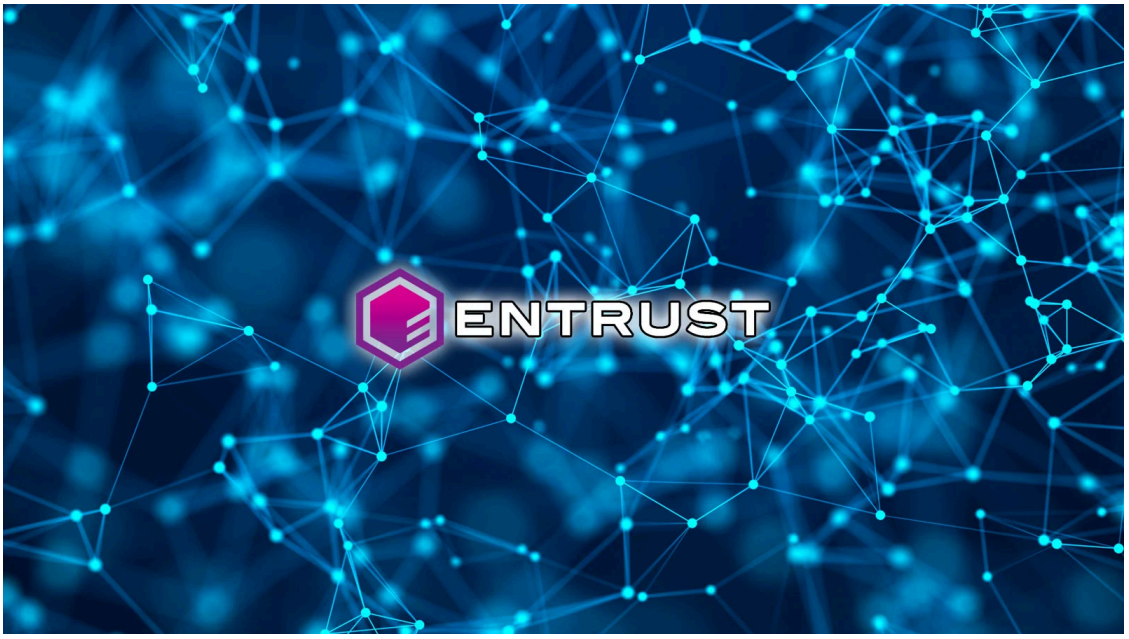
LockBit claims ransomware attack on security giant Entrust, leaks data

By Lawrence Abrams

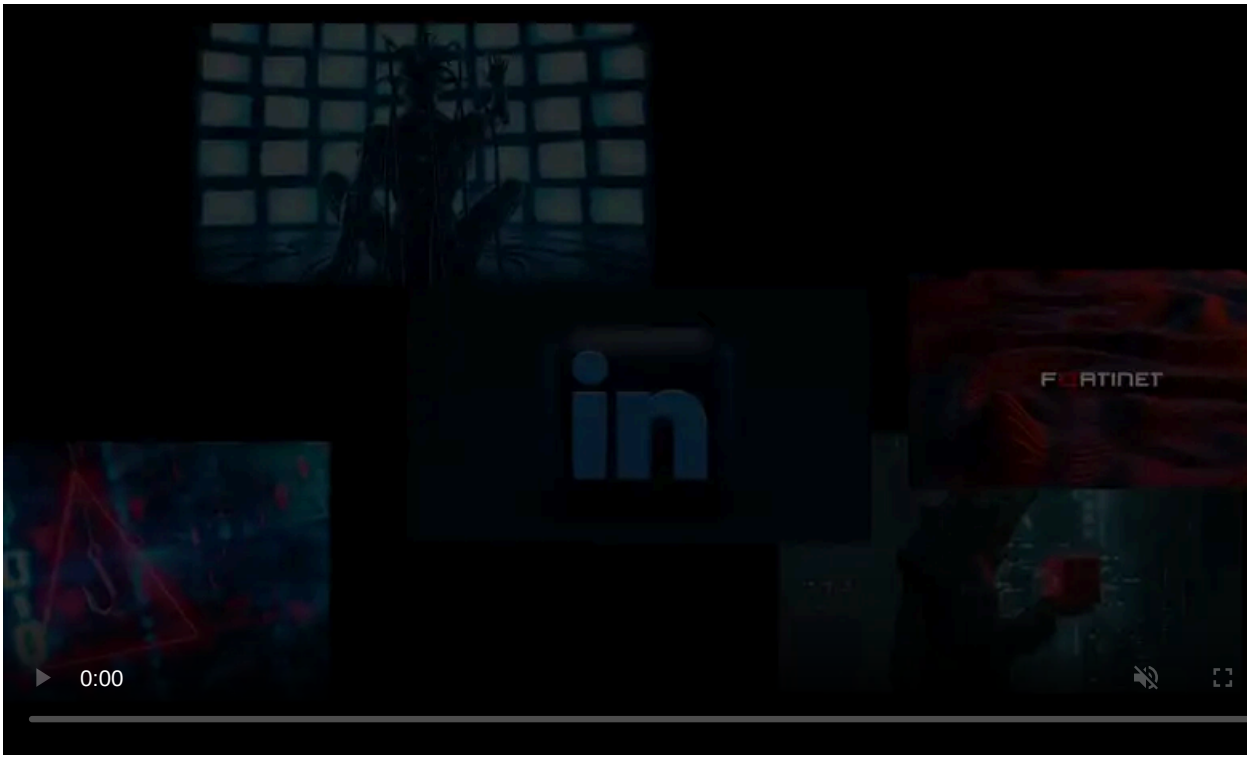
Published: 2022-08-18 · Archived: 2026-04-05 19:02:10 UTC

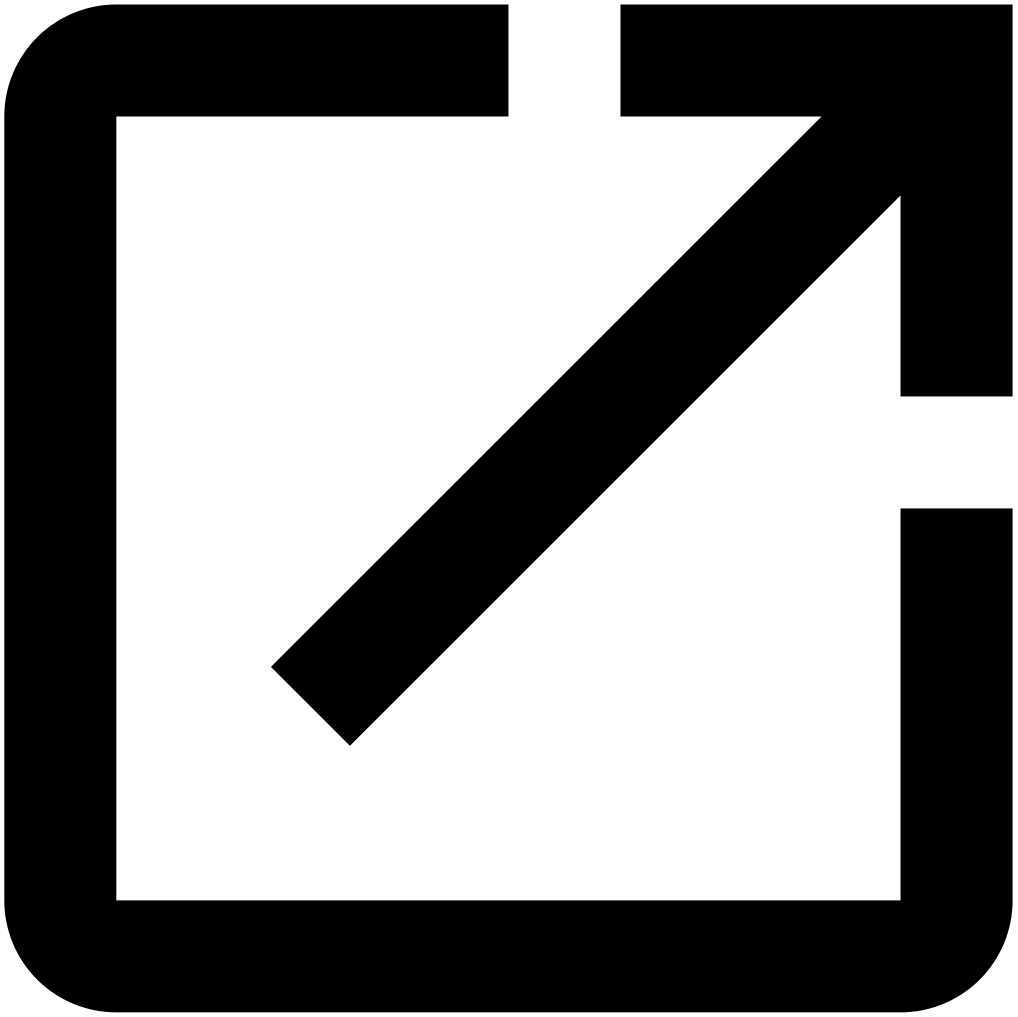


August 21th, 2022 update below. This post was originally published on August 18th.

The LockBit ransomware gang has claimed responsibility for the June cyberattack on digital security giant Entrust.

Last month, BleepingComputer broke the story that Entrust suffered a ransomware attack on June 18th, 2022.


0:00



Starting in early June, Entrust had begun to tell customers that they suffered a cyberattack where data was stolen from internal systems.

"We have determined that some files were taken from our internal systems," Entrust shared in a security notification to customers.

"As we continue to investigate the issue, we will contact you directly if we learn information that we believe would affect the security of the products and services we provide to your organization."

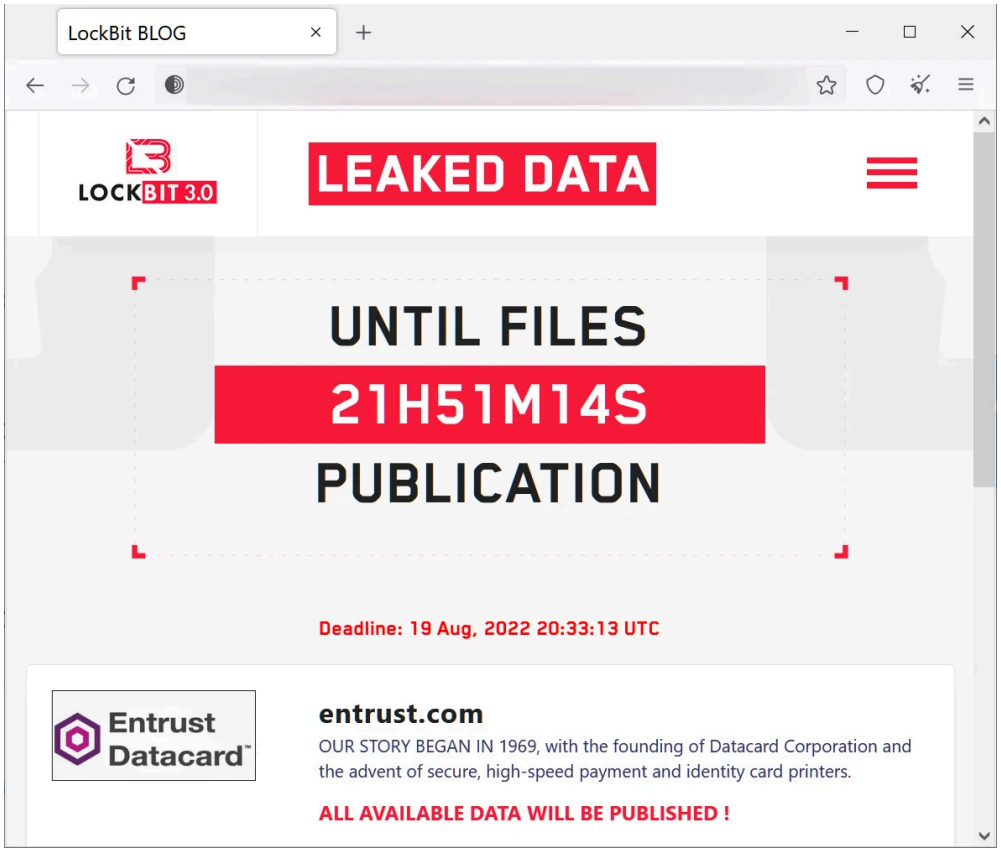
While Entrust would not share any details regarding the attack or confirm if it was ransomware, they told BleepingComputer that they were investigating the incident.

"While our investigation is ongoing, we have found no indication to date that the issue has affected the operation or security of our products and services, which are run in separate, air-gapped environments from our internal systems and are fully operational," Entrust told BleepingComputer.

However, AdvIntel CEO Vitali Kremez told BleepingComputer at the time that a well-known ransomware gang had attacked Entrust after purchasing access to the corporate network through "network access sellers."

LockBit claims attack on Entrust

Today, security researcher Dominic Alvieri told BleepingComputer that LockBit had created a dedicated data leak page for Entrust on their website, stating that they would publish all of the stolen data tomorrow evening.



Entrust page on the LockBit data leak site

Source: BleepingComputer

When ransomware gangs publish data on their data leak sites, they usually leak data over time to scare the victim into returning to the negotiation table.

As LockBit states that they will publish *all* data, it indicates that Entrust has not negotiated with the ransomware operation or refuses to give in to their demands.

However, LockBit claiming of the attack supports what sources had previously told BleepingComputer about who was responsible.

LockBit is considered one of the most active ransomware operations at this time, with its public-facing operation 'LockBitSupp' actively engaging with threat actors and cybersecurity researchers.

In June, LockBit 3.0 was released with new encryptors based on the BlackMatter source code, new payment options, new extortion strategies, and the first ransomware bug bounty program.

Due to its ongoing adoption of new tactics, technology, and payment methods, it is vital for security and network professionals to stay up to date on the evolution of the operation and its TTPs.

Update 8/21/22:

LockBit leaks alleged Entrust data

LockBit began leaking Entrust's data Friday evening, first sharing screenshots of some of the allegedly stolen data, with the threat actors saying they would leak further data later that evening.

Alvieri, who has been monitoring the leak, told BleepingComputer that the leaked data consists of accounting and legal documents and marketing spreadsheets.

However, soon after they began leaking data, the ransomware gang's Tor data leak sites went offline, with the threat actors claiming that they are being DDoSed due to the Entrust attack.

When BleepingComputer contacted Entrust about the leaked data, they told us that they have nothing to add to their original statement from July.

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.
