WastedLoader or DridexLoader?

Jason Reaves

May 31, 2021

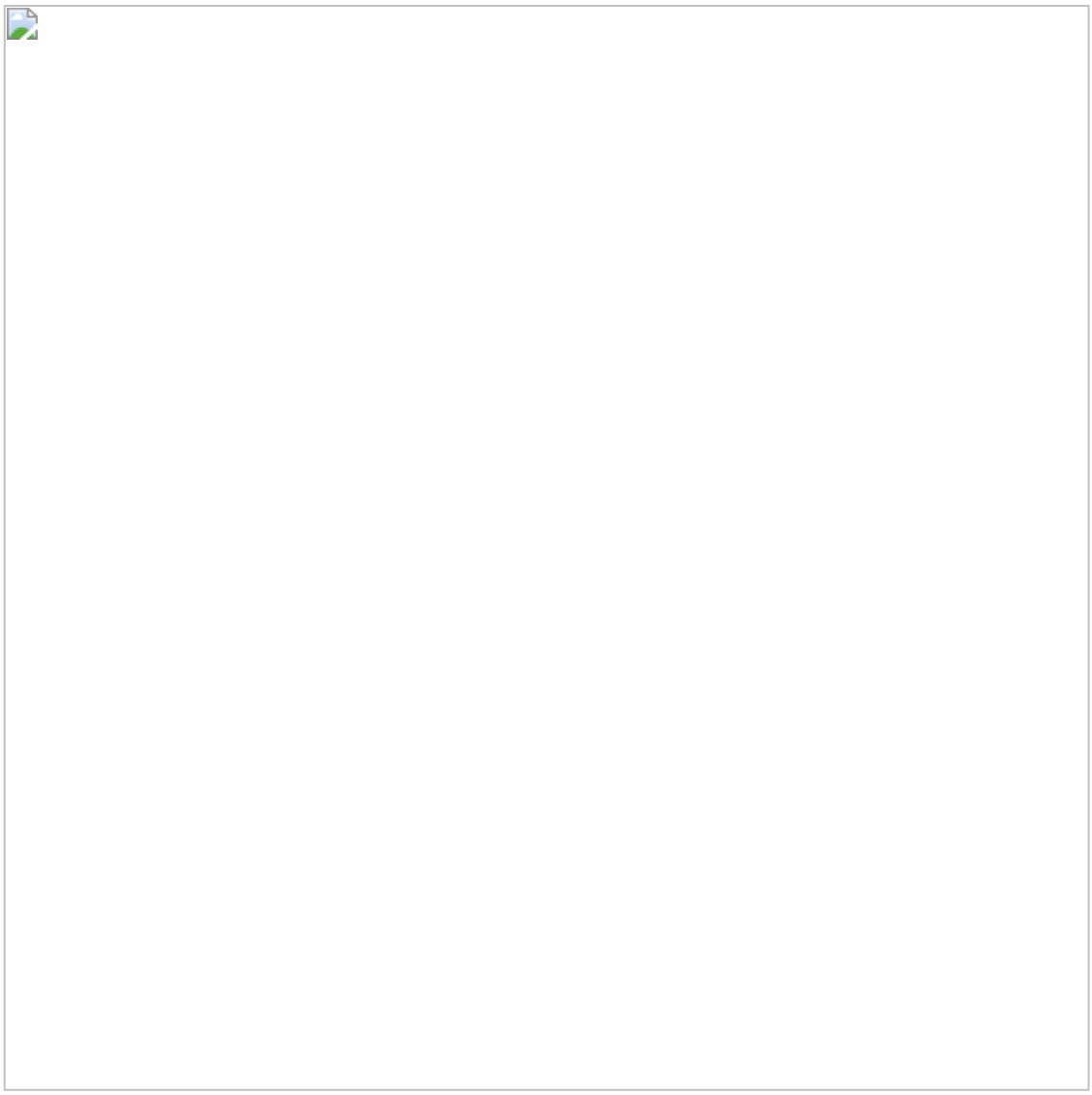
.

3 min read

By: Jason Reaves and Joshua Platt

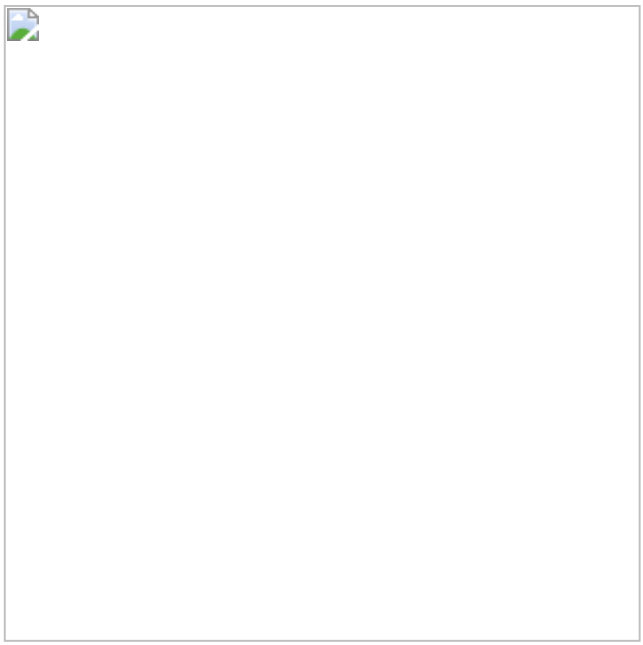
Recent BitDefender wrote up a very detailed report on a loader that shares similarities with WastedLocker being delivered via RIG exploit kit[1]. At the time I was researching Dridex chains and since WastedLocker has code similarities with Dridex[2] and being leveraged by EvilCorp[2,3,4,5,6] I took a quick look at the hashes from the report.

Of the hashes from the report only 1 seems publicly available, 6ee2138d5467da398e02afe2baea9fbe. In the BitDefender report they reference an overlap with WastedLocker in what they label as ‘layer1’, this is actually the crypter layer meaning if the crypter is private to one group then the overlap will show up in known malware associated with this group.

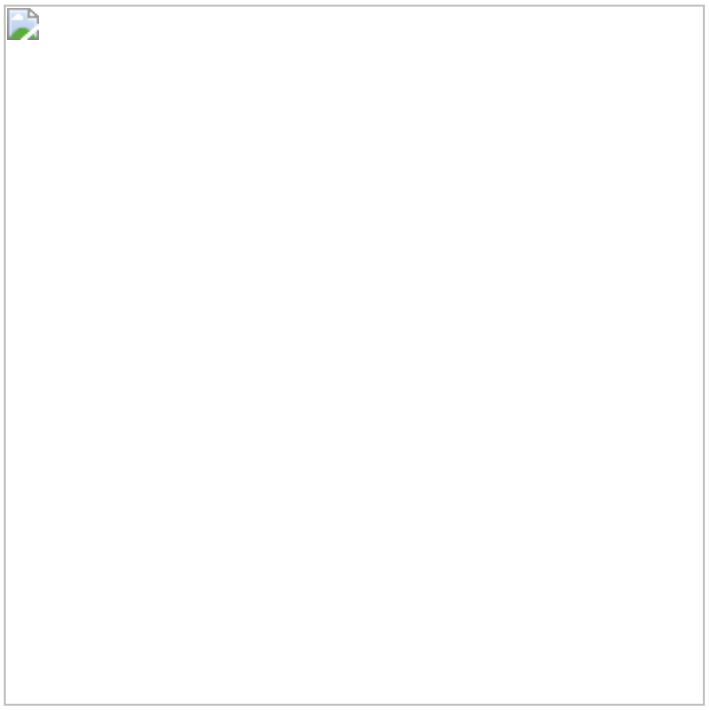


Crypter Registry Check

After unpacking the malware we are left with a sample that lines with the BitDefender report but some of the characteristics also line up with other the other malware families associated with this group such as the love of hiding RC4 encrypted strings using a 40 byte key that is reversed which is also used by Dridex and DoppelPaymer.



Copy key and reverse it



RC4

After beginning to decode some of the strings I started to notice that itlooks more and more like a Dridex Loader. Small snippet of decoded strings below:

```
Starting
path:ShellFolderv0vajEOvEWKQf2dajlupVdyIEZlAQX1T7H994Q;HJPM4qNHuqGU3XeDOkMccS1IZyjev70FC
 xmlns="" version="1.3"><RegistrationInfo></RegistrationInfo><Triggers><LogonTrigger>
<Enabled>true</Enabled><UserId>ROOT\CIMV2SELECT * FROM Win32_Fan*.dll*.exeProgram
ManagerProgmanAdvApi32~PsApi~shlwapi~shell32~WinInet/run /tn "%ws""%ws" /grant:r
"%ws":F\NTUSER.DATwinsxsx86_*amd64_**.exe\Sessions\%d\BaseNamedObjects\SOFTWARE/TrendMic
```

So I decided to check if the CAPE sandbox yara rule perhaps matches this unpacked sample as a Dridex Loader[7], I used the rule from the CAPE decoder and it hit on the unpacked sample. Along with the decoder being about to decode out the Dridex Loader config I believe it is safe to say this is the Dridex Loader, leaving one to guess whether the other two samples are also Dridex Loaders or not?

```
{'C2': ['51.68.224.245:4646', '188.165.17.91:8443', '173.255.246.77:691'], 'RC4_Key':
'v0vajEOvEWKQf2dajlupVdyIEZlAQX1T7H994Q', 'BOTNET': '10111'}
```

References

1:https://www.bitdefender.com/files/News/CaseStudies/study/397/Bitdefender-PR-Whitepaper-RIG-creat5362-en-EN.pdf

2:https://blog.fox-it.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/

3:https://www.wired.com/story/alleged-russian-hacker-evil-corp-indicted/

4:https://home.treasury.gov/news/press-releases/sm845

5:https://www.bellingcat.com/news/uk-and-europe/2020/02/17/v-like-vympel-fsbs-secretive-department-v-behind-assassination-of-zelimkhan-khangoshvili/

6:https://www.rferl.org/a/in-lavish-wedding-photos-clues-to-an-alleged-russian-cyberthief-fsb-family-ties/30320440.html

7:https://github.com/kevoreilly/CAPEv2/blob/1e66d2460276b28b45bea8123cc74daa83295f68/modules/processing/parsers/mwcp/DridexLoader.py