LockBit ransomware blames Entrust for DDoS attacks on leak sites

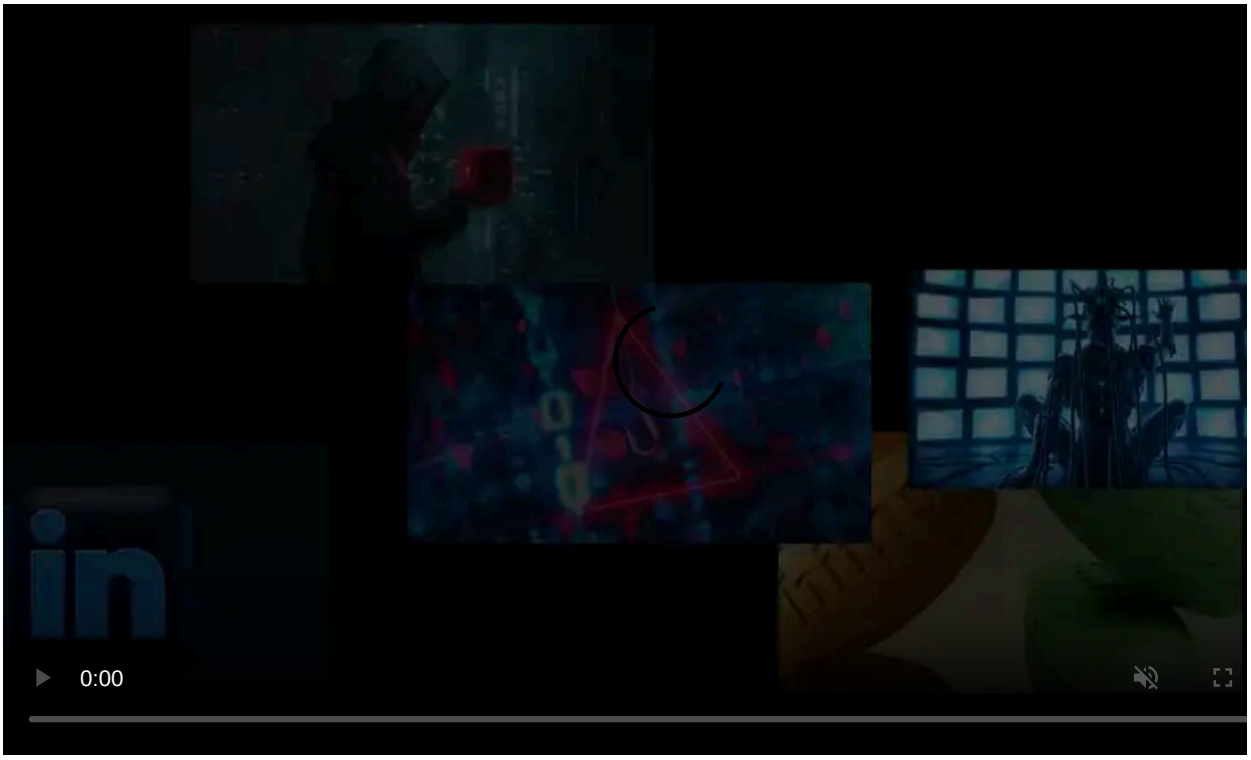
By Lawrence Abrams

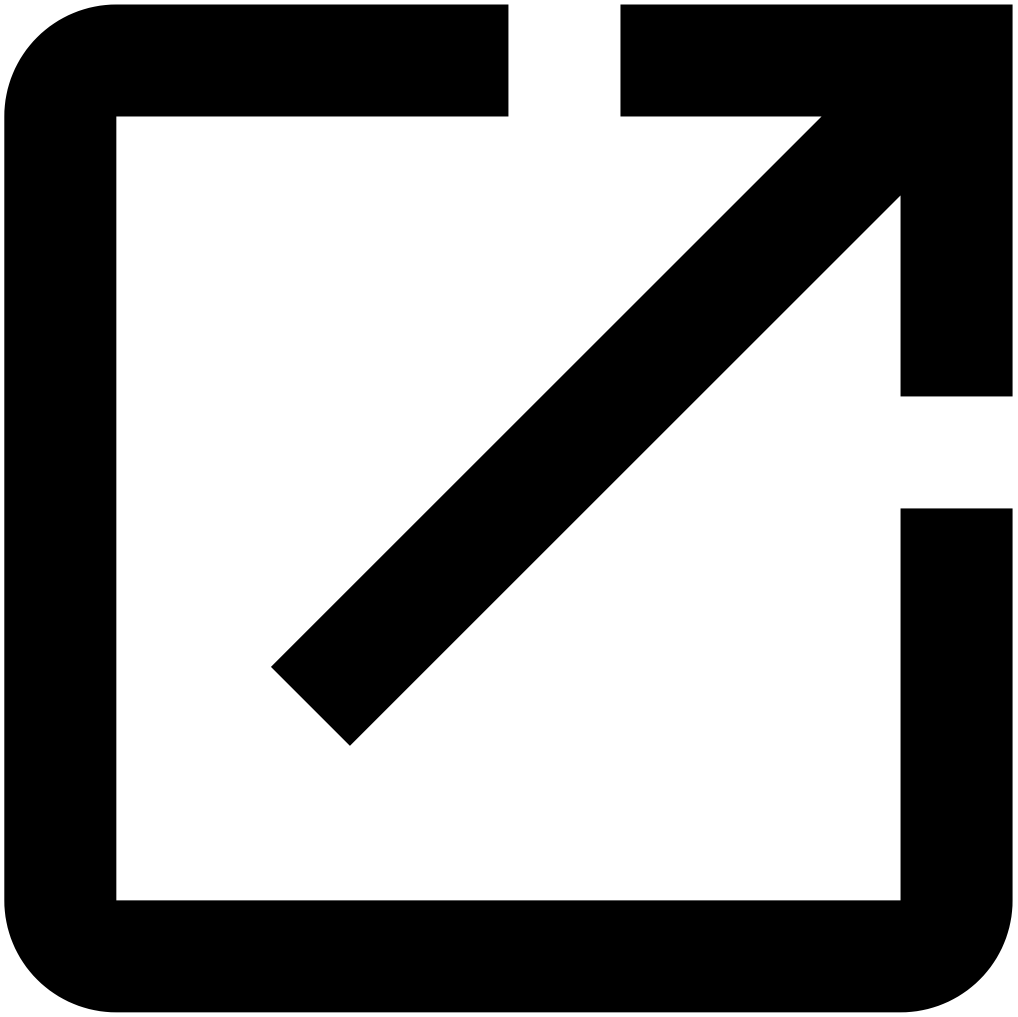
Published: 2022-08-22 · Archived: 2026-04-05 15:34:43 UTC

The LockBit ransomware operation's data leak sites have been shut down over the weekend due to a DDoS attack telling them to remove Entrust's allegedly stolen data.

In late July, digital security giant Entrust confirmed a cyberattack disclosing that threat actors had stolen data from its network during an intrusion in June. At the time, BleepingComputer was told by sources that it was a ransomware attack but we could not independently confirm the one behind it.

Last week, LockBit claimed responsibility for the attack and began leaking data Friday evening.


0:00



This leak consisted of 30 screenshots of data allegedly stolen from Entrust, including legal documents, marketing spreadsheets, and accounting data.

Alleged Entrust data leaked on LockBit's data leak site

Source: Dominic Alvieri

Soon after they started leaking data, researchers began reporting that the ransomware gang's Tor data leak sites were unavailable due to a DDoS attack.

Yesterday, security research group VX-Underground learned from LockBitSupp, the public-facing representative of the LockBit ransomware operation, that their Tor sites were under attack by someone they believed to be connected to Entrust.

"Ddos attack began immediately after the publication of data and negotiations, of course it was them, who else needs it? In addition, in the logs there is an inscription demanding the removal of their data," LockBitSupp told BleepingComputer in response to the questions about the attack.

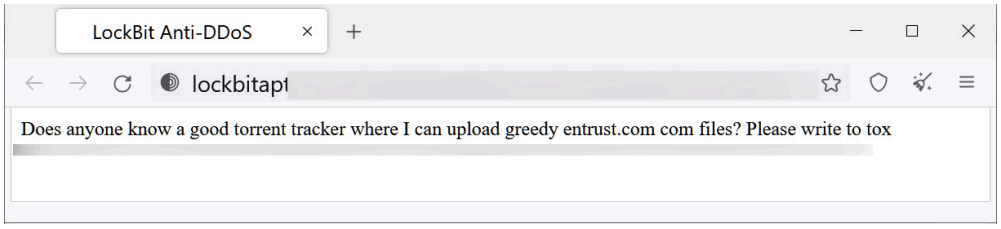
As you can see from these HTTPS requests, the attacker added a message to LockBit in the browser user agent field telling them to delete Entrust's data.

```
"GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
"GET / HTTP/1.1" 200 18869 "-" "DELETE_ENTRUSTCOM_MOTHERFUCKERS"
```

DDoS HTTPS requests with a message to LockBit

Cisco Talos researcher Azim Shukuhi tweeted that the DDoS attack on LockBit's servers consisted of "400 requests a second from over 1000 servers."

In retaliation to the attack, LockBit's data leak sites now show a message warning that the ransomware gang plans to upload all of Entrust's data as a torrent, which will make it almost impossible to take down.



The new message shown on LockBit data leak sites

Furthermore, the threat actors have shared the alleged negotiations between Entrust and the ransomware gang with security researcher Soufiane Tahiri. This chat indicates that the initial ransom demand was $8 million and dropped to $6.8 million later.

LockBitSupp told BleepingComputer that another cybersecurity firm, Accenture, also conducted a similar attack against their data leak sites but was less successful.

"The last ones to do this were the Accenture, but they were not very good at it, the Entrust were much more successful at it," explained LockBitSupp.

BleepingComputer has been unable to confirm if this statement is true.

The ALPHV ransomware operation's data leak sites were also down this weekend in what is believed to be a DDoS attack. However, it is not known if the two attacks are related.

Security firm or threat actor behind attacks?

BleepingComputer has contacted Entrust to ask if they were responsible for the DDoS attack on LockBitSupp but did not receive a reply.

So, at this point, it is unclear if Entrust, an affiliated cybersecurity company, or simply a rival threat actor is taking advantage of the situation by conducting the attacks.

Security researchers are unsure who is attacking LockBit, with some saying that it would be unprecedented for a cybersecurity company to conduct attacks like these.

"I believe this is somehow backed by Entrust at the moment but not another group attacking both. The only group with an interest in attacking both would be the feds or gov entities," security researcher Dominic Alvieri told BleepingComputer.

"Do we have evidence that a cybersecurity firm is carrying out a DDoS? That would be an unprecedented and somewhat of a paradigm shift. it could be competitors or may be someone with animosity towards those top two from within the RaaS world," tweeted Shukuhi.

"The idea that a cybersecurity company would be yeeting a DDoS around would set a dangerous precedence," tweeted a threat intelligence researcher known as Cyberknow.

While we will likely never know who is behind these attacks, it has shown how effective attacks like this can be in disrupting a ransomware gang's operations.

Whether victims, cybersecurity companies, or even governments may adopt such tactics in the future (if not already doing so) remains to be seen.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-blames-entrust-for-ddos-attacks-on-leak-sites/