

LockBit, the new ransomware for hire: a sad and cautionary tale

reader comments

53 with 42 posters participating

Share this story

Ransomware has emerged as one of the top threats facing large organizations over the past few years, with researchers reporting a more than a fourfold increase in detections last year. A recent infection by a fairly new strain called LockBit explains why: after it ransacked one company's poorly secured network in a matter of hours, leaders had no viable choice other than to pay the ransom.

A report published by McAfee documents the effectiveness of this newcomer ransomware. Incident responders with Northwave Intelligent Security Operations aided in the analysis. LockBit is most prevalent in countries including the US, the UK, France, Germany, Ukraine, China, India, and Indonesia.

Attackers started out by researching potential targets with valuable data and the means to make big payouts when faced with the dim prospect of losing access to it. The attackers then used a list of words in hopes of gaining access to one of the accounts. Eventually, they hit the jackpot: an administrative account that had free rein over the entire network. The weak account password, combined with the lack of multi-factor authentication protection, gave the attackers all the system rights they needed.

Stealth, automation, and discretion

Many LockBit competitors like Ryuk rely on live human hackers who, once gaining unauthorized access, spend large amounts of time surveying and surveilling a target's network and then unleash the code that will encrypt it. LockBit worked differently.

"The interesting part about this piece of ransomware is that it is completely self-spreading," said Patrick van Looy, a cybersecurity specialist at Northwave, one of the firms that responded to the infection. "Hence, the attacker was only

inside the network for a few hours. Normally we see that an attacker is inside the network for days or even weeks and does this reconnaissance of the network manually.”

After getting in, LockBit used a dual method to map out and infect the victimized network. ARP tables, which map local IP addresses to device MAC addresses, helped to locate accessible systems, and server message block, a protocol used for sharing files and folders among networked machines, allowed the infected nodes to connect to uninfected ones. LockBit would then execute a PowerShell script that spread the ransomware to those machines.

Using SMB, ARP tables, and PowerShell are an increasingly common way of spreading malware throughout a network, and with good reason. Because almost all networks rely on these tools, it's hard for antivirus and other network defenses to detect their malicious use. LockBit had another means of staying stealthy. The malicious file the PowerShell script downloaded was disguised as a PNG image. In fact, the downloaded file was a program executable that encrypted the files on the machine.

LockBit had another clever trick. Before the ransomware encrypted data, it connected to an attacker-controlled server and then used the machine's IP address to determine where it was located. If it resided in Russia or another country belonging to the Commonwealth of Independent States, it would abort the process. The reason is most likely to prevent being prosecuted by law enforcement authorities there.

Once the data was locked up, organization computers were left with a desktop that looked something like this:

The ransomware note looked like this:

Customer support, determination, and confidence

In a tragic but all-too-common failing, the organization that was hit by LockBit had no recent backup. With its entire network tied up, leaders had a choice of either paying the ransom or losing their data forever. They opted for the first option.

Using a Tor site, the organization paid the ransom and, after several hours, used the same anonymous service to obtain the

decryption key. Like many other ransomware operators, those behind this attack had a support desk that communicated over the anonymized Jabber messenger to resolve several problems the organization had in rebuilding the locked-up network.

LockBit is sold in underground broker forums that often require sellers to put up a deposit that customers can recover in the event the wares don't perform as advertised. In a testament to their confidence and determination, the LockBit sellers have forked out almost \$75,000.

McAfee and Northwave aren't the only security firms that have taken notice of LockBit, which its creators offer as a ransomware-as-a-service to customers, who then use it to infect and exact payments from targets. Last week, Sophos provided its own report on the ransomware.

User beware

Sophos said the new malware has been adding a variety of new capabilities, including a privilege-escalation technique that can bypass the User Account Control that requires a user sign off before an application can run with administrative permissions. This feature is useful in the event the malware gets a toehold in a network but has only limited privileges. Sophos also said the LockBit downloads its victims' data so operators can post it online if victims don't pay up, a tactic followed by other ransomware like Maze, Sodinokibi, Nemty, and DoppelPaymer.

Friday's account is a cautionary tale underscoring the perils of weak passwords, the lack of multi-factor authentication, and other defense-in-depth measures. The analysis, along with the blow-by-blow account of how LockBit steamrolled through one organization's network in a matter of hours, suggests that ransomware may one day gain parity with other feared ransomware packages such as Maze, Sodinokibi, and Ryuk.

"It seems that LockBit has joined the underground scene with clear determination to do business," Friday's report concluded. "The authors have put down a deposit in excess of 10.5 BTC to guarantee it, to build trust, as shown on one of the forums. Our telemetry shows that LockBit activity is still limited today but we can definitely expect to see more bespoke LockBit attacks in the near future."

Post updated to correct the definition of ARP table.

<https://arstechnica.com/?p=1672390>