Everything You Need to Know About LockBit

By Aaron Sandeen

Published: 2022-11-02 · Archived: 2026-04-05 17:52:01 UTC

LockBit ransomware is in the minority group of ransomware families that leverage auto-propagating malware and double encryption methods. After its breaches into security behemoth Entrust and the Italian Revenue Agency earlier this summer, LockBit has continued to gain notoriety while on the lookout for its next victim.

LockBit ransomware began its spree of high-profile attacks as early as September 2019 and has remained one of the most prolific groups to date. Motivated by large payouts, the group doesn't fear targeting larger corporations and enterprises.

The ransomware group is known for its particular qualities of a triple-extortion method, sophisticated technology, high-severity cyberattacks, and heavy marketing to affiliates. LockBit's presence is felt globally, and industries are afforded only short moments of respite when the group retreats to develop more devastating upgrades to their toolkit. Its attack frequency and strategy make the group a force to beware of in the cybersecurity world, demonstrating its determination to cause harm.

LockBit: The Brief

- LockBit markets itself as ransomware-as-a-service (RaaS). It works in conjunction with other bad actors who perform attacks for hire, and then split the funds between the LockBit developer team and other accomplices.
- The LockBit family targets both CVE-2021-22986 and CVE-2018-13379.
- The Russian threat actor group, TA505 (also known as Hive0065) has been observed using the LockBit ransomware payload in its attacks.

New Variants

LockBit's origins began as an ABCD cryptovirus in 2019. Its main targets were government organizations in North America, Europe, and APAC regions and included private companies as well, with crypto as their form of ransom payment.

Early targets of LockBit in 2019 and 2020 included Windows systems within financial and healthcare institutions. The ransomware group then took a hiatus to improve its malware kit and operation strategy. To date, two LockBit versions in addition to the initial version have been released, with each subsequent release possessing increased attack capabilities.

LockBit 2.0

LockBit 2.0 was introduced in June 2021 and was documented in attacks in Taiwan, Chile, and the UK. In the 2.0 version, LockBit added the double-extortion technique and auto-encryption of hardware across Windows domains for which it became known. Later in the fall of 2021, the group began branching out into Linux servers, too, specifically attacking ESXi servers.

LockBit 3.0, Also Known as LockBit Black

After another brief hiatus, LockBit returned in June 2022 with the release of another improved version of the ransomware, including a bug bounty program that financially incentivizes researchers to share bug reports. In addition to the program, version 3.0 includes Zcash payments and developed new extortion tactics. Building on top of architecture found in BlackMatter and DarkSide, LockBit now has refined its evasion practices, passwordless execution, and implemented command-line features.

The updated LockBit ransomware was used to attack and steal data from the Italian Revenue Agency and a county office in Ontario, Canada. On top of encryption and the threat of data leaks, the ransomware group has included denial-of-service attacks to increase the pressure on victims.

In a surprising turn of events, an alleged LockBit developer leaked the group's builder used to design the 3.0 version on Twitter, citing frustration with the group's leadership as their motivation for the leak. A blow to the group but a potential risk to the cybersecurity field as the leaked information can equip new individuals with the necessary tools to start their own ransomware kit. In no more than a week after the leak, a new ransomware group was observed using the builder to target companies.

How Dangerous Is LockBit?

LockBit has a diverse arsenal of technologies and techniques to go after the largest organizations, regardless of industry. Here is a snapshot of the tools, tactics, and methods that make LockBit so dangerous:

- StealBit, a malware tool first found in the 2.0 version, was designed for encryption and is believed to be the most efficient and quickest encryption tool.
- StealBit automatically spreads to other connected devices along a network by taking advantage of Windows PowerShell and Server Message Block.
- LockBit's malware can now infect both Windows and Linux systems when initially it could only exploit Windows systems.
- The creation of the bug bounty program is the group's attempt at establishing itself as a professional group of hackers while simultaneously improving its defenses.
- LockBit 3.0 introduced Zcash payment options for ransom collection and to avoid interference from law enforcement agencies.

How to Prevent a LockBit Attack

- Curb unnecessary permissions: More restrictions on permissions are not a bad practice to get in the habit of applying, as more levels of authentication make it difficult for remote hackers to escalate permissions and gain greater access. Pay close attention to users with IT and admin-level permissions.
- Monitor your attack surface: Incorporate a solution that scans your entire attack surface for potential entry points for attackers. Routinely monitor existing and newly added assets to your organization's network.

Security leadership can keep attackers away by cultivating a culture of vigilance with structured vulnerability management processes that prioritize threats based on severity and risk. Despite LockBit's capabilities, organizations do have options when it comes to protecting their organization and partners.

About the Author

CEO & Co-Founder, Securin

Aaron Sandeen is the CEO and co-founder of Securin (formerly Cyber Security Works), a Department of Homeland Security-sponsored company focused on helping leaders proactively increase their resilience against ever-evolving security threats on-premises and in the cloud. Aaron leads Securin in providing intelligent and actionable security insights at every layer of company operations.

Source: https://www.darkreading.com/vulnerabilities-threats/everything-you-need-to-know-about-lockbit