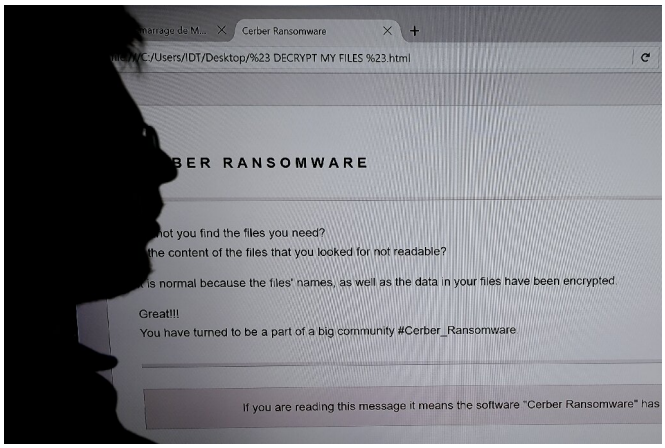
# Ransomware surge imperils hospitals as pandemic intensifies

1 November 2020, by Rob Lever




Hospitals and other health facilities are increasingly being targeted by ransomware even as they try to ramp up for the acceleration in the pandemic

Hackers are stepping up attacks on health care systems with ransomware in the United States and other countries, creating new risks for medical care as the global coronavirus pandemic accelerates.

Alerts from US authorities and security researchers highlight a wave of cyberattacks on hospitals coping with rising virus infections.

An unusual warning this week from the FBI with the Departments of Homeland Security and Health and Human Services, underscored the threat.

The three agencies "have credible information of an increased and imminent cybercrime threat to US hospitals and health care providers," said the alert issued Wednesday, calling on health systems to "take timely and reasonable precautions to protect their networks from these threats."

Media reports have cited several US hospitals hit by ransomware.

One of them, the University of Vermont Medical Center, said in a statement Thursday it was working with law enforcement on "a now confirmed cyberattack that has affected some of our systems" which has had "variable impacts" on patient care.

Daniel dos Santos of the computer security firm Forescout said cash-strapped medical centers are particularly attractive targets for hackers and that at least 400 hospitals had been hit in the past few weeks in the US and Britain.

Hackers are aware that "health care is the most likely to pay the ransom because their services are critical," dos Santos said.

"Stopping services means that people will literally be dying."

For hospitals unable or willing to pay, "it would mean going back to pen and paper, which can cause huge slowdowns," he added.

Forescout said in a report that while many hospitals have upgraded computer systems, most use a variety of connected devices such as patient monitors or CT scanners which "act as the weak links in the network" because they transmit data over insecure channels.

In one sign of the troubles looming, dos Santos and fellow researchers said they discovered data on some three million US patients online, "unprotected and accessible to anyone who knows how to search for it.," the Forescout report said.


Connected devices in hospitals can become weak points for hackers looking to launch ransomware attacks, according to security experts

**Most targeted**

Ransomware is a longstanding security issue and health care has been a frequent target. A September attack disrupted Universal Health Services, which operates hospitals in the US and Britain.

But security experts say the attacks are accelerating as the pandemic worsens.

Researchers at the security firm Check Point said its survey showed health care has been the most targeted industry by ransomware, with a 71 percent jump in attacks on US providers in October from a month earlier.

Check Point said there have been significant rises in ransomware attacks on hospitals in Asia, Europe and the Middle East as well. Globally, the firm said ransomware attacks were up 50 percent in the third quarter compared with the first half of this year.

Many of the attacks use a strain of ransomware known as Ryuk, which security researchers say may be tied to North Korean or Russian cybercriminals.

The US government warning said health organizations are being targeted by phishing attacks to get access to the systems, with hackers using sophisticated tools including TrickBot software which can harvest credentials and exfiltrate data.

The Canadian government's Cyber Centre issued a similar warning in early October, warning of Ryuk ransomware "affecting multiple entities, including municipal governments and public health and safety organizations in Canada and abroad."

"The ransomware problem is steadily worsening and a solution desperately needs to be found," said Brett Callow of the security firm Emsisoft.

"We believe that solution is a prohibition on the payment of demands. Ransomware exists only because it's profitable. If the flow of cash stops, the attacks will stop and hospitals will no longer be at risk."