T2023_04 Ransomware threat actors you should know: LockBit

What is LockBit ransomware

LockBit is a ransomware attack in an extensive line of extortion cyberattacks. It was sometimes called the "ABCD" ransomware, but it has now developed into a distinct and formidable danger among these extortion tools. Because it bases its ransom demands on a monetary payment in exchange for decryption, LockBit is a type of ransomware known as a "crypto virus." Instead of individuals, it primarily focuses on businesses and governmental institutions. LockBit performs ransomware-as-a-service (RaaS) operations. Ransomware as a Service (RaaS) is a business model in which ransomware operators charge affiliates to conduct ransomware attacks devised by the operators. Consider ransomware as a service to be a subset of the software as a service (SaaS) business model.

How does LockBit ransomware work

The first LockBit detection occurred in September 2019. LockBit has changed since then: LockBit 2.0 first emerged in 2021, and LockBit 3.0, the most recent version, was found in June 2022. LockBit mostly uses paid access, unpatched vulnerabilities, insider access, and zero-day exploits to get initial access to targeted networks. "Second-stage" LockBit accomplishes its major objectives, such as stealing and encrypting data, by taking control of the victim's system and gathering network information.

Typical LockBit attacks use a double extortion strategy to persuade victims to pay first to restore access to their encrypted files and then pay again to prevent their stolen data from being made publicly available. An Initial Access Broker (IAB) is a device that, when used as a ransomware-as-a-service (RaaS), deploys first-stage malware, or otherwise acquires access to the infrastructure of a target company. After that, they sell the primary LockBit operator that accesses for later second-stage exploitation.

Indicators of compromises for LockBit ransomware:

https://github.com/sophoslabs/IoCs/blob/master/Ransomware-LockBit

Remediation

Since LockBit normally utilizes spam emails containing harmful documents, it is critical to require multi-factor authentication and to exercise caution when opening email attachments.

Keeping offline backups is the most crucial step in combating ransomware attacks. The organization, however, employs a double extortion approach, stealing the victim's data before encrypting it, rendering even offline backups insufficient to escape paying the ransom. To avoid this, organizations should be aware of any weaknesses in their environment.

The following are some steps users and administrators can take to reduce the risk of infection by LockBit ransomware:

Use multifactor authentication

- Require multifactor authentication to remotely access networks from external sources.

Implement network segmentation and filter traffic

- Implement and ensure robust network segmentation between networks and functions to reduce the spread of ransomware. Define a demilitarized zone that eliminates unregulated communication between networks.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses.
- Enable strong spam filters to prevent phishing emails from reaching end users. Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments. Filter emails containing executable files to prevent them from reaching end users.
- Implement a URL blocklist and/or allowlist to prevent users from accessing malicious websites.

Scan for vulnerabilities and keep software updated.

- Set antivirus/antimalware programs to conduct regular scans of network assets using up-to-date signatures.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner. Consider using a centralized patch management system.

Remove unnecessary applications and apply controls.

- Remove any application not deemed necessary for day-to-day operations. Conti threat actors leverage legitimate applications—such as remote monitoring and management software and remote desktop software applications—to aid in the malicious exploitation of an organization’s enterprise.
- Investigate any unauthorized software, particularly remote desktop or remote monitoring and management software.
- Implement application allow listing, which only allows systems to execute programs known and permitted by the organization's security policy. Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs.
- Implement execution prevention by disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.

Implement endpoint and detection response tools.

- Endpoint and detection response tools allow a high degree of visibility into the security status of endpoints and can help effectively protect against malicious cyber actors.

Limit access to resources over the network, especially by restricting RDP.

- After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources, and require multifactor authentication.

Secure user accounts.

- Regularly audit administrative user accounts and configure access controls under the principles of least privilege and separation of duties.
- Regularly audit logs to ensure new accounts are legitimate users.

References

- Meskauskas, T. (2023). LockBit 2.0 Ransomware. *Decryption, Removal, and Lost Files Recovery (Updated)*. https://www.pcrisk.com/removal-guides/21605-lockbit-2-0-ransomwarev
- Ribeiro, A. (2023, March 17). *Known LockBit 3.0 ransomware IOCs and TTPs found in recent assaults, US security agencies reveal - Industrial Cyber*. Industrial Cyber. https://industrialcyber.co/cisa/known-lockbit-3-0-ransomware-iocs-and-ttps-found-in-recent-assaults-us-security-agencies-reveal/
- Xti, S. (2023). Dark Web Profile: LockBit 3.0 Ransomware - SOCRadar. *SOCRadar® Cyber Intelligence Inc.* https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/