LockBit 3.0 introduces the first ransomware bug bounty program

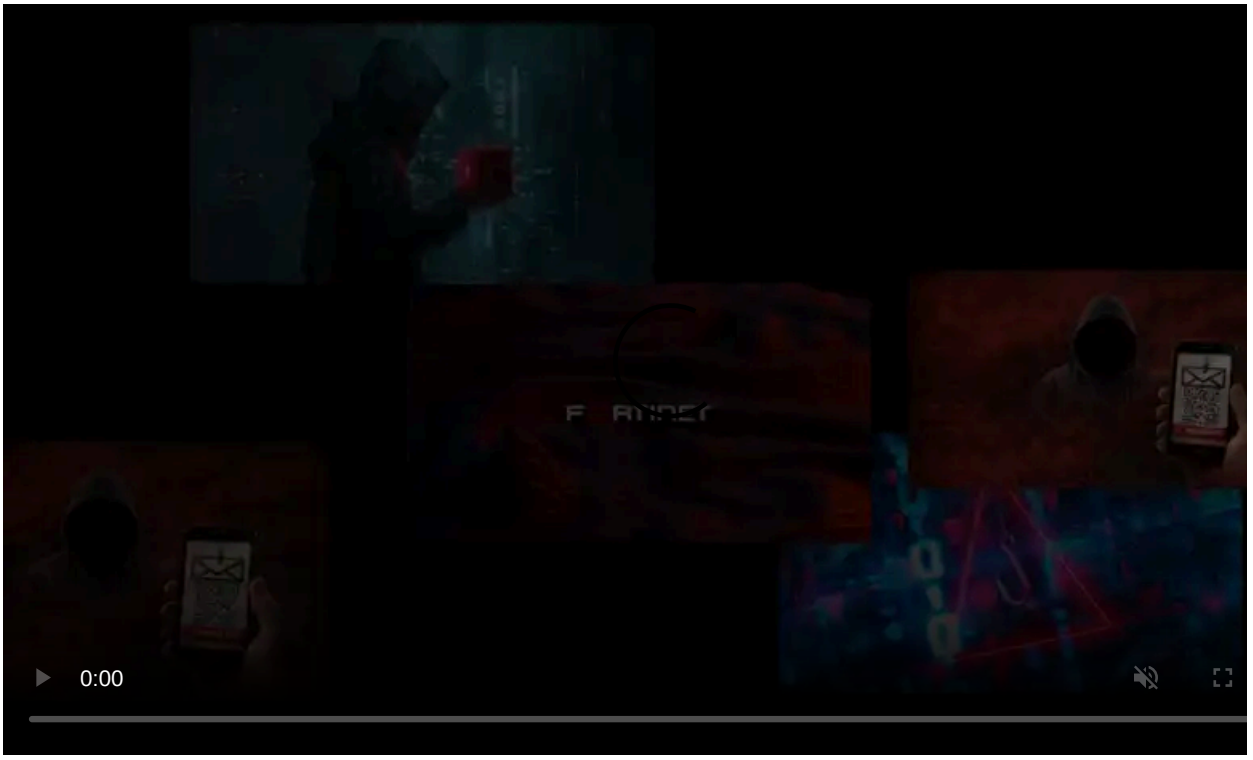
By Lawrence Abrams

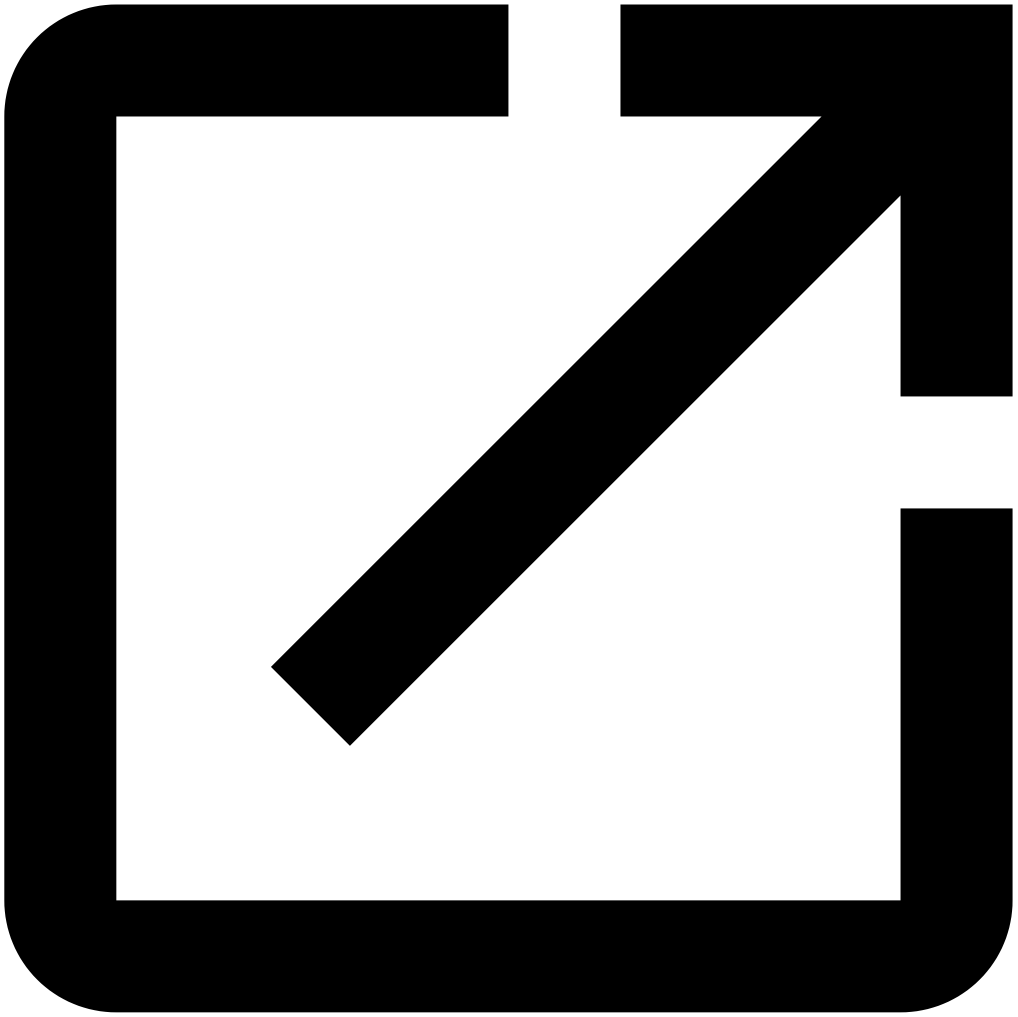
Published: 2022-06-27 · Archived: 2026-04-06 00:37:36 UTC

The LockBit ransomware operation has released 'LockBit 3.0,' introducing the first ransomware bug bounty program and leaking new extortion tactics and Zcash cryptocurrency payment options.

The ransomware operation launched in 2019 and has since grown to be the most prolific ransomware operation, accounting for 40% of all known ransomware attacks in May 2022.

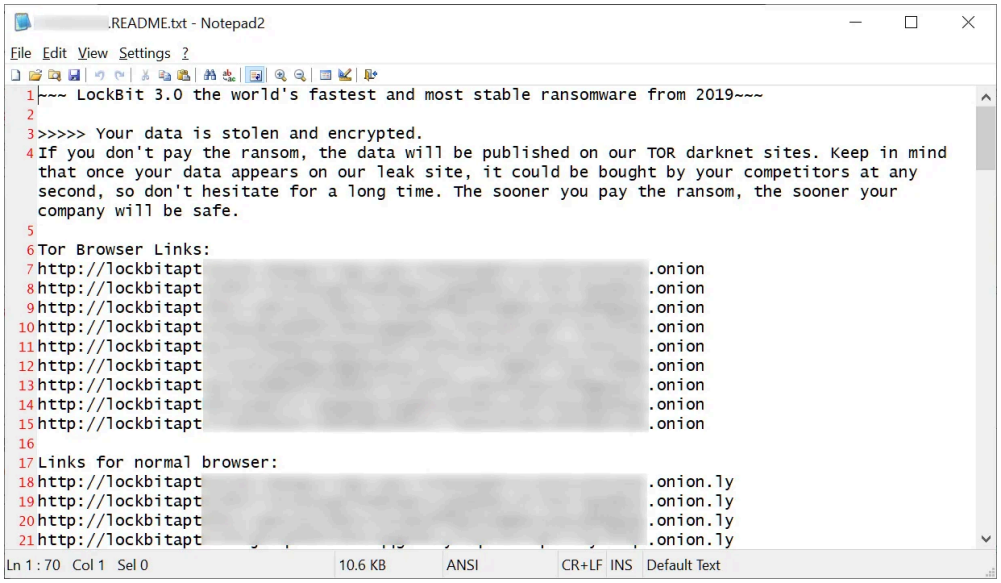
Over the weekend, the cybercrime gang released a revamped ransomware-as-a-service (RaaS) operation called LockBit 3.0 after beta testing for the past two months, with the new version already used in attacks.


0:00



Visit Advertiser websiteGO TO PAGE

While it is unclear what technical changes were made to the encryptor, the ransom notes are no longer named 'Restore-My-Files.txt' and instead have moved to the naming format, [id].README.txt, as shown below.



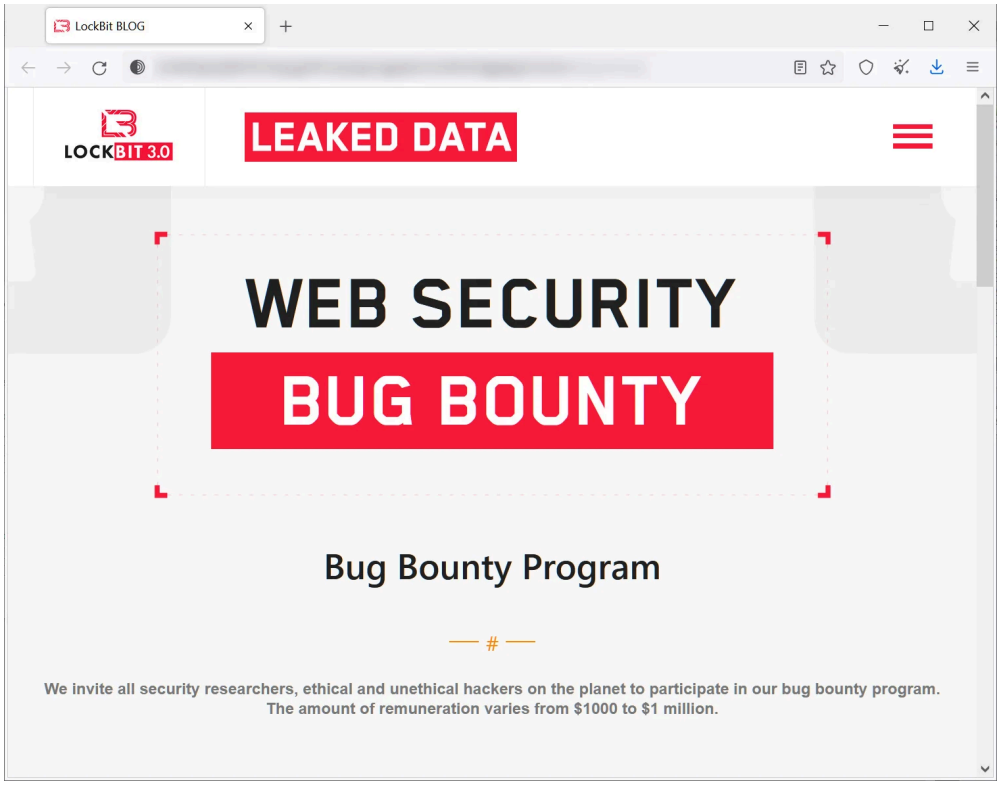
LockBit 3.0 ransom note

Source: BleepingComputer

LockBit 3.0 bug bounty program

With the release of LockBit 3.0, the operation has introduced the first bug bounty program offered by a ransomware gang, asking security researchers to submit bug reports in return for rewards ranging between $1,000 and $1 million.

"We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program. The amount of remuneration varies from $1000 to $1 million," reads the LockBit 3.0 bug bounty page.



LockBit 3.0 bug bounty program
Source: BleepingComputer

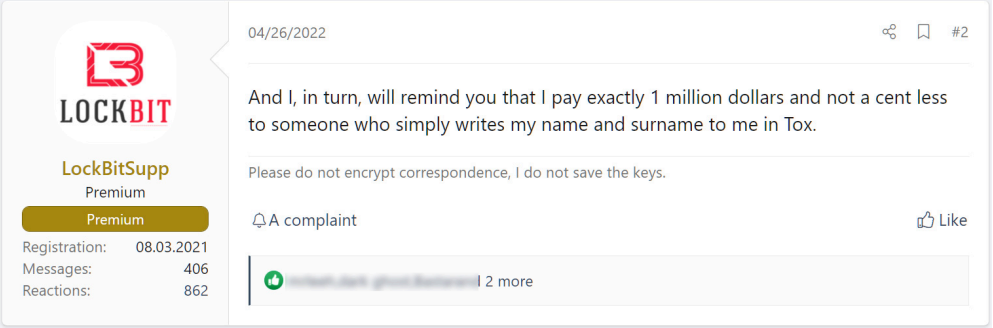
However, this bug bounty program is a bit different than those commonly used by legitimate companies, as helping the criminal enterprise would be illegal in many countries.

Furthermore, LockBit is not only offering bounties for rewards on vulnerabilities but is also paying bounties for "brilliant ideas" on improving the ransomware operation and for doxxing the affiliate program manager.

The following are the various bug bounty categories offered by the LockBit 3.0 operation:

> - **Web Site Bugs:** XSS vulnerabilities, mysql injections, getting a shell to the site and more, will be paid depending on the severity of the bug, the main direction is to get a decryptor through bugs web site, as well as access to the history of correspondence with encrypted companies.
> - **Locker Bugs**: Any errors during encryption by lockers that lead to corrupted files or to the possibility of decrypting files without getting a decryptor.
> - **Brilliant ideas:** We pay for ideas, please write us how to improve our site and our software, the best ideas will be paid. What is so interesting about our competitors that we don't have?
> - **Doxing:** We pay exactly one million dollars, no more and no less, for doxing the affiliate program boss. Whether you're an FBI agent or a very clever hacker who knows how to find anyone, you can write us a TOX messenger, give us your boss's name, and get $1 million in bitcoin or monero for it.
> - **TOX messenger:** Vulnerabilities of TOX messenger that allow you to intercept correspondence, run malware, determine the IP address of the interlocutorand other interesting vulnerabilities.
> - **Tor network:** Any vulnerabilities which help to get the IP address of the server where the site is installed on the onion domain, as well as getting root access to our servers, followed by a database dump and onion domains.

The $1,000,000 reward for identifying the affiliate manager, known as LockBitSupp, was previously offered on the XSS hacking forum in April.



LockBitSupp offering a $1 million bounty to anyone who identifies them
Source: BleepingComputer

Upcoming ZCash payment option?

When opening the Tor sites for the LockBit 3.0 negotiation and data leak sites, visitors are presented with an animated logo with various cryptocurrency icons rotating around it.

The cryptocurrency icons shown in this animation are Monero and Bitcoin, which the operation accepted as ransom payments in the past, but also includes the privacy coin known as Zcash.

New cryptocurrency animation on LockBit 3.0 sites
Source: BleepingComputer

The addition of Zcash as a payment option is not surprising for a ransomware operation.

Cryptocurrency tracking companies and law enforcement seizures have repeatedly shown that Bitcoin can be traced, and while Monero is a privacy coin, it isn't offered for sale by the vast majority of US crypto exchanges.

Zcash is also a privacy coin, making it harder to trace. Still, it is currently offered for sale at the most popular US crypto exchange, Coinbase, making it easier for victims to purchase for ransom payments.

However, if ransomware operations switch to accepting payments in this coin, we will likely see it be removed from US exchanges due to pressure from the US government.

LockBit to sell victim's stolen data?

LeMagIT's Valery Marchive discovered that the LockBit 3.0 operation is utilizing a new extortion model, allowing threat actors to buy data stolen during attacks.

One of the JavaScript files used by the new LockBit 3.0 data leak site shows a new HTML modal dialog that allows people to purchase data leaked on the site.

As you can see below, the modals will offer the ability to buy the data and download it either through a Torrent or directly on the site. The available options may be determined based on the size of the stolen data, with Torrents being used for large data dumps and direct downloads for smaller amounts.

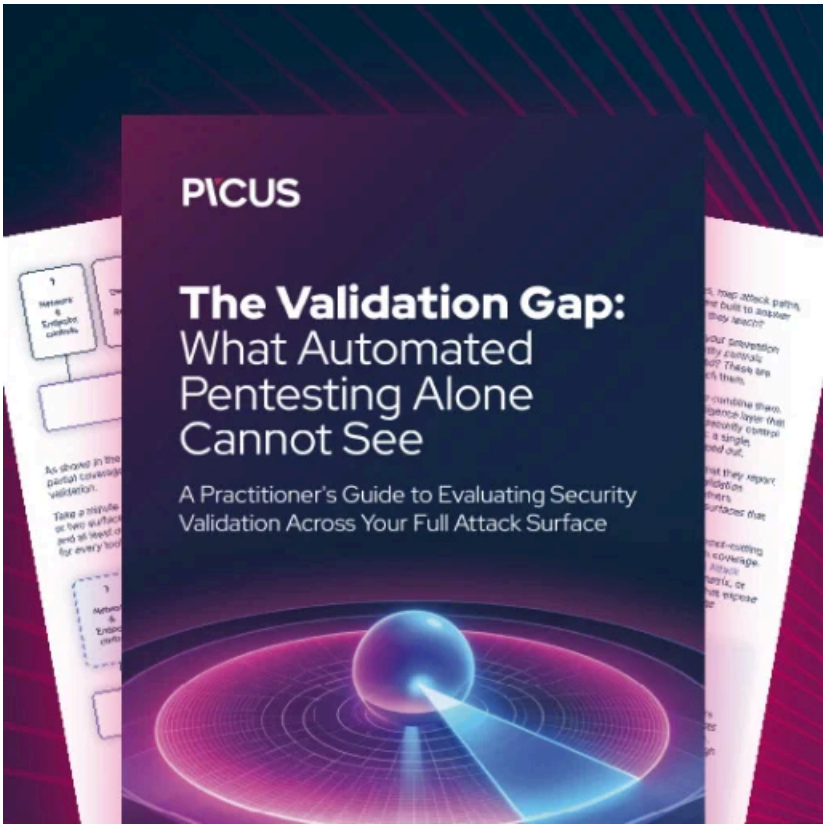
JavaScript source showing new data extortion method

Source: BleepingComputer

As the LockBit 3.0 data leak site does not currently contain any victims, it is not clear how this new extortion tactic will work or if it is even enabled.

LockBit is one of the most active ransomware operations, with its public-facing operator actively engaging with other threat actors and the cybersecurity community.

Due to its ongoing adoption of new tactics, technology, and payment methods, it is vital for security and network professionals to stay up to date on the evolution of the operation.



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-30-introduces-the-first-ransomware-bug-bounty-program/