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

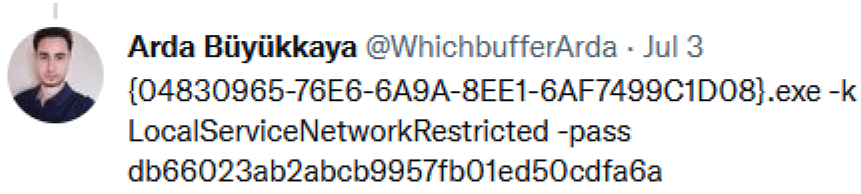
blog.minerva-labs.com/lockbit-3.0-aka-lockbit-black-is-here-with-a-new-icon-new-ransom-note-new-wallpaper-but-less-evasiveness

- 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:



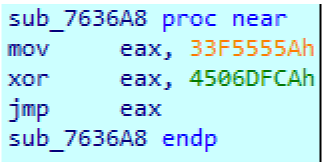
Arda Büyükkaya @WhichbufferArda · Jul 3

{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe -k LocalServiceNetworkRestricted -pass db66023ab2abcb9957fb01ed50cdfa6a

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

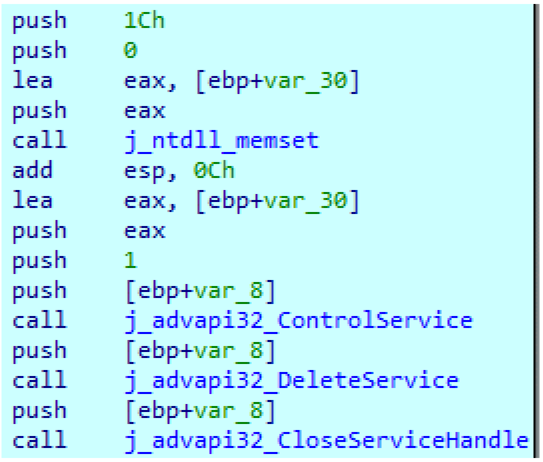
Lockbit Black – UAC bypass

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



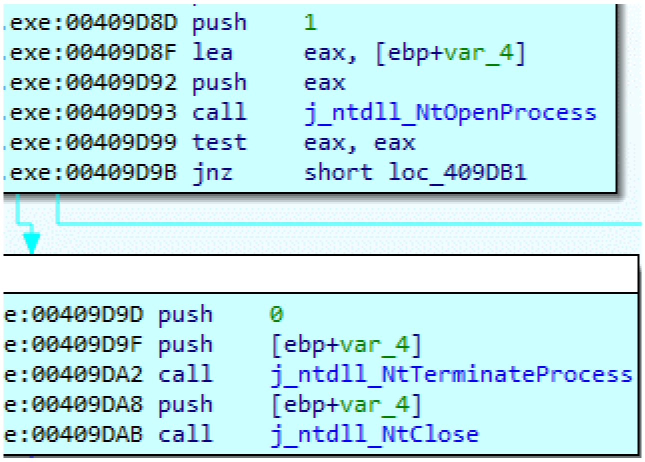
```
push    1Ch
push    0
lea     eax, [ebp+var_30]
push    eax
call    j_ntdll_memset
add     esp, 0Ch
lea     eax, [ebp+var_30]
push    eax
push    1
push    [ebp+var_8]
call    j_advapi32_ControlService
push    [ebp+var_8]
call    j_advapi32_DeleteService
push    [ebp+var_8]
call    j_advapi32_CloseServiceHandle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

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:

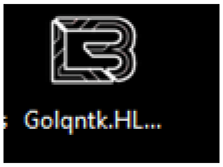
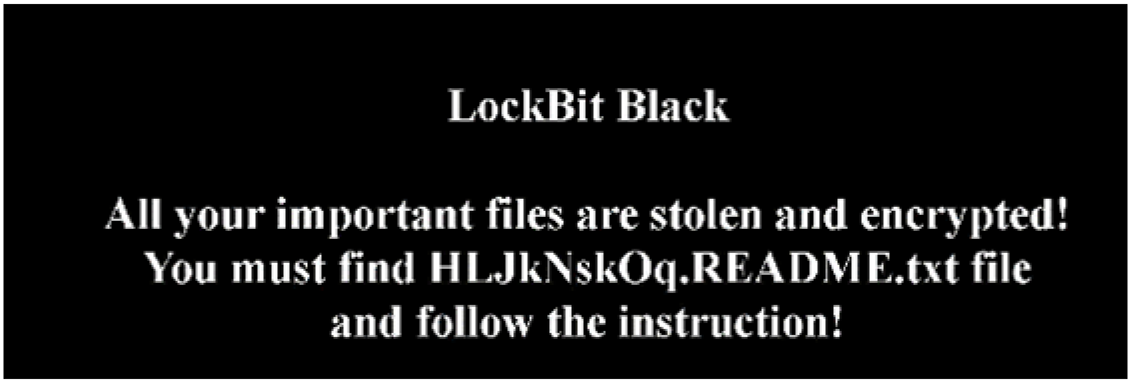


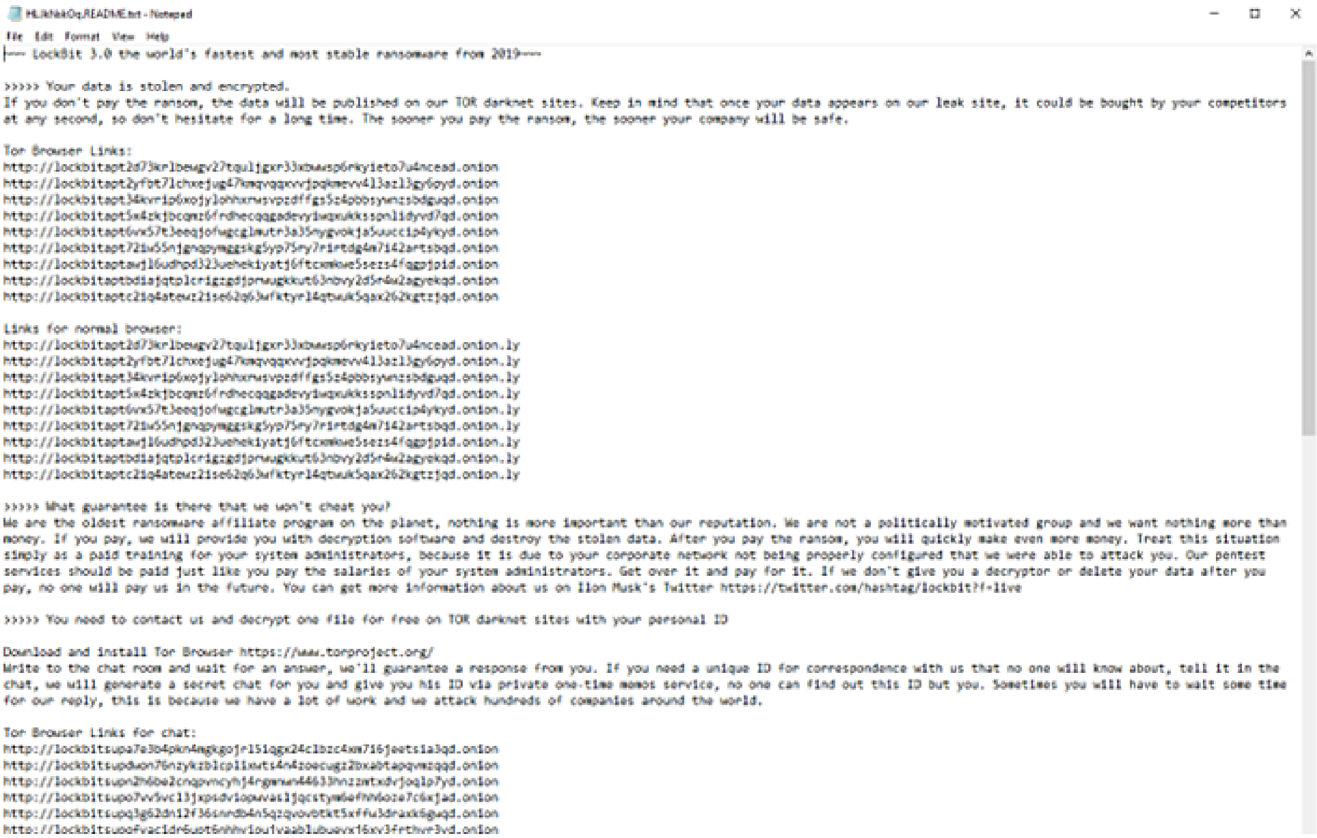
Figure 5 - Lockbit Black icon



LockBit Black

All your important files are stolen and encrypted!
You must find HLJkNskOq.README.txt file
and follow the instruction!

Figure 6 - Lockbit Black wallpaper



```
~~~ 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://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.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 Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=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://lockbitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd.onion
http://lockbitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd.onion
http://lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd.onion
http://lockbitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad.onion
http://lockbitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd.onion
http://lockbitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd.onion
```

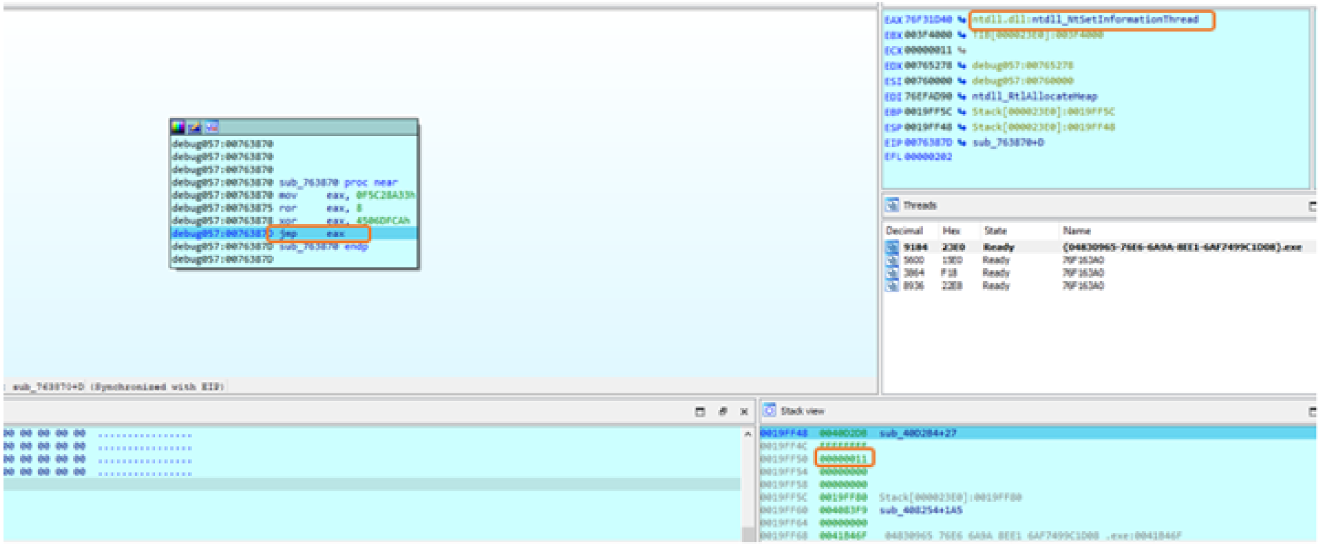
Figure 7 - Part of the new ransom note

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 is 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):



```
debug057:00763870
debug057:00763870
debug057:00763870
debug057:00763870 sub_763870 proc near
debug057:00763870 mov     eax, 0F5C28A33h
debug057:00763875 ror     eax, 8
debug057:0076387A xor     eax, 4506DFCAh
debug057:0076387D jmp     eax
debug057:0076387D sub_763870 endp
debug057:0076387D
```

```
sub_763870+D (Synchronized with EIP)
```

```
EAX 76F31D40 ↳ ntdll.dll:ntdll_NtSetInformationThread
EBX 003F4000 ↳ TIB[000023E0]:003F4000
ECX 00000011 ↳
EDX 00765278 ↳ debug057:00765278
ESI 00760000 ↳ debug057:00760000
EDI 76EFAD90 ↳ ntdll_RtlAllocateHeap
EBP 0019FF5C ↳ Stack[000023E0]:0019FF5C
ESP 0019FF48 ↳ Stack[000023E0]:0019FF48
EIP 0076387D ↳ sub_763870+D
EFL 00000202
```

Decimal	Hex	State	Name
9184	23E0	Ready	(04830965-76E6-6A9A-8EE1-6AF7499C1D08).exe
5600	15E0	Ready	76F163A0
3864	F18	Ready	76F163A0
8936	22E8	Ready	76F163A0

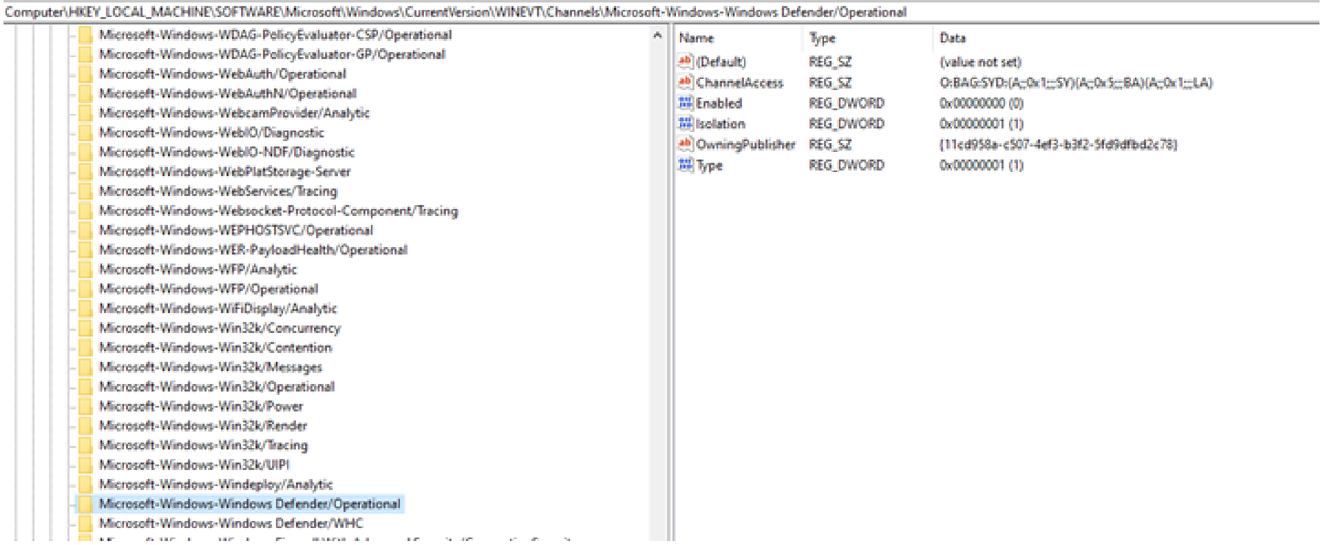
```
00 00 00 00 00  ................
00 00 00 00 00  ................
00 00 00 00 00  ................
00 00 00 00 00  ................
```

```
0019FF48  004002D8  sub_4002B4+27
0019FF4C  FFFFFFFF
0019FF50  00000011
0019FF54  00000000
0019FF58  00000000
0019FF5C  0019FF80  Stack[000023E0]:0019FF80
0019FF60  004003F9  sub_400254+1A5
0019FF64  00000000
0019FF68  0041846F   04830965 76E6 6A9A 8EE1 6AF7499C1D08 .exe:0041846F
```

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)’.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Windows Defender/Operational

Microsoft-Windows-WDAG-PolicyEvaluator-CSP/Operational
Microsoft-Windows-WDAG-PolicyEvaluator-GP/Operational
Microsoft-Windows-WebAuth/Operational
Microsoft-Windows-WebAuthN/Operational
Microsoft-Windows-WebcamProvider/Analytic
Microsoft-Windows-WebIO/Diagnostic
Microsoft-Windows-WebIO-NDF/Diagnostic
Microsoft-Windows-WebPlatStorage-Server
Microsoft-Windows-WebServices/Tracing
Microsoft-Windows-Websocket-Protocol-Component/Tracing
Microsoft-Windows-WEPHOSTSVC/Operational
Microsoft-Windows-WER-PayloadHealth/Operational
Microsoft-Windows-WFP/Analytic
Microsoft-Windows-WFP/Operational
Microsoft-Windows-WiFiDisplay/Analytic
Microsoft-Windows-Win32k/Concurrency
Microsoft-Windows-Win32k/Contention
Microsoft-Windows-Win32k/Messages
Microsoft-Windows-Win32k/Operational
Microsoft-Windows-Win32k/Power
Microsoft-Windows-Win32k/Render
Microsoft-Windows-Win32k/Tracing
Microsoft-Windows-Win32k/UIPI
Microsoft-Windows-Windeploy/Analytic
Microsoft-Windows-Windows Defender/Operational
Microsoft-Windows-Windows Defender/WHC

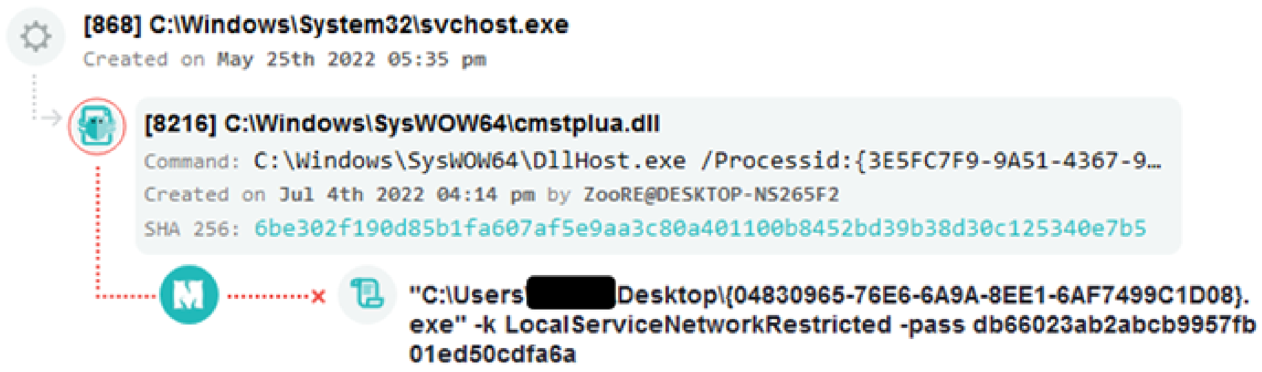
Name	Type	Data
(Default)	REG_SZ	(value not set)
ChannelAccess	REG_SZ	O:BAG:SYD:(A;;0x1;;;SY)(A;;0x5;;;BA)(A;;0x1;;;LA)
Enabled	REG_DWORD	0x00000000 (0)
Isolation	REG_DWORD	0x00000001 (1)
OwningPublisher	REG_SZ	{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
Type	REG_DWORD	0x00000001 (1)

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.



```
[868] C:\Windows\System32\svchost.exe
Created on May 25th 2022 05:35 pm

[8216] C:\Windows\SysWOW64\cmstplua.dll
Command: C:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9…
Created on Jul 4th 2022 04:14 pm by ZooRE@DESKTOP-NS265F2
SHA 256: 6be302f190d85b1fa607af5e9aa3c80a401100b8452bd39b38d30c125340e7b5

"C:\Users[redacted]Desktop\{04830965-76E6-6A9A-8EE1-6AF7499C1D08}.exe" -k LocalServiceNetworkRestricted -pass db66023ab2abcb9957fb01ed50cdfa6a
```

Figure 10 - UAC bypass prevention by Minerva