COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 12. December 09, 2021 HC3 Warns of LockBit Ransomware Threat as Affiliates Ramp Up Attacks

By Jane Anderson

The HHS Health Sector Cybersecurity Coordination Center (HC3) is warning of a rising threat from LockBit, a two-year-old ransomware variant that in June released a new version with faster encryption plus double extortion of victims.

LockBit also has restarted its affiliate program, which allows experienced hackers to set their own ransom and choose the method of payment, paying the LockBit gang around 20% of the total, HC3 said.[1]

"LockBit is ransomware as a service," Senad Aruc, lead cybersecurity architect for Cisco, said during a recent webinar on the variant sponsored by the International Information System Security Certification Consortium.[2] "We all know software as a service, right? We've managed to evolve to ransomware as a service."

Ransomware as a service, or RaaS, is a new business model in which the ransomware creators sell or lease their ransomware variants to affiliates, who then use them to carry out attacks, Aruc said. The business model often includes a platform in the form of a management panel, he said, and customers of LockBit service use this management panel to create new ransomware samples, manage victims and get statistics about their attacks.

"They hire people—actually through a job posting," Aruc said. "They hire very skillful hackers who are going to use their platform for free to attack victims." The creators then receive 10% to 30% of the ransomware proceeds as a commission, he said, adding, "it's a pure, very well designed business."

In addition, the ransomware owners often provide virtual machines, exploits and tools for their affiliates to support their attacks, Aruc said. "Each affiliate has access to a panel where they can monitor their victims and communicate with them," he said. Meanwhile, the ransomware creators "are always going to push [their affiliates] to overachieve," Aruc said, potentially increasing the rewards as affiliates earn money. "The business is huge," he said. "They know, out of 10 victims, two of them are going to pay or one of them is going to pay."

HC3 reported that an anonymous affiliate of LockBit said in an interview that hospitals are easy targets for ransomware. Studies have shown that the health care industry is one of the top industries affected by ransomware.

The hackers do have a code of ethics, HC3 said, and "keeping your word to the victim is an important part of LockBit's business model."

LockBit isn't the only current RaaS threat: three federal agencies (the Cybersecurity & Infrastructure Security Agency, the FBI, and the National Security Agency) warned in October that the BlackMatter RaaS variant was targeting critical infrastructure.[3] BlackMatter was first seen in July 2021, the three agencies said.

LockBit Offers Unique Threat

Aruc said that LockBit, formerly known as ABCD, has grown into a unique threat within the scope of ransomware

extortion tools. "They penetrate the computers, they exfiltrate the data, they check if the data is valuable, and then they start the extortion, forcing you to pay the ransom," he explained. "LockBit can automatically scan the network, it can check for useful targets, it can spread the infection, and it can encrypt every single file with a different key." The LockBit ransomware variant is the third most common ransomware strain in the world, with 7.5% of market share in the first quarter of 2021, he said.

To select a target, LockBit affiliates use mass vulnerability scanning, phishing and credential stuffing (automated use of stolen credentials to find logins that work) as main sources for finding new victims, Aruc said. The affiliates also purchased already-compromised servers and remote desktop protocol access from underground shops that sell them, he said: "They buy victims."

In the preparation phase, the hackers gain access to the compromised computers and attempt to identify all the mission-critical systems, such as domain controllers, backup servers and network attached storage devices, he said.

"When the enumeration is done, the data exfiltration begins," Aruc said. "Before encryption, they do the exfiltration." Once the exfiltration is done, the hackers check the data manually to see if it's valuable and important for the target company. Aruc noted that "if you don't pay, it goes public," uploaded to free file upload services such as MEGA. Uploaded data is used for extortion while negotiating with victims, he added.

After the data exfiltration process, a unique LockBit ransomware sample is generated from the build page of the LockBit management panel, Aruc said. This helps ensure that specific affiliates are communicating with the correct victims, and not the victim of another LockBit affiliate, he added.

LockBit ransomware is executed manually inside the target company systems, Aruc said. "Once the LockBit is executed in a system, it will immediately begin the reconnaissance phase. In this phase LockBit will try to enumerate all the accessible directories and network shares," he explained. "After the enumeration, Lockbit encrypts each file with a random AES [advanced encryption standard] key, which is encrypted with the static public key inside the LockBit sample. Finally, the encrypted AES key is inserted into a specific offset inside the file. Thus, every file inside the target system is encrypted with a different key, and each file can only be opened by the randomly generated RSA private key during the build of the unique sample on the management panel."

Once the ransomware is executed, all important files will be encrypted and backups will be deleted, Aruc said. The victim organization will see wallpaper on their screens explaining what they need to do. LockBit ransomware creates "Restore-My-Files.txt" and "LockBit-note.hta" files on the target system desktop explaining how to get the files back, he said.

The hackers will push the victims to install Tor and will include instructions if the victims aren't familiar with the darknet browser, Aruc said. The contact page also includes "Chat with Support" and "Trial Decrypt" sections. Once a victim sends a message over their unique contact link, a new victim tab with the corresponding build comment shows up on the LockBit management panel dashboard.

"This is not an automatic ransomware attack where they don't care who is the target," Aruc said. "Here, they are choosing the targets very granularly—they are speaking with them, extorting them and negotiating with them."

Once payment has been negotiated and received, the hackers press the decrypt button for that particular victim on the management panel and a unique decryptor ".exe" file is generated for that particular victim's ID, Aruc said. Victims then can download the decryptor file and run it inside their encrypted systems to decrypt their files, he said.

To protect against threats like LockBit, organizations should consider deploying data security solutions such as

content threat removal (CTR), Aruc said. CTR intercepts data that users share with each other, such as documents and emails, and removes risky elements such as macros or scripts that could be hiding malware. CTR can reduce time to detection, and advanced malware protection can help organizations respond faster, he said.

HC3 recommends two specific actions to help prevent LockBit ransomware attacks:

1. Monitoring for, and alerting on, the anomalous execution of legitimate Windows command line tools such as the use of net.exe, taskkill.exe, vssadmin.exe and wmic.exe.

2. Making use of network segregation to limit communications between nodes, especially endpoints, to provide damage limitation and limit the propagation of threats.

1 U.S. Department of Health & Human Services, Health Sector Cybersecurity Coordination Center, "LockBit Ransomware," September 23, 2021, https://bit.ly/3bqiFjA.
2 Senad Aruc, "A Deep Dive into the Operations of the LockBit Ransomware Group," webinar, September 21, 2021, https://bit.ly/2ZBDHcj.
3 Cybersecurity & Infrastructure Security Agency, "BlackMatter Ransomware," alert AA21-291A, October 18, 2021, https://bit.ly/3Gz4pDK.