

Lockbit 3.0 AKA Lockbit Black is here, with a new icon, new ransom note, new wallpaper, but less evasiveness?

blog.minerva-labs.com/lockbit-3.0-aka-lockbit-black-is-here-with-a-new-icon-new-ransom-note-new-wallpaper-but-less-evasiveness



- [Tweet](#)
-

This month the Lockbit ransomware gang announced their first Bug Bounty program as part of their evolution into Lockbit 3.0. A first sample of the new version was published by [Arda Büyükkaya](#). According to their new ransomware wallpaper that appears after encryption, this specific version has been named ‘Lockbit Black’, which interestingly follows their new execution method which is pretty similar to the BlackCat ransomware execution method. There are actually even more similarities between the two ransomwares.

Lockbit Black - Execution

The new Lockbit ransomware requires a “pass” to be supplied as a parameter upon execution, Similar to BlackCat with requires an “access-token”. The “pass” for the published sample was also provided by [Arda Büyükkaya](#):



Figure 1 - The execution command

Lockbit Black – Packer and dynamic imports

Lockbit Black is well packed, and its imports table is almost empty. Most API functions calls are resolved dynamically by calling a trampoline function which decrypts the API function using XOR encryption:

```
sub_7636A8 proc near
mov     eax, 33F5555Ah
xor     eax, 4506DFCAh
jmp     eax
sub_7636A8 endp
```

Figure 2 - Trampoline function performing XOR encryption

Lockbit Black – UAC bypass

When executing without Admin privileges, Lockbit Black (much like its previous versions) performs a CMSTPLUA COM UAC bypass.

Lockbit Black – Service Delete and Process Termination

Lockbit Black enumerates services and processes against a pre-defined “Blacklist”. The new version however has a much shorter list than its predecessors. The list is effectively a “Blacklist”, and all services that appear in the list are designated to be either deleted. The

service list of the new version seems like a combined and shorter version of the services that were previously deleted by Lockbit and BlackCat together and contains:

1. vss
2. sql
3. svc\$
4. memtas
5. mepocs
6. msexchange
7. sophos
8. veeam
9. backup
10. GxVss
11. GxBlr
12. GxFWD
13. GxCVD
14. GxCIMgr

```
push    1Ch
push    0
lea     eax, [ebp+var_30]
push    eax
call    j_ntdll_memset
add     esp, 0Ch
lea     eax, [ebp+var_30]
push    eax
push    1
push    [ebp+var_8]
call    j_advapi32_ControlService
push    [ebp+var_8]
call    j_advapi32_DeleteService
push    [ebp+var_8]
call    j_advapi32_CloseServiceHandle
```

Figure 3 - Service deletion by Lockbit Black

The new Lockbit also uses the same method to terminate a number of processes if they are found to be running on victim's PC:

1. sql
2. oracle
3. ocssd
4. dbsnmp
5. synctime
6. agntsvc
7. isqlplussvc
8. xfssvccon
9. mydesktopservice

10. ocautoupds
11. ncsvc
12. firefox
13. tbirdconfig
14. mydesktopqos
15. ocomm
16. dbeng50
17. sqbcoreservice
18. excel
19. infopath
20. msaccess
21. mspub
22. onenote
23. outlook
24. powerpnt
25. steam
26. thebat
27. thunderbird
28. visio
29. winword
30. wordpad
31. notepad

```

exe:00409D8D push    1
exe:00409D8F lea    eax, [ebp+var_4]
exe:00409D92 push    eax
exe:00409D93 call   j_ntdll_NtOpenProcess
exe:00409D99 test   eax, eax
exe:00409D9B jnz    short loc_409DB1

e:00409D9D push    0
e:00409D9F push    [ebp+var_4]
e:00409DA2 call   j_ntdll_NtTerminateProcess
e:00409DA8 push    [ebp+var_4]
e:00409DAB call   j_ntdll_NtClose

```

Figure 4 - Process Termination

Lockbit Black – Default language check

Previous versions of the Lockbit ransomware performed a default language check on the system and the current user through the Windows API calls `GetSystemDefaultUILanguage` and `GetUserDefaultUILanguage`. If the language code identifier matched the one specified, the program shuts down. The new version seems to extend the country list to also include Syria:

New Version

419 – Russian

422 – Ukrainian

423 – Belarusian

428 – Tajik

42B - Armenian

42C – Azerbaijani (Latin)

437 – Georgian

43F – Kazakh

440 – Kyrgyz

442 – Turkmen

443 – Uzbek (Latin)

444 – Tatar

818 - Romanian (Moldova)

819 - Russian (Moldova)

82C – Azerbaijani (Cyrillic)

843 - Uzbek (Cyrillic)

2801 - Arabic (Syria)

Lockbit Black – Mutex

Lockbit Black creates a “2cae82bd1366f4e0fdc7a9a7c12e2a6b” mutex.

Lockbit Black – New icon, wallpaper and ransom note

Lockbit's Black's icon, wallpaper and ransom note were updated in the new version:

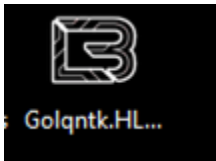


Figure 5 - Lockbit Black icon



Figure 6 - Lockbit Black wallpaper

```
HLNkAqREADME.txt - Notepad
File Edit Format View Help
LockBit 3.0 the world's fastest and most stable ransomware from 2019

>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors
at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Tor Browser Links:
http://lockbitapt2d73kr1bewgv27tquljgr33xbwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt71chwejug47kmvqavvvpqkewv413az13gy6pyd.onion
http://lockbitapt34kvr1p6xojy1ohhxwsvpzdffgs524pobssywnzsb0gugd.onion
http://lockbitapt5x4zkjbcqz16rdhccagqadevy1wqwkkspn11dyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwggglawtr3a35nygvokja5uucc1p4kykd.onion
http://lockbitapt72bu5n1gnapymggskg5yp75ny7r1rtdg4e714zartsbqd.onion
http://lockbitaptawj16udhd323uehekiyatj6ftcmkwe5sers4faggjpid.onion
http://lockbitaptbdiajqtalcr1gzzgfpjrwgkku63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc21q4atewz21se62q63ufktyr14qtwk5qax262kgrtjgd.onion

Links for normal browser:
http://lockbitapt2d73kr1bewgv27tquljgr33xbwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt71chwejug47kmvqavvvpqkewv413az13gy6pyd.onion.ly
http://lockbitapt34kvr1p6xojy1ohhxwsvpzdffgs524pobssywnzsb0gugd.onion.ly
http://lockbitapt5x4zkjbcqz16rdhccagqadevy1wqwkkspn11dyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwggglawtr3a35nygvokja5uucc1p4kykd.onion.ly
http://lockbitapt72bu5n1gnapymggskg5yp75ny7r1rtdg4e714zartsbqd.onion.ly
http://lockbitaptawj16udhd323uehekiyatj6ftcmkwe5sers4faggjpid.onion.ly
http://lockbitaptbdiajqtalcr1gzzgfpjrwgkku63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc21q4atewz21se62q63ufktyr14qtwk5qax262kgrtjgd.onion.ly

>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than
money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation
simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest
services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after you
pay, no one will pay us in the future. You can get more information about us on Elon Musk's Twitter https://twitter.com/hashtag/lockbit?live

>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one will know about, tell it in the
chat, we will generate a secret chat for you and give you his ID via private one-time memos service, no one can find out this ID but you. Sometimes you will have to wait some time
for our reply, this is because we have a lot of work and we attack hundreds of companies around the world.

Tor Browser Links for chat:
http://lockbitsupa7a3b4pkn4gkgojr151qgx24c1bzc4m716jeetsia3qd.onion
http://lockbitsupawon76nzykzblcp1ixut4n42oecugz20xabtaoqvmzqgd.onion
http://lockbitsupn2h6be2cnqvmcyh54ngmwn44633hnzzwtxdrjoq1p7yd.onion
http://lockbitsupo7vv5vc13jxpsdv1oqvvas1jgcstymefh60za7c6xjad.onion
http://lockbitsupq3g2dn12f36snrdb4n5qzqvovotkt5xfw3draxk8gugd.onion
http://lockbitsuofvac1dr6uot6n9hv1ou1vaab1ubuvavx16xv3f8thvr3vd.onion
```

Figure 7 - Part of the new ransom note

The new ransom note comes in the form of a text file and contains a reference to Elon Musk's Twitter (Ilon Musk), but with a link to a more generic #lockbit hashtag page on Twitter.

There are several chat list URLs added to the link which lead to several Lockbit Darknet websites.

Lockbit Black – hiding threads from the debugger

Hiding threads from the debugger is not a new behavior for Lockbit but it has increased usage in the new version. The thread hiding is performed by calling the NtSetInformationThread API with the undocumented value THREAD_INFORMATION_CLASS::ThreadHideFromDebugger (0x11):

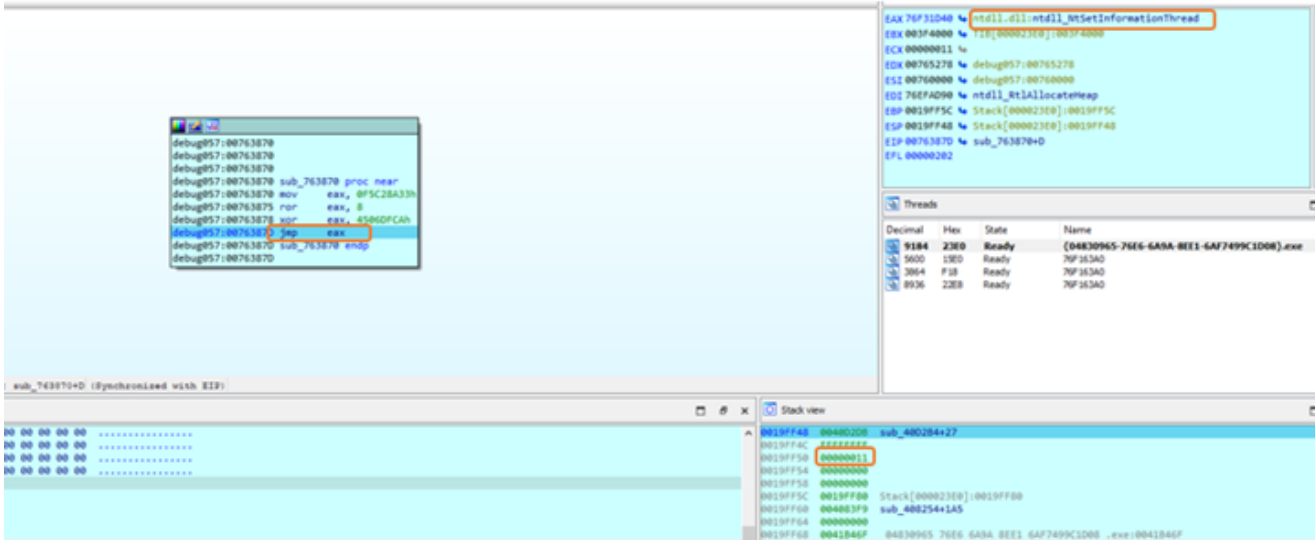


Figure 8 - hiding thread from the debugger

Lockbit Black –Windows Defender Log tampering

In order to disable Windows Defender logs, Lockbit Black sets 'HKLMSoftware\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Windows Defender\Operational\Enabled' to '0' as well changing the 'ChannelAccess' to '(O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)'.

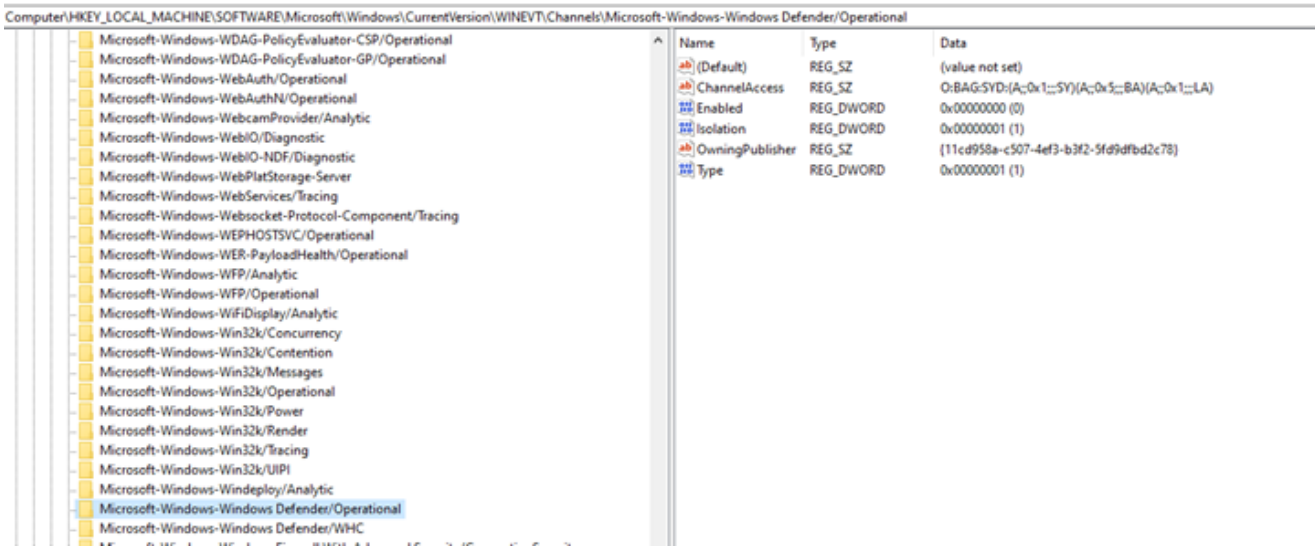


Figure 9 - Windows Defender Log Disabled

As in most ransomware cases the encryption is performed by several threads for faster and efficient work.

Minerva Lockbit 3.0 Prevention of the UAC bypass

Minerva customers don't need to worry, as many of Minerva's modules block Lockbit Black in its earliest stages, including the UAC Bypass stage, shutting it down completely before the encryption stage even begins.

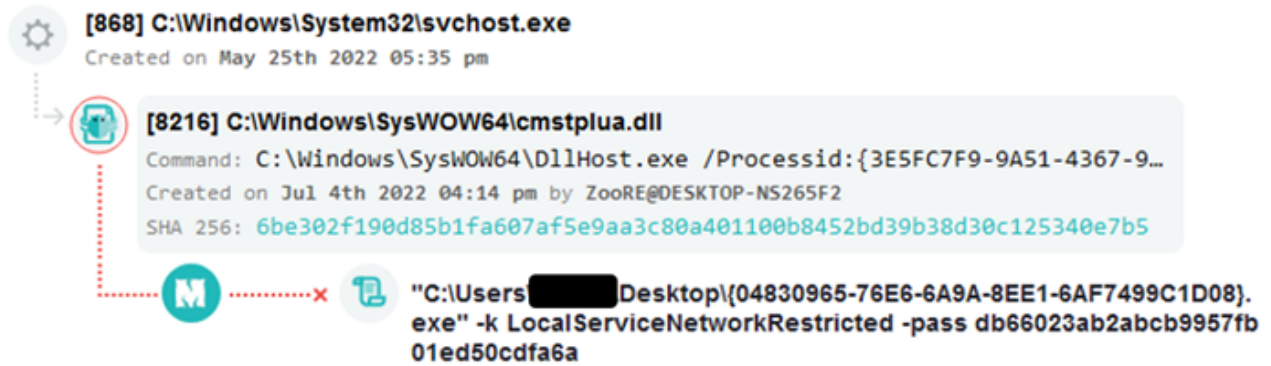


Figure 10 - UAC bypass prevention by Minerva