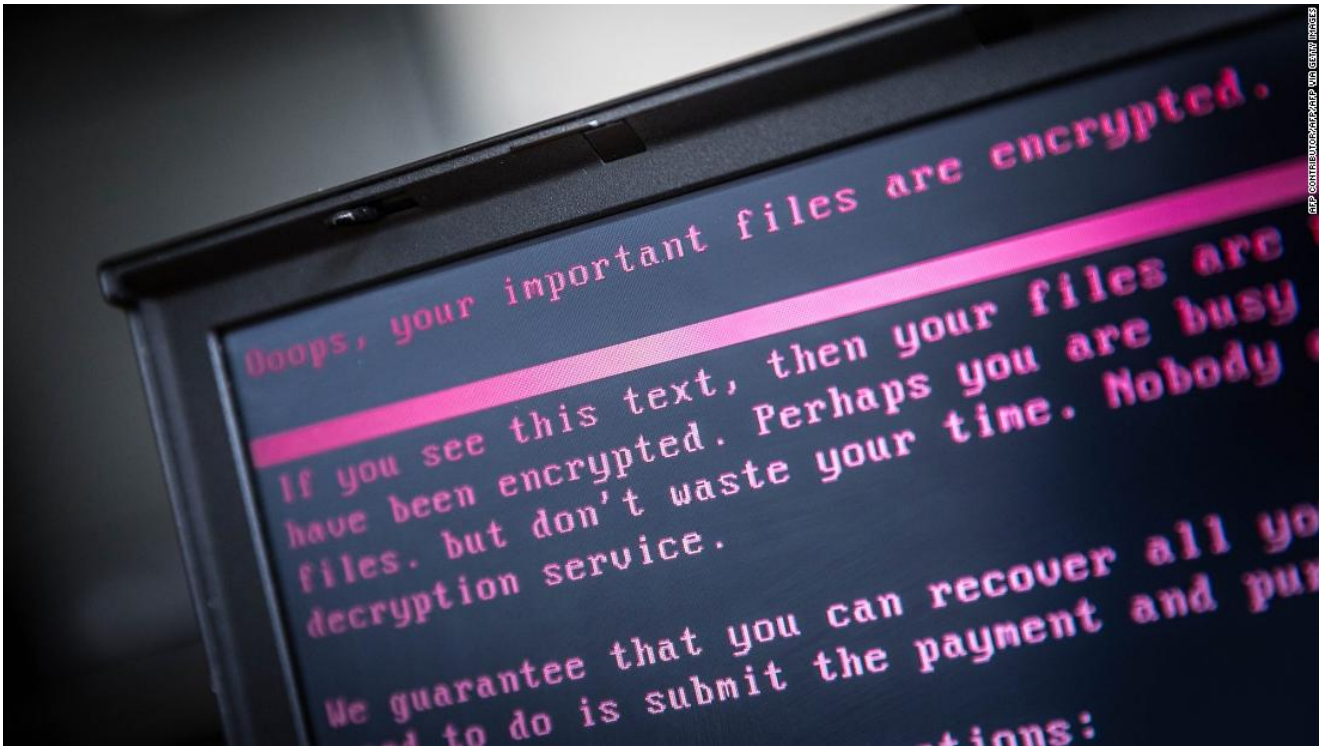
Several hospitals targeted in new wave of ransomware attacks

edition.cnn.com/2020/10/28/politics/hospitals-targeted-ransomware-attacks/index.html

October 28, 2020



*(CNN)*Several hospitals across the United States have been targeted in ransomware attacks in what appears to be an escalation and expansion of similar attacks previously launched on other hospitals and medical facilities.

The US Cybersecurity and Infrastructure Security Agency released a warning advisory Wednesday night regarding ransomware activity targeting health care facilities. On Twitter, CISA said "there is an imminent and increased cybercrime threat to U.S. hospitals and healthcare providers."

"CISA, FBI, and (the Department of Health and Human Services) have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers," the advisory stated. "CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats."

A Trump administration official told CNN that some hospitals have already been affected.

Ransomware is a type of malware, or malicious software, that encrypts a victim's files. The attacker then typically demands a ransom from the victim to restore access to the data upon payment. Users are often shown instructions for how to pay a fee to get the decryption key.

The costs can range from a few hundred dollars to thousands, often payable to cybercriminals in Bitcoin.

Read More

Ransomware and other cyber attacks have seen a sharp rise this year, and hospitals have been particularly vulnerable since the start of the global pandemic. Since July, hospitals in states including New York, Nebraska, Ohio, Missouri and Michigan have all been attacked by some form of ransomware.

A Trump administration official told CNN that several hospitals have been targeted in the attacks over the past two days, and while it's still early, the official said the incidents may be connected. The federal government is investigating the attacks, the official said.

So far, St. Lawrence Health Systems in New York and the Sky Lakes Medical Center in Oregon confirmed to CNN that they were targeted over the past few days. The University of Vermont Health Network said in a press release Thursday that it is experiencing a "significant" and "ongoing" system-wide network issue, and is investigating all possible causes, including "a malicious cyberattack."

Experts with Mandiant, a cybersecurity firm, said they identified at least three attacks on Tuesday and one on Wednesday, with patients getting diverted to other hospitals as a result.

"We are experiencing the most significant cyber security threat we've ever seen in the United States," Charles Carmakal, SVP and CTO of Mandiant, said. "An Eastern European financially motivated threat actor, is deliberately targeting and disrupting U.S. hospitals, forcing them to divert patients to other healthcare providers. Patients may experience prolonged wait time to receive critical care."

Allan Liska, an intelligence analyst for the firm Recorded Future, told CNN that his company knows of at least six attacks in the last 24 hours and "there are probably more."

It is "absolutely the biggest thing we've ever seen. In terms of ransomware it's the biggest attack we've ever seen," he said, adding that it's "crushing to see so many hospitals hit at the same time."

Chris Krebs, director of CISA, warned health care and public health individuals to have their "shields up! Assume Ryuk is inside the house. Executives - be ready to activate business continuity and disaster recovery plans. IT sec teams - patch, MFA, check logs, make sure you have a good backup point."

In a statement from the St. Lawrence Health Systems, the virus has been identified as a new variant of Ryuk ransomware, previously unknown to antivirus software providers and security agencies.

It is not known who carried out the attacks, but overall, the incidents represent a solid expansion of hospital targets in a short period of time who have sought to take advantage of the crush facing hospitals in the wake of the global pandemic.

Ransomware can have devastating effects. Most recently, it crippled the IT network of a German hospital resulting in the death of a woman seeking emergency treatment.

According to Microsoft Corporate Vice President for Customer Security and Trust Tom Burt, Ryuk is a sophisticated crypto-ransomware because it identifies and encrypts network files and disables Windows System Restore to prevent people from being able to recover from

the attack without external backups. Ryuk has been attacking organizations, including municipal governments, state courts, hospitals, nursing homes, enterprises and large universities.

According to Burt, Ryuk has been attributed to attacks targeting a contractor for the Department of Defense, the North Carolina city of Durham, an IT provider for 110 nursing homes and a number of hospitals during the Covid-19 pandemic.

CORRECTION: This story has been corrected to remove references to Universal Health Services, which was not targeted in the most recent attack.