LockBit ransomware goes 'Green,' uses new Conti-based encryptor

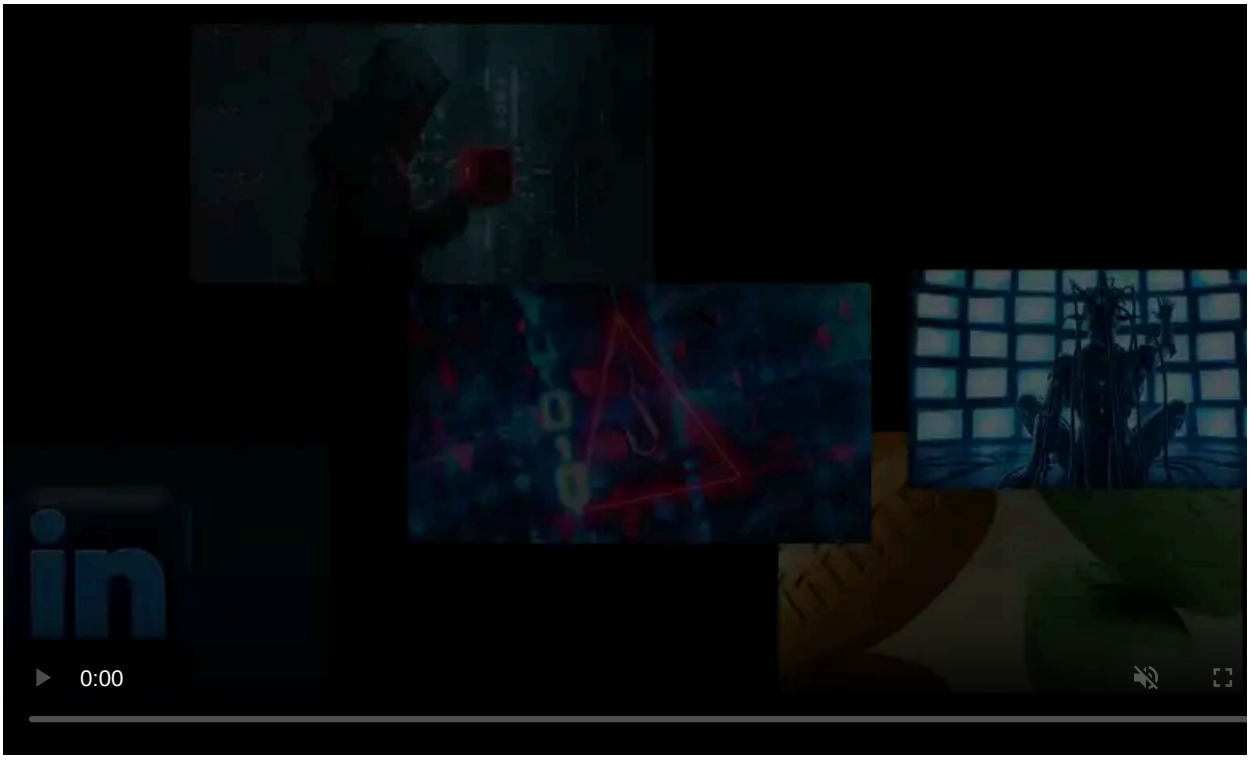
By Lawrence Abrams

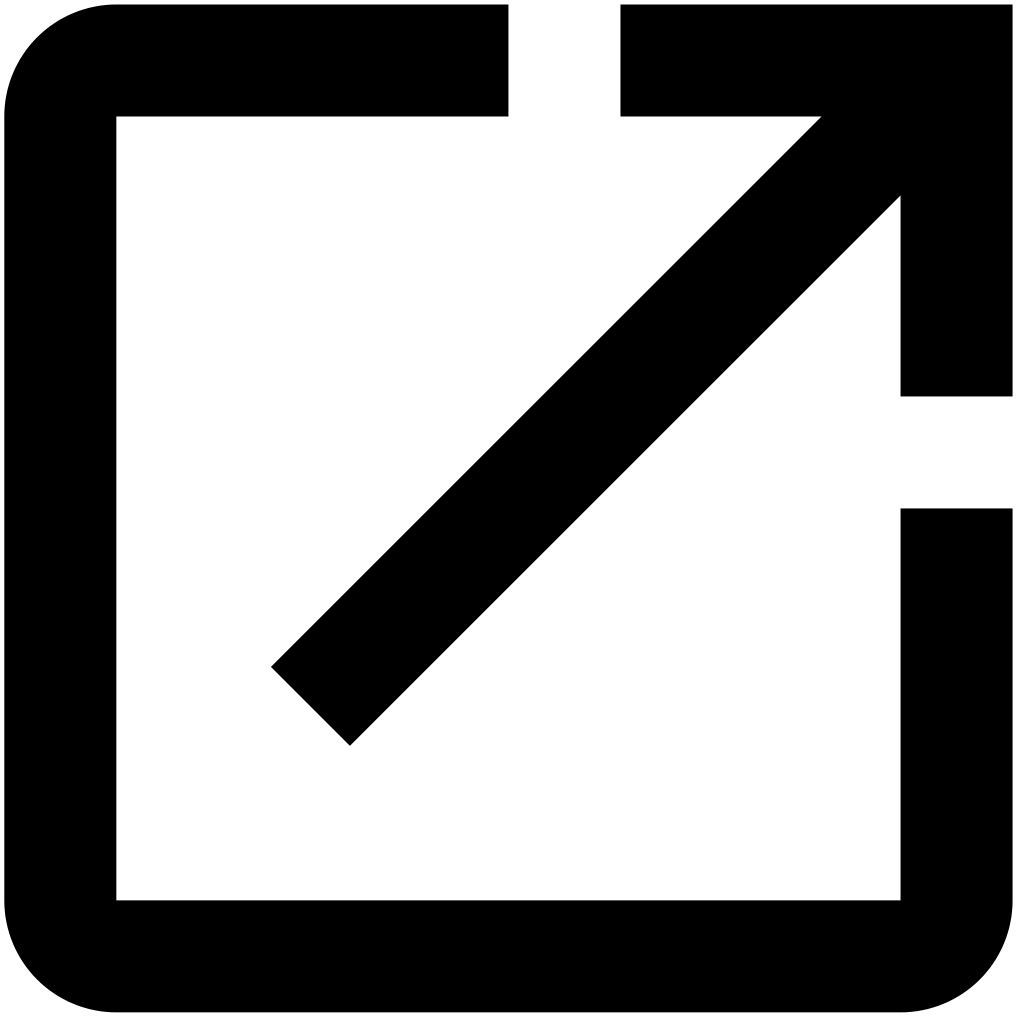
Published: 2023-02-01 · Archived: 2026-04-05 19:00:42 UTC

The LockBit ransomware gang has again started using encryptors based on other operations, this time switching to one based on the leaked source code for the Conti ransomware.

Since its launch, the LockBit operation has gone through numerous iterations of its encryptor, starting with a custom one and moving to LockBit 3.0 (aka LockBit Black), which is derived from the BlackMatter gang's source code.

This week, cybersecurity collective VX-Underground first reported that the ransomware gang is now using a new encryptor named 'LockBit Green,' based on the leaked source code of the now-disbanded Conti gang.


0:00



The Conti ransomware gang shut down after a series of embarrassing data breaches caused by the leaking of 170,000 internal messages and the source code for their encryptor.

Soon after the source code was leaked, other hacking groups began utilizing it to create their own encryptors, with some ironically used against Russian companies.

A look at LockBit Green

Since the news of LockBit Green became public, researchers have found samples of the new encryptor circulating on VirusTotal and other malware-sharing sites.

A malware analyst known as CyberGeeksTech reverse-engineered a sample of LockBit Green and told BleepingComputer that it was definitely based on the Conti encryptor they previously analyzed.

"I've analyzed the sample and it's 100% based on the Conti source code," the researcher told BleepingComputer.

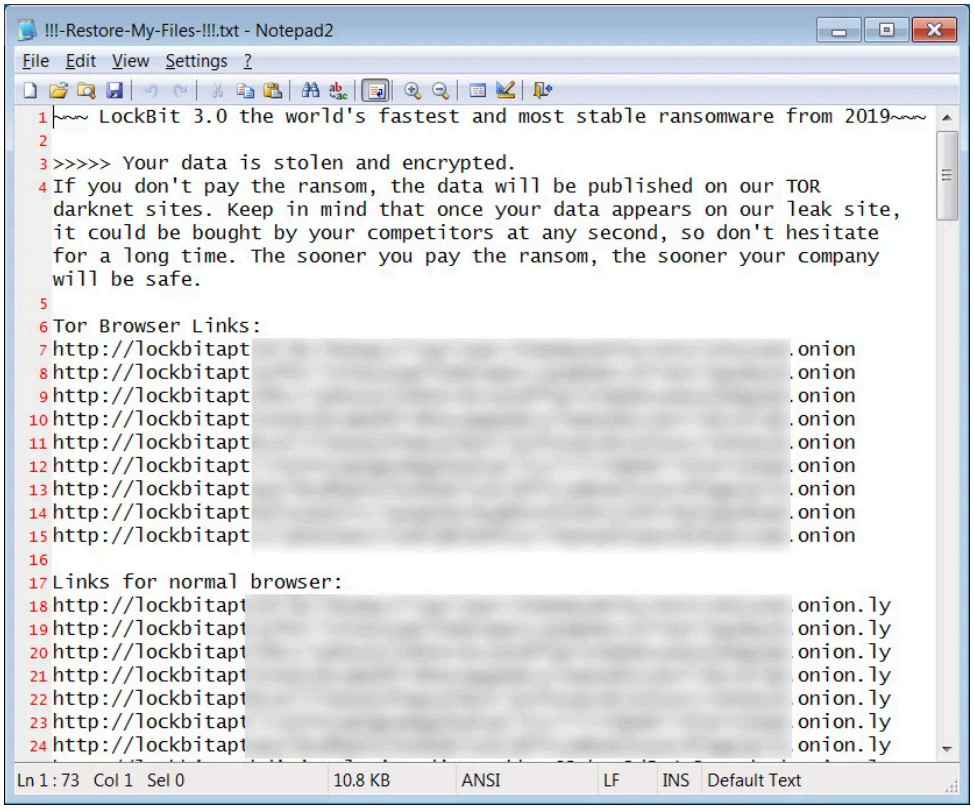
"The decryption algorithm is just an example of a similarity. It's weird that they've chosen to build a payload based on Conti, they have their own encryptor for some time."

Cybersecurity firm PRODAFT also shared four MD5 hashes of LockBit Green samples that they found, including a Yara rule that can detect the new variant.

PRODAFT told BleepingComputer that they know of at least five victims that have been attacked using the new LockBit Green variant.

BleepingComputer tested one of the samples shared by PRODAFT, which utilizes the same command-line arguments as the previous Conti encryptors.

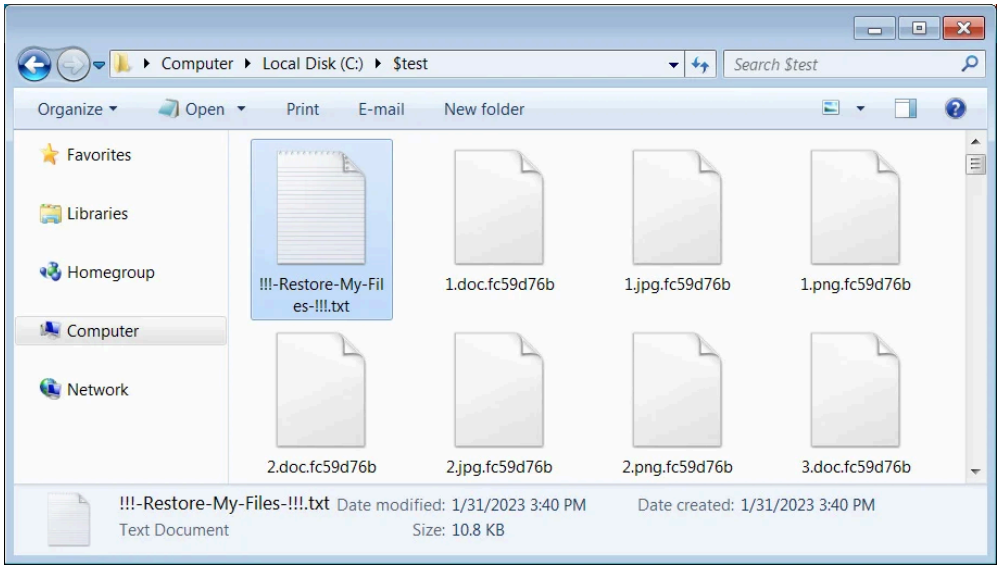
The ransom notes have been modified to use the LockBit 3.0 ransom note rather than Conti's format, as shown below.



LockBit Green ransom note

Source: BleepingComputer

However, one change we noticed is that LockBit Green uses what appears to be a random extension rather than the standard **.lockbit** extension.



Different encrypted file extension used in LockBit Green

Source: BleepingComputer

While it's unclear why the LockBit operation is utilizing a new Conti-based encryptor when their previous one works fine, PRODAFT may have the answer.

"We especially observed that ex-Conti members preferred LockBit Green after the announcement. They probably feel comfortable using conti-based ransomware," PRODAFT told BleepingComputer.

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.
