# Ransomware, Lockbit

SI-0724-0001

TLP-WHITE

## TYPE

Ransomware

## SUSPECTED RELATION

LockBit 2.0 ( LockBit Red), LockBit Linux – ESXi Locker, LockBit 3.0, LockBit Green, ABCD, Lock2Bits, LockBit BLACK, LockBit MacOS (ARM), SteakBit

## TARGETED INDUSTRIES

Financial services, food and agriculture, education, energy, government and emergency services, healthcare, manufacturing, and transportation.

## EXECUTIVE SUMMARY

LockBit is a highly advanced and targeted ransomware that presents a significant danger to organizations worldwide. Operating as a ransomware-as-a-service (RaaS), it is accessible to various cybercriminal groups, amplifying its reach and impact. Upon infiltration, LockBit rapidly encrypts crucial data, rendering it inaccessible to victims, and subsequently demands payment in cryptocurrency to provide the decryption key. This ransomware employs a double-extortion strategy, compelling victims to comply by threatening to expose sensitive information publicly. The identity of the threat actors responsible for LockBit remains elusive due to their expert use of concealment techniques. To mitigate the risk of LockBit and other ransomware attacks, it is essential for organizations to prioritize robust cybersecurity measures, maintain regular data backups, conduct employee training, and implement up-to-date security solutions to safeguard against this ever-evolving threat.

## TECHNICAL OVERVIEW

LockBit is a notorious ransomware that gained attention for its sophisticated and targeted attacks. It typically used phishing emails, social engineering, or exploiting vulnerabilities to gain initial access to a victim's system. Once inside the network, LockBit conducted thorough reconnaissance to identify critical assets and data. The ransomware used strong encryption algorithms to lock victim data, and it had a unique feature of threatening to leak sensitive information from the compromised network to increase pressure on the victim to pay the ransom. Communication with victims was established to provide instructions on how to pay the ransom and negotiate the amount. LockBit was distributed through an affiliate model, allowing different cybercriminal groups to use the ransomware in exchange for a percentage of the ransom proceeds. As with other ransomware strains, LockBit's developers constantly updated the malware to evade detection by security solutions, making it challenging to defend against. The best protection involves a multi-layered cybersecurity approach, including regular data backups, network segmentation, strong endpoint security, employee training, and keeping software up to date with the latest security patches.

## TTPs

Select and infiltrate victim organizations and deploy the ransomware provided by the LockBit developer. LockBit uses a dual extortion tactic, demanding that victims pay a ransom to recover their files and not release the stolen information to the public. LockBit is also believed to threaten Distributed Denial of Service (DDoS) attacks against victims if the demanded ransom is not paid.

## MITRE ATT&CK MATRIX

ID: T1207, Tactic: Defense Evasion, Platforms: Windows, User Execution Malicious File
ID: T1204.002, Tactic: Execution, Platforms: Linux, Windows, macOS
ID: T1598, Sub-techniques: T1598.001, T1598.002, T1598.003, Tactic: Reconnaissance, Platforms: PRE
ID: T1078, Valid Accounts, Tactic: Initial Access, ID:T1190, Exploit Public-Facing Application, ID: T1047, Windows Management Instrumentation, Tactic: Execution, ID: T1059, Command and Scripting Interpreter, Tactic: Execution, ID: T1059, Windows Command Shell, Tactic: Execution, ID: T1547.001, Boot Logon Autostart Execution: Registery Run Keys / Startup Folder, Tactic: Persistence, ID: T1055 Process Injection, Tactic: Defense Evasion, ID: T1070.004 Indicator Removal on Host: File Deletion, Tactic: Defense Evasion, ID: T1112 Modify Registery, Tactic: Defense Evasion, ID: T1497, Virtualization/Sandbox Evasion, Tactic: Defense Evasion, ID: T1056.004 Credential API Hooking, Tactic: Credential Access, ID: T1110, Brute Force, Tactic: Credential Access, ID: T1012 Query Registry, Tactic: Discovery, ID: T1018, Remote System Discovery, Tactic: Discovery, ID: T1057, Process Discovery, Tactic: Discovery, ID: T1021, Remote Services, Tactic: Lateral Movement, ID: T1021.001, Remote Services: Remote Desktop Protocol, Tactic: Lateral Movement, ID: T1021.002, Remote Services: SMB/Windows Admin Shares, Tactic: Lateral Movement, ID: T1056.004, Credential API Hooking, Tactic: Collection, ID: T1090.003, Proxy: Multi-hop Proxy, Tactic: Command and Control (C2), ID: T1567.002, Exfiltration Over Web Service: Exfiltration to Cloud Storage, Tactic: Exfiltration, ID: T1486, Data Encrypted for Impact, Tactic: Impact, ID: T1490, Inhibit System Recovery, Tactic: Impact

## IOCs

0987946ba3d8ac69086f9aaf4c920977, MD5 Hash - ff301a7c2b403e58fc74b5d1d39dde9632180e9d, SHA1 Hash - 6ff1ccdfb1c55f590b80df1907ee0273dffa549b17a19ae7bb0f5d46324c90e6, SHA256 Hash - 5b6028e8a0ebab39995828b3233e430f, MD5 Hash - de27c80237d90b92b82c2d450d53f6de760facbc2f489e8f6caa4e166f8d7f73, SHA256 Hash - 0f6658df421faa20a08d52d1dc78b12b5b832475, SHA1 Hash - a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, SHA256 Hash, 006ec5709d5f9254e06950d69278d48f97bc7397 – SHA1 Hash, f81fd11473201207e64107c7c6a8f79961f04305 – SHA1 Hash, 9284809de2a3becccff65bc07092d083 – MD5 Hash, 36a634340920b553ed4d538eda3bba67 – MD5 Hash, 2563761a3d4c547f3c822dba2b932c47cb277845d149c042149cc9e279c53607 – SA256 Hash, f81fd11473201207e64107c7c6a8f79961f04305 – SHA1 Hash, 006ec5709d5f9254e06950d69278d48f97bc7397 – SHA1 Hash, 0be6f1e927f973df35dad6fc661048236d46879ad59f824233d757ec6e722bde – SHA256 Hash, 7699ce6bd0713da64c5806b352acc9de – MD5 Hash

## RESOURCES

https://attack.mitre.org/
Crowdstrike
https://www.fortinet.com/blog/threat-research/lockbit-most-prevalent-ransomware#:~:text=The%20developer%20has%20consistently%20worked,%2C%E2%80%9D%20appeared%20in%20early%202023.