LockBit ransomware gang gets aggressive with triple-extortion tactic

By Ionut Ilascu

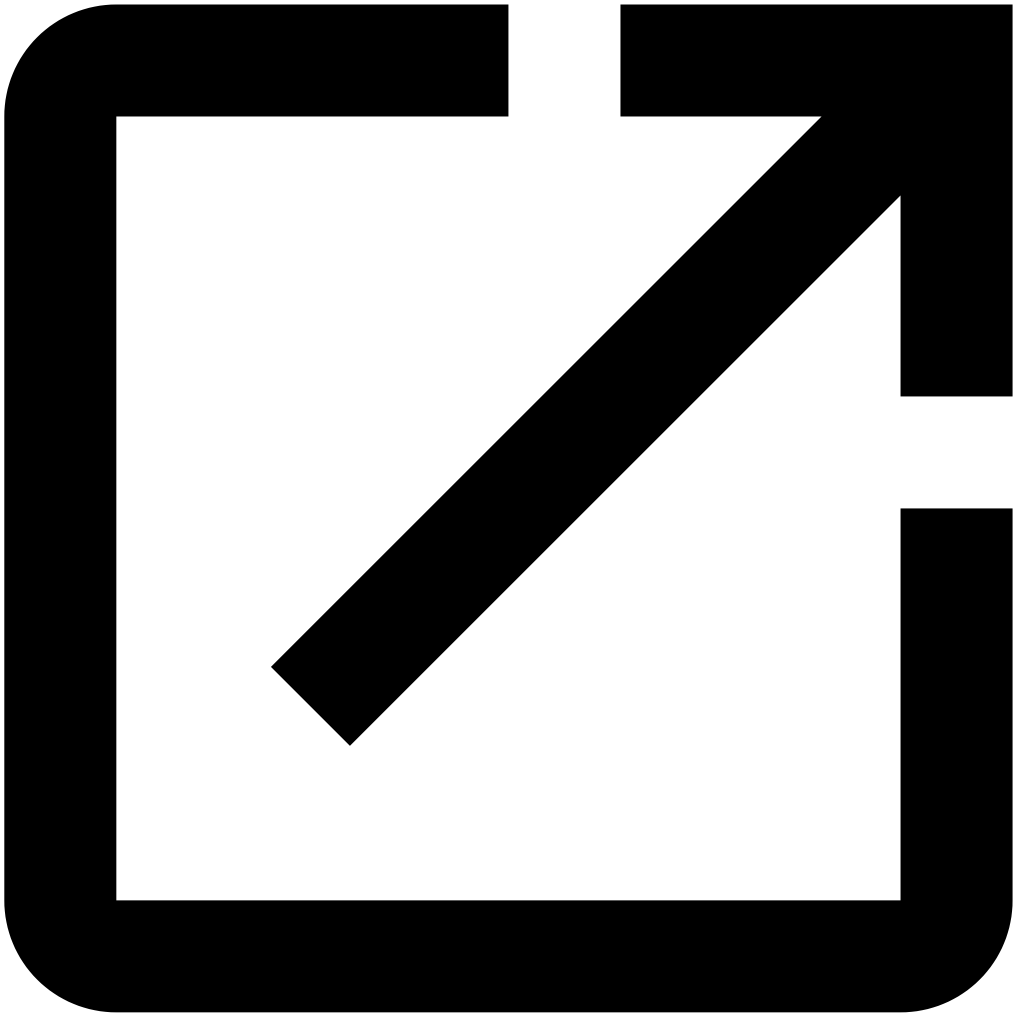
Published: 2022-08-28 · Archived: 2026-04-05 13:23:42 UTC

LockBit ransomware gang announced that it is improving defenses against distributed denial-of-service (DDoS) attacks and working to take the operation to triple extortion level.

The gang has recently suffered a DDoS attack, allegedly on behalf of digital security giant Entrust, that prevented access to data published on its corporate leaks site.

Data from Entrust was stolen by LockBit ransomware in an attack on June 18, according to a BleepingComputer source. The company confirmed the incident and that data had been stolen.


DIE LINKE.
0:00



Entrust did not pay the ransom and LockBit announced that it would publish all the stolen data on August 19. This did not happen, though, because the gang's leak site was hit by a DDoS attack believed to be connected to Entrust.

LockBit getting into DDoS

Earlier this week, LockBitSupp, the public-facing figure of the LockBit ransomware operation, announced that the group is back in business with a larger infrastructure to give access to leaks unfazed by DDoS attacks.

The DDoS attack last weekend that put a temporary stop to leaking Entrust data was seen as an opportunity to explore the triple extortion tactic to apply more pressure on victims to pay a ransom.

LockBitSupp said that the ransomware operator is now looking to add DDoS as an extortion tactic on top of encrypting data and leaking it.

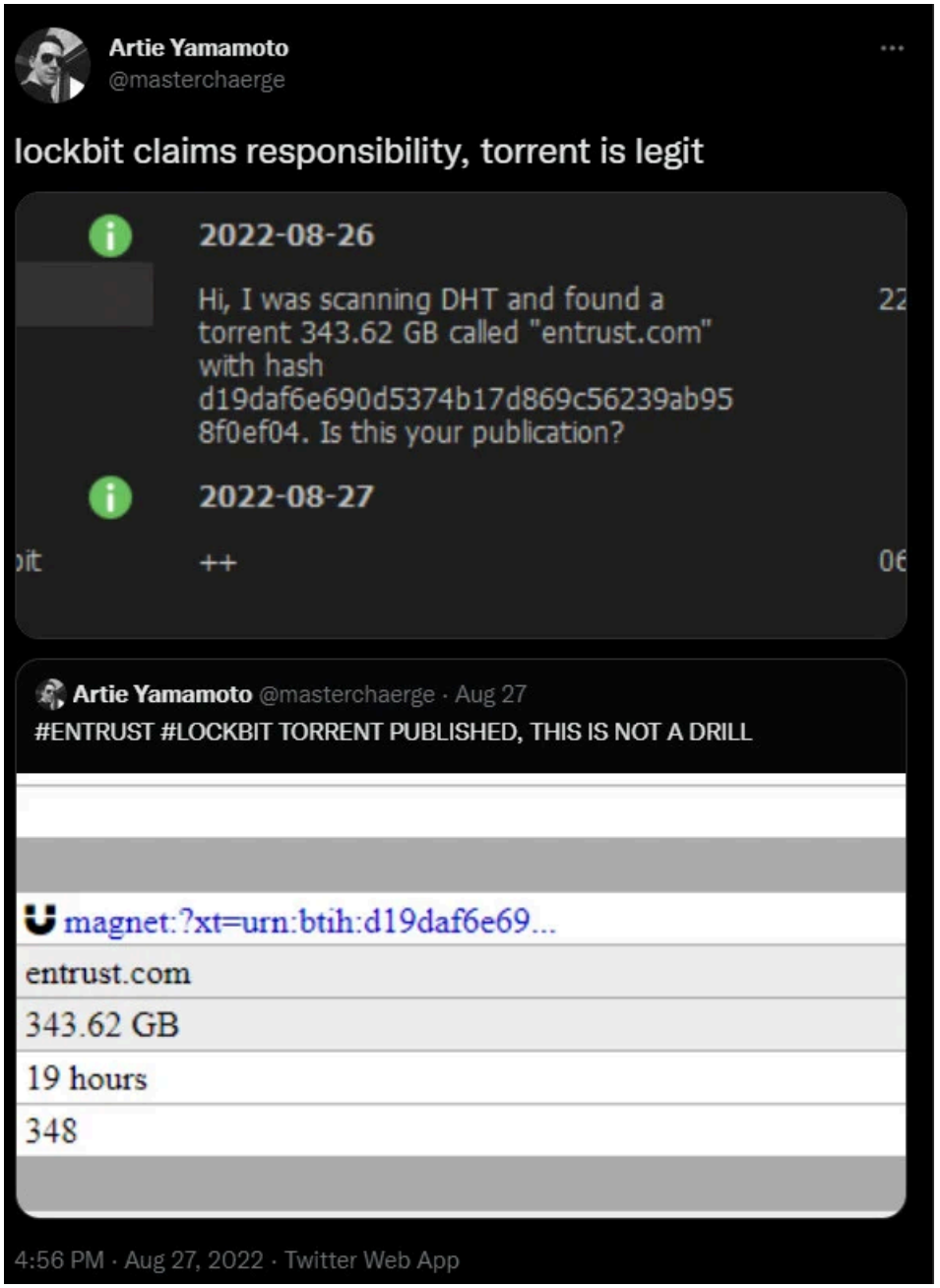
"I am looking for dudosers [DDoSers] in the team, most likely now we will attack targets and provide triple extortion, encryption + date leak + dudos, because I have felt the power of dudos and how it invigorates and makes life more interesting," LockBitSupp wrote in a post on a hacker forum.

Leaking Entrust data

The gang also promised to share over torrent 300GB of data stolen from Entrust so "the whole world will know your secrets."

LockBit's spokesperson said that they would share the Entrust data leak privately with anyone that contacts them before making it available over torrent.

It appears that LockBit has kept its promise and released this weekend a torrent called "entrust.com" with 343GB of files.



Lockbit ransomware leaks Entrust data

source: Artie Yamamoto

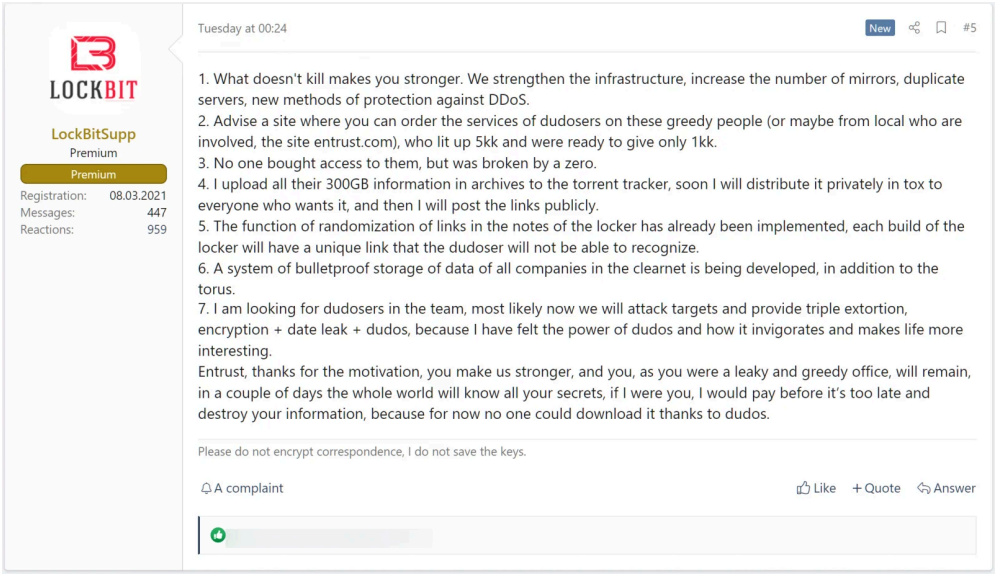
The operators wanted to make sure that Entrust's data is available from multiple sources and, besides publishing it on their site, they also shared the torrent over at least two file storage services, with one of them no longer making it available.

DDoS defenses

One method already implemented to prevent further DDoS attacks is to use unique links in the ransom notes for the victims.

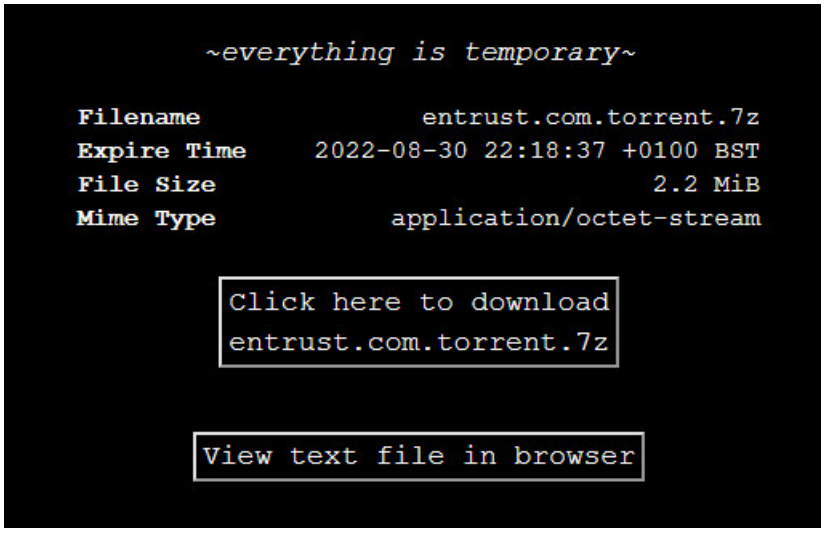
“The function of randomization of links in the notes of the locker has already been implemented, each build of the locker will have a unique link that the dudoser [DDoSer] will not be able to recognize,” LockBitSupp posted.

They also announced an increase in the number of mirrors and duplicate servers, and a plan to increase the availability of stolen data by making it accessible over clearnet, too, via a bulletproof storage service.



Lockbit ransomware changes after suffering DDoS attack
source: BleepingComputer

After publishing this article, BleepingComputer learned that LockBit has made the stolen Entrust data available over clearnet, on a website that provides files for a limited period.

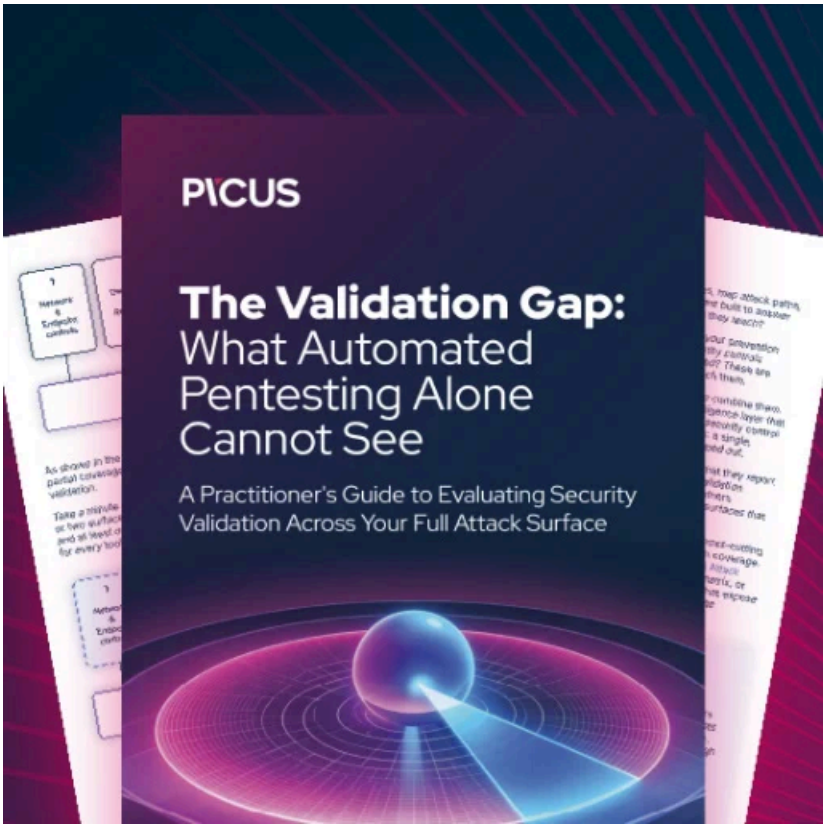


LockBit shares over clearnet the torrent for stolen Entrust data
source: BleepingComputer (h/t Phantom Radar)

LockBit ransomware operation has been active for almost three years, since September 2019. At the time of writing, LockBit's data leak site is up and running.

The gang is listing more than 700 victims and Entrust is one of them, with data for the company leaked on August 27.

Update [August 29, 09:12]: Article updated with info on Entrust data being shared over clearnet.



[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.
