Building wave of ransomware attacks strike U.S. hospitals

reuters.com/article/usa-healthcare-cyber-idUSKBN27E0EP

Christopher Bing, Joseph Menn

Internet News
Updated

By Christopher Bing, Joseph Menn

4 Min Read

WASHINGTON/SAN FRANCISCO (Reuters) - Eastern European criminals are targeting dozens of U.S. hospitals with ransomware, and federal officials on Wednesday urged healthcare facilities to beef up preparations rapidly in case they are next.

FILE PHOTO: An empty hallway is pictured in a hospital in Philadelphia , Pennsylvania, U.S. May 30, 2017. REUTERS/Carlo Allegri

The FBI is investigating the recent attacks, which include incidents in Oregon, California and New York made public just this week, according to three cybersecurity consultants familiar with the matter.

A doctor at one hospital told Reuters that the facility was functioning on paper after an attack and unable to transfer patients because the nearest alternative was an hour away. The doctor declined to be named because staff were not authorized to speak with reporters.

“We can still watch vitals and getting imaging done, but all results are being communicated via paper only,” the doctor said. Staff could see historic records but not update those files.

Experts said the likely group behind the attacks was known as Wizard Spider or UNC 1878. They warned that such attacks can disrupt hospital operations and lead to loss of life.

The attacks prompted a teleconference call on Wednesday led by FBI and Homeland Security officials for hospital administrators and cybersecurity experts.

A participant told Reuters that government officials warned hospitals to make sure their backup systems were in order, disconnect systems from the internet where possible, and avoid using personal email accounts.

The FBI did not immediately respond to a request for comment.

“This appears to have been a coordinated attack designed to disrupt hospitals specifically all around the country,” said Allan Liska, a threat intelligence analyst with U.S. cybersecurity firm Recorded Future.

“While multiple ransomware attacks against healthcare providers each week have been commonplace, this is the first time we have seen six hospitals targeted in the same day by the same ransomware actor.”

In the past, ransomware infections at hospitals have downed patient record-keeping databases, which critically store up-to-date medical information, affecting hospitals’ ability to provide healthcare.

Ransomware attacks have jumped 50% over the past three months, security firm Check Point said Wednesday, with the proportion of polled healthcare organizations impacted jumping to 4% in the third quarter from 2.3% in the previous quarter.

Two of the three consultants familiar with the attacks said the cyber criminals were commonly using a type of ransomware known as “Ryuk,” which locks up a victim’s computer until a payment is received.

The teleconference call participant said government officials disclosed that the attackers used Ryuk and another trojan, known as Trickbot, against the hospitals.

“UNC1878 is one of the most brazen, heartless, and disruptive threat actors I’ve observed over my career,” said Charles Carmakal, senior vice president for U.S. cyber incident response firm Mandiant.

“Multiple hospitals have already been significantly impacted by Ryuk ransomware and their networks have been taken offline.”

Experts say the deployment of Trickbot is significant after efforts by Microsoft MSFT.O to disrupt the hacking network earlier this month.

That initiative was designed to handicap the cyber criminals, but they seem to have recovered quickly, said Stefan Tanase, a cyber crime analyst.

“What we are seeing here is confirmation that the reports of the Trickbot takedown were greatly exaggerated,” he said.

Microsoft did not answer a request for comment.

Reporting by Christopher Bing and Joseph Menn; Editing by Tom Brown and Stephen Coates

for-phone-onlyfor-tablet-portrait-upfor-tablet-landscape-upfor-desktop-upfor-wide-desktop-up