WastedLoader or DridexLoader?

By Jason Reaves

Published: 2021-05-31 · Archived: 2026-04-05 21:59:05 UTC

3 min read

May 31, 2021

By: Jason Reaves and Joshua Platt

Press enter or click to view image in full size

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.

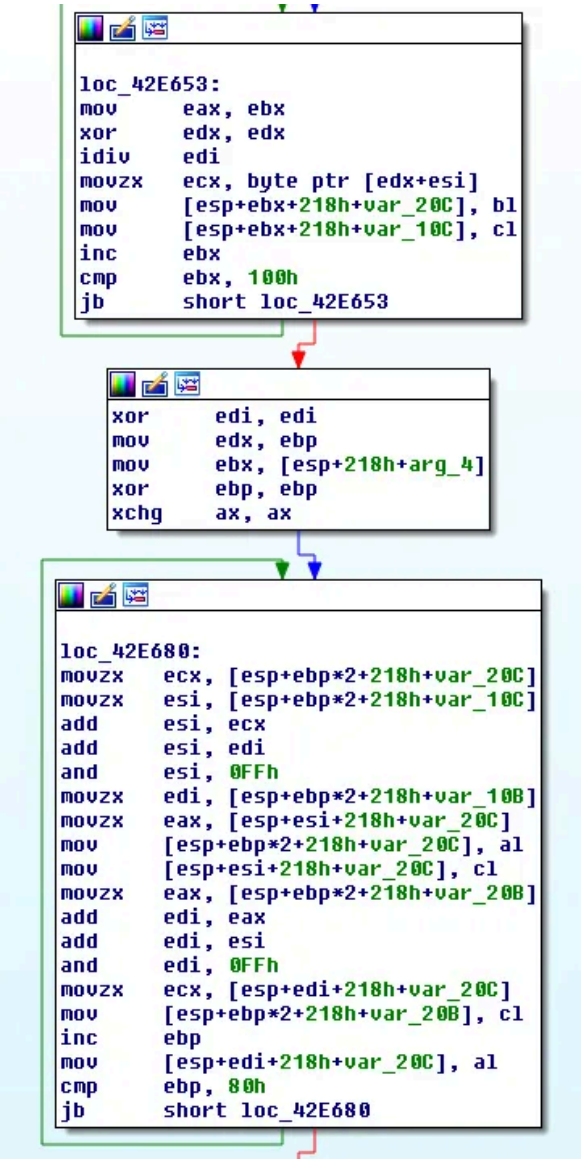
```
Check_Registry_Key_for_UCOMIEnumConnections_4011E0 proc near

var_8= dword ptr -8
var_4= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 8
mov     [ebp+var_8], offset aVcg6pk5fqdzqx3 ; "Vcg6pk5FQdzqX3917a2ISJus
mov     eax, 0BDh
mov     ecx, [ebp+var_8]
mov     [ecx], ax
mov     edx, [ebp+var_8]
movzx   eax, word ptr [edx]
sub     eax, 54h
mov     ecx, [ebp+var_8]
mov     [ecx], ax
mov     edx, 0C2h
mov     eax, [ebp+var_8]
mov     [eax+2], dx
mov     ecx, [ebp+var_8]
movzx   edx, word ptr [ecx+2]
sub     edx, 54h
```

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.

```
mov     ecx, ebp
push    2800h
mov     esi, edx
call    sub_418810
push    28h
mov     ebx, [ebp+0]
xor     edx, edx
push    esi
lea     ecx, [esp+3Ch+var_20]
mov     [ebx], dx
call    CopyData_429470
push    0
lea     ecx, [esp+38h+var_20]
call    GetBuffAddress_429640
mov     [esp+34h+var_34], eax
lea     ecx, [esp+34h+var_20]
call    GetBufLength_429650
mov     edx, eax
mov     ecx, [esp+34h+var_34]
call    ReverseString_42E780
mov     [esp+34h+var_30], ebx
xor     ebx, ebx
xor     edx, edx
cmp     edi, 1
```

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:
ShellFolder
v0vajEOvEWKQf2dajlupVdyIEZlAQX1T7H994Q;HJPM4qNHuqGU3XeDOkMccS1IZyjev70FCelRDHTXLJszFZqshgVlsiV27SrJbCO3LMap
<autoElevate>true
true
false
<Task xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task" version="1.3"><RegistrationInfo>
</RegistrationInfo><Triggers><LogonTrigger><Enabled>true</Enabled><UserId>
ROOT\CIMV2
SELECT * FROM Win32_Fan
*.dll
*.exe
Program Manager
Progman
AdvApi32~PsApi~shlwapi~shell32~WinInet
/run /tn "%ws"
"%ws" /grant:r "%ws":F
```

```
\NTUSER.DAT
winsxs
x86_*
amd64_*
*.exe
\Sessions\%d\BaseNamedObjects\
SOFTWARE/TrendMicro/Vizor\VizorUniclientLibrary.dllProductPath
```

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': 'v0vajEOvEWKQf2dajlupVd
```

References

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

Get Jason Reaves's stories in your inbox

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/DridexJ
