SECURITY ADVISORY

CYBER STASH

March, 2023

MULTIPLE CVEs

Lockbit 3.0 Ransomware

Context

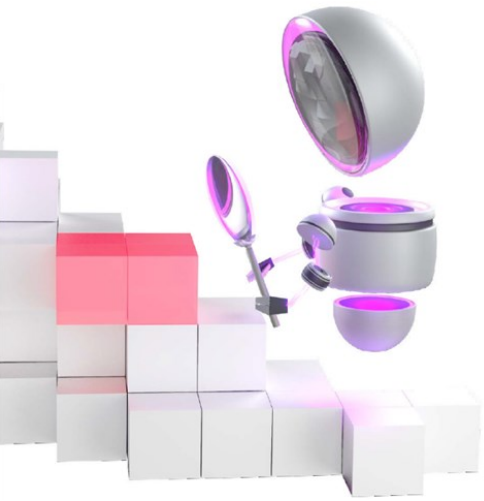
Lockbit 3.0 is a pernicious form of ransomware that encrypts files on infected systems and demands payment for the decryption key. This Ransomware-as-a-Service (RaaS) variant first emerged in March 2023 and employs various distribution vectors, including phishing emails, exploit kits, compromised credentials, and brute-force attacks against exposed public services. The threat actors behind Lockbit 3.0 also leverage remote administration tools such as AnyDesk, Splashtop, and Atera RMM to establish persistent access to the victim's network.

Once a system is infected with Lockbit 3.0 ransomware, it employs advanced Living-off-the-Land (LoL) techniques and additional tools to spread itself across the network, seeking out other vulnerable devices. This allows the ransomware to maximise its impact, potentially causing significant damage to the affected organisation. Given the sophisticated tactics used by Lockbit 3.0 threat actors, organisations must remain vigilant and adopt a multi-layered security approach to detect and prevent attacks in real-time.

Mitigation

To reduce the chances of being affected by Lockbit 3.0 cyber attacks, it is advised to implement the following measures for risk mitigation:

- Keep all software up-to-date, including anti-virus and anti-malware software.
- Implement multi-factor authentication on all accounts accessible remotely.



- Enforce application whitelisting policies to control which applications can run on your systems and how they interact with their environment.
- Control and monitor privileged tools such as PsExec and WMI to prevent misuse and unauthorised access to sensitive systems and data.
- Minimise exposure to high-risk infrastructures by limiting network access of systems using tactical and operational threat intelligence.

Technical Details

Tactics, Techniques and Procedures

After gaining access inside the victim network, Lockbit 3.0 ransomware uses the following post-exploitation adversary techniques:

- Credential harvesting using Mimikatz.
- Disabling Microsoft Defender and other endpoint security software by abusing group policy and tools such as GMER, PCHunter, and Process Hacker, respectively.
- Deleting volume shadow copies using WMI through COM objects.
- Exfiltrating data using RClone to publicly available cloud file-sharing services like MEGASync, and FileZilla.
- Using Netscan and Advanced Port Scanner to enumerate internal network.
- Using ICMLuaUtil COM interface under dllhost.exe to bypass user account control (UAC) for privilege escalation.
- Using the AdFind tool to locate the Domain Controller or Active Directory server.

Cyber Threat Intelligence

LockBit 3.0 is a notorious ransomware that comes in two variants, LockBit RED and LockBit BLACK. Of the two, LockBit BLACK is the most prevalent ransomware variant worldwide, and both are suspected to have reused the source code from another ransomware, BlackMatter. Recently, in February 2023, the LockBit ransomware threat actors have advertised a new variant called LockBit GREEN. Reports indicate that LockBit GREEN shares a significant portion of its source code with Conti ransomware. These findings suggest that LockBit threat actors are continually evolving their tactics to bypass security measures and carry out cyberattacks.

It is highly likely that LockBit ransomware will continue to evolve with new variants that utilise additional Living-off-the-Land (LOL) techniques and commonly used software for conducting credential harvesting, lateral movement, and data exfiltration. This is a concerning trend as LockBit threat actors have already shown their willingness to adapt to the latest security measures and leverage advanced tactics to achieve their objectives.

References

Yara Rules

https://github.com/reversinglabs/reversinglabs-yara-rules/blob/develop/yara/ransomware/Win32.Ransomware.LockBit.yara

https://twitter.com/ochsenmeier/status/1543949415777542145?lang=en

Related IOC's

https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques/

Public Intelligence

https://thehackernews.com/2023/03/lockbit-30-ransomware-inside.html

https://www.cyber.gov.au/about-us/advisories/2023-03-acsc-ransomware-profile-lockbit-3.0

https://www.kaspersky.com/resource-center/threats/lockbit-ransomware

https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html

https://www.securin.io/all-about-lockbit-ransomware/