THREAT ANALYSIS: Assemble LockBit 3.0

By Cybereason Global SOC Team

Archived: 2026-04-05 17:56:10 UTC

Cybereason issues Threat Analysis reports to investigate emerging threats and provide practical recommendations for protecting against them.

In this Threat Analysis report, Cybereason investigates the LockBit 3.0 builder and DLL binaries, which are not well known in the wild.

Key Points

- **Expanding the markets:** The LockBit ransomware group provides various tools with constant version updates for specific purposes, such as exfiltrations. The ransomware group has expanded their region target by making the location check an option. These updates are made to appeal to wider audiences within the underground market.
- **Binary customizations:** The LockBit builder provides a variety of options to build the LockBit ransomware binaries. LockBit builder provides configuration settings to alter the LockBit behavior, as well as binary types. These options allow ransomware affiliates to customize LockBit to their operational needs.
- **Invest in obfuscations:** The LockBit 3.0 ransomware is well known for passphrase protection; however the ransomware also has other obfuscation techniques such as removing debugger hooking and self deletion. The ransomware is known to invest in its obfuscation and anti-analysis techniques to protect itself from the defenders.

what's happening?

The LockBit ransomware operation group has been active since 2019. LockBit ransomware has been a popular choice of Ransomware-as-a-Service (RaaS) amongst the ransomware affiliates community. Due to its popularity, the group has updated and created various versions to meet the market demand.

LockBit 3.0 affiliates operate following an initial access vector (RDP, Phishing campaigns or CVE exploitation). Once in their victim network, they spread laterally using SMB, PsExec, and Group Policy.

Before executing ransomware that will encrypt the victim’s files, data exfiltration is carried out, employing tools like Stealbit, Rclone or WinSCP, and data is uploaded either to private servers or public upload websites such as MEGA. Once LockBit 3.0 is executed, it erases logs, uses AES and RSA for hybrid encryption and tamper with potential data backup mechanisms.

LockBit: Comes in different colors

The current known versions of LockBits targeting Windows are as follows:

- LockBit
- LockBit 2.0
- LockBit 3.0 (LockBit Black)
- Since 2023, two new versions were introduced :
    - LockBit Green (Based on Conti ransomware)
    - Lockbit Red (which is actually Lockbit 2.0)

LockBit ransomware launched the first version in September 2019, and updates were made constantly. Some notable updates include the following:

- LockBit to Lockbit 2.0
    - Shadow copy deletion via *vssadmin*
    - User Account Control (UAC) Bypass
    - Ransom note printing via printers
    - Self-Propagation
- LockBit 2.0 to LockBit 3.0
    - Implementing BlackMatter Ransomware logic
        - Shadow copy deletion via Windows Management Instrumentation (WMI)
        - Password protection
        - Persistence via System Services
        - API Harvesting
        - Prints the ransom note as a Desktop Wallpaper

The LockBit ransomware group is heavily invested in the development of their own tool, which is evident from the timely version updates as well as creating their own exfiltration tool *StealBit*.

The LockBit ransomware group is also keen to expand their market by adding additional target OS such as *LockBit Linux/ESXi*, which targets Linux machines. A MacOS X variant was also released in April 2023.

The LockBit ransomware group was also known to introduce a bug bounty program to "improve" ransomware group's operation.

Lockbit Builder

Despite their active operations and meeting affiliates demands, in September 2022, Twitter/X user ali_qushji (account is now suspended) uploaded LockBit 3.0 builder to GitHub and made it available to the public for download. This leak allowed defenders to further analyze and better understand the ransomware. However, this leak also led to other ransomware gangs abusing builders such as BlooDy Ransomware Gang.

Tweet on LockBit Builder leak by @3xp0rt

Although the LockBit executable is the most common binary used by ransomware affiliates, the builder also provides two additional executable types:

- Lb3_rundll32.dll: Regular Dynamic-link library (DLL), having multiple exported functions to execute necessary functionality of LockBit.
- Lb3_reflectivedll_dllmain.dll: DLL designed to implement Reflective injection.

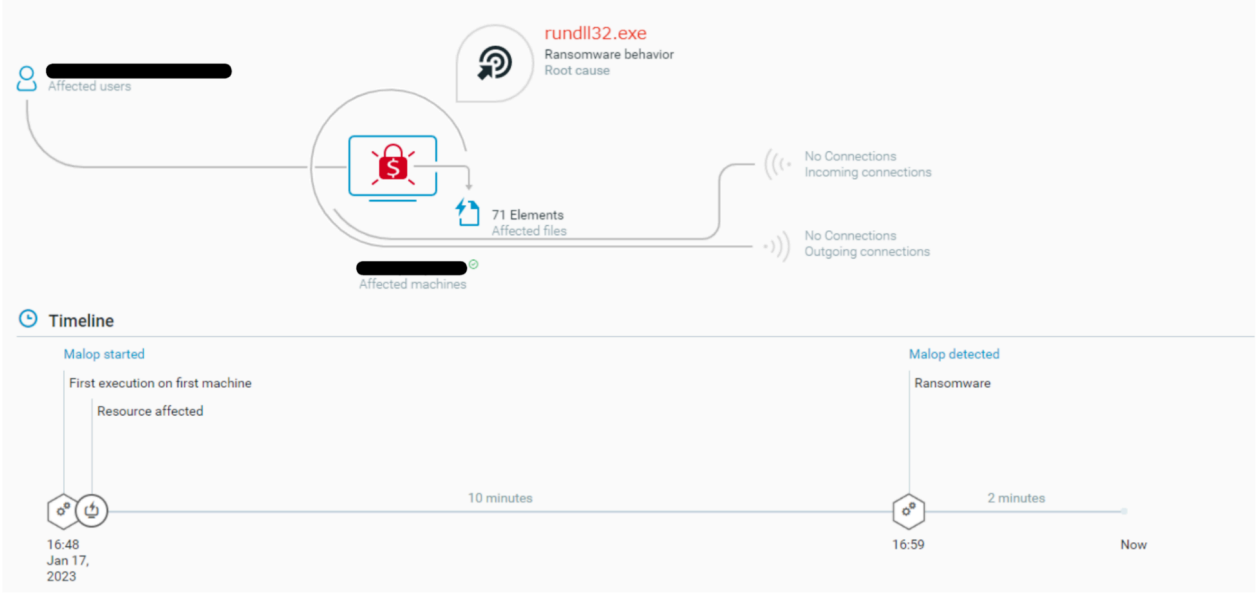
In this report, the technical analysis includes two sections:

- **LockBit Builder Analysis:** Overview of builder's configurations and the process of creating the binaries.

- **LockBit Binary Analysis:** The analysis covers DLL binaries' key points.

DETECTION AND PREVENTION OF THE LOCKBIT RANSOMWARE

The Cybereason Defense Platform is able to detect and prevent infections with LockBit using multi-layer protection that detects and blocks malware with threat intelligence, machine learning, and Next-Gen Antivirus (NGAV) capabilities:



The Cybereason Defense Platform creates a MalOp based ransomware behavior

Cybereason Recommendations:

- **Follow and hunt** Lockbit's affiliates activity in order to identify pre-ransomware behaviors.
    - CISA provides valuable insights about common behaviors of this Threat Actor.
- **Monitor and patch** Common Vulnerabilities and Exposures (CVEs) exploited by this Threat Actor such as :
    - CVE-2023-0669: Fortra GoAnyhwere Managed File Transfer (MFT) Remote Code Execution Vulnerability
    - CVE-2023-27350: PaperCut MF/NG Improper Access Control Vulnerability
    - CVE-2018-13379: Fortinet FortiOS Secure Sockets Layer (SSL) Virtual Private Network (VPN) Path Traversal Vulnerability
- **Promote cybersecurity best practices** such as multifactor authentication and patch management.
- **For Cybereason customers** on the Cybereason Defense Platform:
    - Enable Application Control to block the execution of malicious files.

- Enable Anti-Ransomware in your environment's policies, set the Anti-Ransomware mode to Prevent, and enable Shadow Copy detection to ensure maximum protection against ransomware.
- Enable Variant Payload Prevention with prevent mode on Cybereason Behavioral execution prevention.

MITRE ATT&CK MAPPING

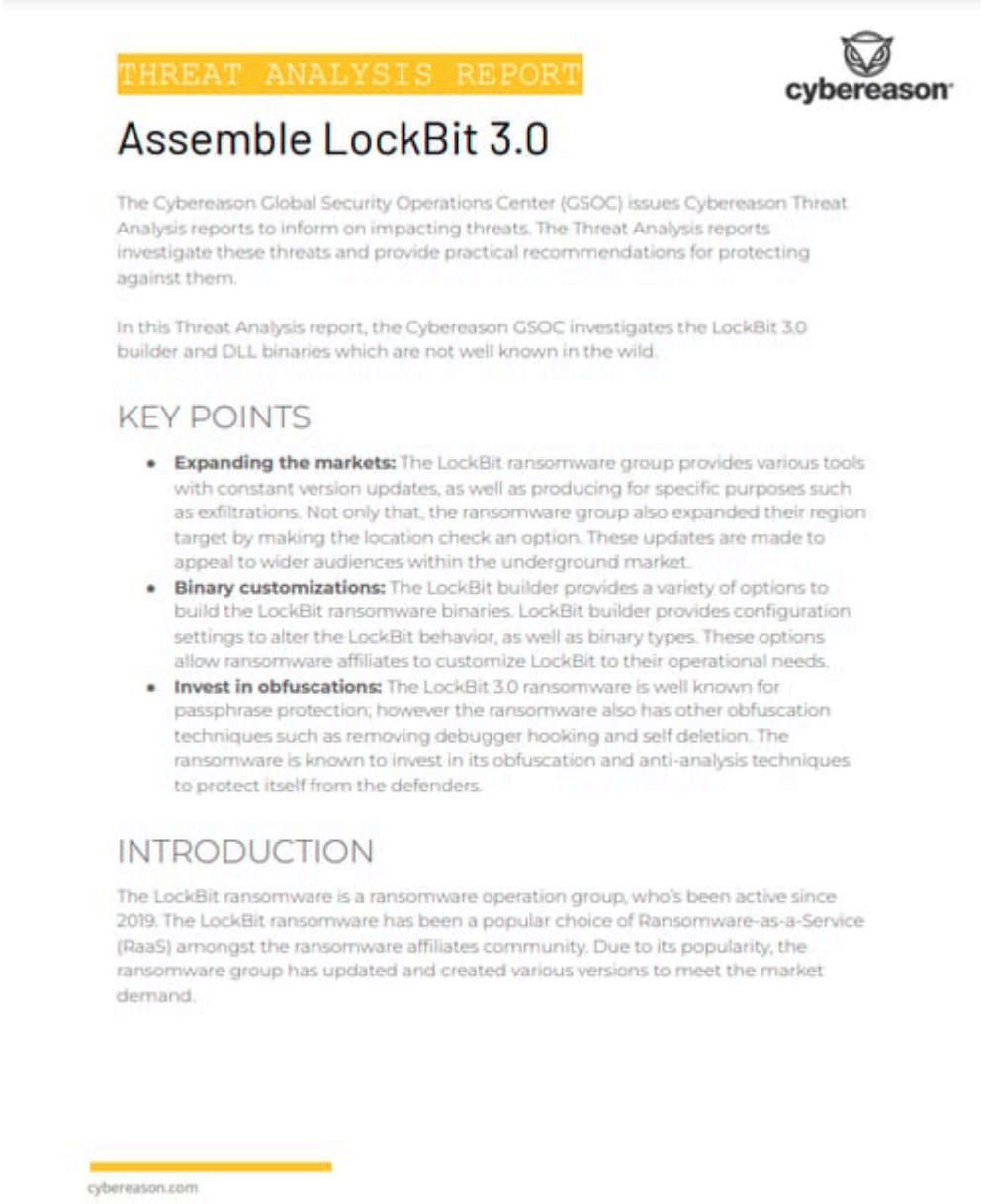
Tactic	Techniques / Sub-Techniques
TA0002: Execution	T1047 – Windows Management Instrumentation
TA0002: Execution	T1106 - Native API
TA0003: Persistence	T1543.003 – Create or Modify System Process: Windows Service
TA0003: Persistence	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
TA0004: Privilege Escalation	T1078.001 – Valid Accounts: Default Accounts
TA0004: Privilege Escalation	T1078.002 – Valid Accounts: Domain Accounts
TA0004: Privilege Escalation	T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control
TA0005: Defense Evasion	T1055 – Process Injection
TA0005: Defense Evasion	T1070.001 – Indicator Removal on Host: Clear Windows Event Logs
TA0005: Defense Evasion	T1218.003 – System Binary Proxy Execution: CMSTP

TA0005: Defense Evasion	T1406.002 – Obfuscated Files or Information: Software Packing
TA0005: Defense Evasion	T1620 - Reflective Code Loading
TA0005: Defense Evasion	T1622 – Debugger Evasion
TA0006: Credential Access	T1003.001 – OS Credential Dumping: LSASS Memory
TA0008: Lateral Movement	T1021.002 - Remote Service: SMB/Windows Admin Shares
TA0009: Collection	T1119 – Automated Collection
TA0040: Impact	T1485 – Data Destruction
TA0040: Impact	T1489 – Service Stop
TA0040: Impact	T1490 – Inhibit System Recovery

Cybereason is dedicated to teaming with Defenders to end cyber attacks from endpoints to the enterprise to everywhere. Learn more about Cybereason XDR, check out our Extended Detection and Response (XDR) Toolkit, or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.

DOWNLOAD THE FULL THREAT ANALYSIS

This blog post is a summary of a full 35-page Threat Analysis Report, which can be downloaded below.



THREAT ANALYSIS REPORT

cybereason

Assemble LockBit 3.0

The Cybereason Global Security Operations Center (GSOC) issues Cybereason Threat Analysis reports to inform on impacting threats. The Threat Analysis reports investigate these threats and provide practical recommendations for protecting against them.

In this Threat Analysis report, the Cybereason GSOC investigates the LockBit 3.0 builder and DLL binaries which are not well known in the wild.

KEY POINTS

- **Expanding the markets:** The LockBit ransomware group provides various tools with constant version updates, as well as producing for specific purposes such as exfiltrations. Not only that, the ransomware group also expanded their region target by making the location check an option. These updates are made to appeal to wider audiences within the underground market.
- **Binary customizations:** The LockBit builder provides a variety of options to build the LockBit ransomware binaries. LockBit builder provides configuration settings to alter the LockBit behavior, as well as binary types. These options allow ransomware affiliates to customize LockBit to their operational needs.
- **Invest in obfuscations:** The LockBit 3.0 ransomware is well known for passphrase protection; however the ransomware also has other obfuscation techniques such as removing debugger hooking and self deletion. The ransomware is known to invest in its obfuscation and anti-analysis techniques to protect itself from the defenders.

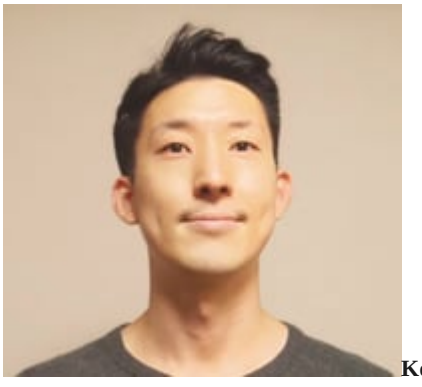
INTRODUCTION

The LockBit ransomware is a ransomware operation group, who's been active since 2019. The LockBit ransomware has been a popular choice of Ransomware-as-a-Service (RaaS) amongst the ransomware affiliates community. Due to its popularity, the ransomware group has updated and created various versions to meet the market demand.

cybereason.com

[Click here](#) to read the full report.

About the Researcher



Kotaro Ogino, Senior Security Analyst, Cybereason Global SOC

Kotaro Ogino is a Senior Security Analyst with the Cybereason Global SOC team. He is involved in threat hunting, administration of Security Orchestration, Automation, and Response (SOAR) systems, and Extended Detection and Response (XDR). Kotaro has a bachelor of science degree in information and computer science

About the Author

Cybereason Global SOC Team

The Cybereason Global SOC Team delivers 24/7 Managed Detection and Response services to customers on every continent. Led by cybersecurity experts with experience working for government, the military and multiple industry verticals, the Cybereason Global SOC Team continuously hunts for the most sophisticated and pervasive threats to support our mission to end cyberattacks on the endpoint, across the enterprise, and everywhere the battle moves.

All Posts by Cybereason Global SOC Team
