Lockbit 3.0: Another Upgrade to World's Most Active Ransomware - SOCRadar® Cyber Intelligence Inc.

Published: 2023-04-17 · Archived: 2026-04-02 10:36:22 UTC

Last Update: April 17, 2023

LockBit Ransomware gang, also known as Bitwise Spider, are the cybercriminal masterminds behind the popular Lockbit Ransomware-as-a-service. They are one of the most active ransomware gangs with generally multiple victims per day, sometimes higher. On March 16, 2022, they began continuously announcing new victims on their **Dark Web site** much faster than any ransomware group. SOCRadar has detected more than 22 victims in 48 hours.

Origins of the LockBit Ransomware

They have begun their operations in September 2019 as ABCD ransomware and then changed its name to Lockbit. They have rebranded and came back with even better ransomware on June 2021, as **Lockbit 2.0**. We have seen that the Lockbit 2.0 ransomware introduced new features such as shadow copy and **log file deletion** to make recovery harder for the victims. In addition, Lockbit has the fastest encryption speed among the most popular ransomware gangs, with around 25 thousand files encrypted in under one minute.

The gang is believed to be originated in Russia. According to a detailed analysis of Lockbit 2.0, the ransomware checks the default system language and avoids encryption, and stops the attack if the **victim system's** language is Russian or the language of one of the nearby countries.

> Lockbit 2.0 checks the language of the victim machine

Lockbit on Russia – Ukraine Cyberwar

In the cyber crisis between Russia and Ukraine, which began on February 23rd, 2022, Lockbit announced that it would not participate in the **cyberattacks**. They announced that they would not take part in cyberattacks on international conflicts. They are only in it for the business and do not care about politics. Another very active ransomware gang also believed to be from Russia, Conti, had stated that they would be siding with Russia, which some members of Conti were not pleased with. Following the events, some insider members of **Conti** began leaking internal chat logs and source code for the Conti locker and decryptor. You can read more about the Conti Leaks in our blog post.

> Lockbit's announcement on the Russia-Ukraine Cyberwar

A funny detail about the gang is that they are confident in their skills and arrogant. On March 25, 2022, a member of Lockbit has announced on a hacker forum that they'll be giving a million dollars to an FBI agent who can doxx them, placing a million-dollar bounty on its own head.

A member of Lockbit placing bounty on its own head

Dark Web Gossips: Lockbit 3.0 Emerging

FBI's cyber division published an FBI Flash security advisory on Lockbit 2.0's **Indicators of Compromise (IOCs)** on March 4th, 2022. After the FBI's advisory, a user in a Dark Web forum has posted a forum entry with the title "Kockbit fuckup thread." In the post, the user addresses the bugs found in Lockbit 2.0 ransomware and a recovery method for the victims, addressing the FBI's advisory along with Microsoft's Detection and Response Team's (DART's) research on Lockbit. Below, you can find the links for Microsoft DART's research. Microsoft DART researchers have discovered a method by uncovering and exploiting bugs found in the Lockbit 2.0 ransomware, enabling them to successfully revert the encryption process on an MSSQL database of one of Lockbit's victims.

- https://techcommunity.microsoft.com/t5/security-compliance-and-identity/part-1-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254354
- https://techcommunity.microsoft.com/t5/security-compliance-and-identity/part-2-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254421

Dark web forum post on Lockbit bugs and a recovery method

A member of the Lockbit ransomware group has commented on the post explaining the reason for the MSSQL bug. The Lockbit member says the bug will not exist in Lockbit 3.0, signaling the newest version's release.

Lockbit member's comment on the post

After a couple of days, on March 17, the cyber research team **vx-underground** has posted a screenshot of their talks with one of Lockbit's associates. On the screenshot, the vx-underground researcher asks when Lockbit 3.0 is being released, and the Lockbit affiliate says the newest version will be released in one or two weeks.

Source: vx-underground

LockBit Ransomware Gang Develops Encryptors Targeting MacOS For The First Time

The LockBit ransomware gang has created encryptors targeting macOS for the first time, making them the first major ransomware group to specifically target macOS.

Cybersecurity researchers discovered previously unknown encryptors for ARM, FreeBSD, MIPS, and SPARC CPUs, including an encryptor named 'locker_Apple_M1_64' [VirusTotal] for newer Macs running on Apple Silicon.

The encryptors appear to be in the testing phase and are not yet ready for deployment in actual attacks against macOS devices.

Wardle, a macOS cybersecurity expert, confirmed that the macOS encryptor is based on the Linux version and is far from complete, lacking the functionality to encrypt Macs properly. On Objective See, you can read Wardle's

comprehensive technical analysis of the new Mac encryptor.

The LockBit ransomware gang has confirmed to BleepingComputer that they are actively developing a Mac encryptor, but given their history of misleading researchers, it is unclear whether this is true. If true, we may see more sophisticated and production-ready versions of the Mac encryptor.

The Lockbit group is still using the Lockbit 2.0 name, but we can expect an update in the following month. It has been two weeks since vx-underground tweeted their conversation with the Lockbit affiliate, but the Lockbit team has no deadline to uphold. They can release the new version whenever they want.

The new features and upgrades in Lockbit 3.0 is still a mystery. **SOCRadar CTIA** team will follow the updates regarding Lockbit 3.0 and bring you the latest updates.,

Stay Up-to-date About Lockbit and Other Ransomware Groups

> SOCRadar's ThreatShare keeps you updated about ransomware gangs

SOCRadar's Extended Threat Intelligence module, **ThreatShare**, allows you to keep up to date with the developments regarding ransomware groups by following communication channels such as deep and darknet forums, social media, Telegram, ICQ, etc. Shares along with screenshots and texts.

SOCRadar's analyst team translates the collected raw data into contextual intelligence and presents it in a searchable interface. It helps your SOC team develop security strategies based on country, sector, or region.
