HC3: Analyst Note
December 12, 2022 TLP:CLEAR Report: 202212121700

LockBit 3.0 Ransomware

Executive Summary
LockBit 3.0 is the newest version of the LockBit ransomware that was first discovered in September 2019. The ransomware family has a history of using the Ransomware-as-a-service (RaaS) model and typically targets organizations that could pay higher ransoms. Historically, this ransomware employs a double extortion technique where sensitive data is encrypted and exfiltrated. The actor requests payment to decrypt data and threatens to leak the sensitive data if the payment is not made. With the new release, it appears that the ransomware is using a triple extortion model where the affected victim may also be asked to purchase their sensitive information. Since its appearance, HC3 is aware of LockBit 3.0 attacks against the Healthcare and Public Healthcare (HPH) sector. Due to the historical nature of ransomware victimizing the healthcare community, LockBit 3.0 should be considered a threat to the HPH sector.

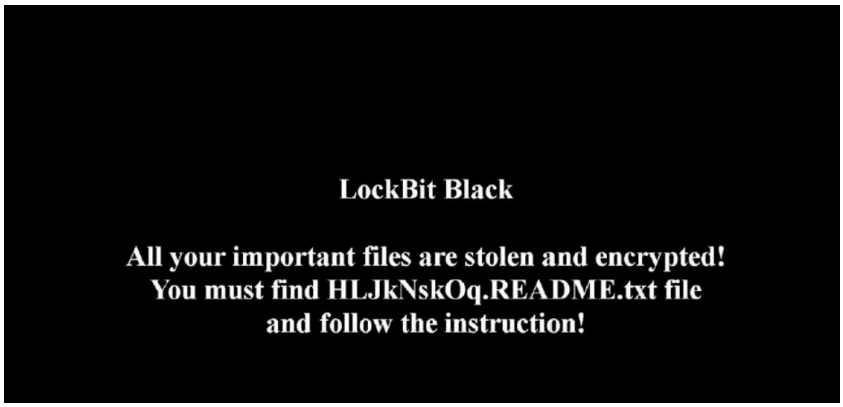
Report
LockBit 3.0, also called LockBit Black, was discovered in June 2022. LockBit operates with the RaaS model, where they will work with affiliates who may not already have the resources for creating and deploying attacks. In this situation, a percentage of the ransom would go back to the affiliated hacker. Open-sourced reporting generates multiple variations of ransom cost, but numbers have been seen to go well into the millions of U.S. Dollars (USD). Like most ransomware groups, the motivation behind the attacks appears to be financial gain. The ransomware has been a challenge for many security researchers because the malware sometimes requires a unique 32-character password each time it is launched, giving it anti-analysis features. LockBit 3.0 is also protected against analysis due to many undocumented kernel level Windows functions, according to a report from VMware.

Research from Sophos suggests that the ransomware has carried over most of the functions from LockBit 2.0 but has been observed to have new capabilities. Also, the malware appears to be utilizing features of another well-known ransomware, BlackMatter. These similarities include the ability to send ransom notes to a printer on the network, deleting Volume Shadow Copies, obtaining the victim's operating system, and several debugging features. LockBit 3.0 will take additional steps to attempt to obfuscate itself. Due to the striking number of similarities, Sophos suggest that LockBit 3.0 could be reusing some of the code from BlackMatter.

Further research states that LockBit 3.0 is a Win32.exe file, and uses the "-pass" argument for execution. The encryption uses a Base64-encoded hash and an RSA public key in its configuration and hashes it with MD5. The malware is capable of targeting Windows and Linux systems. Additionally, the new strain contains worm capabilities to spread itself without human interaction. Encrypted files can only be unlocked with LockBit's decryption tool. Once on the network, the ransomware attempts to download command and control (C2) tools such as Cobalt Strike, Metasploit, and Mimikatz.

Operating as a RaaS, the malware can use various infection techniques. Affiliates will typically purchase access to targets which could be obtained through phishing, brute forcing remote desktop protocol (RDP) accounts, or exploiting other known vulnerabilities. It has also been observed to exploit CVE-2018-13379 and CVE-2021-22986. After encryption is complete, the files extension changes to 'HLjkNskOq' and will alter the desktop wallpaper to inform the infected user of the compromise. Finally, there will be a dropped **README.TXT** with payment instructions.

HC3: Analyst Note
December 12, 2022 TLP:CLEAR Report: 202212121700



Source: Infosec

LockBit 3.0 checks the following user interface (UI) language to avoid infection on these machines:

- Arabic (Syria)
- Armenian (Armenia)
- Azerbaijani (Cyrillic Azerbaijan)
- Azerbaijani (Latin Azerbaijan)
- Belarusian (Belarus)
- Georgian (Georgia)
- Kazakh (Kazakhstan)
- Kyrgyz (Kyrgyzstan)
- Romanian (Moldova)
- Russian (Moldova)
- Russian (Russia)
- Tajik (Cyrillic Tajikistan)
- Turkmen (Turkmenistan)
- Tatar (Russia)
- Ukrainian (Ukraine)
- Uzbek (Cyrillic Uzbekistan)
- Uzbek (Latin Uzbekistan

Analyst Comment

LockBit 3.0 is the newest strain of the LockBit ransomware which appeared in June 2022. After a leak on Twitter, the builder has been used by other threat attackers like the Bl0Ody ransomware gang. Additionally, LockBit has unveiled their own bug bounty program for reporting vulnerabilities which is open to both ethical and unethical hackers. LockBit has been seen to target multiple organizations globally but has heavily victimized the United States and HPH sector. On previous compromises in the HPH sector, the threat actor has occasionally shared proof via screenshots that the network has been compromised and will threaten to publish the stolen data after a set timeline.

Outside of the techniques addressed in this report, HC3 continues to see the following attack vectors frequently associated with ransomware:

- Phishing
- Remote Desktop Protocol (RDP) compromises and credential abuse
- Compromises of exploited vulnerabilities, such as VPN servers
- Compromises in other known vulnerabilities

HC3: Analyst Note
December 12, 2022 TLP:CLEAR Report: 202212121700

The following sources contain indicators of compromise:

- https://cybersecurityworks.com/blog/ransomware/all-about-lockbit-ransomware.html#:~:text=LockBit%20is%20known%20for%20its,%2C%20encryption%2C%20and%20DDoS%20attacks.
- https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit
- LockBit 3.0: A Deeper Look - Packt - SecPro

References

Abrams, Lawrence. "Leaked LockBit 3.0 builder used by 'Bl00dy' ransomware gang in attacks". Bleepingcomputer. Sep 28, 2022. https://www.bleepingcomputer.com/news/security/leaked-lockbit-30-builder-used-by-bl00dy-ransomware-gang-in-attacks/

Abrams, Lawrence. "LockBit ransomware builder leaked online by angry developer". Bleepingcomputer. Sep 21, 2022. LockBit ransomware builder leaked online by "angry developer" (bleepingcomputer.com)

Behling, Dana. "LockBit 3.0 Ransomware Unlocked". Vmware. Oct 15, 2022. https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html

Brandt, Andrew. "LockBit 3.0 'Black' attacks and leaks reveal wormable capabilities and tooling". Sophos. Nov 30, 2022. https://news.sophos.com/en-us/2022/11/30/lockbit-3-0-black-attacks-and-leaks-reveal-wormable-capabilities-and-tooling/

Chavez, Ivan. Gelera, Byron. Casona, Katherine. Morales, Nathaniel. Gonzalez, Ieriz. Ragasa, Nathaniel. "LockBit Ransomware Group Augments Its Latest Variant, LockBit 3.0, With BlackMatter Capabilities". Trendmicro. July 25, 2022. https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant--lockbit-3-.html

"Let's Talk About LockBit - An In-depth Analysis". Cyware. Sep, 2019. Let's Talk About LockBit - An In-depth Analysis | Cyware | Research and Analysis

Trend Micro Research. "Ransomware Spotlight LockBit". Trendmicro. July 14, 2022. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

Rees, Katie. "What Is the LockBit 3.0 Ransomware and What Can You Do About It?". Makeuseof. Aug 12, 2022. https://www.makeuseof.com/what-is-lockbit-ransomware-what-can-you-do-about-it/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback