French hospital CHC-SV refuses to pay LockBit extortion demand

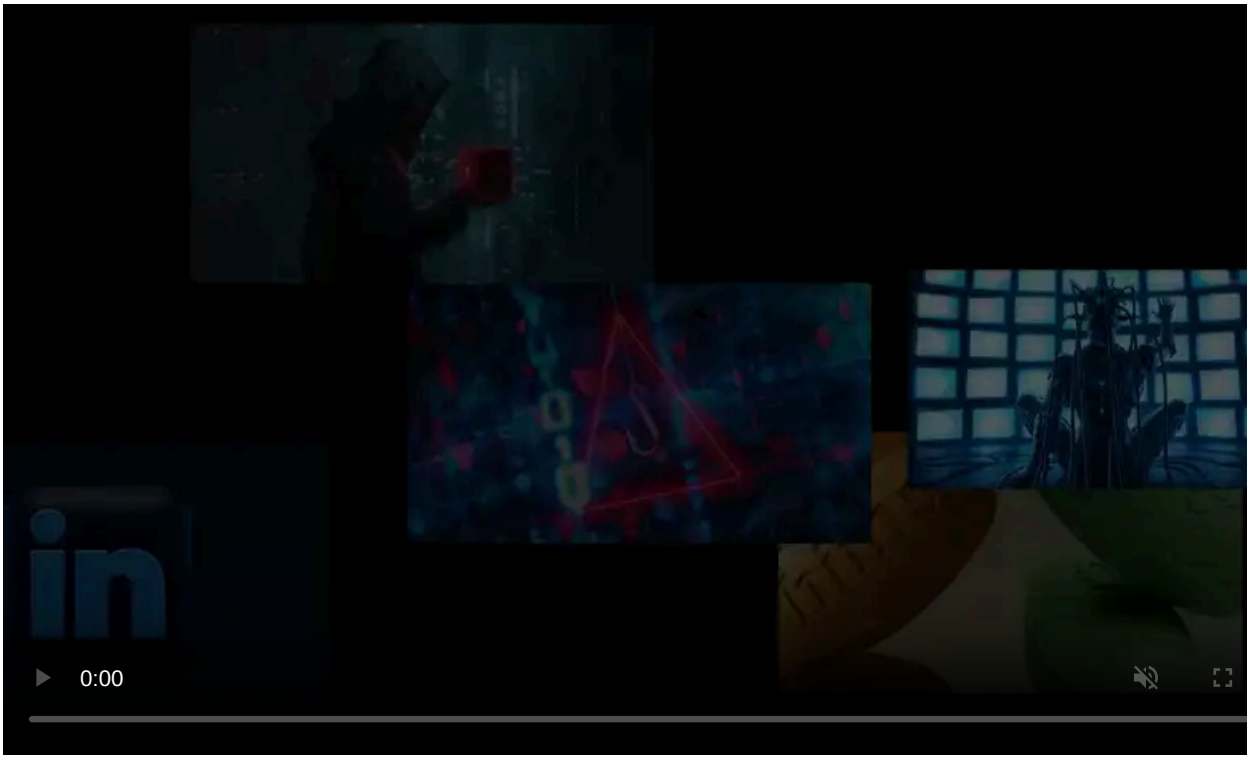
By Bill Toulas

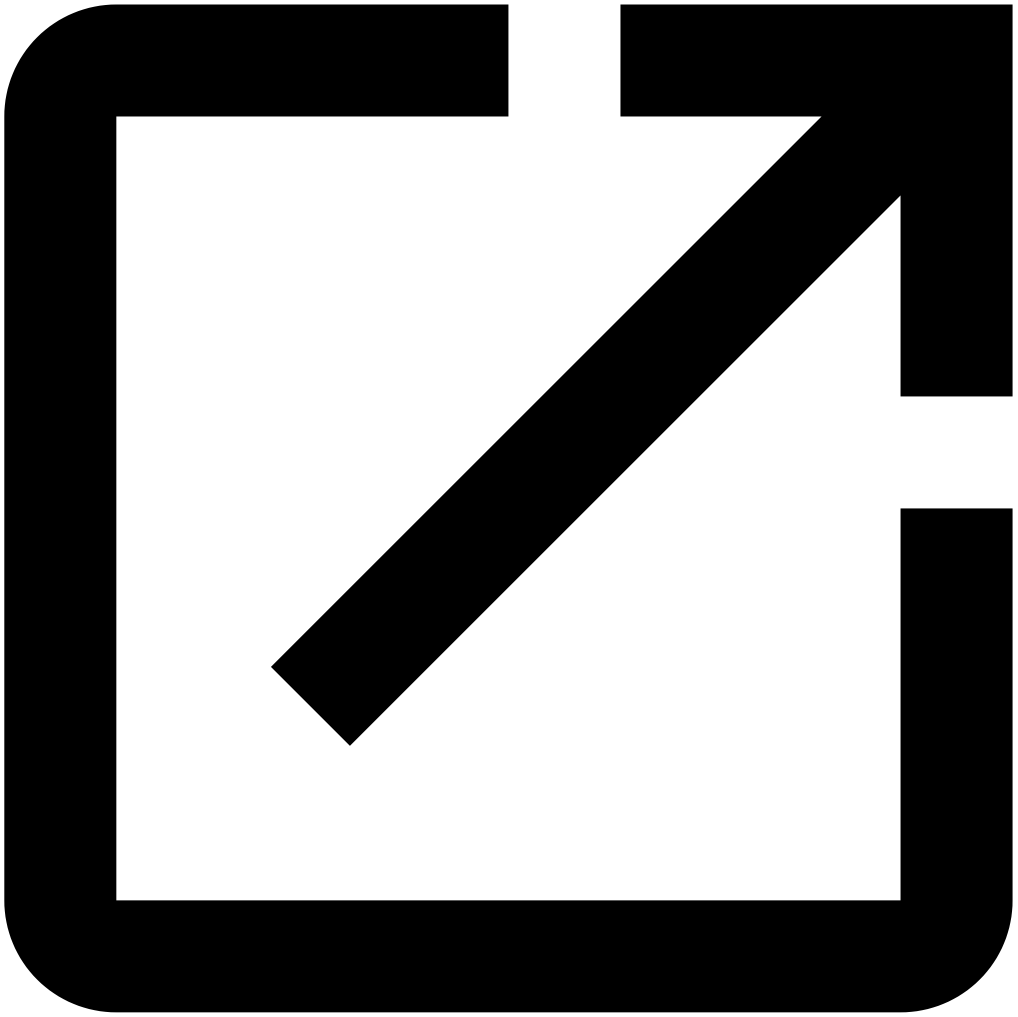
Published: 2024-05-01 · Archived: 2026-04-05 16:48:53 UTC

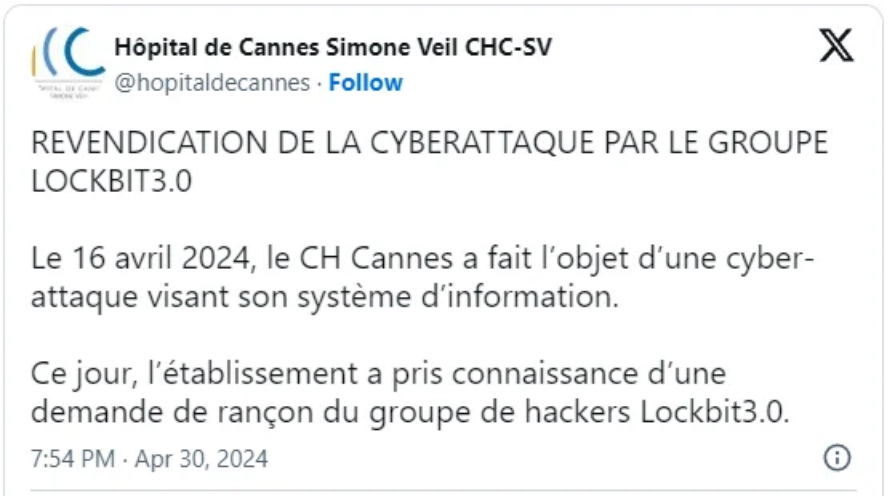
The Hôpital de Cannes - Simone Veil (CHC-SV) in France announced it received a ransom demand from the Lockbit 3.0 ransomware gang, saying they refuse to pay the ransom.

On April 17, the 840-bed hospital announced a severe operational disruption caused by a cyberattack that forced it to take all computers offline and reschedule non-emergency procedures and appointments.

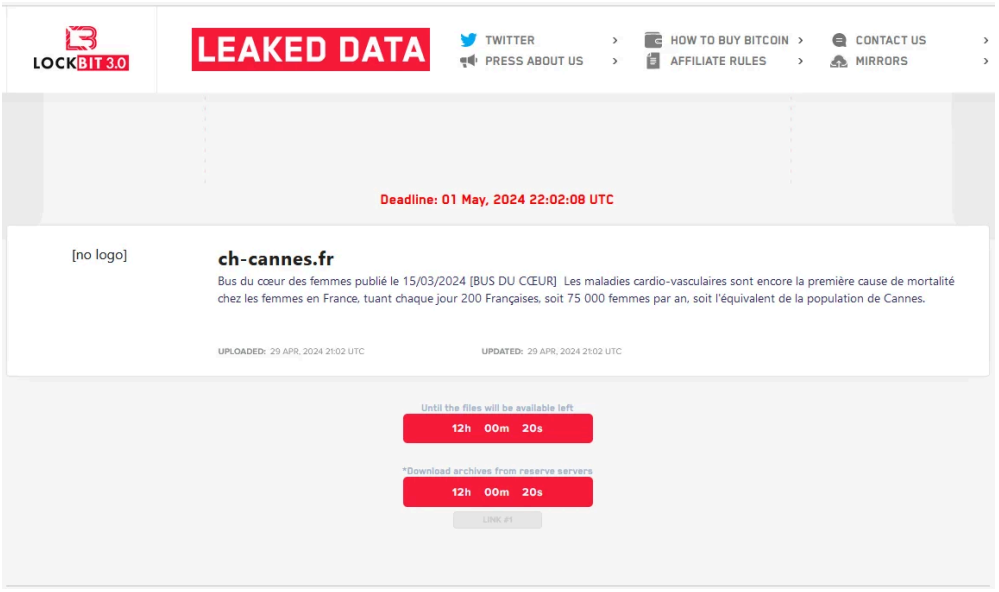
Yesterday, the establishment announced on X that it has received a ransom demand by the Lockbit 3.0 ransomware operation, which it forwarded to the Gendarmerie and the National Agency for Information Systems Security (ANSSI).


0:00





At the same time, the LockBit ransomware group added CHC-SV on their extortion portal on the darkweb, threatening to leak the first sample pack of files stolen during the attack by the end of the day.



LockBit threatens to leak stolen data soon
BleepingComputer

The healthcare organization tweeted that they will not pay the ransom and promised to inform impacted individuals if the threat actors begin leaking data.

"In the event of a data release potentially belonging to the hospital, we will communicate to our patients and stakeholders, after a detailed review of the files that may have been exfiltrated, about the nature of the stolen information."

Meanwhile, the hospital's IT staff are still fighting to bring impacted systems back to normal operational status, as internal investigations on the incident remain ongoing.

Hurt but still ruthless

FBI's disruption of the LockBit ransomware-as-a-service operation via 'Operation Cronos' and the simultaneous release of a decryptor in mid February 2024, have had an adverse impact on the threat group.

Affiliates have lost their trust in the project, and some members opted to lay low in fear of identification and prosecution.

Despite the disruption, the ransomware project performed a restart only a week later, setting up new data leak sites and using updated encryptors and ransom notes.

LockBit's policy about attacks on healthcare providers has always been muddy at best, with the group's leaders not enforcing the declared restrictions on affiliates performing attacks that impacted patient care.

The attack on CHC-SV acts as a confirmation of the threat group's complete disregard for the sensitive matter of avoiding disruption of healthcare services.

Source: https://www.bleepingcomputer.com/news/security/french-hospital-chc-sv-refuses-to-pay-lockbit-extortion-demand/