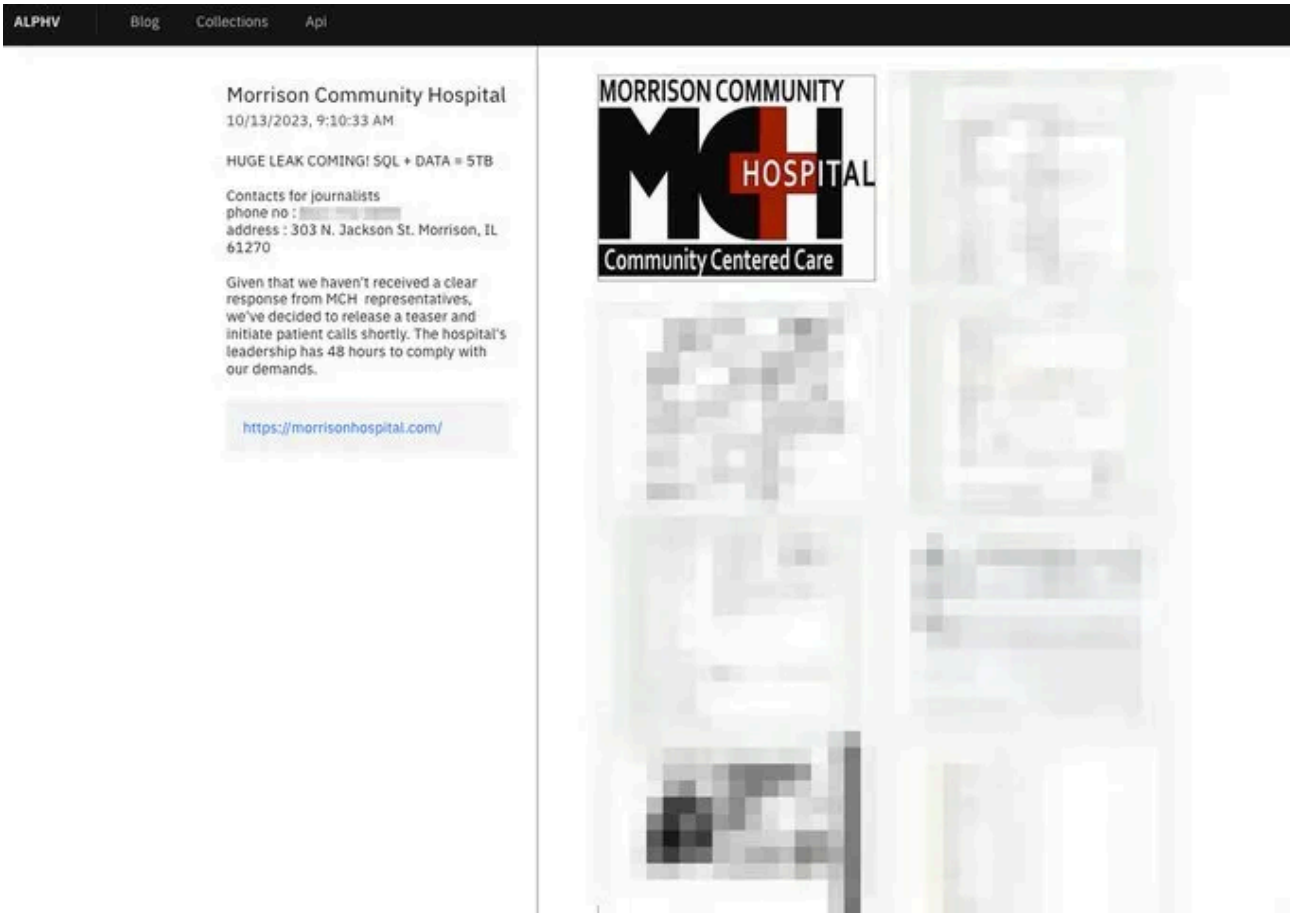
The Alphv ransomware gang stole 5TB of data from the Morrison Community Hospital

By Pierluigi Paganini

Published: 2023-10-15 · Archived: 2026-04-05 21:25:25 UTC



The Alphv ransomware group added the Morrison Community Hospital to its dark web leak site. Threat actors continue to target hospitals.

The ALPHV/BlackCat ransomware group claims to have hacked the Morrison Community Hospital and added it to its dark web Tor leak site.

The group claims to have stolen 5TB of patients' and employee's information, backups, PII documents, and more. The gang also published a sample as proof of the stolen data.

The group states that it has started contacting journalists because the representatives of the Morrison Community Hospital haven't provided a clear response. The Alphv gang also threatens to initiate patient calls shortly.

The popular researcher Brett Callow states that far this year, 29 US health systems with 90 hospitals between them have been impacted by #ransomware, and at least 23/29 had data stolen.

In September, the LockBit ransomware group breached two hospitals, the Carthage Area Hospital and the Clayton-Hepburn Medical Center in New York.

This isn't the first time the Lockbit gang or its affiliates hit a hospital. In January, the LockBit ransomware gang formally apologized for the attack on the Hospital for Sick Children (SickKids) and released a free decryptor for the Hospital.

The group is known to have a role for its affiliated that prohibits attacking healthcare organizations. Its policy forbids to encrypt systems of organizations where damage could lead to the death of individuals.

The gang explained that one of its partners attacked SickKids violating its rules, for this reason, it blocked the affiliate.

Affiliates of the Lockbit gang have also hit other healthcare organizations in the past, in early December 2022, the Hospital Centre of Versailles was hit by a cyber attack that was attributed to the group. Hospital Centre of Versailles, which includes Andre-Mignot Hospital, Richaud Hospital and the Despagne Retirement Home, canceled operations and transferred some patients due to the cyberattack.

In August, the gang attacked the Center Hospitalier Sud Francilien (CHSF), a hospital southeast of Paris. The attack disrupted the emergency services and surgeries and forced the hospital to refer patients to other structures. According to local media, threat actors demand a $10 million ransom to provide the decryption key to restore encrypted data.

Other ransomware attacks recently hit US hospitals. Recently the Rhysida ransomware group made the headlines because it **announced** the hack of Prospect Medical Holdings and the theft of sensitive information from the organization.

The Rhysida ransomware group threatened Prospect Medical Holdings to leak the stolen data if the company did not pay a 50 Bitcoins ransom (worth $1.3 million). The same group this week claimed to have breached other three US hospitals.

The systems at three hospitals and other medical facilities operated by Singing River Health System were hit by a cyber attack at the end of August.

Follow me on Twitter: **@securityaffairs** and **Facebook** and **Mastodon**

Pierluigi Paganini

(SecurityAffairs – hacking, ransomware)
