Missed opportunity: Bug in LockBit ransomware allowed free decryptions

therecord.media/missed-opportunity-bug-in-lockbit-ransomware-allowed-free-decryptions/

March 17, 2021

A member of the cybercriminal community has discovered and disclosed a bug in the LockBit ransomware that could have been used for free decryptions.

The bug impacts LockBit, a ransomware-as-a-service (RaaS) operation that launched in January 2020 and through which the LockBit gang rents access to a version of their ransomware strain.

Customers of the LockBit RaaS, also known as “affiliates,” execute intrusions into corporate networks, where they deploy the ransomware to encrypt files and demand a ransom from victims to provide a decryption key that unlocks their files.

Through a ransom note left on their desktop, LockBit victims are told to access a dark web portal where they can negotiate the ransom payment. This “payment” portal also allows victims access to a one-time free decryption operation, so victims can confirm that the hackers have a legitimate and working copy of the decryption key.

LockBit bug posted on cybercrime forum

In a message posted on an underground cybercrime forum today, a threat actor has posted details about a bug in LockBit's one-time free decryption mechanism that could have been abused for unlimited free decryptions.

> #Malware #Ransomware #LockBit
>
> In LockBit ransomware, clients found a bug that allows using trial decryptor infinitely. Also, one client reminded about critical bugs due to not usable LockBit in big ransomware attacks. pic.twitter.com/D98Na8MZ7r
>
> — 3xp0rt (@3xp0rtblog) March 16, 2021

Giving legitimacy to the disclosure, the bug was made public by Bassterlord, a suspected Russian-speaking threat actor who previously served as an affiliate for the LockBit ransomware gang, but also other rival RaaS operations, such as REvil, Avaddon, and RansomExx.

With details about the bug being posted in such a public manner, Bassterlord's actions have also sparked a discussion among security professionals about the proper way of reporting bugs in ransomware strains.

John Fokker, Head of Cyber Investigations & Principal Engineer at security firm McAfee, told *The Record* that the proper way would be to report any ransomware-related bugs to a security vendor or the No More Ransom project.

Both security vendors and the No More Ransom project have well-established mechanisms in place to take advantage of this information and help ransomware victims without alerting the ransomware authors, Fokker said.

The McAfee exec said the advice applies to both independent security researchers but also underground threat actors looking to sabotage their rivals. 😉

Bug expected to be patched

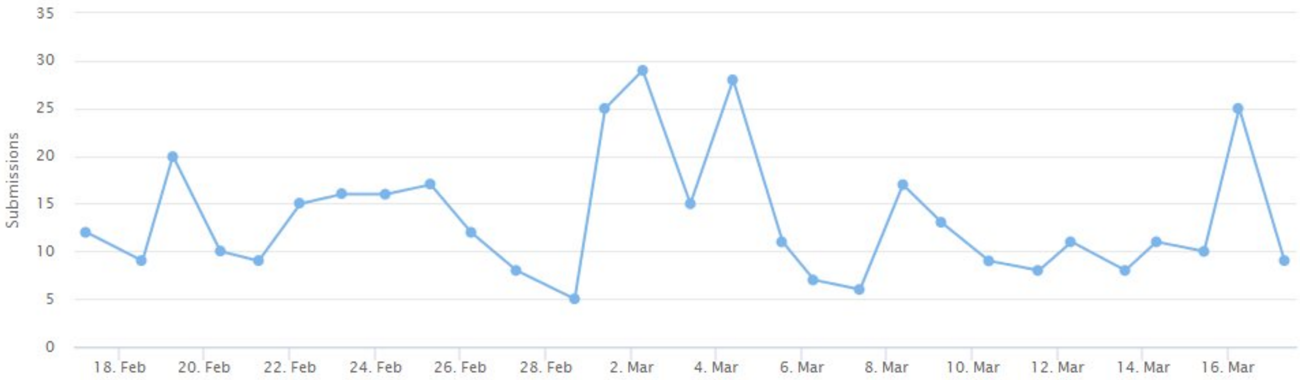
Just like in previous instances when a bug in ransomware code was exposed, the LockBit gang is now expected to patch the issue within days, making future free decryption operations impossible. The LockBit portal was also conspicuously down all day today, suggesting that fixes are possibly being implemented, Marcelo Rivero, a Malware Intelligence Analyst at security firm Malwarebytes told *The Record*.

In addition, several other members of the security community have also told *The Record* that the LockBit bug was something they were not aware of and which could have been very useful.

It may not have been possible to decrypt large batches of files at once without alerting the LockBit crew, but the bug could have been used to decrypt selected sensitive files for which backups did not exist.

Currently, the LockBit ransomware is one of the most active ransomware groups today. Security firm Coveware listed the LockBit ransomware as one of the top 15 ransomware strains in Q4 2020.

According to data provided by the ID-Ransomware platform, the LockBit operation still infects tens of victims every week.



LockBit submissions to ID-Ransomware service (Image via MalwareHunterTeam)

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.