datto

LockBit Threat Profile

LockBit, LockBit 2.0, ABCD

LockBit is a family of ransomware that has been in operation and actively developed since September 2019. LockBit 2.0 was released in June 2021 and made headlines in August 2021 for its successful attacks against multiple large companies.

LockBit 2.0 is sold under a Ransomware-as-a-Service (RaaS) model. Those who buy into the service become 'affiliates' and are given access to the administrator panel, which provides the ability to create LockBit binaries, view current attacks and payment statuses, and communicate with the LockBit group via live chat.

All ransom payments are split with the LockBit developers, with affiliates keeping 70-80% of the ransom. This favorable split for affiliates is likely set up to attract affiliates from other RaaS groups.

The operators of Lockbit 2.0 claim to have the fastest encryption and data exfiltration programs on the ransomware market. LockBit's encryption speed is achieved by encrypting only approximately 4KB of each file.

Motives

LockBit developers and its affiliates are financially motivated. LockBit runs a "double extortion" model where data is first exfiltrated from the victim's network before encryption is performed. The actors then threaten to publish the stolen data online to further pressure victims to pay the ransom demands. If the ransom isn't paid, the stolen data is published on LockBit's TOR site.

Tactics, Techniques, and Procedures (TTPs)

LockBit 2.0 post-incident reports indicate that initial access is mainly achieved through valid credentials, exploitation of unpatched internet-facing devices, and email phishing.

LockBit developers actively recruit company insiders, such as disgruntled employees, who can provide access to their company's network or purposely execute the malware on a corporate device from a malicious email in exchange for payment.

Once access has been established, LockBit actors work to gain access to the domain controllers. The actors also exfiltrate victim data with the StealBit information stealer, supplied by the LockBit development team.

Once on the Domain Controller, actors run LockBit 2.0, creating new user group policies and pushing them out to all domain-joined devices. The policies disable built-in Windows security features and create a scheduled task for LockBit 2.0 to run.

Once executed, LockBit 2.0 will delete local Windows backups, add itself to a startup registry run key, and begin encrypting files on the device. LockBit 2.0 also attempts to encrypt shared drives. All encrypted files have their extension changed to .lockbit, and a ransom note is dropped in each successfully encrypted folder.

MITRE ATT&CK:

The following maps LockBit's TTPs to MITRE ATT&CK:

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application	Command and Scripting Interpreter	Boot or Logon Autostart Execution	Abuse Elevation Control Mechanism	Domain Policy Modification	Network Share Discovery	Remote Services	Data from Local System	Traffic Signaling	Exfiltration Over C2 Channel	Data Encrypted for Impact
Valid Accounts	Windows Command Shell	Registry Run Keys / Startup Folder	Bypass User Account Control	Group Policy Modification	Process Discovery	SMB/ Windows Admin Shares	Data from Network Shared Drive			Inhibit System Recovery
	Scheduled Task/Job			Impair Defenses	Query Registry					Service Stop
	Scheduled Task			Disable or Modify Tools						
				Indicator Removal on Host						
				Clear Windows Event Logs						
				File Deletion						
				Obfuscated Files or Information						

Initial Access

- **Exploit Public-Facing Application (T1190) -** LockBit actors have exploited Fortinet vulnerabilities to gain initial access to victim networks.
- **Valid Accounts (T1078) -** LockBit actors actively advertise partnership opportunities for actors who can provide credential-based access.

Execution

- **Scheduled Task/Job: Scheduled Task (T1053.005) -** LockBit creates a scheduled task to execute the ransomware.
- **Command and Scripting Interpreter: Windows Command Shell (T1059.003) -** LockBit has used the Windows command shell to execute commands.

Persistence

- **Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) -** LockBit creates an autostart registry key in 'HKey_Current_User\Software\Microsoft\Windows\CurrentVersion\Run'

Privilege Escalation

- **Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002) -** LockBit bypasses UAC by modifying the registry

Defense Evasion

- **Indicator Removal on Host: Clear Windows Event Logs (T1070:001) -** LockBit uses WEVTUTIL.exe to clear the security, system, and application Windows event logs
- **Indicator Removal on Host: File Deletion (T1070.004) -** LockBit deletes shadow drive data
- **Domain Policy Modification: Group Policy Modification (T1484.001) -** LockBit modifies group policy to deploy ransomware to domain-joined devices
- **Impair Defenses: Disable or Modify Tools (T1562.001) -** LockBit disables antivirus and other tools using batch files and legitimate tools.
- **Obfuscated Files or Information (T1027) -** LockBit uses code obfuscation techniques.

Discovery

- **Query Registry (T1012) -** LockBit reads multiple registry keys to check the device's language and read the computer name.
- **Process Discovery (T1057) -** LockBit lists all running processes.
- **Network Share Discovery (T1135) -** LockBit encrypts network share drives.

Lateral Movement

- **Remote Services: SMB/Windows Admin Shares (T1021.002) -** LockBit uses SMB shares for lateral movement.

Collection

- **Data from Local System (T1005) -** LockBit actors have exfiltrated files from local systems.
- **Data from Network Shared Drive (T1039) -** LockBit actors have exfiltrated files from network shares.

Command and Control

- **Traffic Signaling (T1205) -** If enabled, LockBit actors use Wake-On-LAN to encrypt network-connected endpoints that were powered off.

Exfiltration

- **Exfiltration Over C2 Channel (T1041) -** LockBit actors automatically exfiltrates data using StealBit, a custom data exfiltration tool

Impact

- **Service Stop (T1489) -** LockBit disables antivirus and stops critical services before encrypting devices.
- **Inhibit System Recovery (T1490) -** LockBit deletes shadow copies by running "vssadmin delete shadows /all /quiet" and disables automatic recovery by running "bcdedit /set {default} recoveryenabled no".
- **Data Encrypted for Impact (T1486) -** LockBit uses a combination of symmetric (AES) and asymmetric (ECC) encryption to encrypt files. LockBit encrypts 4 kilobytes of each file, and files are given the extension of '.lockbit'. Encrypted directories have a ransom note titled 'Restore-My-Files.txt' written to the directory.

Table of Contents

Mitigations/Defenses

Implementing a strong foundation of security controls is recommended to defend your network against the LockBit threat actors.

The Center for Internet Security (CIS) Controls are a prioritized set of safeguards designed to defend against cyber attacks. The CIS Controls have three tiers, known as Implementation Groups, that build on each other.

The following table maps LockBit's MITRE ATT&CK techniques to CIS v8 Safeguards:

MITRE ATT&CK	CIS Safeguards
Exploit public-facing application (T1190)	**IG1** 4.4: Implement and Manage a Firewall on Servers
Valid Accounts (T1078)	**IG1** 5.1: Establish and Maintain an Inventory of Accounts 5.3: Disable Dormant Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Scheduled Task/Job: Scheduled Task (T1053.005)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 8.3: Ensure Adequate Audit Log Storage
Command and Scripting Interpreter: Windows Command Shell (T1059.003)	**IG1** 2.5: Allowlist Authorized Software
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 8.2: Collect Audit Logs
Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process

— IG1 — IG2 — IG3

Table of Contents

Indicator Removal on Host: Clear Windows Event Logs (T1070.001)	**IG1** 8.1: Establish and Maintain an Audit Log Management Process 8.2: Collect Audit Logs 8.3: Ensure Adequate Audit Log Storage
Domain Policy Modification: Group Policy Modification (T1484.001)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Impair Defenses: Disable or Modify Tools (T1562.001)	**IG1** 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Obfuscated Files or Information (T1027)	**IG1** 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates
Network Share Discovery (T1135)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process
Remote Services: SMB/ Windows Admin Shares (T1021.002)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 4.5: Implement and Manage a Firewall on End-User Devices 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Traffic Signaling (T1205)	**IG1** 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers
Exfiltration Over C2 Channel (T1041)	**IG2** 13.3: Deploy a Network Intrusion Detection Solution **IG3** 13.8: Deploy a Network Intrusion Prevention Solution

— IG1 — IG2 — IG3

Table of Contents

Service Stop (T1489)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Inhibit System Recovery (T1490)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data
Data Encrypted for Impact (T1486)	**IG1** 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data

— IG1 — IG2 — IG3

Detection Opportunities

Detecting LockBit threat actors targeting your network requires understanding their attack vectors, mapping them to actionable defensive controls, and validating your defenses through reliable, repeatable testing.

The following detection opportunities are mapped to MITRE ATT&CK v9 methods, CIS v8 Safeguards, and provide appropriate Red Canary Atomic Red Team tests to undertake for validation:

Detection Opportunity 1: Shadow Copy Deletion & Disabling Windows Recovery

MITRE ATT&CK: Inhibit System Recovery (T1490)

CIS Control(s): 11.1: Establish and Maintain a Data Recovery Process & 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Red Canary Atomic Red Team Test(s): T1490 - Inhibit System Recovery Atomic Tests #1 & #2

Detecting the deletion of shadow copies and the disabling of automatic Windows recovery is a great way to detect LockBit actors preparing to encrypt your device.

To detect the deletion of shadow copies, write a custom rule in your EDR or SIEM that will alert the execution of commands containing: "vssadmin delete shadows".

To detect the disabling of Windows recovery, write a custom rule in your EDR or SIEM that will alert on the execution of commands containing: "bcdedit /set {default} recoveryenabled no"

These commands are commonly run in ransomware attacks, making restoring without paying the ransom far more difficult. By looking for unauthorized vssadmin and bcdedit activity, you will defend against many ransomware strains, not just LockBit.

Detection Opportunity 2: Detecting Registry Run Key creation or persistence

MITRE ATT&CK: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

CIS Control(s): 4.1: Establish and Maintain a Secure Configuration Process, 8.2: Collect Audit Logs

Red Canary Atomic Red Team Test(s): T1547.001 - Registry Run Keys / Startup Folder Test #1

Establishing persistence via registry run keys is a well-known persistence tactic still in use with modern malware, including LockBit 2.0.

By alerting on the creation of new run keys, you can discover malicious executables establishing persistence on your device.

There are four run keys that executables can add themselves to for startup persistence:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

LockBit 2.0 has been observed adding itself to: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, which allows it to run each time the current user logs back into the device.

Writing alert logic to notify whenever a new program adds itself to any of the four run keys will allow you and your team to respond to LockBit 2.0 ransomware attacks quickly.

Detection Opportunity 3: Detecting Data Exfiltration

MITRE ATT&CK: Exfiltration Over C2 Channel (T1041)

CIS Control(s): 13.3: Deploy a Network Intrusion Detection Solution, 13.8: Deploy a Network Intrusion Prevention Solution

Red Canary Atomic Red Team Test(s): T1041 - Exfiltration Over C2 Channel Atomic Test #1

LockBit threat actors utilize a bespoke data exfiltration tool developed by the LockBit developers named StealBit. Samples of StealBit show that the data is exfiltrated to actor-controlled infrastructure over HTTP port 80. This gives an opportunity for network defenders to detect data exfiltration by alerting on high-volume activity to IPs not previously interacted with.

Resources

cisecurity.org

analyze.intezer.com

joesandbox.com

app.any.run

rendmicro.com

cyber.gov.au

kaspersky.com

cyber.gov.au

socradar.io

blog.cyble.com

kaspersky.com

joesandbox.com

otx.alienvault.com

cynet.com

Table of Contents