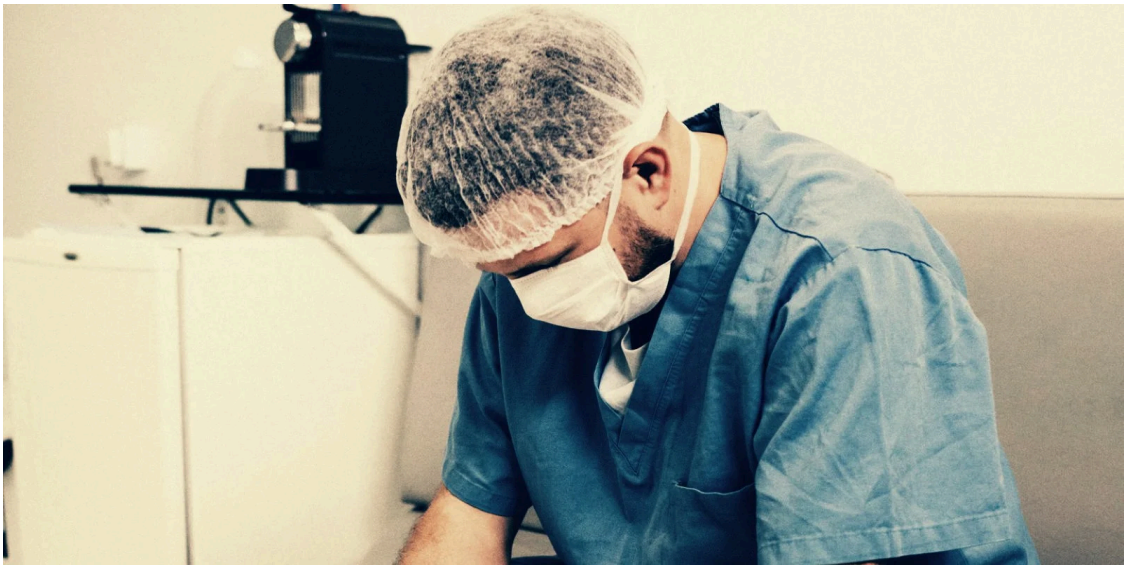
Brooklyn & Vermont hospitals are latest Ryuk ransomware victims

By Lawrence Abrams

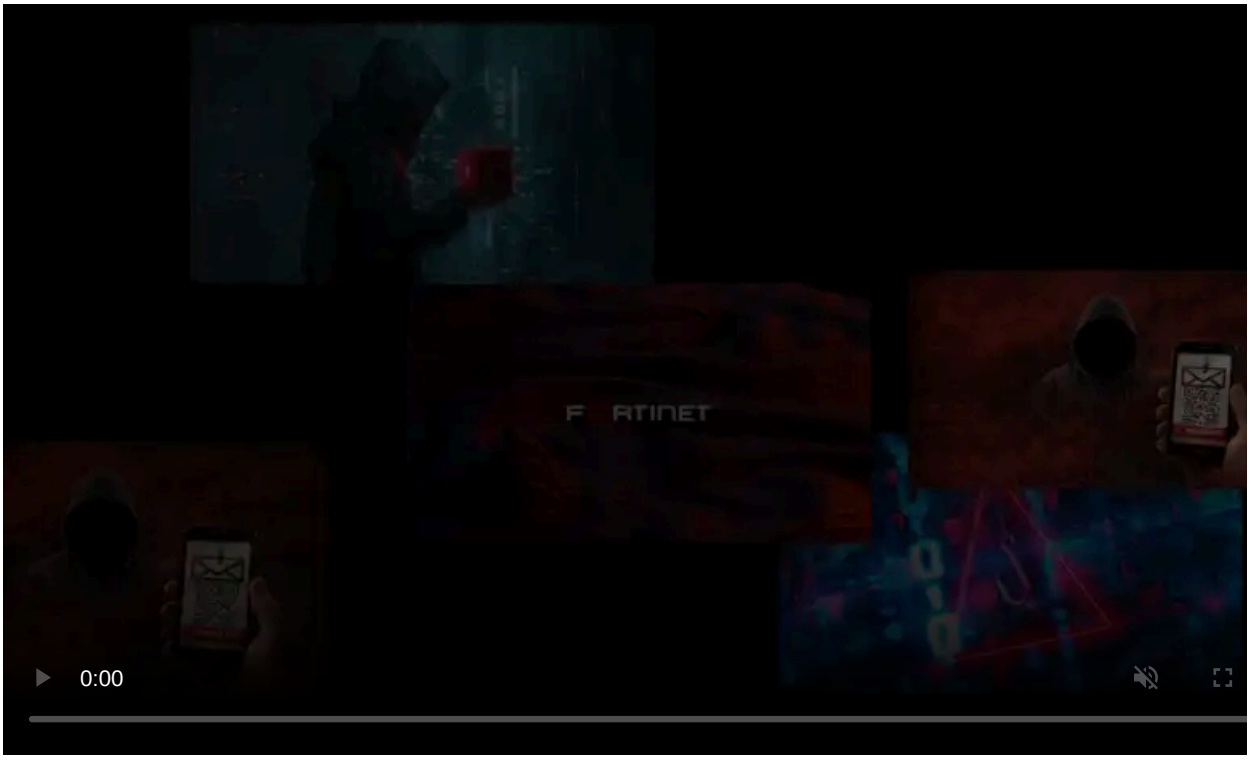
Published: 2020-10-29 · Archived: 2026-04-06 01:00:58 UTC



Wyckoff Heights Medical Center in Brooklyn and the University of Vermont Health Network are the latest victims of the Ryuk ransomware attack spree covering the healthcare industry across the U.S.

Yesterday, the U.S. government hosted an emergency call with stakeholders in the healthcare industry to alert them to an "increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."

Later in the day, CISA issued a joint advisory publicly warning that U.S. hospitals and healthcare providers are actively targeted in cyberattacks deploying the Ryuk ransomware.


F RTINET
0:00

Charles Carmakal, senior vice president and CTO of Mandiant, told BleepingComputer that an Eastern European hacking group known as UNC1878 is responsible for these attacks and that they intend to attack hundreds of hospitals.

This week, Sky Lakes Medical Center in Oregon and St. Lawrence Health System in New York were hit in Ryuk ransomware attacks. Last month, hospital operator Universal Health Services was hit by a corporate-wide Ryuk attack, which impacted over 200 medical facilities nationwide.

In a new report released today, Check Point states that they have seen a 71% increase in ransomware attacks in October targeting the U.S. healthcare sector.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

Wyckoff Hospital suffered a Ryuk attack yesterday

Today, an employee of Wycoff contacted BleepingComputer and stated that their hospital suffered a Ryuk ransomware attack yesterday.

Wyckoff Heights Medical Center is a 350-bed teaching hospital located in Brooklyn, NY.

To prevent the spread of the attack to other devices, we were told that Wyckoff Hospital shut down portions of their network, but by then, it was too late, and many of the devices had been encrypted.

It is unknown if the hospital is redirecting patients to other hospitals and what impact the attack has had on patients' treatment.

BleepingComputer has reached out to Wyckoff for further comment but has not received a response.

Vermont network of hospitals hit as well

Today, the AP reported that the University of Vermont Health Network had suffered a cyberattack affecting all the hospitals in their network to varying degrees.

"The attack has caused variable impacts at each of our affiliates. Staff are continuing to follow well-practiced standby procedures to ensure safe patient care. We understand the difficulty this causes for our patients and the community and apologize for the impact. There have been some changes to patient appointments and we are attempting to reach those patients who have been affected. We will continue to provide systems and patient service updates when they are available," read a statement from the University of Vermont Health Network.

The current status of each affected hospital is:

- Alice Hyde Medical Center – Malone, NY - Maintaining all patient care services.
- Central Vermont Medical Center – Berlin, VT - Maintaining all patient care services, but patients may experience delays
- Champlain Valley Physicians Hospital – Plattsburgh, NY - Maintaining all patient care services, but physician practice patients may experience slight delays.
- Elizabethtown Community Hospital – Elizabethtown, NY - Maintaining all patient care services.
- Porter Medical Center – Middlebury, VT Maintaining all patient care services.
- UVMHN Home Health and Hospice Maintaining all patient and resident care services
- UVM Medical Center – Burlington, VT Rescheduling some elective procedures scheduled for Thursday, 10/29, with the hope of resuming procedures on Friday, 10/30.

The hospital network is working with the FBI and the Vermont Department of Public to investigate the attack.

"FBI Albany can confirm we are investigating a potential cyber attack at UVM Health, along with our federal, state and local partners. This is an active investigation, and we decline to comment further at this time," the FBI told BleepingComputer in a statement.

It is unknown if Ryuk was utilized in this particular attack.

Cybersecurity firm offering free ransomware assistance

Hospitals that are forced to pay a Ryuk ransom need to be careful of using their decryptor as it is known to corrupt certain types of files.

Emsisoft is offering free ransomware recovery services to healthcare organizations during the pandemic, which include custom decryptors that fix known decryption bugs and can recover files faster than the threat actor's decryptors.

"There are multiple factors and it depends a bit on the hardware, but there are three major factors: We heavily optimised I/O (so the reading and writing has been optimised a lot and been adjusted for modern mass storage), we use hardware accelerated cryptography, and we make creating a backup first unnecessary, because unlike the TA's tool, we operate on copies of data."

"The real benefit is in the fact that we focus on data safety first. So our decryptors generally are more stable, are safer to use, and produce correct results," Emsisoft CTO Fabian Wosar told BleepingComputer in a conversation.
