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

By Dan Goodin

Published: 2020-05-01 · Archived: 2026-04-05 13:46:36 UTC

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.

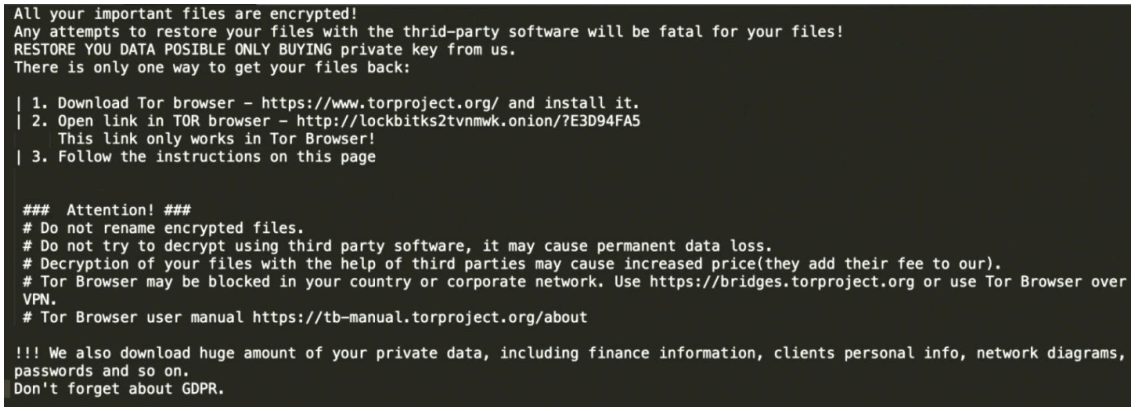
LockBit had another clever trick. Before the ransomware encrypted data, it connected to an attacker-controlled server and then used the machine's IP address to determine where it was located. If it resided in Russia or another country belonging to the Commonwealth of Independent States, it would abort 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:

Credit: McAfee

Credit: McAfee

The ransomware note looked like this:



Credit: McAfee

Credit: McAfee

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.
