Quorum Cyber

Threat Intelligence LockBit 3.0 Ransomware

TLP Status: White

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version		Date	Summary of Changes
0.1		01/02/2023	Initial Report
1.0		13/04/2023	Final PDF Formatting
1.1		17/04/2023	Update one

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
-	-	-

LockBit 3.0 Ransomware

Overview

LockBit 3.0 is the third generation of the gang's original malware which poses a significant threat to organisations across the public and private sector spectrums. In October 2022, LockBit 3.0 was the most prolific ransomware strain in the world, accounting for almost a third of all reported ransomware attacks[1]. LockBit maintained this position as the most prolific until April 2023 where it was a close second.

LockBit 3.0 can infiltrate a system via a variety of methods. However, the most common initial access point is via a spear phishing campaign.

Historically, LockBit 3.0 has been designed to target WindowsOS, Linux and VMware ESXi, but not MacOS. However recent reporting suggests that a new Mac encryptors are in development therefore it is likely that LockBit will soon have the capability to target Mac devices[2].

Impact

Successful exploitation by LockBit 3.0 will result in the encryption and exfiltration of significant quantities of data held on the compromised device or system, prior to a ransom of a predetermined amount being demanded.

Encrypted data may include private customer data, corporate finance data, and system credentials that, if released, could provide threat actors with further targeting opportunities.

Vulnerability Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide additional protection against ransomware threats such as LockBit 3.0. EDRs can alert system users of potential breaches and prevent further progress, prior to the malware being able to implement significant damage.

If an EDR solution is not being used, the first instance of detection is likely to be the ransom note. A copy of a LockBit 3.0 ransom note can be found below:

```
Ransom note:

All your important files are encrypted!

Any attempts to restore your files with the third-party software will be fatal for your files!

RESTORE YOUR DATA POSIBLE ONLY BUYING private key from us.

There is only one way to get your files back:

| 1. Download Tor browser - hxxps://www[.]torproject.org/ and install it.

| 2. Open link in TOR browser - hxxp://lockbitks2tvnmwk[.]onion/?

This link only works in Tor Browser!
```

[1] https://therecord.media/ransomware-tracker-the-latest-figures/
[2] https://www.bleepingcomputer.com/news/security/lockbit-ransomware-encryptors-found-targeting-mac-devices/

| 3. Follow the instructions on this page

Attention!

 # 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 hxxps://bridges[.]torproject[.]org

 # Tor Browser user manual hxxps://tb-manual[.]torproject[.]org/about

!!! We also download huge amount of your private data, including finance information, clients personal info, network diagrams, passwords and so on. Don't forget about GDPR.

Affected Products

- Windows OS
- Linux
- VMware ESXi servers
- MacOS (encryption capability likely in development)

Containment, Mitigations & Remediations

As stated above, the main method of reducing the threat of ransomware attacks is to attain the added protection of an EDR solution. An effective EDR will increase detection of malicious attempts of ransomware compromise, including LockBit 3.0, and halt such attempts if detected.

It is also recommended that employees receive training on how to detect markers of phishing emails. Due to the abundant implementation of phishing attacks by threat actors, this training will serve to reduce the possibility of not only LockBit 3.0 compromise, but also that of many other strains of offensive malware.

Organisations can also perform routine back-ups of sensitive data that is required to operate business procedures. Therefore, if a breach occurs and the business can no longer function, a back-up is ready to use, and the business can continue to operate with minimal disruption. However, this does not nullify the fact that customer and employee data may have also been lost, and potentially released at will by the attacker if demands are not met.

Indicators of Compromise

LockBit 3.0 Associated Domains:

- manfil[.]com[.]br

- cobcreditunion[.]com
- df[.]senac[.]br
- electronicsystem[.]it
- garrottbros[.]com
- grupcovesa[.]com
- piramal[.]com
- rimex[.]com
- skywayendo[.]com
- swiftatlanta[.]com
- tecnosysitalia[.]eu
- valleywomenshealth[.]com
- hacla[.]org
- capsonic[.]com
- cornwelltools[.]com
- farms[.]com
- imacorp[.]com
- info[.]openjdklab[.]xyz
- sappi[.]com
- sterlingcheck[.]com

LockBit 3.0 Associated File Hashes (SHA-256):

- 060bd55768e0edc037651bf50c54248e9451d57d4da795b9d8ea03829085cea1
- 6490c1fec33f70d41c8112be2022d5f656c5d060b12db00a8f945938fda2cab5

LockBit 3.0 Associated File Hashes (SHA-1):

- 729eb505c36c08860c4408db7be85d707bdcbf1b
- 091b490500b5f827cc8cde41c9a7f68174d11302
- e35a702db47cb11337f523933acd3bce2f60346d
- a512215a000d1b21f92dbef5d8d57a420197d262
- c05216f896b289b9b426e249eae8a091a3358182
- 10039d5e5ee5710a067c58e76cd8200451e54b55
- 82bd4273fa76f20d51ca514e1070a3369a89313b
- eed31d16d3673199b34b48fb74278df8ec15ae33
- 0815277e12d206c5bbb18fd1ade99bf225ede5db
- ff01473073c5460d1e544f5b17cd25dadf9da513

LockBit 3.0 Associated File Hash (MD5):

- f9ab1c6ad6e788686509d5abedfd1001
- 5e54923e6dc9508ae25fb6148d5b2e55
- 13b12238e3a44bcdf89a7686e7179e16
- bf331800dbb46bb32a8ac89e4543cafa
- ad444dcdadfe5ba7901ec58be714cf57
- 1690f558aa93267b8bcd14c1d5b9ce34
- 56c9c8f181803ece490087ebe053ef72

LockBit 3.0 Associated IP Addresses:

- 139[.]180[.]184[.]147
- 149[.]28[.]137[.]7
- 45[.]32[.]108[.]54

Threat Group

For six months between October 2022 and April 2023 the LockBit ransomware gang was the most prevalent ransomware gang in the world, with their malware accounting for nearly a third of all reported ransomware attacks globally. Their choice of targeting is diverse and does not focus on a single industry sector, making it challenging to predict their next victim.

Additionally, the LockBit gang functions via two main methods of operation. These include direct action taken by the gang against a chosen target using their own ransomware strain, and the sale of temporary licences to cybercriminals. This distribution of licences forms LockBit's RaaS and is especially dangerous, as it enables threat actors to independently target organisations deemed to be of interest. The RaaS is likely to be responsible for the LockBit 3.0's status as the most popular current ransomware family in circulation.

Due to the LockBit gang's strategy of using RaaS, the process of identifying an adversary exploiting a system using the ransomware becomes increasingly challenging, as any party can purchase and utilise the malware.

Mitre Methodologies

Resource Development
T1587.002 – Develop Capabilities: Code Signing Certificates[3]

Initial Access
T1078 – Valid Accounts[4]
T1133 – External Remote Services[5]
T1190 – Exploit Public-Facing Application[6]
T1195 – Supply Chain Compromise[7]

Execution
T1059.001 – Command and Scripting Interpreter: PowerShell[8]
T1059.003 – Command and Scripting Interpreter: Windows Command Shell[9]
T1059.007 – Command and Scripting Interpreter: JavaScript[10]

Persistence
T1078 – Valid Accounts[11]
T1098 – Account Manipulation[12]
T1133 – External Remote Services[13]

[3] https://attack.mitre.org/techniques/T1587/002/
[4] https://attack.mitre.org/techniques/T1078/
[5] https://attack.mitre.org/techniques/T1133/
[6] https://attack.mitre.org/techniques/T1190/
[7] https://attack.mitre.org/techniques/T1195/
[8] https://attack.mitre.org/techniques/T1059/001/
[9] https://attack.mitre.org/techniques/T1059/003/
[10] https://attack.mitre.org/techniques/T1059/007/
[11] https://attack.mitre.org/techniques/T1078/
[12] https://attack.mitre.org/techniques/T1098/
[13] https://attack.mitre.org/techniques/T1133/

T1574.002 – Hijack Execution Flow: DLL Side-Loading[14]

Privilege Escalation
T1078 – Valid Accounts[15]
T1574.002 – Hijack Execution Flow: DLL Side-Loading[16]

Defence Evasion
T1078 – Valid Accounts[17]
T1140 – Deobfuscate/Decode Files or Information[18]
T1497 – Virtualisation/Sandbox Evasion[19]
T1574.002 – Hijack Execution Flow: DLL Side-Loading[20]

Discovery
T1082 – System Information Discovery[21]
T1497 – Virtualisation/Sandbox Evasion[22]

Lateral Movement
T1021.001 – Remote Services: Remote Desktop Protocol[23]

Collection
T1005 – Data from Local System[24]

Command and Control
T1105 – Ingress Tool Transfer[25]

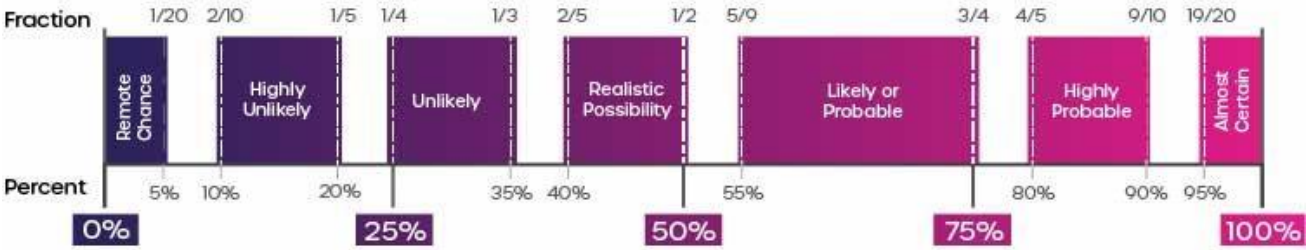
Impact
T1486 – Data Encrypted for Impact[26]
T1489 – Service Stop[27]
T1498 – Denial of Service[28]
T1498.001 – Denial of Service: Direct Network Flood[29]

Further Information

Intelligence Cut-off Date (ICoD): 17/04/2023 10:00 GMT

[14] https://attack.mitre.org/techniques/T1574/002/
[15] https://attack.mitre.org/techniques/T1078/
[16] https://attack.mitre.org/techniques/T1574/002/
[17] https://attack.mitre.org/techniques/T1078/
[18] https://attack.mitre.org/techniques/T1140/
[19] https://attack.mitre.org/techniques/T1497/
[20] https://attack.mitre.org/techniques/T1574/002/
[21] https://attack.mitre.org/techniques/T1082/
[22] https://attack.mitre.org/techniques/T1497/
[23] https://attack.mitre.org/techniques/T1021/001/
[24] https://attack.mitre.org/techniques/T1005/
[25] https://attack.mitre.org/techniques/T1105/
[26] https://attack.mitre.org/techniques/T1486/
[27] https://attack.mitre.org/techniques/T1489/
[28] https://attack.mitre.org/techniques/T1498/
[29] https://attack.mitre.org/techniques/T1498/001/

Intelligence Terminology Yardstick



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events