FBI probing virus behind outage at MedStar Health facilities

March 28 2016, by Jack Gillum, David Dishneau And Tami Abdollah

A woman walks out of the MedStar Georgetown University Hospital in Washington, Monday, March 28, 2016. Hackers crippled computer systems at a major hospital chain, MedStar Health Inc., on Monday, forcing records systems offline for thousands of patients and doctors. The FBI said it was investigating whether the unknown hackers demanded a ransom to restore systems. (AP Photo/Molly Riley)

Hackers crippled computer systems Monday at a major hospital chain, MedStar Health Inc., forcing records systems offline for thousands of patients and doctors. The FBI said it was investigating whether the unknown hackers demanded a ransom to restore systems.

A computer virus paralyzed some operations at Washington-area hospitals and doctors' offices, leaving patients unable to book appointments and staff locked out of their email accounts. Some employees were required to turn off all computers since Monday morning.

A law enforcement official said the FBI was assessing whether the virus was so-called ransomware, in which hackers extort money in exchange for returning a victim's systems to normal. The official spoke on condition of anonymity because the person was not authorized to discuss publicly details about the ongoing criminal investigation.

"We can't do anything at all. There's only one system we use, and now it's just paper," said one MedStar employee who, like others, spoke on condition of anonymity because this person was not authorized to speak to reporters.

MedStar said in a statement that the virus prevented some employees from logging into systems. It said all of its clinics remain open and functioning and there was no immediate evidence that patient information had been stolen.

A sign designates an entrance to the MedStar Georgetown University Hospital in Washington, Monday, March 28, 2016. Hackers crippled computer systems at a major hospital chain, MedStar Health Inc., on Monday, forcing records systems offline for thousands of patients and doctors. The FBI said it was investigating whether the unknown hackers demanded a ransom to restore systems. (AP Photo/Molly Riley)

Company spokeswoman Ann Nickels said she couldn't say whether it was a ransomware attack. She said patient care was not affected and the hospitals were using a paper backup system.

When asked whether hackers demanded payment, Nickels said: "I don't have an answer to that," and referred to the company's statement.

Dr. Richard Alcorta, medical director for Maryland's emergency medical services network, said he suspects it was a ransomware attack. He said his suspicion was based on multiple earlier ransomware attempts on

individual hospitals in the state. Alcorta said he was unaware of any ransoms paid by Maryland hospitals or health care systems.

"People view this, I think, as a form of terrorism and are attempting to extort money by attempting to infect them with this type of virus," he said.

A sign designates an entrance to the MedStar Georgetown University Hospital in Washington, Monday, March 28, 2016. Hackers crippled computer systems at a major hospital chain, MedStar Health Inc., on Monday, forcing records systems offline for thousands of patients and doctors. The FBI said it was investigating whether the unknown hackers demanded a ransom to restore systems. (AP Photo/Molly Riley)

Alcorta said his agency first learned of MedStar's problems about 10:30 a.m., when the company's Good Samaritan Hospital in Baltimore called in a request to divert emergency medical services traffic from that

facility. He said that was followed by a similar request from Union Memorial, another MedStar hospital in Baltimore. The diversions were lifted as the hospitals' backup systems started operating, he said.

MedStar operates 10 hospitals in Maryland and Washington, including the MedStar Georgetown University Hospital, along with other facilities. It employs 30,000 staff and has 6,000 affiliated physicians.

Monday's hacking at MedStar came one month after a Los Angeles hospital paid hackers $17,000 to regain control of its computer system, which hackers had seized with ransomware using an infected email attachment.

Hollywood Presbyterian Medical Center, which is owned by CHA Medical Center of South Korea, paid 40 bitcoins—or about $420 per coin of the digital currency—to restore normal operations and disclosed the attack publicly. That hack was first noticed Feb. 5 and operations didn't fully recover until 10 days later.

Hospitals are considered critical infrastructure, but unless patient data is impacted there is no requirement to disclose such hackings even if operations are disrupted.

Computer security of the hospital industry is generally regarded as poor, and the federal Health and Human Services Department regularly publishes a list of health care providers that have been hacked with patient information stolen. The agency said Monday it was aware of the MedStar incident.

https://phys.org/news/2016-03-fbi-probing-virus-outage-medstar.html