LockBit ransomware returns to attacks with new encryptors, servers

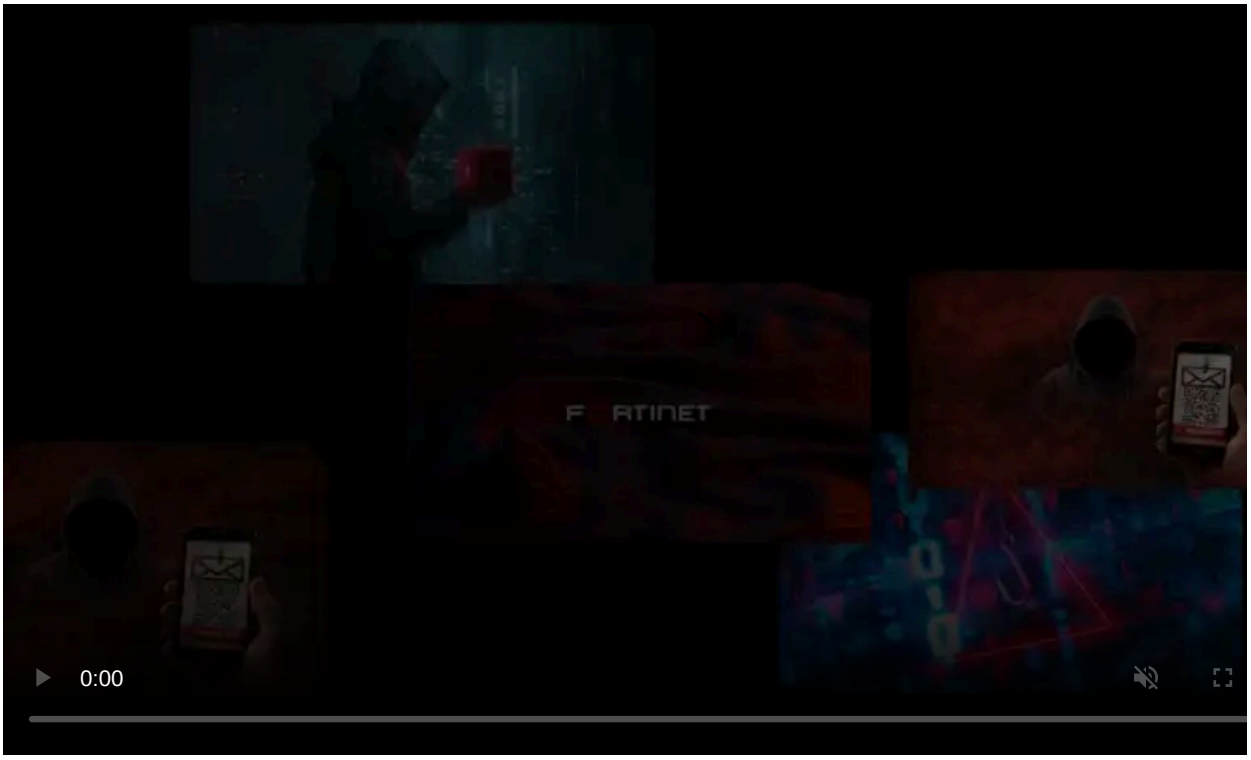
By Lawrence Abrams

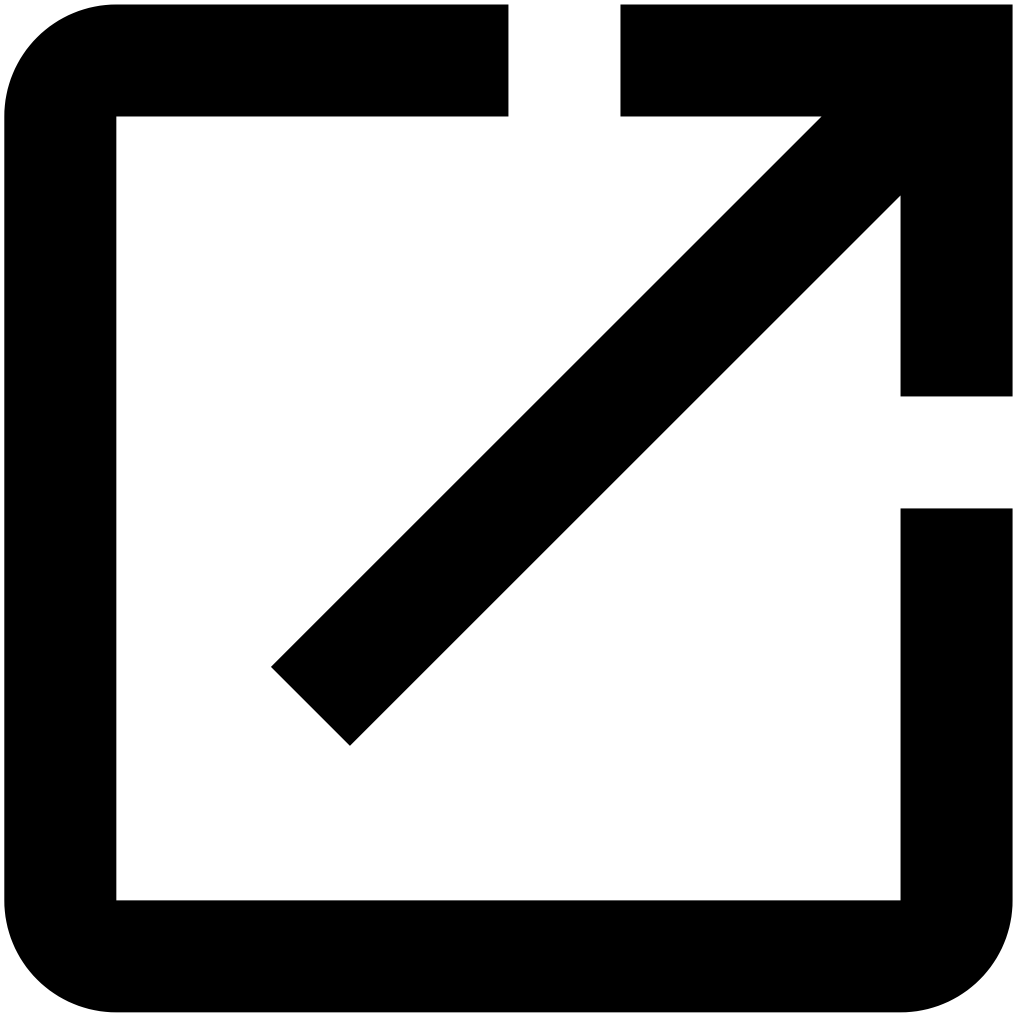
Published: 2024-02-28 · Archived: 2026-04-06 00:05:16 UTC

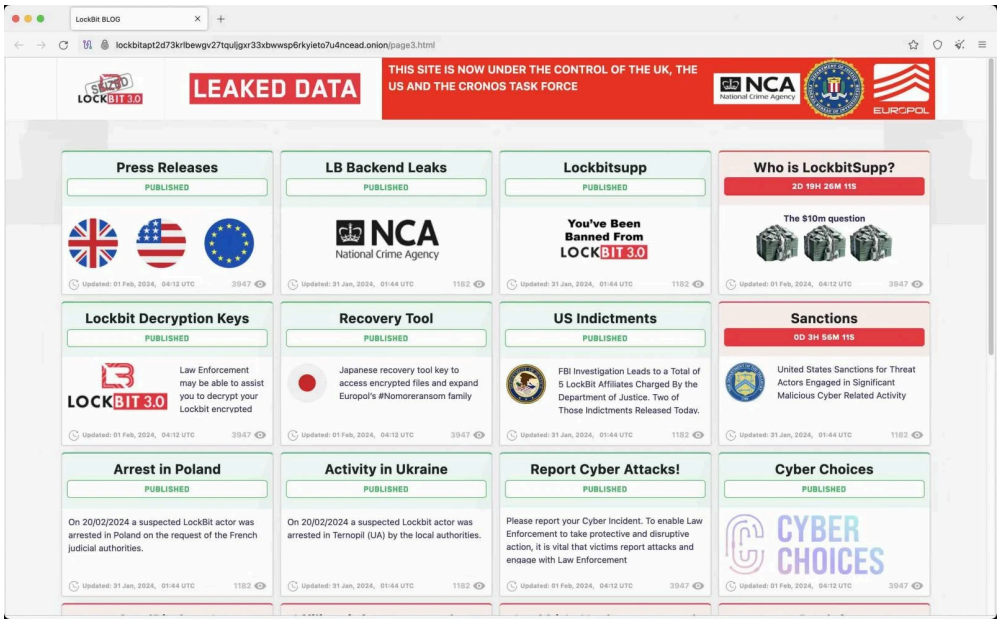
The LockBit ransomware gang is once again conducting attacks, using updated encryptors with ransom notes linking to new servers after last week's law enforcement disruption.

Last week, the NCA, FBI, and Europol conducted a coordinated disruption called 'Operation Cronos' against the LockBit ransomware operation.

As part of this operation, law enforcement seized infrastructure, retrieved decryptors, and, in an embarrassing moment for LockBit, converted the ransomware gang's data leak site into a police press portal.


F RTINET
0:00





LockBit data leak site converted into a press site
Source: BleepingComputer

Soon after, LockBit set up a new data leak site and left a long note addressed to the FBI, claiming law enforcement breached their servers using a PHP bug.

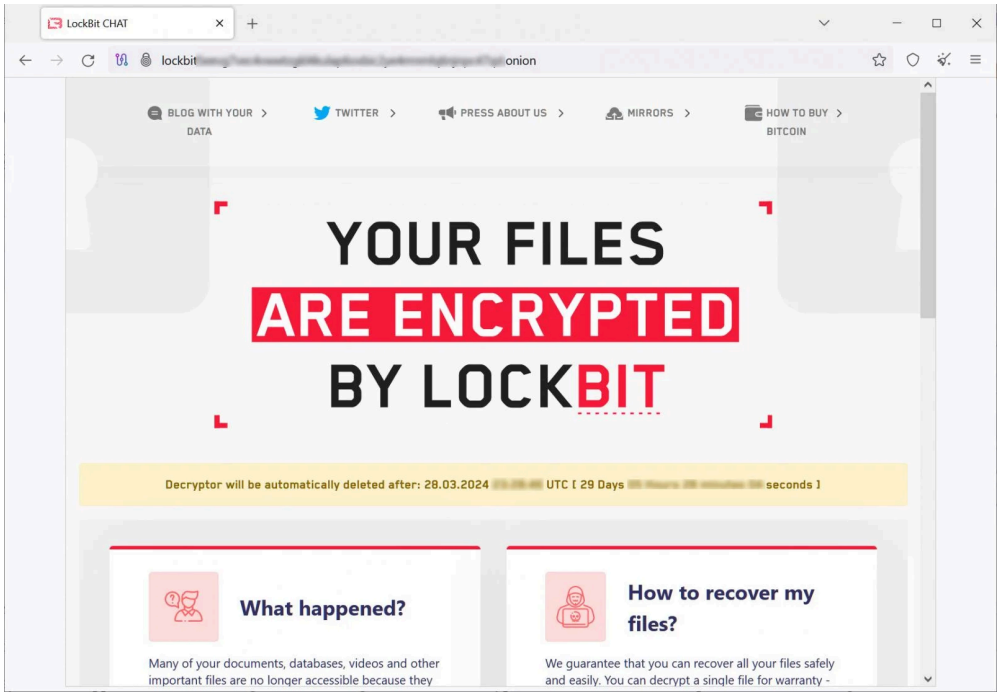
However, instead of rebranding, they promised to return with updated infrastructure and new security mechanisms to prevent law enforcement from performing operation-wide attacks and gaining access to decryptors.

Updated LockBit encryptors used in attacks

As of yesterday, LockBit appears to be conducting attacks again, with new encryptors and infrastructure setup for data leak and negotiation sites.

As first reported by Zscaler, the ransomware gang updated their encryptor's ransom notes with Tor URLs for the gang's new infrastructure. BleepingComputer later found samples of the encryptors uploaded to VirusTotal yesterday [Sample] (shared by MalwareHunterTeam) and today [Sample], containing the updated ransom notes.

BleepingComputer also confirmed that the operation's negotiation servers are live again but only work for victims of new attacks.



New LockBit negotiation sites

Source: BleepingComputer

At the time of LockBit's takedown, the ransomware operation had approximately 180 affiliates working with them to conduct attacks.

It is not known how many are still working with the Ransomware-as-a-Service, as one has publicly lashed out at the operation on X.

However, LockBit states that they are now actively recruiting experienced pentesters to join their operation again, which will likely lead to increased attacks in the future.

Whether this is a grand plan for LockBit to slowly fade away and rebrand as we saw with Conti remains to be seen. For now, though, it is safer to assume that LockBit continues to be a threat.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-to-attacks-with-new-encryptors-servers/