

Dreambot Business overview 2019



Who's who

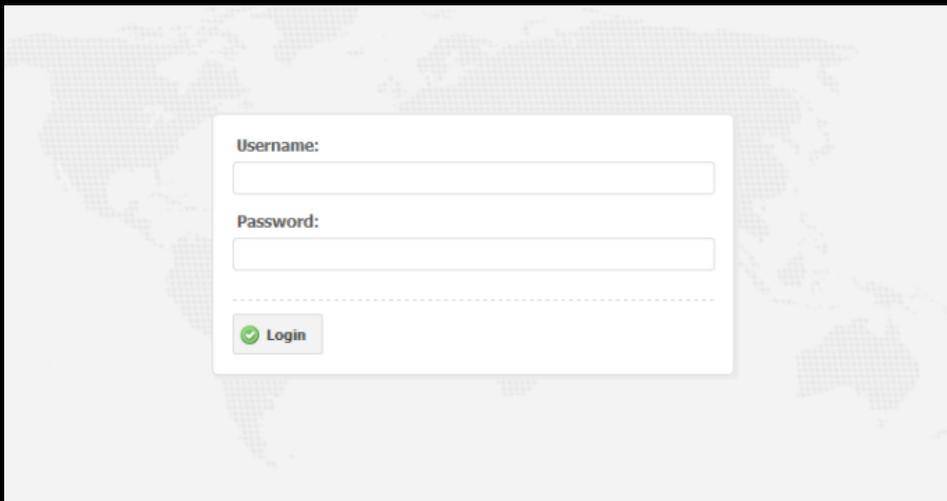


Benoît ANCEL
@benkow_



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

Members BrazzzzersFF

BrazzzzersFF
New Member, Male, 23
BrazzzzersFF was last seen: 27 Sep 2018

Profile Posts Recent Activity Postings Information Reputations

About

Gender: Male
Birthday: 5 Feb 1995 (Age: 23)

А ты купил абуроустойчивый хостинг от BraZZerS?
Такого еще не видели, реальная круглосуточная техническая поддержка!
Финансовый отдел (для заказа услуг):
Jabber: sales.brazzzzers@exploit.im
Telegram: @brazzzzers_sales (https://t.me/brazzzzers_sales)

Резервные контакты джабберов:
support.brazzzzers@exploit.im - круглосуточная техническая поддержка.
sales.brazzzzers@exploit.im - отдел заказов.
admin.brazzzzers@exploit.im - администрация.

Interact

Content: Find all content by BrazzzzersFF
Find all threads by BrazzzzersFF

Jabber: sales@brazzzzers.store

English (US)

- 3 different ways to communicate:

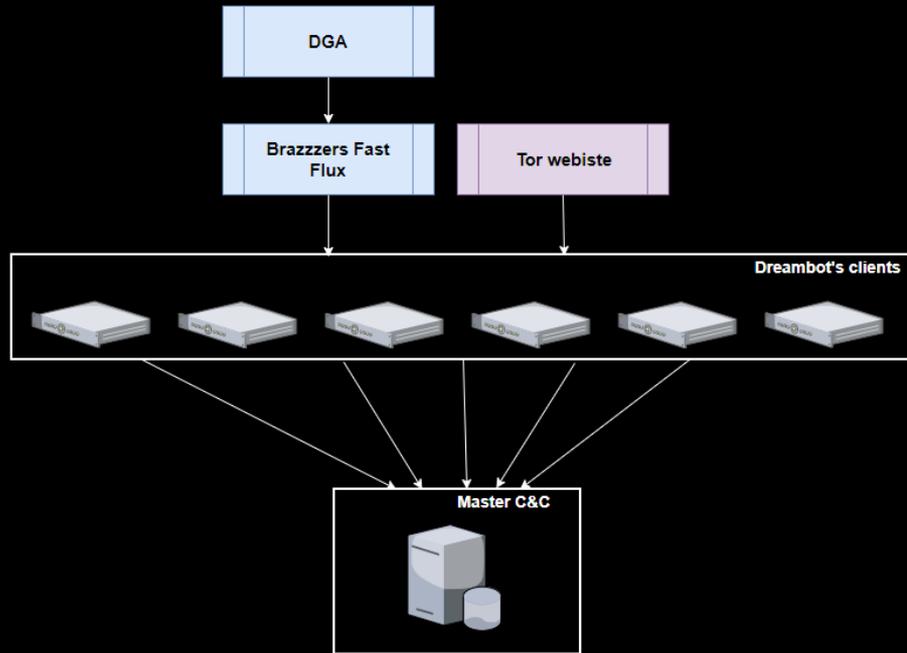
- Hard coded domains (BrazzzzersFF)
- DGA (BrazzzzersFF)
- Onion website

- Gozi features:

- Webinjects
- Keylogger
- FormGrabber
- email grabber
- Screenshots
- Socks
- VNC



Dreambot



- 2 kinds of C&C:

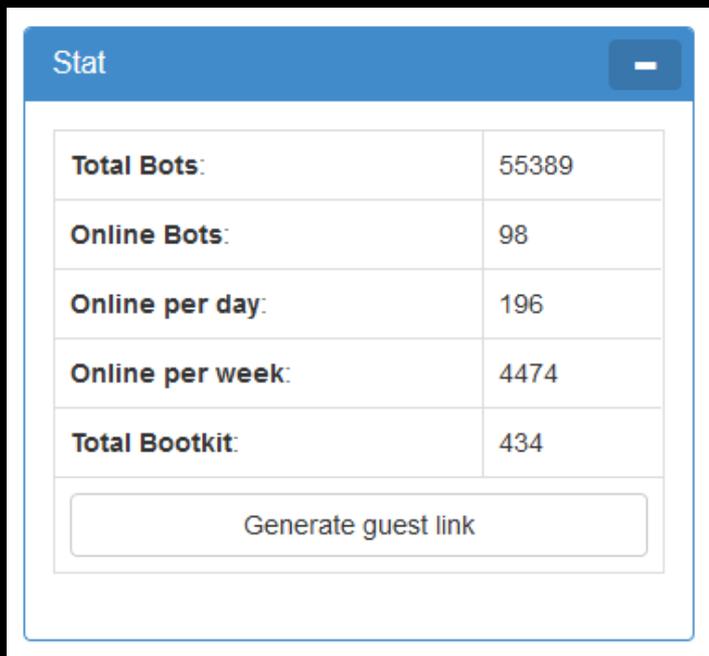
- Dreambot client's C&C
- "Master" C&C

- "Master" is used for:

- Bots storage
- Banks frauds
- Targeted attacks



Dreambot's client



The screenshot shows a dashboard titled "Stat" with a table of statistics and a button labeled "Generate guest link".

| | |
|-------------------------|-------|
| Total Bots: | 55389 |
| Online Bots: | 98 |
| Online per day: | 196 |
| Online per week: | 4474 |
| Total Bootkit: | 434 |

Generate guest link

- 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

Bots Loggers Parsers Total stat VNC Traffic filter AV Bot Jabber bot Users Logout

Stat

| | |
|------------------|-------|
| Total Bots: | 50116 |
| Online Bots: | 333 |
| Online per day: | 5626 |
| Online per week: | 28012 |
| Total Bootkit: | 0 |

Generate guest link

Config

Config File
Browse... No file selected.

Country Code
 Group ID

Send

| Current Configs | | | | | |
|-----------------|--------|---------|---|---|--|
| ID group | Loaded | Country | | | |
| 106 | 1131 | DE | - | ↺ | |
| 130 | 1 | CA | - | ↺ | |

Task

Task File
Browse... No file selected.

Country Code
 Group ID

Send

| Current Tasks | | |
|---------------|--------|---------|
| ID group | Loaded | Country |

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: 50106 rows

Prev 1 2 3 4 ... 5011 Next

| ID Bot | Group | Country | City | Version | Browser | OS | Status | IP | Reg | Comment | Sys |
|----------------------------------|-------|---------|--------|---------|-------------------|-------|--------|----|---------------------|---------|---------|
| 4f89490aab63e3efb7aa016c71a6313c | 140 | BR | Recife | 216994 | Internet Explorer | Win_7 | OK | | 2019-02-11 15:28:00 | | details |



Dreambot

Panel 2

Bots Loggers Parsers Total stat VNC Traffic filter AV Bot Jabber bot Users Logout

Statistics

| | | | | | |
|---------------------|---------------------------------|---------------------------------|----------------------------------|-------------------------------|--------------------------------|
| 56685 Total Bots | 108 0.19 % Current Online | 543 0.96 % Online Per Day | 951 1.68 % Online Per Week | 0 0.00 % Total Carantin | 437 0.77 % Total Bootkit |
|---------------------|---------------------------------|---------------------------------|----------------------------------|-------------------------------|--------------------------------|

Task & Config

Search

| | | | | | |
|----------------------|---------------|----------------------|--------------|----------------------|---------------|
| <input type="text"/> | ID Bot | <input type="text"/> | Organization | <input type="text"/> | Version soft |
| <input type="text"/> | ID group | <input type="text"/> | Ip address | <input type="text"/> | Comment |
| <input type="text"/> | Country | <input type="text"/> | City | <input type="text"/> | Browser |
| <input type="text"/> | Domain | <input type="text"/> | Network | <input type="text"/> | Process/Desc. |
| none | Last activity | none | OS type | 10 | Rows on page |

expand

Total: 56685 rows

Prev 1 2 3 4 ... 5669 Next

| ID Bot | Group | Country | City | Version | Browser | OS | IP | Reg | Comment | Sys |
|----------------------------------|--------|---------|-------|---------|-----------------------|------------|----|---------------------|-------------------|-------------------------|
| 36be59f710d5b5cc005832e95d67441f | 201810 | | | 216996 | Internet Explorer 8.0 | Win_8_1_64 | | 2018-12-27 14:12:38 | | details |
| 76b38b99f6a2c262765d189702d027a6 | 99999 | | Hanoi | 216996 | Internet Explorer 8.0 | Win_10_64 | | 2018-10-16 15:32:52 | | details |
| ae386533757045264d48071e9184e4 | 201810 | | | 216996 | Internet Explorer 8.0 | Win_7_64 | | 2018-11-22 03:09:16 | amz use 454141... | details |
| 29aa5d2a8ec87fed58d74a21305a8968 | 201810 | | Tokyo | 216996 | Internet Explorer 8.0 | Win_7 | | 2018-12-14 03:00:03 | | details |
| 130988880007050a10b4c0f17081704 | 201810 | | Tampa | 216996 | Internet Explorer 8.0 | Win_10_64 | | 2018-12-24 | | details |



Dreambot

Panel 3

ip, bot_id, @name, #hasi +

Statistics

Botnet since 3 months ago

63,733
Total bots

OS Versions

| OS | Total | Active |
|-------------|--------|--------|
| Win 7 x64 | 42,434 | — |
| Win 7 | 19,125 | — |
| XP | 1,228 | — |
| Win 10 x64 | 445 | — |
| Vista | 208 | — |
| Win 8.1 x64 | 145 | — |
| Win 10 | 74 | — |
| Win 8.1 | 25 | — |
| Unknown | 22 | — |
| Vista x64 | 10 | — |
| Win 8 | 9 | — |
| Win 8 x64 | 8 | — |

Browsers

| Browser | Total | Active |
|------------|--------|--------|
| Firefox 40 | 40,382 | — |
| IE 8 | 21,867 | — |
| n/a | 1,382 | — |
| IE 6 | 77 | — |
| Unknown | 19 | — |
| IE 7 | 5 | — |
| Chrome 69 | 1 | — |

Countries

| Country | Total | Active |
|---------------|--------|--------|
| Japan | 45,848 | — |
| Poland | 3,166 | — |
| Italy | 2,419 | — |
| Canada | 2,367 | — |
| Germany | 2,365 | — |
| United States | 2,312 | — |
| n/a | 1,677 | — |
| Australia | 1,456 | — |
| Spain | 918 | — |
| Vietnam | 286 | — |
| India | 173 | — |
| Indonesia | 95 | — |
| Russia | 80 | — |
| Philippines | 75 | — |

Servers

Manage +

| Name | Total | Active |
|------|-------|--------|
|------|-------|--------|

Top 10 domains

| Domain | Total | Active |
|------------------------------|--------|--------|
| iod5tem372udbzu2.onion | 61,538 | — |
| | 1,458 | — |
| promotionteam.ac.ug | 329 | — |
| meanwiusenoticepatent.online | 248 | — |
| otherwiseapache.online | 80 | — |
| theincludingte.online | 49 | — |
| tformlicensable.online | 31 | — |

Installs sources

| | |
|------|--------|
| 1000 | 1,102 |
| n/a | 62,631 |



Dreambot

The screenshot shows the 'Setup' page in the Dreambot interface. The top navigation bar includes tabs for Bots, Reports, Classics, Screens, Videos, Files, URLs, Groups, Servers, Triggers, Blocking, and Setup. A search bar on the right contains the text 'ip, bot_id, @name, #hasi'. The main content area is titled 'Setup' and 'Panel and botnet settings'. It features several configuration panels:

- Address books:** Includes an 'Export' button and a 'Date' field with two input boxes containing '2019-04-01'.
- Notifications:** Includes a 'Test' button, a status toggle set to 'Enabled', and fields for 'Server: xmpp.jp', 'Port: 5222', 'User:', 'Password:', and 'Send to:'.
- Bot modules:** A table listing various bot modules with their CRC values and last update times.
- Configuration:** A table listing configuration items with their CRC values and last update times.
- Socks backconnect:** Includes a refresh icon and a plus sign.

| 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 |

| CRC | Last update |
|----------|--------------|
| 1c9402b9 | 2 months ago |



Dreambot

Home Bots Reports Classics Screens Videos Files URLs Groups Servers Triggers Blocking Setup ip_bot_id,@name,#hasi +

Select preset - [trash icon]

Reports

1949910 items on 19500 pages

[refresh] [received] [up/down arrows] [100 per page]

Group: Any -

Country: Any -

Type: Formgrabber -

Date: 2019-01-04 2019-01-23

URL: wildcards (*) allowed [info]

Referrer: wildcards (*) allowed

Content: wildcards (*) allowed

IP: [input]

Bot: [input]

Online: Socks VNC

[Save preset] [Search]

| | | | | |
|--|------------------|-------------------------------------|------------|-------------------------|
| [+] | Jan 05, 17:03:19 | www.youtube.com/ad_data_204 | [redacted] | no group |
| [-] | Jan 03, 09:56:04 | collect.ptengine.jp/oc | [redacted] | 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 | | | | |
| <pre>{ "sid": "5508f6f8", "uid": "L06zofsx6sL9w1JQ2Hd0Yg", "vid": "j*9/ZYIilwaR92sHwH2pfw", "pid": "o8GJlmg1XYLq0109f4CjQ", "peid": "uew074UeVEXemLjyV3qaA", "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%280%29%3Ediv%3Aeq%281%29%3Eu1%3Aeq%280%29%3E%23none_on_click-3%3Espan%3Aeq%280%29%3Espan%3Aeq%280%29.0.1190.1816.3892.503.1538", "ptif": "2" }</pre> | | | | |
| [+] | Jan 03, 09:56:00 | collect.ptengine.jp/os | [redacted] | no group |
| [+] | Jan 03, 09:55:48 | collect.ptengine.jp/pv | [redacted] | no group |
| [+] | Jan 03, 09:55:47 | google.com/domainreliability/upload | [redacted] | no group |
| [+] | Jan 03, | collect.ptengine.jp/oc | [redacted] | no group |



Dreambot

Navigation: Home, Bots, Reports, Classics, Screens, Videos, Files, URLs, Groups, Servers, Triggers, Blocking, Setup

Search: ip, bot_id, @name, #hasi

Select feature:

- Bots analyzer
- Masks blacklist
- ISP blacklist**

ISP blacklist

60 items on 4 pages

Actions: + Import from file, Refresh, Created filter, Sort (up/down), 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 : // route extensions
const ENCRYPTI
const DECRYPTI
const USE_ZIP :
const VIDEOS_P
const ONLINE_T
// route extentions for download files
const PARSE_AC
const ExtConfig = 'jpeg';
const ExtTask = 'gif';
const ExtData = 'bmp';
const ExtBinary = 'ttf';
// bot writer decided to add vali is for tor only,
require_once('
// url is generated automatically, so i also need
// connect to
// to check for OS version, thank you author...
$mongo = new M
$db = $mongo->
const ExtTor = 'avi';

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

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

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

;
install.txt';

/server.conf';
enss1-1.0.0.cnf';

rey.exe';
;
ite.key';

's';
's';

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



Dreambot

Customer use case



Dreambot customer in Germany

The screenshot displays the Dreambot control panel with a navigation bar at the top containing: Bots, Loggers, Parsers, Total stat, VNC, Traffic filter, AV Bot, Jabber bot, Users, Logout.

Stat

| | |
|------------------|-------|
| Total Bots: | 22319 |
| Online Bots: | 274 |
| Online per day: | 577 |
| Online per week: | 4366 |
| Total Bootkit: | 0 |

Generate guest link

Config

Config File

No file selected.

Country Code

Group ID

Current Configs

| ID group | Loaded | Country | | |
|----------|--------|---------|---|---|
| 130 | 1 | CA | - | ↻ |
| 106 | 137 | CA | - | ↻ |
| 106 | 1919 | DE | - | ↻ |

- 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 | | 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 |
| ad69f14fdffa710d6cdb7ec5ebf37c1b | 10 | DE | Ennepetal | 216998 | Internet Explorer 8.0 | Win_10_64 | OFF | | 2019-03-18 20:40:48 | gp cant pay thru pp | details |
| 122a3b0e00f3a067ef82f90422982149 | 10 | DE | | 216998 | Internet Explorer 8.0 | Win_8.1_64 | OFF | | 2019-03-18 20:36:08 | chrome untouched | 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 |

Task

Task File
 No file selected.

Country Code

Current Task

| Time | Loaded | Country | |
|---------------------|--------|---------|---------------------|
| 2019-03-27 14:18:02 | yes | All | del |

Comment

pp wait pass

Dreambot

“Master” C&C



Dreambot

| Group | Country | City | Version | Browser | OS | IP | Reg | Comment | Sys |
|-------|---------|------------|---------|-----------------------|-----------------------|----|---------------------|-------------------|-------------------------|
| 1068 | US | Gig Harbor | 216989 | Internet Explorer 8.0 | Win_7_64 | | 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 customer 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 Буярац

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: | COOLBOX |
| 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

ETIAS, Malta!



Dreambot

Bot Info —

| | |
|---------------|-----------------------|
| OS: | Win_7_64 |
| Browser: | Internet Explorer 8.0 |
| Country: | KR |
| City: | |
| Organization: | SK Broadband |
| Version: | 216989 |
| IP: | ██████████ |
| AV | |

Comment —

neventure!!

Bot Info —

| | |
|---------------|-----------------------|
| OS: | Win_8.1_64 |
| Browser: | Internet Explorer 8.0 |
| Country: | KR |
| City: | Daegu |
| Organization: | Korea Telecom |
| Version: | 216989 |
| IP: | ██████████ |
| 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: | ██████████ |
| AV | |

Comment —

mini energy station



Dreambot

Bot Info -

| | |
|---------------|-----------------------|
| OS: | Win_7_64 |
| Browser: | Internet Explorer 8.0 |
| Country: | US |
| City: | Glen Eilyn |
| 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

biazhko.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

pollanskyi@mon.gov.ua +



Dreambot

Bot Info -

| | |
|----------------------|---|
| OS: | Win_7_64 |
| Browser: | Internet Explorer 8.0 |
| Country: | PL |
| City: | Sopot |
| Organization: | Naukowa I Akademyka Siec Komputerowa Instytut Bad |
| Version: | 216989 |
| IP: | [REDACTED] |
| AV: | |

Comment -

Naukowa I Akademyka 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 !

Search

ID Bot: Organization: Version soft:
ID group: Ip address: Comment:
Country: NL City: Browser:
Domain: Network: Process/Desc.:
Last activity: none OS type: none Rows on page: 10

expand

Total: 6 rows 1

| ID Bot | Group | Country | City | Version | Browser | OS | IP | Reg | Comment | Sys |
|----------------------------------|-------|---------|----------|---------|-----------------------|-----------------------|------------|---------------------|---------|-------------------------|
| 84958977acc2bd2175506f029e12e154 | 1050 | NL | Nunspeet | 216962 | Internet Explorer 8.0 | Win_7_64 | [REDACTED] | 2018-12-19 22:50:38 | | details |
| 18e989ac97d993e91ab15c0b269b3825 | 501 | NL | | 216994 | Internet Explorer 8.0 | Win_7 | [REDACTED] | 2018-12-28 12:49:04 | | details |
| f4db55478baa2c998520ff5223412086 | 500 | NL | | 216994 | Internet Explorer 8.0 | Win_XP | [REDACTED] | 2019-01-29 09:26:48 | | details |
| ce4acade6dd0aad3b7aa016ca183837e | 200 | NL | | 216994 | Internet Explorer 8.0 | Win_7_64 | [REDACTED] | 2019-01-14 17:31:13 | | details |
| ce4acade6dd0aad3b7aa016ceef62f0c | 300 | NL | | 216994 | Internet Explorer 8.0 | Win_7_64 | [REDACTED] | 2019-01-11 13:50:59 | | details |
| ba15df5cbf5669a20f2219a456deb217 | 200 | NL | | 216994 | Chrome 4.0 | Intel Mac OS X 10_5_8 | [REDACTED] | 2018-12-19 15:16:21 | | details |



#TheSAS2019

Let's Talk?

pk@csis.dk

PGP-ID: 0x715FB4BD

