March 13, 2025

EMERGING THREATS

LockBit 4.0

UPDATE 03/13/2025: Lockbit 4.0, the most recent iteration of the notorious ransomware family at this time, continues to pose significant threats to organizations worldwide. Researchers have observed this version to have enhanced its techniques related to stealth and adaptability. This can be seen in the inclusion of various evasion techniques, including disabling security features and utilizing obfuscation methods to hinder detection(s). The attack initiates with a modified PowerShell script that executes a secondary script, extracting and deploying a malicious DLL payload. After file encryption, the appending of the ".lockbit" extension and dropping of a ransom note in .txt format mirrors previous iterations of the variant. With new information and research uncovering techniques most recently baked into Lockbit 4.0, threat hunters at Intel 471 have updated the collection with applicable Hunt Packages.

THREAT SUMMARY

Lockbit 4.0, the most recent iteration of the notorious ransomware family at this time, continues to pose significant threats to organizations worldwide. Researchers have observed this version to have enhanced its techniques related to stealth and adaptability. This can be seen in the inclusion of various evasion techniques, including disabling security features and utilizing obfuscation methods to hinder detection(s). The attack initiates with a modified PowerShell script that executes a secondary script, extracting and deploying a malicious DLL payload. After file encryption, the appending of the ".lockbit" extension and dropping of a ransom note in .txt format mirrors previous iterations of the variant. With new information and research uncovering techniques most recently baked into Lockbit 4.0, threat hunters at Intel471 have updated the collection with Hunt Packages related to the following:

- Mshta.exe executing atypically
- PowerShell abuse for the downloading of file(s) and their preceding execution(s)\n- Installation of malicious tooling
- Privilege escalation via user addition(s) to security groupings
- Remote Desktop Protocol configuration modification
- Obfuscated activity related to exfiltration (via Rclone, MegaCMD) and execution (launching binaries or scripts from Common Configuration or System Related Folders)

Prior Information:

The LockBit ransomware variant, previously known as the ".abcd" ransomware was first observed and has been active since September of 2019 - seen targeting organizations throughout the world, including the United States, China, India, U.K, and various other countries across Europe and Asia. In early 2021, the evolution of the variant dubbed "LockBit 2.0" began to circulate in Russian-language cybercrime forums, and shortly after was observed attacking manufacturing, retail, and professional services within countries such as Italy, U.K, Taiwan and Chile. Then in August of 2021, Accenture (a large tech services firm) was attacked by the variant - leading to 2,500 computers being compromised and $50 million in ransom demanded for 6 terabytes of data.

LockBit is considered a "ransomware-as-a-service", meaning the operators provide affiliates the capabilities and access to their developed ransomware. The variant relies on Living off the land binaries (or tools that are native to the operating system) to help

achieve their purpose and make it more difficult to detect, due to these tools being utilized on a day-to-day basis. Similarly to other ransomware variants, LockBit encrypts the victim's system and extorts the victim with ransom demands. However, the variant also identifies and exfiltrates pertinent and sensitive information before the encryption takes place - threatening to publish or sell the obtained data if demands are not met. Due to the variant's TTPs (Tactics, Techniques and Procedures), LockBit is considered similar to known malware "LockerGoga" and "MegaCortex".

In February of 2022, the FBI (Federal Bureau of Investigation) released an update to the LockBit variant, mentioning a few recent discoveries and a new list of discovered IOCs that could be helpful in the security related to LockBit. The full report can be found at: https://www.ic3.gov/Media/News/2022/220204.pdf

Hunt Package Collection:
https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('7ece1eae-8b68-4c95-b2fe-029a8ef22a72'),touched:!t)

SYNOPSIS

In September of 2019, the LockBit ransomware variant (previously known as the .abcd ransomware variant, due to the extension being appended to files during encryption) emerged targeting several countries around the world. The variant evolved to the now infamous LockBit 2.0 in 2021, attacking several companies and organizations, but most notably Accenture in August of the same year. The differences between the versions being attributed to sophistication (less CPU usage, updates ransom note) and the usage of the extension ".lockbit" instead of ".abcd".

The variant abuses Living off the Land Binaries such as Windows PowerShell and SMB (server message block) in order to disguise activities as "normal" and obfuscate their procedures - they have also been observed utilizing publicly accessible tools such as Mimikatz. When a machine is compromised, the variant is self spreading, not needing manual interaction for the infection to spread and propagate on a victim's machine (as well as other hosts that are reachable). The operators of LockBit 2.0 also utilize a method called "double extortion", which means that the system is not only encrypted, but the pertinent and sensitive data is also exfiltrated before the encryption is completed. Therefore, the operator is capable of not only threatening the loss of data, but the public release or sale of the data as well.

The variant is known to initially breach the network via social engineering (phishing e-mails for example) or the abuse of unpatched vulnerabilities that are taken advantage of. After the initial access vector is achieved, the variant utilizes post exploitation tools to attain escalated privileges (such as Mimikatz) and move laterally - also abusing legitimate windows tools such as "net.exe", "taskkill.exe" and "wmic.exe" for reconnaissance and execution. Techniques such as UAC Bypass for elevated execution, and Wevutil cleanup for defense evasion purposes can be noted as well. After disabling security programs and disabling recovery options (deleting shadow copies for example), the encryption payload is deployed. Similar to other ransomware variants, LockBit will then sprawl through the system and lock/encrypt files - recent developments also observing the exfiltration of these files before full encryption is achieved with the "Stealbit" application. A ransom note in a text file will also be dropped in every system folder, giving the victim instructions on decryption.

In February of 2022, the FBI (Federal Bureau of Investigation) released an update to the LockBit variant, with recent discovery of the addition of a Linux encryptor being used to

target VMware ESXi servers for example. The report also mentions a hidden debug window, as well as a new list of discovered IOCs. With the recent vulnerability developments of the Log4j software library, there is more reason to be aware of potential initial access vectors of ransomware variants such as LockBit.

The full report can be found at: https://www.ic3.gov/Media/News/2022/220204.pdf

HUNT PACKAGE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('7ece1eae-8b68-4c95-b2fe-029a8ef22a72'),touched:!t)

RELATED HUNT PACKAGES

AUTORUN OR ASEP REGISTRY KEY MODIFICATION

https://hunter.cyborgsecurity.io/details/use-case/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

POSSIBLE DELAYED EXECUTION IN COMMANDLINE ARGUMENT USING PING.EXE AND LOOPBACK ADDRESS

https://hunter.cyborgsecurity.io/details/use-case/a2e40a77-69b7-4cdc-bf89-e04288bbe2c5

WINDOWS MANAGEMENT INSTRUMENTATION (WMI) CALL TO DELETE SHADOWCOPY VIA WMIC COMMAND

https://hunter.cyborgsecurity.io/details/use-case/f047c78d-d761-4e34-b4fd-fc1902e4f8b1

RANSOMWARE DESKTOP WALLPAPER NOTIFICATIONS

https://hunter.cyborgsecurity.io/details/use-case/bd1e3ea3-c9ec-44b6-a34d-fe7f349954ce

POTENTIAL EXFILTRATION - COMMON RCLONE ARGUMENTS

https://hunter.cyborgsecurity.io/details/use-case/f075c217-783e-459a-aeb4-42ea91e07af7

UAC BYPASS ATTEMPT VIA ELEVATED COM ABUSE

https://hunter.cyborgsecurity.io/details/use-case/03036b01-dc04-4cd1-9388-bd62e1b0ff2d

UAC BYPASS METHOD - CMSTPLUA COM (PROCESS EXECUTION)

https://hunter.cyborgsecurity.io/details/use-case/6a26c900-3e20-4796-b4db-c66276f086ee

DISPLAY CALIBRATOR REGISTRY KEY MODIFICATION - POTENTIAL UAC BYPASS ATTEMPT

https://hunter.cyborgsecurity.io/details/use-case/1a4e1ad3-18fa-45db-b437-d10dc70dcdfb

REMOTE DESKTOP PROTOCOL CONFIGURATION FILE CREATED

https://hunter.cyborgsecurity.io/details/use-case/8c05b760-c982-4630-80cd-b1a92b1057f1

ACTIVE DIRECTORY DISCOVERY AND RECONNAISSANCE - ADFIND.EXE EXECUTION

https://hunter.cyborgsecurity.io/details/use-case/dac3faed-30b5-4e03-aab4-f96eb7b5b3a4

FORCE GROUP POLICY UPDATE ACROSS ENTIRE DOMAIN - POWERSHELL

https://hunter.cyborgsecurity.io/details/use-case/c5d5f9cf-cd81-4c7d-bf29-0141e294cc68

METHODS FOR DOWNLOADING FILES WITH POWERSHELL

https://hunter.cyborgsecurity.io/details/use-case/c7b320fb-ac67-45b0-92c4-b0f1e10b4e46

WEVTUTIL CLEARED LOG

https://hunter.cyborgsecurity.io/details/use-case/7ceada06-54e2-4b44-9dca-b4e8d4ba401d

POTENTIAL UAC BYPASS VIA DISPLAY CALIBRATOR REGISTRY KEY - POWERSHELL SCRIPT BLOCK LOGGING

https://hunter.cyborgsecurity.io/details/use-case/6e324edb-e721-4606-bb5f-84310f3bf5a0

SUSPICIOUS EXECUTABLE OR SCRIPTS LAUNCHED IN COMMON CONFIGURATION OR SYSTEM RELATED FOLDERS

https://hunter.cyborgsecurity.io/details/use-case/F2DD3A46-1C5D-42D3-B3FA-5BEC58D75E0B

USER ADDED TO DEFAULT PRIVILEGED WINDOWS SECURITY GROUPS

https://hunter.cyborgsecurity.io/details/use-case/b6365ad5-0ccd-4426-97bc-b9484eb9579f

MIMIKATZ DRIVER INSTALLED

https://hunter.cyborgsecurity.io/details/use-case/dd5c7bee-80bf-492a-afa1-fe547d048a10

DISPLAY CALIBRATOR REGISTRY KEY MODIFICATION - COMMAND LINE ARGUMENTS

https://hunter.cyborgsecurity.io/details/use-case/afe850d6-07ca-4597-9745-b405ddc6b6eb

ZEROING OUT A FILE WITH 'FSUTIL.EXE'

https://hunter.cyborgsecurity.io/details/use-case/5fd77015-9ca6-4951-b9ea-9c783cd962c4

SUSPICIOUS BCDEDIT ACTIVITY - POTENTIAL RANSOMWARE

https://hunter.cyborgsecurity.io/details/use-case/8a4f0a60-2b55-4dfd-8788-8691e11e1ca1

MSHTA EXECUTING EMBEDDED OR APPENDED CODE

https://hunter.cyborgsecurity.io/details/use-case/20d8238c-54eb-4b2c-b3ef-eb814e933a5e

LOCAL DATA STAGING - ADFIND.EXE

https://hunter.cyborgsecurity.io/details/use-case/1fe16ece-e03d-444e-bebc-fcd2bab5c974

EXCESSIVE WINDOWS DISCOVERY COMMANDLINE ARGUMENTS - POTENTIAL MALWARE INSTALLATION

https://hunter.cyborgsecurity.io/details/use-case/8bb5819f-06a4-4e5d-9099-e43115601999

MICROSOFT DEFENDER ANTIVIRUS DISABLED VIA REGISTRY KEY MANIPULATION

https://hunter.cyborgsecurity.io/details/use-case/81d218e6-0c53-42c4-9275-4aac0eef5bc6

SHADOW COPIES DELETION USING OPERATING SYSTEMS UTILITIES

https://hunter.cyborgsecurity.io/details/use-case/2e3e9910-70c1-4822-804a-ee9919b0c419

MEGA CMD ACTIVITY POTENTIAL DATA EXFILTRATION

https://hunter.cyborgsecurity.io/details/use-case/8aa2eb57-0584-4baa-b734-088147458839

MITRE CONTEXT

- Exploits Vulnerabilities:
  - CVE-2024-1709
  - CVE-2024-1708
- MITRE Tactic Names:
  - Execution
  - Command and Control
  - Exfiltration
  - Privilege Escalation
  - Credential Access
  - Lateral Movement
  - Defense Evasion
  - Persistence
  - Initial Access
  - Discovery
  - Impact
- MITRE Technique Names:
  - Inhibit System Recovery
  - Windows Management Instrumentation
  - Mshta
  - Group Policy Modification
  - Exfiltration Over Alternative Protocol
  - Malicious File
  - Spearphishing Attachment
  - Domain Account
  - Domain Trust Discovery
  - Registry Run Keys / Startup Folder
  - Exfiltration to Cloud Storage
  - Remote Desktop Protocol
  - Disable or Modify Tools
  - Bypass User Account Control
  - Modify Registry
  - Clear Windows Event Logs
  - Ingress Tool Transfer
  - Time Based Evasion

    - Local Accounts
    - Internal Defacement
    - LSASS Memory
    - PowerShell
    - Remote System Discovery
    - Indicator Removal
- MITRE Technique IDs:
    - T1482
    - T1136.002
    - T1070
    - T1490
    - T1567.002
    - T1021.001
    - T1497.003
    - T1548.002
    - T1547.001
    - T1566.001
    - T1218.005
    - T1484.001
    - T1047
    - T1491.001
    - T1562.001
    - T1204.002
    - T1070.001
    - T1048
    - T1059.001
    - T1003.001
    - T1078.003
    - T1105
    - T1112
    - T1018
- Threat Names:
    - Lockbit 4.0
    - Lockbit 3.0

REFERENCES

1. https://www.ic3.gov/Media/News/2022/220204.pdf
2. https://aksk.gov.al/wp-content/uploads/2025/01/Lockbit-4.0-en-2.pdf