LockBit ransomware gang gets aggressive with triple-extortion tactic

bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/

Ionut Ilascu

By
Ionut Ilascu

- August 28, 2022
- 06:44 PM
- 0

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.

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.

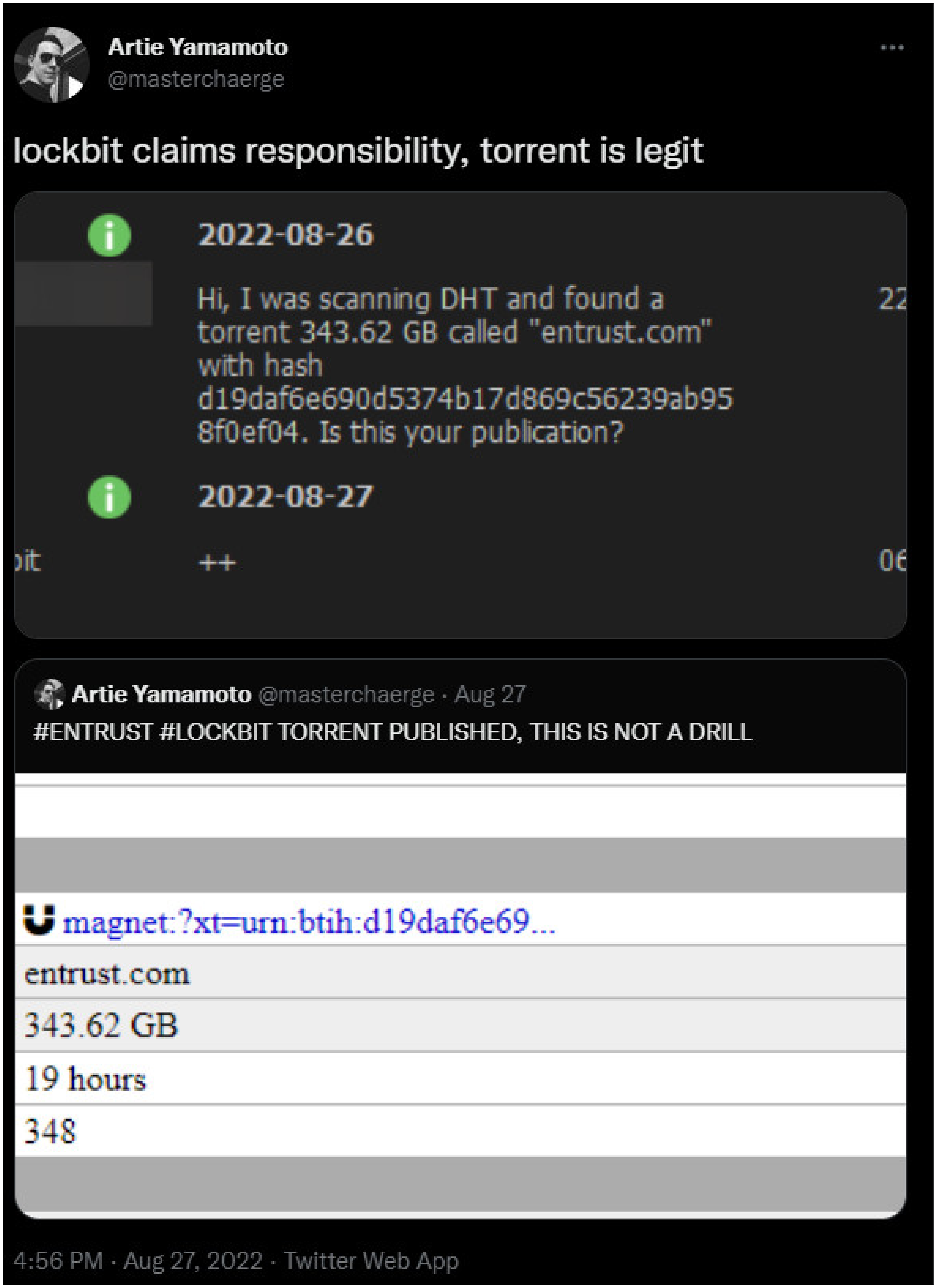
"I am looking for dudosers [DDoSers] in the team, most likely now we will attack targets and provide triple extortion, encryption + date leak + dudos, because I have felt the power of dudos and how it invigorates and makes life more interesting," LockBitSupp wrote in a post on a hacker forum.

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.



Artie Yamamoto
@masterchaerge

lockbit claims responsibility, torrent is legit

2022-08-26

Hi, I was scanning DHT and found a torrent 343.62 GB called "entrust.com" with hash d19daf6e690d5374b17d869c56239ab958f0ef04. Is this your publication? 22

2022-08-27

oit ++ 06

Artie Yamamoto @masterchaerge · Aug 27
#ENTRUST #LOCKBIT TORRENT PUBLISHED, THIS IS NOT A DRILL

magnet:?xt=urn:btih:d19daf6e69...
entrust.com
343.62 GB
19 hours
348

4:56 PM · Aug 27, 2022 · Twitter Web App

Lockbit ransomware leaks Entrust data

source: Artie Yamamoto

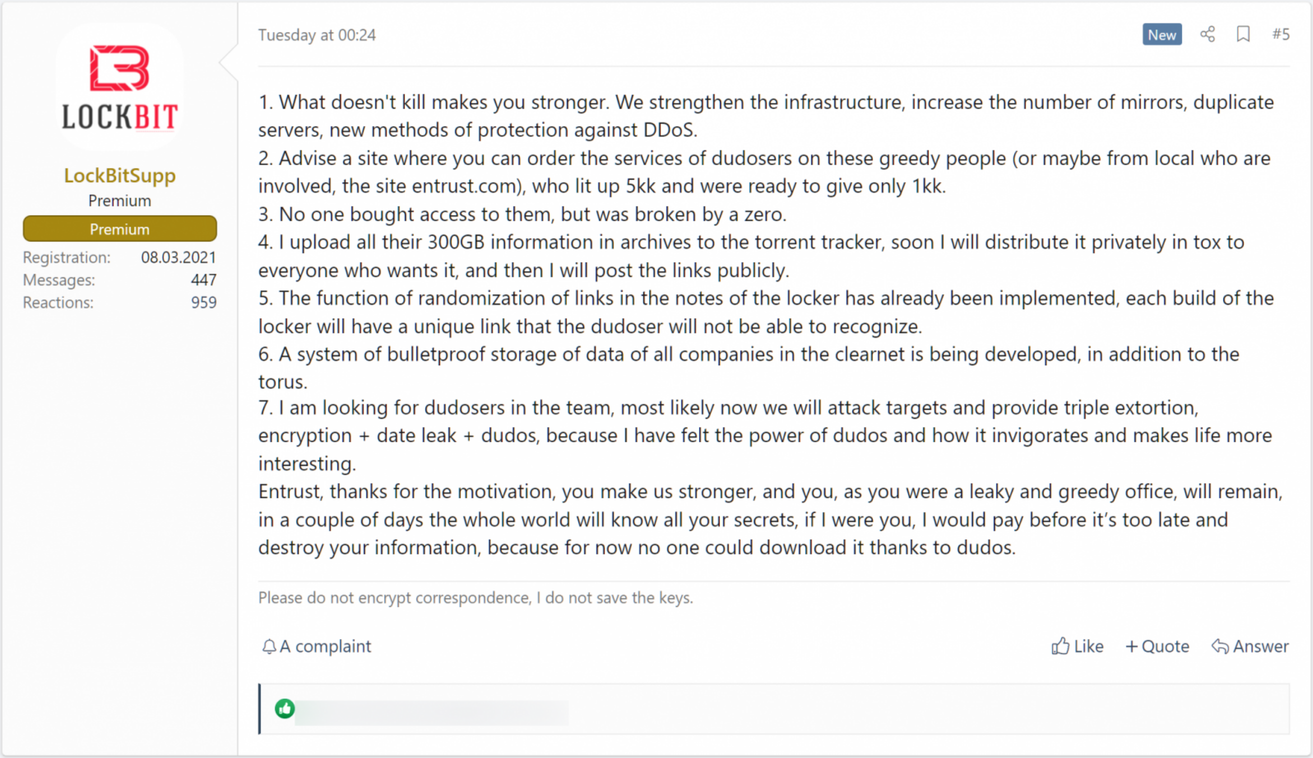
The operators wanted to make sure that Entrust's data is available from multiple sources and, besides publishing it on their site, they also shared the torrent over at least two file storage services, with one of them no longer making it available.

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.



LockBitSupp
Premium
Premium
Registration: 08.03.2021
Messages: 447
Reactions: 959

Tuesday at 00:24

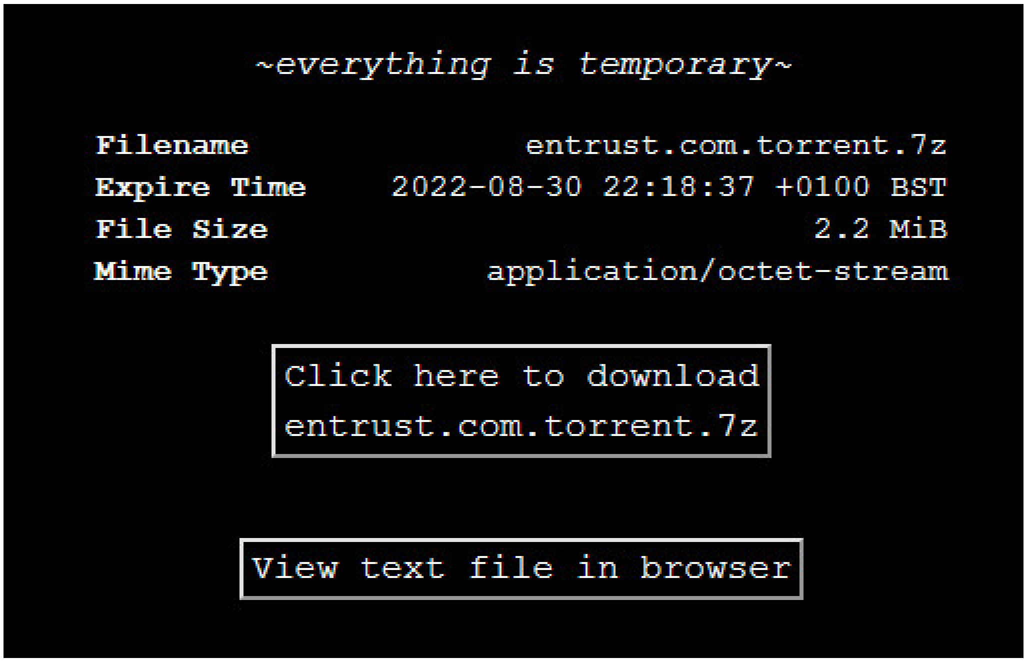
1. What doesn't kill makes you stronger. We strengthen the infrastructure, increase the number of mirrors, duplicate servers, new methods of protection against DDoS.
2. Advise a site where you can order the services of dudosers on these greedy people (or maybe from local who are involved, the site entrust.com), who lit up 5kk and were ready to give only 1kk.
3. No one bought access to them, but was broken by a zero.
4. I upload all their 300GB information in archives to the torrent tracker, soon I will distribute it privately in tox to everyone who wants it, and then I will post the links publicly.
5. 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 will not be able to recognize.
6. A system of bulletproof storage of data of all companies in the clearnet is being developed, in addition to the torus.
7. I am looking for dudosers 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.

Entrust, thanks for the motivation, you make us stronger, and you, as you were a leaky and greedy office, will remain, in a couple of days the whole world will know all your secrets, if I were you, I would pay before it’s too late and destroy your information, because for now no one could download it thanks to dudos.

Please do not encrypt correspondence, I do not save the keys.

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.



```
        ~everything is temporary~

  Filename                entrust.com.torrent.7z
  Expire Time     2022-08-30 22:18:37 +0100 BST
  File Size                             2.2 MiB
  Mime Type            application/octet-stream

           Click here to download
           entrust.com.torrent.7z

         View text file in browser
```

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

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.

Related Articles:

LockBit ransomware blames Entrust for DDoS attacks on leak sites

The Week in Ransomware - August 26th 2022 - Fighting back

RansomEXX claims ransomware attack on Sea-Doo, Ski-Doo maker

LockBit claims ransomware attack on security giant Entrust, leaks data

BlackByte ransomware gang is back with new extortion tactics

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.