Capital Health attack claimed by LockBit ransomware, risk of data leak

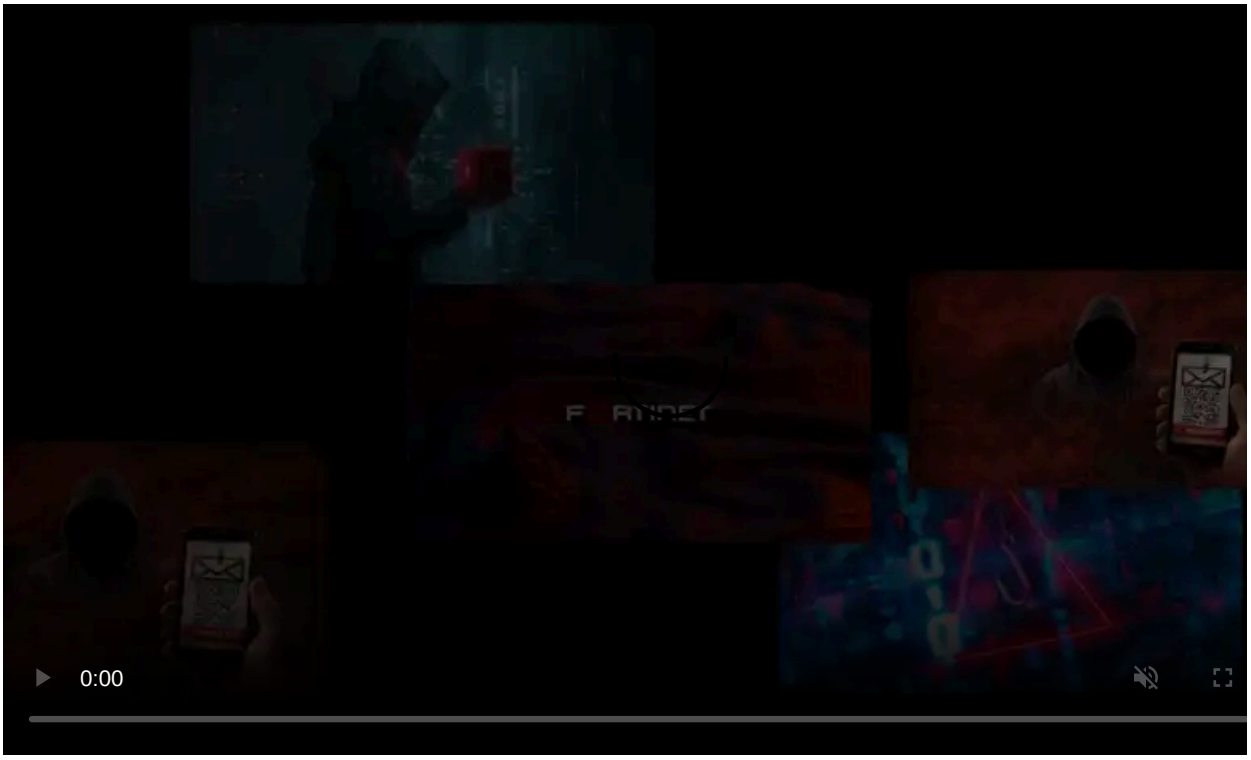
By Bill Toulas

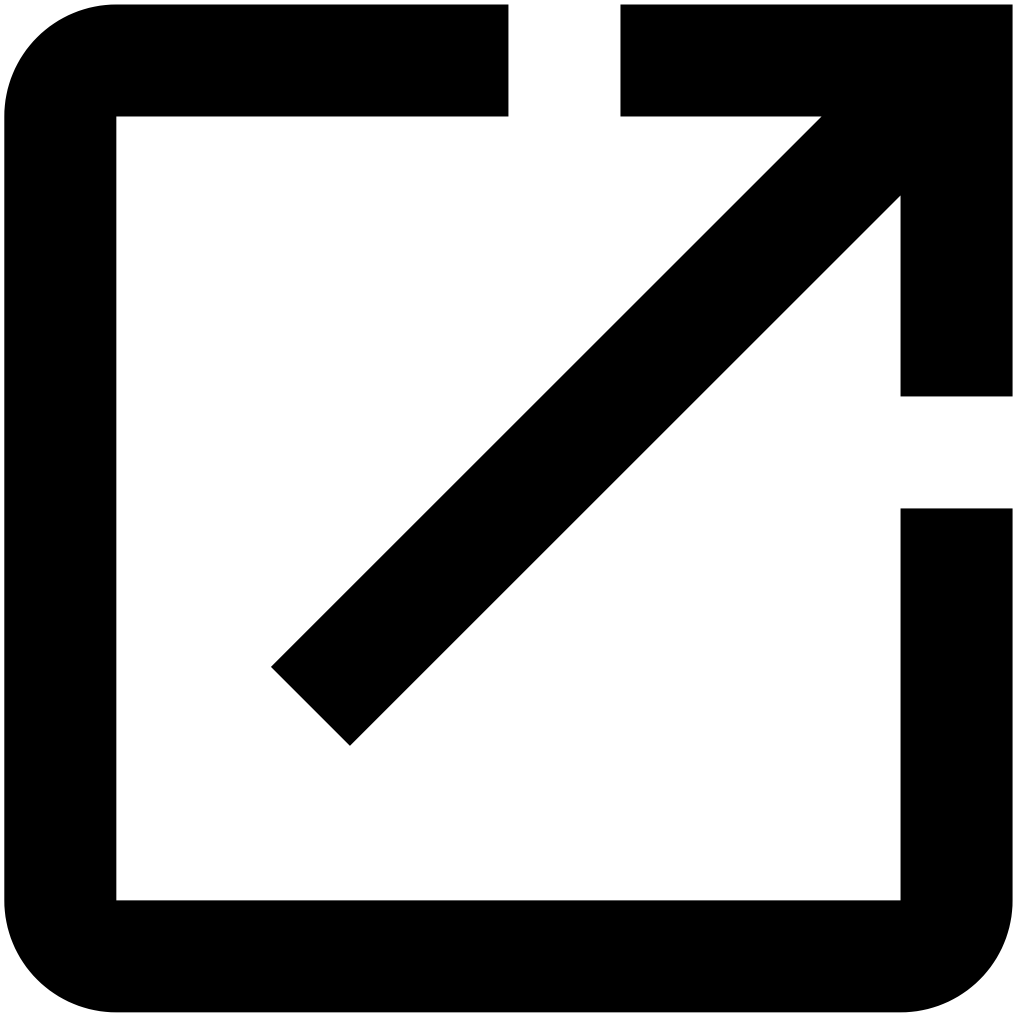
Published: 2024-01-08 · Archived: 2026-04-06 03:18:13 UTC

The LockBit ransomware operation has claimed responsibility for a November 2023 cyberattack on the Capital Health hospital network and threatens to leak stolen data and negotiation chats by tomorrow.

Capital Health is a primary healthcare service provider in New Jersey and parts of Pennsylvania, operating two major hospitals and several satellite and specialty clinics.

Last November, the organization experienced an IT systems outage following a cyberattack on its network, warning that the incident would impact its operations for at least a week.


0:00

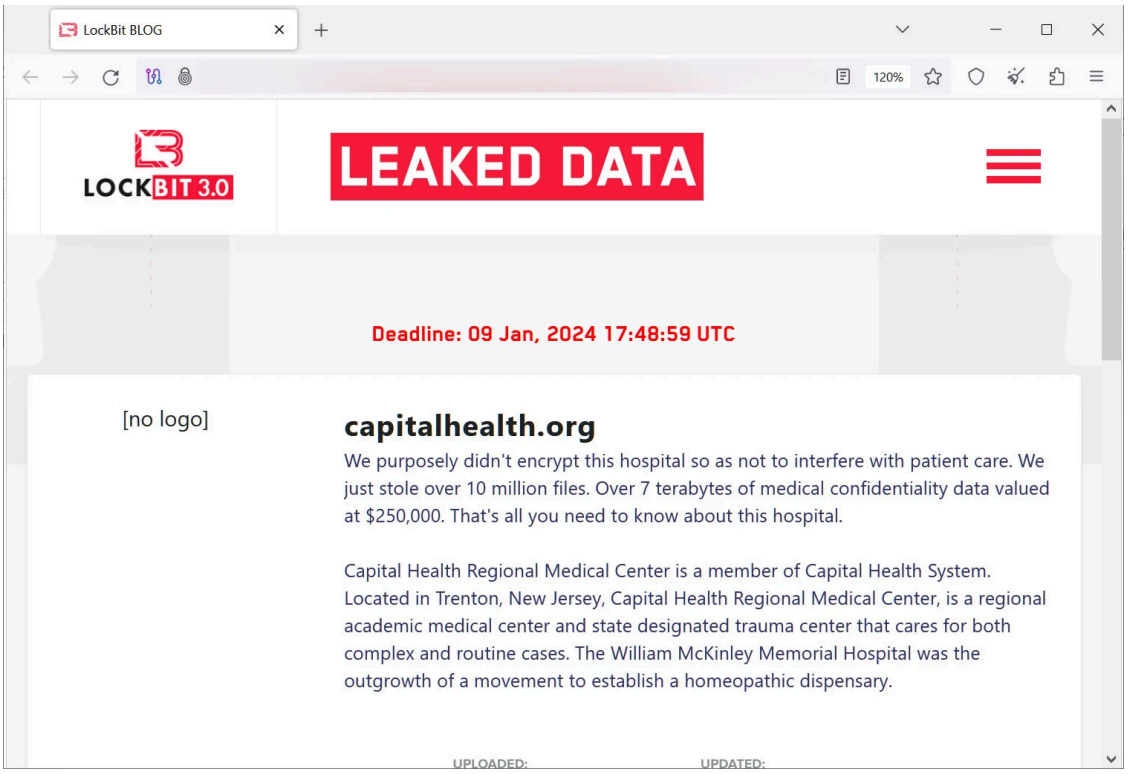


A security incident notification on the Capital Health website informs that all systems have been restored and operations have returned to normal, while additional security measures have been implemented to prevent similar incidents from re-occurring.

Capital Health's latest updates indicate they are still investigating whether data was stolen in the cyberattack.

LockBit claims attack on Capital Health

The LockBit ransomware gang has now claimed responsibility for the attack on Capital Health by listing the healthcare company on its data leak extortion portal yesterday.



Moreover, the cybercriminals allege to have stolen seven terabytes of sensitive medical data they threaten to leak tomorrow if the organization fails to meet their ransom payment demands.

LockBit has an affiliate rule that states their affiliates (hackers) will not encrypt files on hospital networks but allow them to steal data for extortion.

While this policy has been broken numerous times by the operation's affiliates, in the attack on Capital Health, the LockBit operation says they purposely avoided encrypting the organization's files and instead only stole data.

"We purposely didn't encrypt this hospital so as not to interfere with patient care. We just stole over 10 million files," the ransomware gang stated on their data leak site.

Most ransomware groups tend to have strict policies regarding healthcare service providers, advising their affiliates not to perform such assaults for ethical reasons and banning them if they deviate from that instruction.

However, the LockBit operation has repeatedly targeted healthcare networks, including the SickKids children's cancer hospital, the Katholische Hospitalvereinigung Ostwestfalen (KHO) in Germany, and the Carthage Area Hospital and Claxton-Hepburn Medical Center in upstate New York.

It should be noted that the LockBit operators claim that they are not behind the attack on KHO, but rather its another ransomware gang who used their leaked ransomware builder. BleepingComputer has not been able to independently verify

these claims.

If LockBit and other cybercrime gangs continue to follow a pure data-theft approach, extorting hospital operators without touching infrastructure would create a false sense of "harmless" cyberattacks.

Encryption-less ransomware attacks can still lead to system outages as part of the victim's response action, catastrophic data breaches for many people who received care in the targeted hospitals, and significant financial losses for already underfunded or economically stressed institutions.

Unfortunately, recent examples of high-impact ransomware attacks in the healthcare sector are abundant, including other victims, such as Ardent Health Services, Integris Health, ESO Solutions, and the Fred Hutchinson Cancer Center (Fred Hutch).

Source: https://www.bleepingcomputer.com/news/security/capital-health-attack-claimed-by-lockbit-ransomware-risk-of-data-leak/