LockBit ransomware builder leaked online by "angry developer"

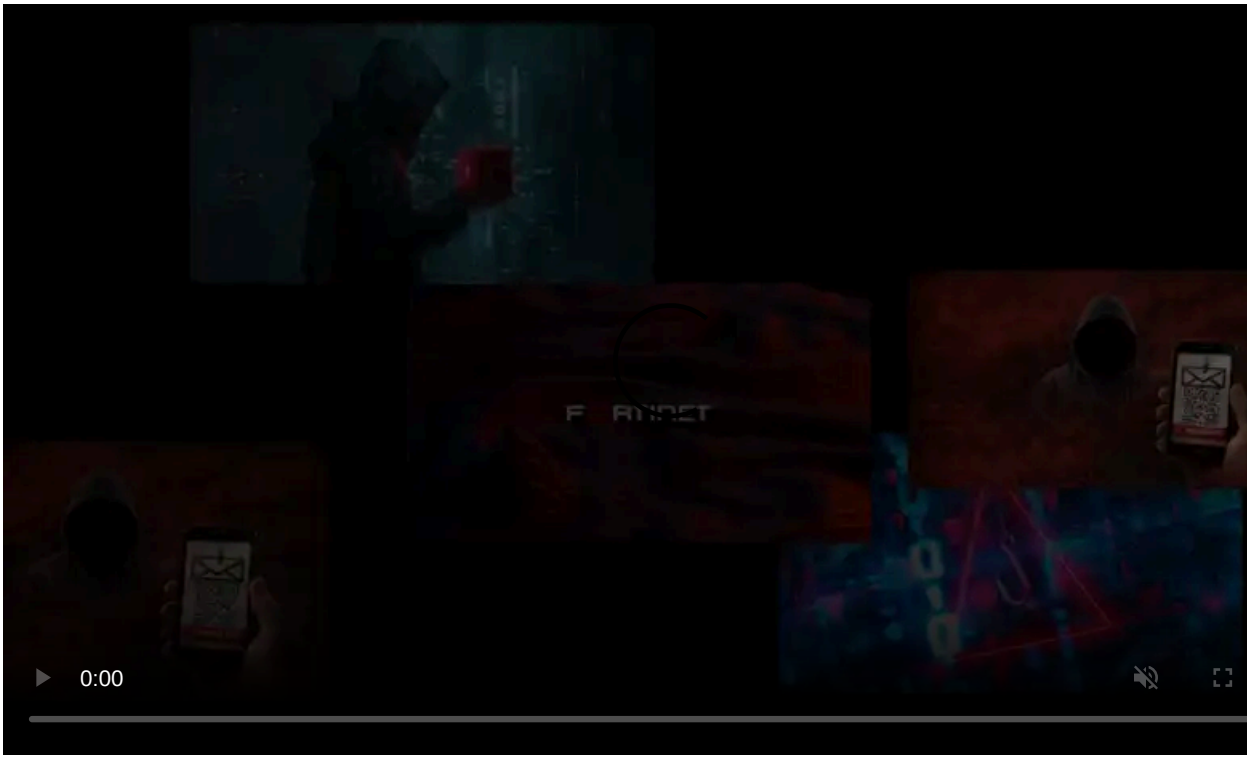
By Lawrence Abrams

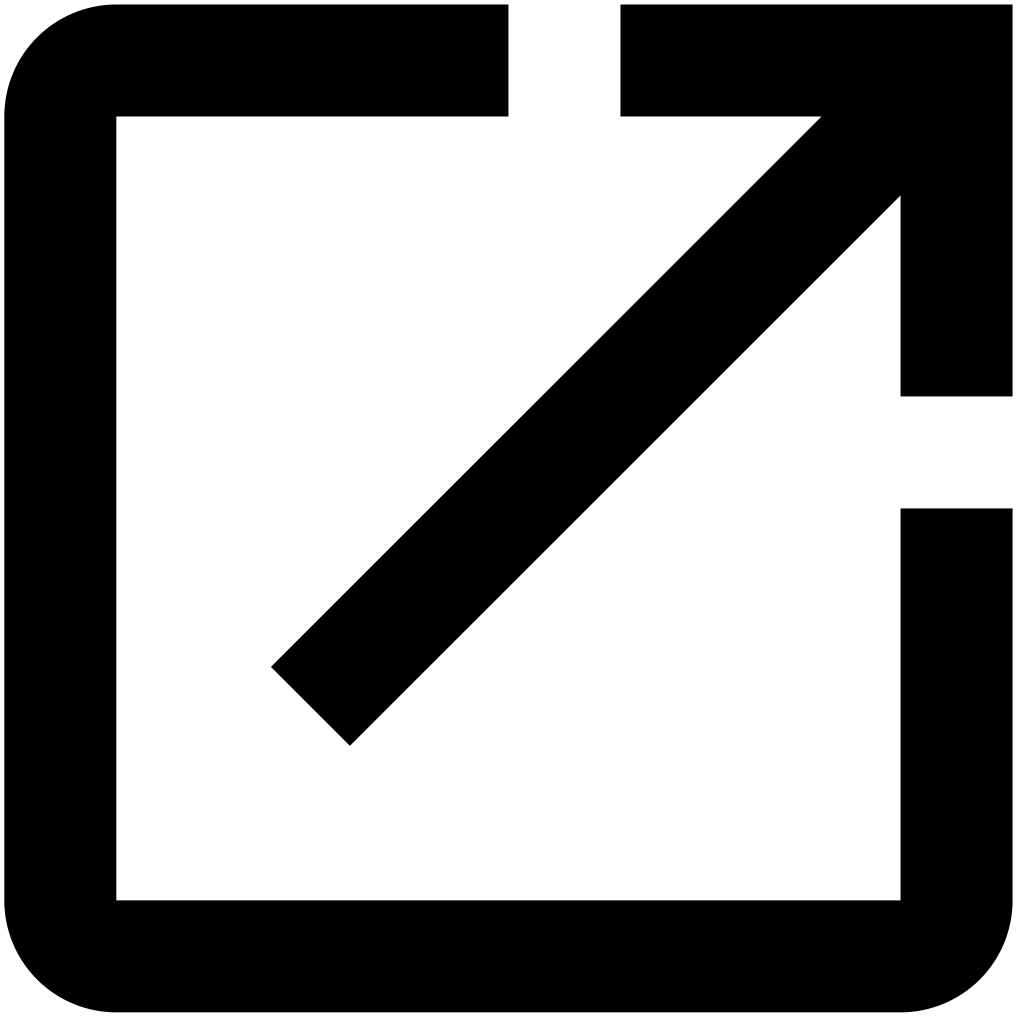
Published: 2022-09-21 · Archived: 2026-04-05 20:27:20 UTC

The LockBit ransomware operation has suffered a breach, with an allegedly disgruntled developer leaking the builder for the gang's newest encryptor.

In June, the LockBit ransomware operation released version 3.0 of their encryptor, codenamed LockBit Black, after testing it for two months.

The new version promised to 'Make Ransomware Great Again,' adding new anti-analysis features, a ransomware bug bounty program, and new extortion methods.

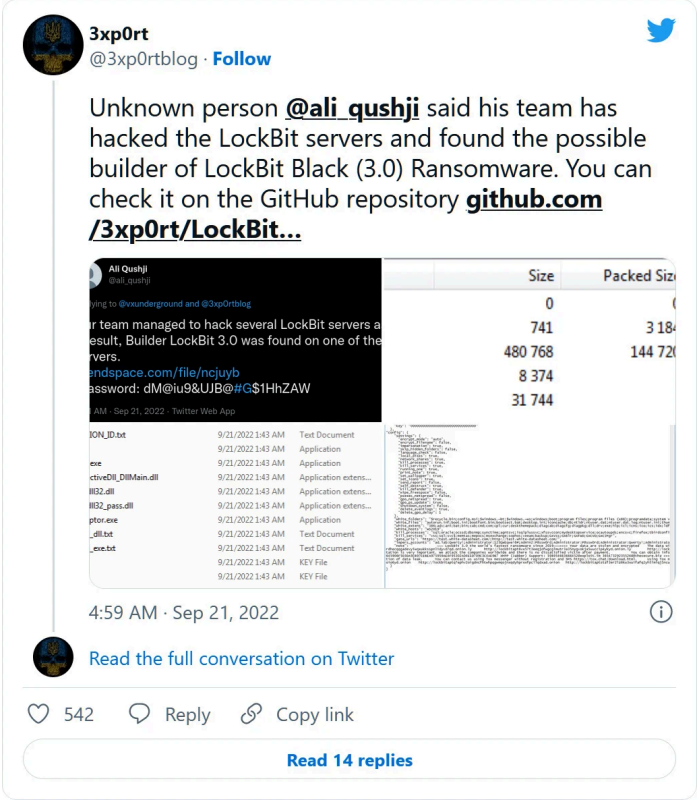

0:00



However, it looks like LockBit has suffered a breach, with two people (or maybe the same person) leaking the LockBit 3.0 builder on Twitter.

LockBit 3.0 builder leaked on Twitter

According to security researcher 3xp0rt, a newly registered Twitter user named 'Ali Qushji' states their team hacked LockBits servers and found a builder for the LockBit 3.0 ransomware encryptor.



After security researcher 3xp0rt shared the tweet about the leaked LockBit 3.0 builder, VX-Underground shared that they were contacted on September 10th by a user named 'protonleaks,' who also shared a copy of the builder.

However, VX-Underground says that LockBitSupp, the public representative of the LockBit operation, claims they were not hacked, but rather a disgruntled developer leaked the private ransomware builder.

"We reached out to Lockbit ransomware group regarding this and discovered this leaker was a programmer employed by Lockbit ransomware group," VX-Underground shared in a now-deleted tweet.

"They were upset with Lockbit leadership and leaked the builder."

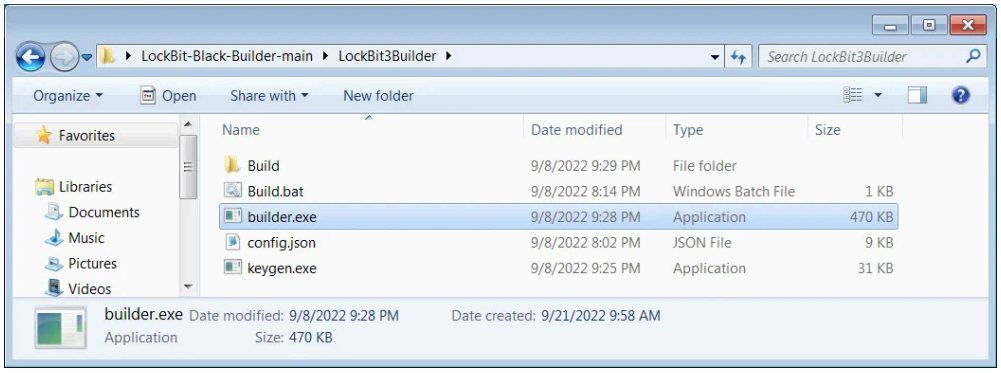
BleepingComputer has spoken to multiple security researchers who have confirmed that the builder is legitimate.

Builder lets anyone start a ransomware gang

Regardless of how the private ransomware builder was leaked, this is not only a severe blow to the LockBit ransomware operation but also to the enterprise, which will see a rise in threat actors using it to launch their own attacks.

The leaked LockBit 3.0 builder allows anyone to quickly build the executables required to launch their own operation, including an encryptor, decryptor, and specialized tools to launch the decryptor in certain ways.

The builder consists of four files, an encryption key generator, a builder, a modifiable configuration file, and a batch file to build all of the files.

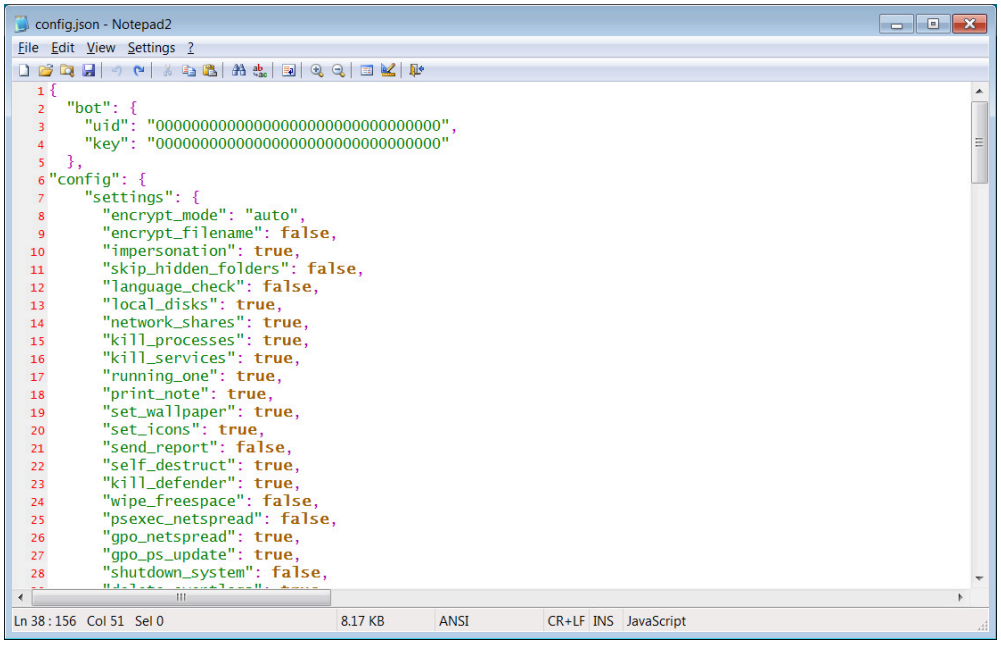


LockBit 3.0 builder files

Source: BleepingComputer

The included 'config.json' can be used to customize an encryptor, including modifying the ransom note, changing configuration options, deciding what processes and services to terminate, and even specifying the command and control server that the encryptor will send data.

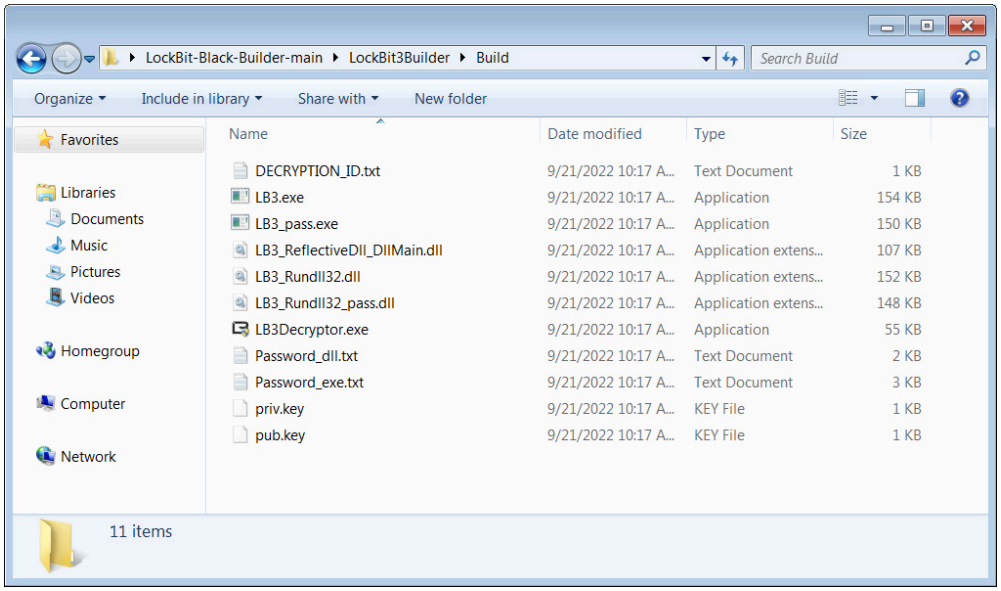
By modifying the configuration file, any threat actor can customize it to their own needs and modify the created ransom note to link to their own infrastructure.



LockBit 3.0 configuration file

Source: BleepingComputer

When the batch file is executed, the builder will create all of the files necessary to launch a successful ransomware campaign, as shown below.



Ransomware executables created by the LockBit 3.0 builder

Source: BleepingComputer

BleepingComputer tested the leaked ransomware builder and was easily able to customize it to use our own local command and control server, encrypt our files, and then decrypt them, as shown below.

Demonstration of the built LockBit 3.0 decryptor

Source: BleepingComputer

This builder is not the first time a ransomware builder or source code was leaked online, leading to increased attacks by other threat actors who launched their own operations.

In June 2021, the Babuk ransomware builder was leaked, allowing anyone to create encryptors and decryptors for Windows and VMware ESXi, which other threat actors used in attacks.

In March 2022, when the Conti ransomware operation suffered a data breach, their source code was leaked online as well. This source code was quickly used by the NB65 hacking group to launch ransomware attacks on Russia.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-builder-leaked-online-by-angry-developer-/