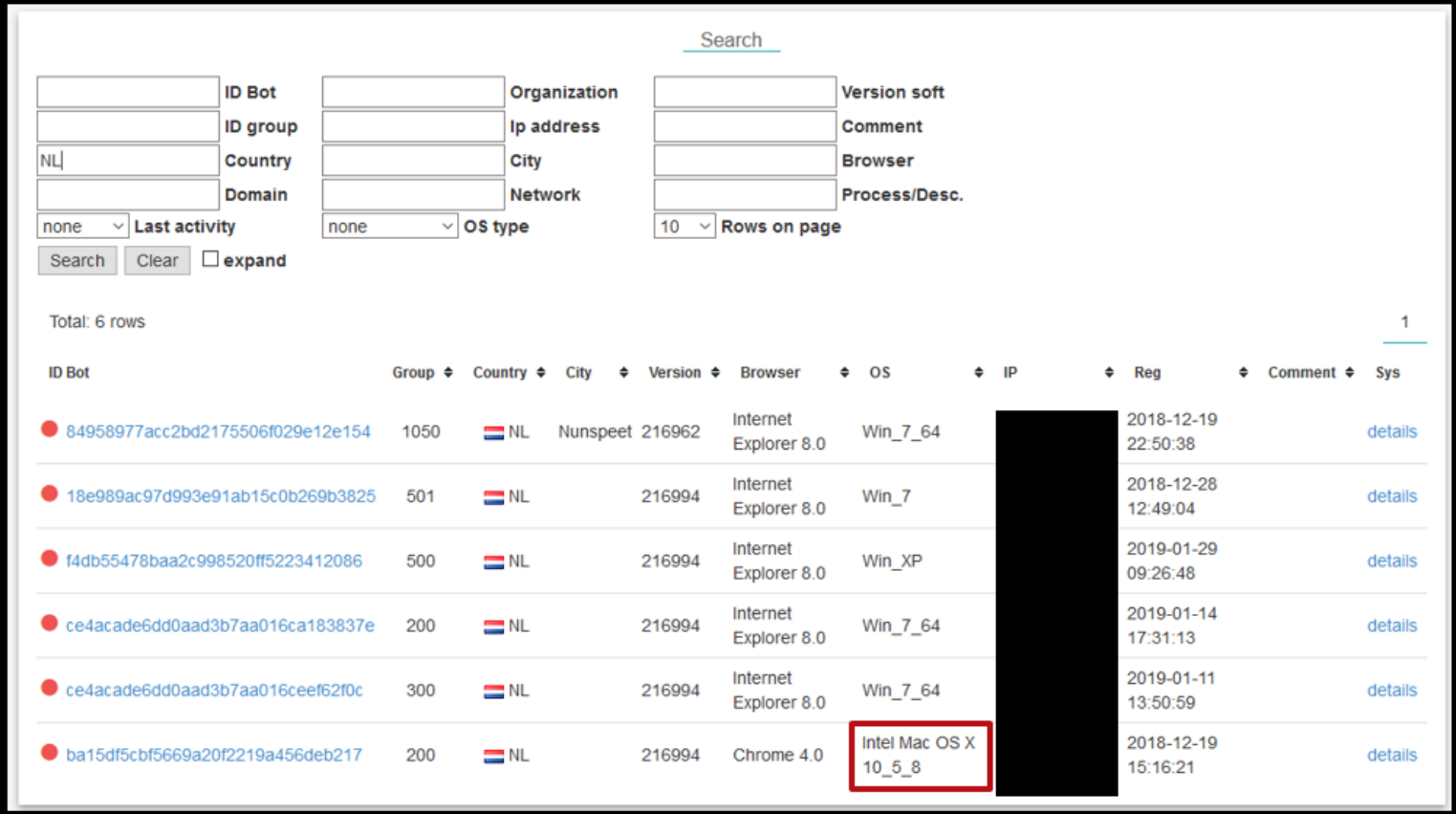
- Gozi still going strong and continuously being improved
- Crime as a services getting trendy
- Vector used by APT groups
- Attribution getting harder
- Gozi will never die despite of takedowns

- Thanks to:
    Kafeine
    Maciej Kotowicz

Dreambot

One more thing....

Dreambot – OSX !



#TheSAS2019

Let’s Talk?

pkr@csis.dk
PGP-ID: 0x715FB4BD

CSIS