LockBit ransomware — What You Need to Know

By Kaspersky

Published: 2020-09-25 · Archived: 2026-04-05 13:45:34 UTC

LockBit Definition

LockBit ransomware is malicious software designed to block user access to computer systems in exchange for a ransom payment. LockBit will automatically vet for valuable targets, spread the infection, and encrypt all accessible computer systems on a network. This ransomware is used for highly targeted attacks against enterprises and other organizations. As a self-piloted cyberattack, LockBit attackers have made a mark by threatening organizations globally with some of the following threats:

- **Operations disruption** with essential functions coming to a sudden halt.
- **Extortion** for the hacker's financial gain.
- **Data theft and illegal publication** as blackmail if the victim does not comply.

What is LockBit ransomware?

LockBit is a new ransomware attack in a long line of extortion cyberattacks. Formerly known as "ABCD" ransomware, it has since grown into a unique threat within the scope of these extortion tools. LockBit is a subclass of ransomware known as a 'crypto virus' due to forming its ransom requests around financial payment in exchange for decryption. It focuses mostly on enterprises and government organizations rather than individuals.

Attacks using LockBit originally began in September 2019, when it was dubbed the ".abcd virus." The moniker was in reference to the file extension name used when encrypting a victim's files. Notable past targets include organizations in the United States, China, India, Indonesia, Ukraine. Additionally, various countries throughout Europe (France, UK, Germany) have seen attacks.

Viable targets are ones that will feel hindered enough by the disruption to pay a heavy sum — and have the funds to do so. As such, this can result in sprawling attacks against large enterprises from healthcare to financial institutions. In its automated vetting process, it seems to also intentionally avoid attacking systems local to Russia or any other countries within the Commonwealth of Independent States. Presumably, this is to avoid prosecution in those areas.

LockBit functions as ransomware-as-a-service (RaaS). Willing parties put a deposit down for the use of custom for-hire attacks, and profit under an affiliate framework. Ransom payments are divided between the LockBit developer team and the attacking affiliates, who receive up to ¾ of the ransom funds.

How does LockBit ransomware work?

LockBit ransomware is considered by many authorities to be part of the “LockerGoga & MegaCortex” malware family. This simply means that it shares behaviors with these established forms of targeted ransomware. As a quick explanation, we understand that these attacks are:

- **Self-spreading** within an organization rather than requiring manual direction.
- **Targeted** rather than spread in a scattershot fashion like spam malware.
- **Using similar tools** to spread, like Windows Powershell and Server Message Block (SMB).

Most significant is its ability to self-propagate, meaning it spreads on its own. In its programming, LockBit is directed by pre-designed automated processes. This makes it unique from many other ransomware attacks that are driven by manually living in the network — sometimes for weeks — to complete recon and surveillance.

After the attacker has manually infected a single host, it can find other accessible hosts, connect them to infected ones, and share the infection using a script. This is completed and repeated entirely without human intervention.

Furthermore, it uses tools in patterns that are native to nearly all Windows computer systems. Endpoint security systems have a hard time flagging malicious activity. It also hides the executable encrypting file by disguising it as the common .PNG image file format, further deceiving system defenses.

Stages of LockBit attacks

LockBit attacks can be understood in roughly three stages:

1. Exploit
2. Infiltrate
3. Deploy

Stage 1: Exploit weaknesses in a network. The initial breach looks much like other malicious attacks. An organization may be exploited by social engineering tactics like phishing, in which attackers impersonate trusted personnel or authorities to request access credentials. Equally viable is the use of brute force attacks on an organization’s intranet servers and network systems. Without proper network configuration, attack probes may only take a few days to complete.

Once LockBit has made it into a network, the ransomware prepares the system to release its encrypting payload across every device it can. However, an attacker may have to ensure a few additional steps are completed before they can make their final move.

Stage 2: Infiltrate deeper to complete attack setup if needed. From this point forward, the LockBit program directs all activity independently. It is programmed to use what are known as “post-exploitation” tools to get escalate privileges to achieve an attack-ready level of access. It also roots through access already available via lateral movement to vet for target viability.

It is at this stage that LockBit will take any preparative actions before deploying the encryption portion of the ransomware. This includes disabling security programs and any other infrastructure that could permit system recovery.

The goal of infiltration is to make unassisted recovery impossible, or slow enough that succumbing to the attacker's ransom is the only practical solution. When the victim is desperate to get operations back to normal, this is when they will pay the ransom fee.

Stage 3: Deploy the encryption payload. Once the network has been prepared for LockBit to be fully mobilized, the ransomware will begin its propagation across any machine it can touch. As stated previously, LockBit doesn't need much to complete this stage. A single system unit with high access can issue commands to other network units to download LockBit and run it.

The encryption portion will place a "lock" on all the system files. Victims can only unlock their systems via a custom key created by LockBit's proprietary decryption tool. The process also leaves copies of a simple ransom note text file in every system folder. It provides the victim with instructions to restore their system and has even included threatening blackmail in some LockBit versions.

With all the stages completed, the next steps are left up to the victim. They may decide to contact LockBit's support desk and pay the ransom. However, following their demands is not advised. Victims have no guarantee that the attackers will follow through on their end of the bargain.

Types of LockBit threats

As the latest ransomware attack, the LockBit threat can be a significant concern. We cannot rule out the possibility that it can take hold across many industries and organizations, especially with a recent increase in remote working. Spotting LockBit's variants can help with identifying exactly what you're dealing with.

Variant 1 —. abcd extension

LockBit's original version renames files with the ".abcd" extension name. Additionally, it includes a ransom note with demands and instructions for alleged restorations in the "Restore-My-Files.txt" file, which has been inserted into every folder.

Variant 2 —. LockBit extension

The second known version of this ransomware adopted the ".LockBit" file extension, giving it the current moniker. However, victims will find that other traits of this version appear mostly identical despite some backend revisions.

Variant 3 —. LockBit version 2

The next identifiable version of LockBit no longer requires downloading the Tor browser in its ransom instructions. Instead, it sends victims to an alternate website via traditional internet access.

Ongoing updates and revisions to LockBit

Recently, LockBit has been enhanced with more nefarious features such as negating administrative permission checkpoints. LockBit now disables the safety prompts that users may see when an application attempts to run as an administrator.

Also, the malware now is set up to steal copies of server data and includes additional lines of blackmail included in the ransom note. In case the victim does not follow instructions, LockBit now threatens the public release of the victim's private data.

LockBit removal and decryption

With all the trouble that LockBit can cause, endpoint devices need thorough protection standards across your entire organization. This first step is to have a comprehensive endpoint security solution, such as Kaspersky Next EDR Optimum.

If your organization is already infected, the removal of LockBit ransomware alone doesn't give you access to your files. You will still require a tool to restore your system, as encryption requires a "key" to unlock. Alternatively, you may be able to restore your systems by reimaging them if you've got pre-infection backup images already created.

How to protect against LockBit ransomware

Ultimately, you'll have to set up protective measures to ensure your organization is resilient against any ransomware or malicious attacks from the offset. Here are a few practices that can help you prepare:

1. **Strong passwords should be implemented.** Many account breaches occur due to easy-to-guess passwords, or those that are simple enough for an algorithm tool to discover within a few days of probing. Male sure you pick secure password, such as choosing longer ones with character variations, and using self-created rules to craft passphrases.
2. **Activate multi-factor authentication.** Deter brute force attacks by adding layers atop your initial password-based logins. Include measures like biometrics or physical USB key authenticators on all your systems when possible.
3. **Reassess and simplify user account permissions.** Limit permissions to more strict levels to limit potential threats from passing undeterred. Pay special attention to those accessed by endpoint users and IT accounts

with admin-level permissions. Web domains, collaborative platforms, web meeting services, and enterprise databases should all be secured.

4. **Clean out outdated and unused user accounts.** Some older systems may have accounts from past employees that were never deactivated and closed. Completing a check-up on your systems should include removing these potential weak points.
5. **Ensure system configurations are following all security procedures.** This may take time, but revisiting existing setups may reveal new issues and outdated policies that put your organization at risk of attack. Standard operation procedures must be reassessed periodically to stay current against new cyber threats.
6. **Always have system-wide backups and clean local machine images prepared.** Incidents will happen and the only true safeguard against permanent data loss is an offline copy. Periodically, your organization should be creating backups to keep up-to-date with any important changes to your systems. In case of a backup becoming tainted with a malware infection, consider having multiple rotating backup points for the option to select a clean period.
7. **Be sure to have a comprehensive enterprise cyber security solution in place.** While LockBit can try to disable protections once in a unit, enterprise cyber security protection software would help you catch file downloads across the entire organization with real-time protection. Learn more about Kaspersky Security Solutions for Enterprise to help you protect your business and devices.

Related Articles:

- Ways hackers can violate your online privacy
- What is a security breach?
- Internet of Things Security Threats
- How to protect your privacy against hackers
- Phishing - A Guide

Source: https://www.kaspersky.com/resource-center/threats/lockbit-ransomware