

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 fee 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:
3065889A0C515D2F8124D645906F5D3DA5C897CEBA875959AE4F95302A04E1D709C3C4AE9B7
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://lockbit2.0@tvg573eagfnwqjgmuib3a35mgvokja5uacscj4dyhpl.onion>

LOCKBIT 2.0 RANSOMWARE

Malware Analysis Report

Theodoros Vergos "cde"

Table of Contents

Executive Report	2
Yara Rule.....	3
High Level Technical Summary.....	4
Static Analysis.....	8
Basic Static Analysis	8
Wide ASCII strings (UTF-16):	8
Tight/encoded strings:	9
Advanced Static Analysis.....	10
Dynamic Analysis	11
Basic Dynamic Analysis	11
Advanced Dynamic Analysis:.....	17

Executive Report

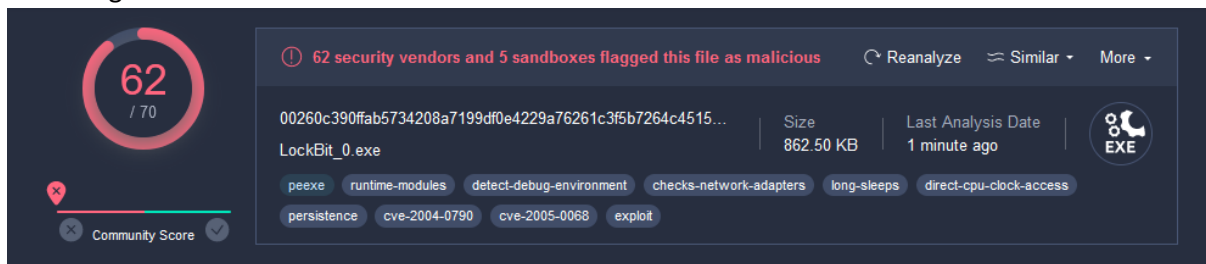
Malware Family	LOCKBIT 2.0 Ransomware
MD5	96de05212b30ec85d4cf03386c1b84af
SHA1	dbe5243c6ea5cc4cfb3edf042bd94a59cf9a0e64
SHA256	00260c390ffab5734208a7199df0e4229a76261c3f5b7264c4515acb8eb9c2f8
Architecture	x86

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.



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)
}

```

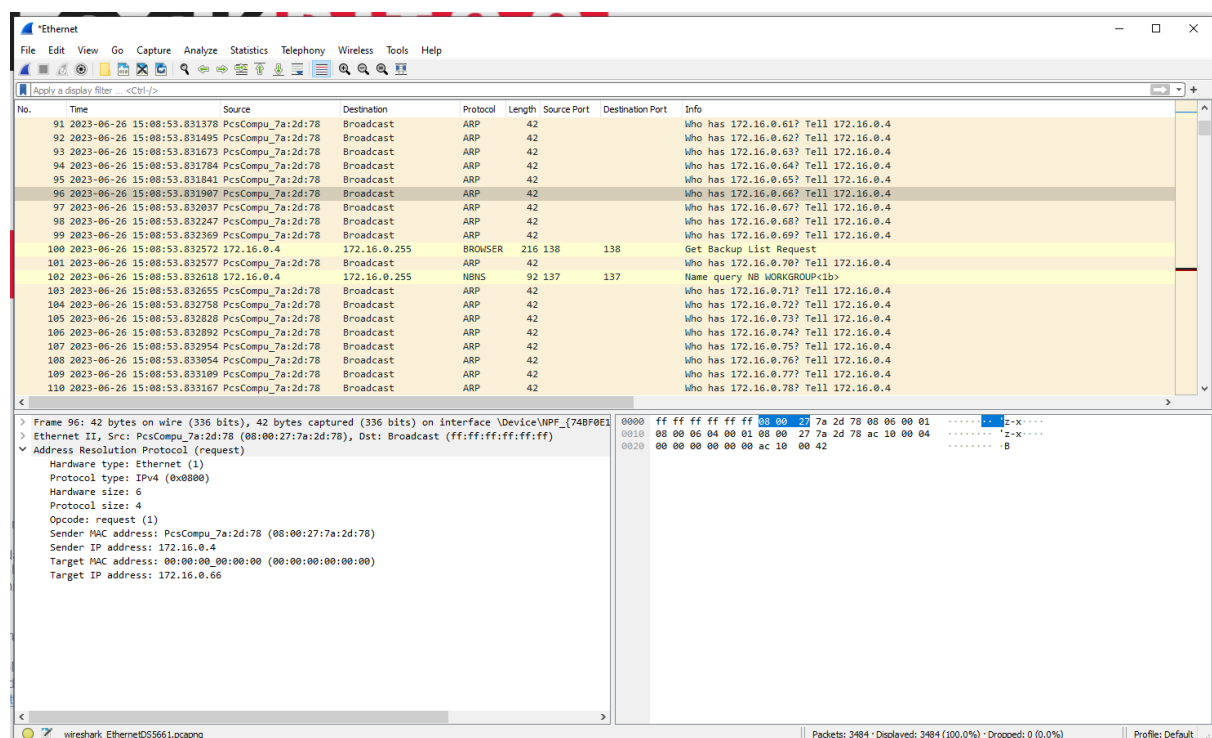
High Level Technical Summary

The malware was tested and analyzed under the following scenarios:

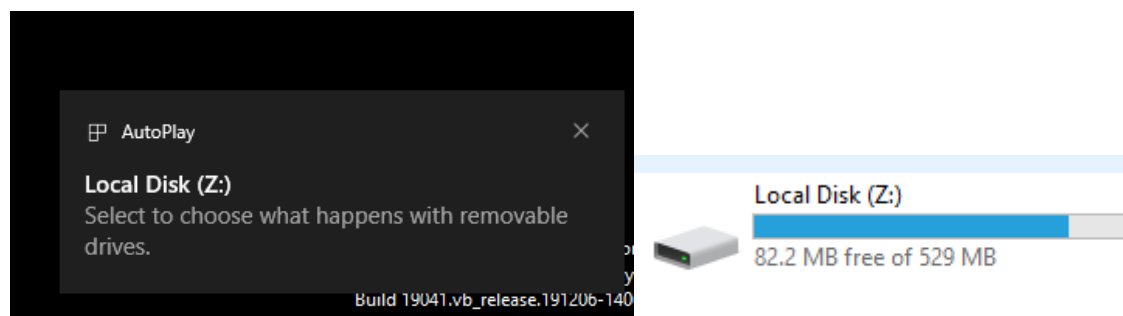
1. Execution with user privileges and no Internet access
2. Execution with user privileges and simulated Internet access with inetsim
3. Execution with administrative privileges and no Internet access
4. Execution with administrative privileges and simulated Internet access with inetsim

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.



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



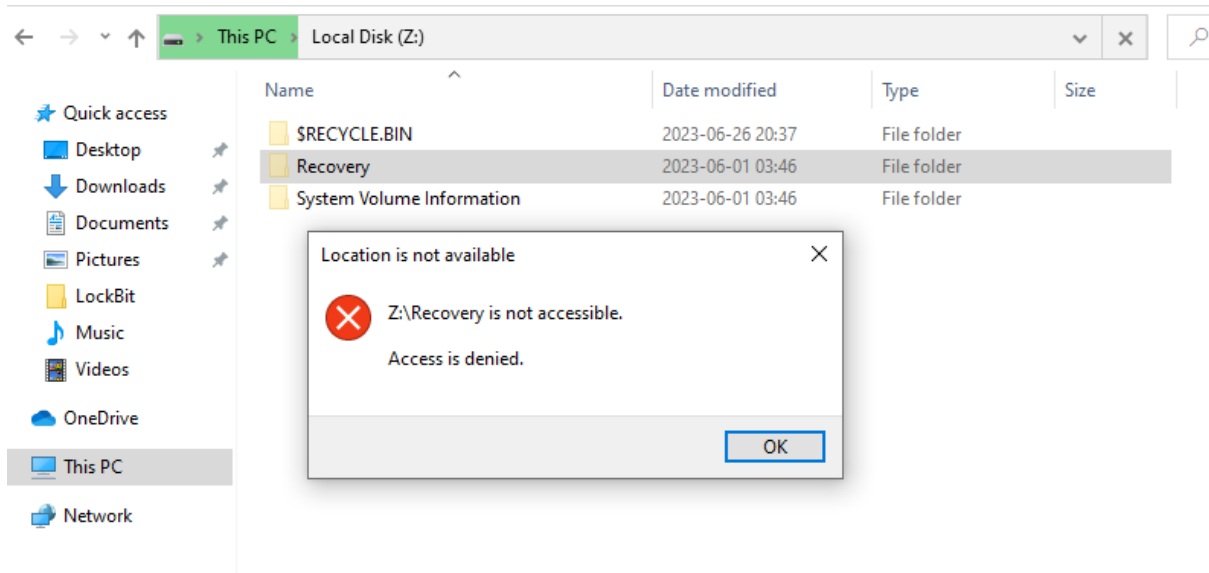
The malware does not create any new users, but still is able to complete the execution sequence without the need for administrative rights.

LOCKBIT 2.0 RANSOMWARE

```
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\Administrator	DESKTOP-DEH1E4T	S-1-5-21-2860406012-28484
cde	DESKTOP-DEH1E4T\cde	DESKTOP-DEH1E4T\cde	DESKTOP-DEH1E4T	S-1-5-21-2860406012-28484
DefaultAccount	DESKTOP-DEH1E4T\DefaultAccount	DESKTOP-DEH1E4T\DefaultAccount	DESKTOP-DEH1E4T	S-1-5-21-2860406012-28484
Guest	DESKTOP-DEH1E4T\Guest	DESKTOP-DEH1E4T\Guest	DESKTOP-DEH1E4T	S-1-5-21-2860406012-28484
WDAGUtilityAccount	DESKTOP-DEH1E4T\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.



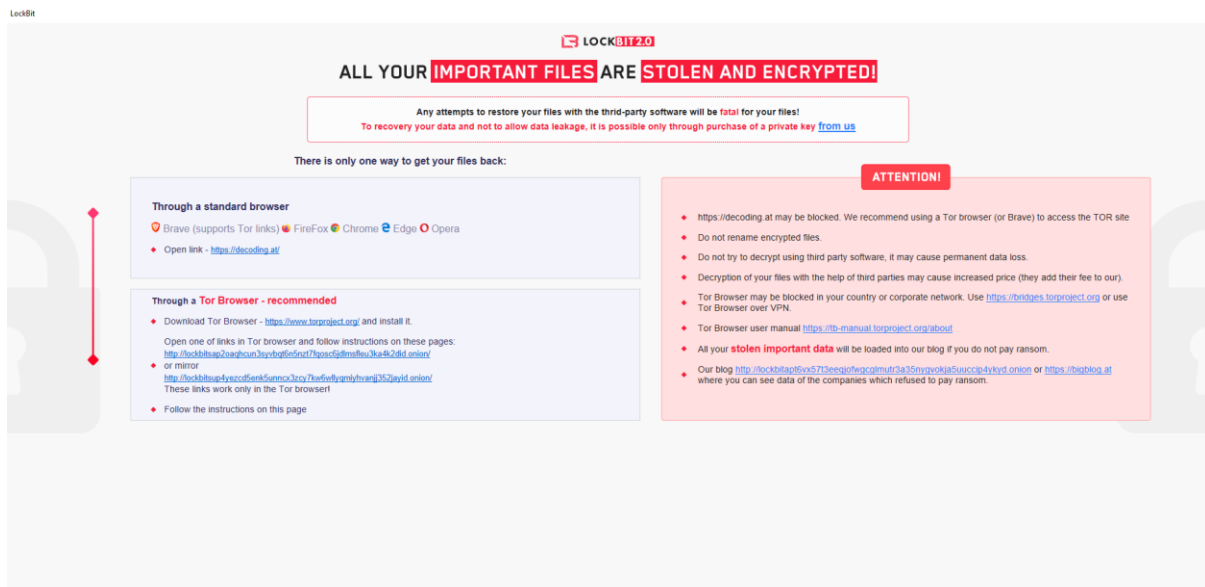
Then, the user wallpaper changes, all the encrypted files have the ".lockbit" suffix appended to them and on every folder that a file was encrypted a txt with the same instructions is generated.

```
Restore-My-Files.txt
1 LockBit 2.0 Ransomware
2
3 Your data are stolen and encrypted
4 The data will be published on TOR website http://lockbitapt6vx57t3eegiofwgcqlmutr3a35nygvokja5uuccip4ykyd.onion and https://bigblog.at if you do not
5 pay the ransom
6 You can contact us and decrypt one file for free on these TOR sites
7 http://lockbitsup4yvezcd5enk5unnx3zcy7kw6wilyqmiyhvanj1352jayid.onion
8 http://lockbitsap2oaghcun3syvbt6n5nt7fqsc6jdmsfleu3ka4k2did.onion
9 OR
10 https://decoding.at
11 Decryption ID: 172375D30BE340B46BB6B3B4D8C1D1D3
```

LOCKBIT 2.0 RANSOMWARE



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 RANSOMWARE

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?

LOCKBIT 2.0 RANSOMWARE

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\[.\]lat](https://bigblog.lat)

```

1544 %a%02X0202X02X02X02X.lock
1545 SOFTWARE\Microsoft\Windows\CurrentVersion\Run
1546 {2C5F9FCC-F266-43F6-BFD7-838DAE269E11}
1547 \LockBit_Ransomware.hta
1548 /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0 length=524288 "%s" & Del /f /q "%s"
1549 cmd.exe
1550 (%XX%XX%XX-%XX%-XX%X-%XX%-XX%XX%XX%XX%)
1551 SOFTWARE\%02X02X02X02X02X02X02X02X02X02X02X02X
1552 Volume %s mounted to %s
1553 Found volume %s on %s
1554 %s\bootmgr
1555 \\%s%\s
1556 Microsoft Print to PDF
1557 Microsoft XPS Document Writer
1558 C:\windows\system32\%XX%XX%.ico
1559 \Registry\Machine\Software\Classes\.lockbit
1560 LockBit
1561 \Registry\Machine\Software\Classes\Lockbit
1562 \Registry\Machine\Software\Classes\Lockbit\DefaultIcon
1563 \Registry\Machine\Software\Classes\Lockbit\shell
1564 LockBit Class
1565 \Registry\Machine\Software\Classes\Lockbit\shell\Open
1566 \Registry\Machine\Software\Classes\Lockbit\shell\Open\Command
1567 "C:\Windows\system32\mshta.exe" "%s"
1568 \Registry\Machine\Software\Classes\
1569 \DefaultIcon
1570 [??C:\windows\system32\%XX%XX%.ico
1571 \Registry\Machine\Software\Classes\.lockbit\DefaultIcon
1572 \explorer.exe
1573 explorer.exe
1574 Elevation:Administrator:new:
1575 {3EFCTCF9-9A51-4367-9063-A120244FBEC7}
1576 DisplayCalibrator
1577 Software\Microsoft\Windows NT\CurrentVersion\ICM\Calibration
1578 {D2E7041B-2927-42fb-8Ef9-7CE93B6DC937}
1579 Proxima Nova
1580 All your files stolen and encrypted
1581 for more information see
1582 RESTORE-MY-FILES.TXT
1583 that is located in every encrypted folder.
1584 Would you like to earn millions of dollars?
1585 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.
1586 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.
1587 Companies pay us the foreclosure for the decryption of files and prevention of data leak.
1588 You can communicate with us through the Tox messenger
1589 https://tox.chat/download.html
1590 Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
1591 If you want to contact us, use ToxID: 305B89A0C515D2FB124DE45906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
1592 If this contact is expired, and we do not respond you, look for the relevant contact on our website via Tor or Brave Browser
1593 http://lockbitapt6vx5t73eeqjofwgqimutr3a53nygvokja5uuuccip4ykyd.onion
1594 https://bigblog.at
1595 %s.bmp
1596 image/bmp
1597 \BaseNamedObjects\(%XX%XX%XX-%XX%-XX%X-%XX%-XX%XX%XX%XX%XX%)

```

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

LOCKBIT 2.0 RANSOMWARE

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

[illegible]

Advanced Static Analysis

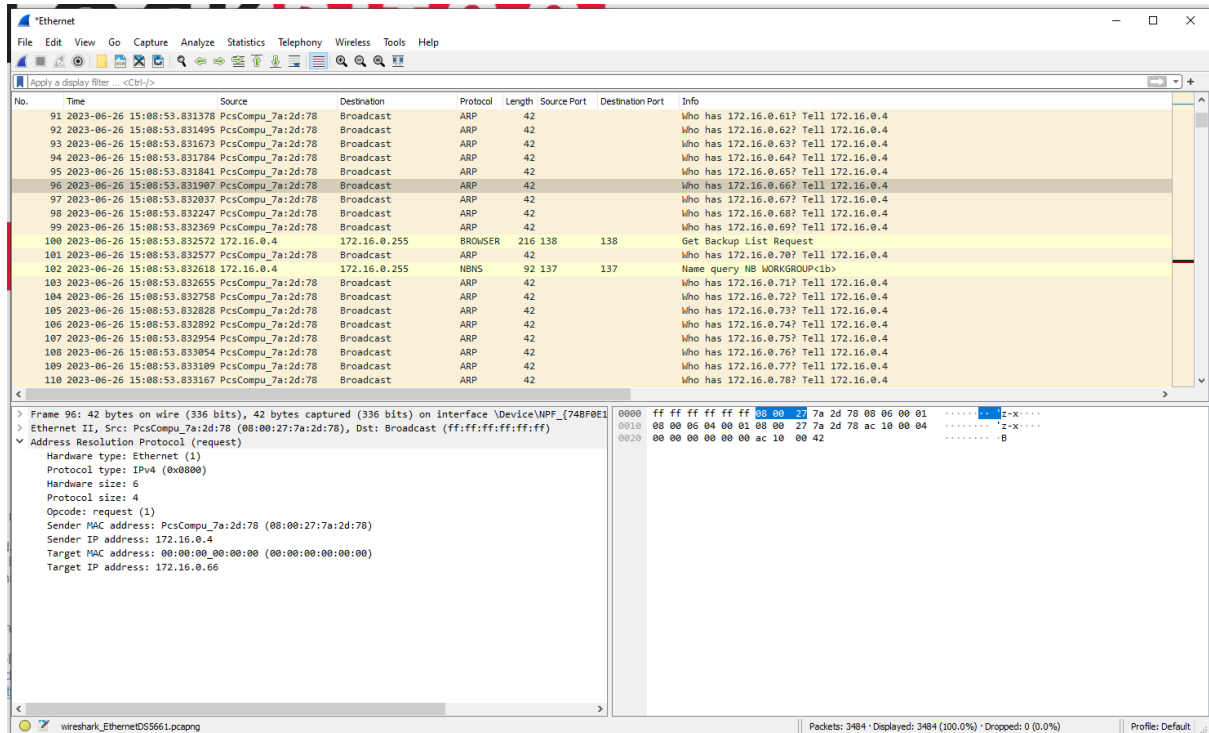
The malware is very complex and highly obfuscated leaving the researcher little opportunities for statically analyzing the malware code. The findings regarding to the malware code come from the dynamic analysis section of the investigation.

Dynamic Analysis

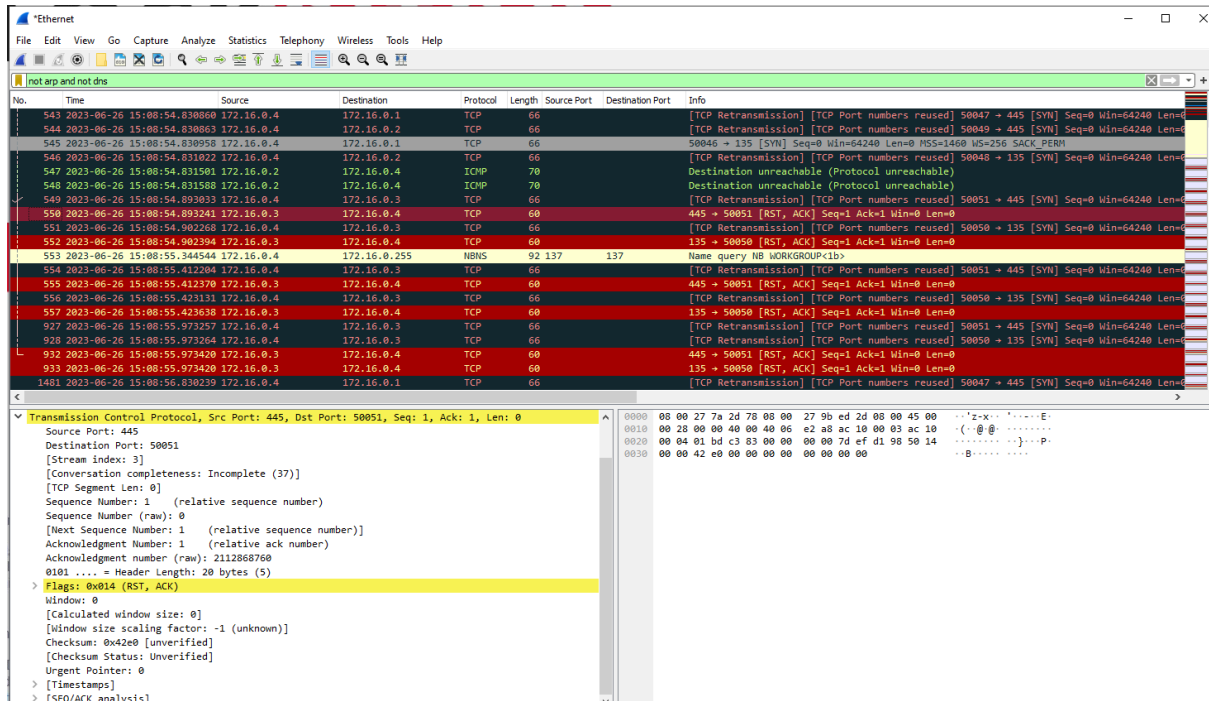
Basic Dynamic Analysis

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.



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



LOCKBIT 2.0 RANSOMWARE

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	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	50554 → 443 [FIN, ACK] Seq=305 Ack=1525 Win=2102272 Len=0
2469	2023-06-26 15:09:47.408580	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	50554 → 443 [RST, ACK] Seq=306 Ack=1556 Win=0 Len=0
2471	2023-06-26 15:09:47.408715	172.16.0.3	172.16.0.4	TCP	60			443 → 50554 [FIN, ACK] Seq=1556 Ack=206 Win=64128 Len=0
2472	2023-06-26 15:09:47.408778	172.16.0.4	172.16.0.3	TCP	54	50554	443	50554 → 443 [RST] Seq=306 Win=0 Len=0
2473	2023-06-26 15:09:47.418493	172.16.0.4	172.16.0.3	TCP	66	50555	443	50555 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2474	2023-06-26 15:09:47.418591	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 15:09:47.418623	172.16.0.4	172.16.0.3	TCP	54	50555	443	50555 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
2476	2023-06-26 15:09:47.418773	172.16.0.4	172.16.0.3	TLSv1.2	265			Client Hello
2477	2023-06-26 15:09:47.418863	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 15:09:47.418924	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	50555 → 443 [FIN, ACK] Seq=305 Ack=1525 Win=262656 Len=0
2483	2023-06-26 15:09:47.418531	172.16.0.4	172.16.0.3	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	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

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): 341856667

[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 00 06 00 00 ac 10 00 04 ac 10 ... 4>B

0020 00 03 c5 7b 01 35 cb c3 30 15 00 00 00 00 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	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	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	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	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	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

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): 783924095

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 00 06 00 00 ac 10 00 04 ac 10 ... 2>B

0020 00 03 c5 04 31 0e 17 5a ea b6 2e b9 bb 25 50 18 ... 2:Z

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 65 7a 09 65 e7 0f 47 76 52 e9 da 01 ... ez:e ->R

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 0a 00 08 00 06 ...

00c0 00 1d 00 17 00 18 00 0b 00 02 01 00 00 0d 0a 1a ...

00d0 00 18 00 04 00 05 08 06 04 01 05 01 02 01 04 03 ...

00e0 05 03 02 03 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
(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.

LOCKBIT 2.0 RANSOMWARE

[illegible]

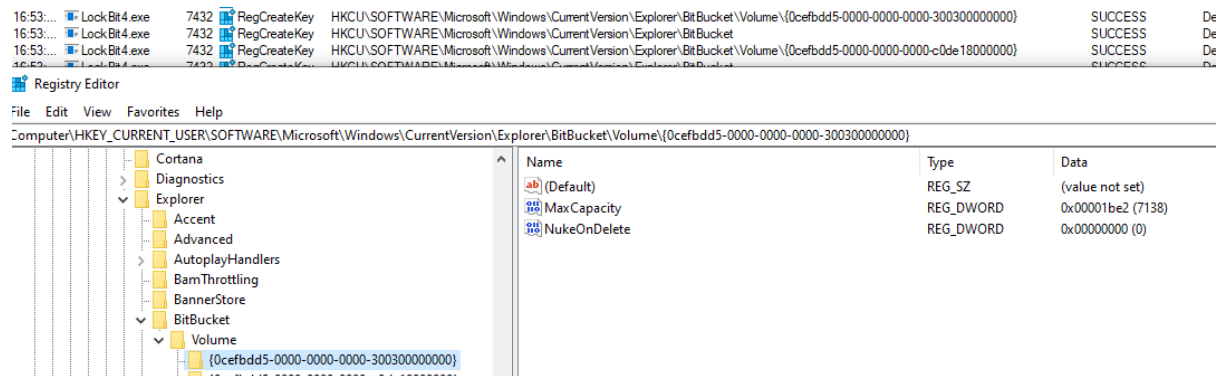
16-34	Look-Bit4.exe	1634	RegCreateKey	HKLM\Local	314C1ED3	Desired Access: Maximum Allowed, Granted Access: None, Obj. Disposition: REG_CREATE_NEW
16-34	Look-Bit4.exe	7432	RegCreateKey	HKCR\Local\DefaultIcon	SUCCESS	Desired Access: Maximum Allowed, Granted Access: None, Obj. Disposition: REG_CREATED_NEW
16-34	Look-Bit4.exe	7432	RegCreateKey	HKCR\Local\shell	SUCCESS	Desired Access: Maximum Allowed, Granted Access: None, Obj. Disposition: REG_CREATED_NEW
16-34	Look-Bit4.exe	7432	RegCreateKey	HKCR\Local\shell\Open\Command	SUCCESS	Desired Access: Maximum Allowed, Granted Access: None, Obj. Disposition: REG_CREATED_NEW

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>.

[illegible]

LOCKBIT 2.0 RANSOMWARE

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.



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:ifao;0"
004A7DB8	74 08	je lockbit4.exe.4A7DC2	
004A7DBA	66:0F1F4400 00	nop word ptr ds:[eax+eax],ax	
004A7DC0	E8 FE	jmp lockbit4.exe.4A7DC0	
004A7DC2	C78424 40010000 7D	mov dword ptr ss:[esp+140],7D	7D:'}}'
004A7DCD	33F6	xor esi,esi	
004A7DCE	C68424 44010000 1A	mov byte ptr ss:[esp+144],1A	

Which is verified on the main function - entry0

<pre> ; 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, 0xffffffff 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 </pre>			
<pre> [0x004a7dba] 0x004a7dba nop word [eax + eax] </pre>			
<pre> [0x004a7dc0] 0x004a7dc0 jmp 0x4a7dc0 </pre>			
<pre> [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] </pre>			

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

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

004A80B8	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:"D\vEv"
004A80C6	8D4424 34	lea eax, dword ptr ss:[esp+34]	eax:"shell32.dll"
004A80CF	50	push eax	
004A80D1	FFD1	call ecx	
004A80D3	C78424 34020000 28	mov dword ptr ss:[esp+234],28	28:'C'

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.

004A9E9C	E8 0FEEF6FF	call lockbit4.exe.410070	
004A9E9D	A3 54084E00	mov dword ptr ds:[4E0854],eax	
004A9E9E	6A 00	push 0	
004A9E9A	E8 A182F9FF	call lockbit4.exe.442140	New Drive connected and execution
004A9E9F	6A 08	push 8	
004A9EA0	E8 4A020000	call lockbit4.exe.4A0F0	
004A9EA6	85C0	test eax, eax	
004A9EAB	74 05	je lockbit4.exe.4A9EAF	
004A9EAA	E8 5166FEFF	call lockbit4.exe.490500	
004A9EAC	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.

LOCKBIT 2.0 RANSOMWARE

