Hackers broke into hospitals despite software flaw warnings

April 5 2016, by Tami Abdollah

In this March 28, 2016 file photo, a sign covers the door to MedStar Georgetown University Hospital in Washington. The hackers who seriously disrupted operations at a large hospital chain for days and held its data hostage broke into a computer server left vulnerable on its corporate network despite urgent public warnings since at least 2007 that it needed to be fixed with a simple update, The Associated Press has learned. (AP Photo/Molly Riley, File)

The hackers who seriously disrupted operations at a large hospital chain

recently and held some data hostage broke into a computer server left vulnerable despite urgent public warnings since at least 2007 that it needed to be fixed with a simple update, The Associated Press has learned.

The hackers exploited design flaws that had persisted on the MedStar Health Inc. network, according to a person familiar with the investigation who spoke on condition of anonymity because this person was not authorized to discuss the findings publicly. The flaws were in a JBoss application server supported by Red Hat Inc. and other organizations, the person said.

The FBI, which is investigating, declined to discuss how the hackers broke in.

The JBoss technology is popular because it allows programmers to write custom-built software tools that can be quickly made available across a company, but security researchers discovered it was routinely misconfigured to allow unauthorized outside users to gain control. The U.S. government, Red Hat and others issued urgent warnings about the security problem and a related flaw in February 2007, March 2010 and again earlier this week. The government warned in 2007 the problem could disrupt operations and allow for unauthorized disclosures of confidential information.

Fixing the problem involved installing an available update or manually deleting two lines of software code.

It was not immediately clear why the hospital chain, which operates 10 hospitals in Maryland and Washington including the MedStar Georgetown University Hospital, was still vulnerable years after those warnings. The new disclosure doesn't diminish the potential culpability of the hackers responsible for the break-in, but it reveals important

details about how the crime unfolded. And it could affect MedStar's civil or administrative exposure under U.S. laws and regulations that require health providers to exercise reasonable diligence to protect their systems.

MedStar's assistant vice president, Ann C. Nickles, said in a statement Tuesday to the AP that the company "maintains constant surveillance of its IT networks in concert with our outside IT partners and cybersecurity experts. We continuously apply patches and other defenses to protect the security and confidentiality of patient and associate information." MedStar said Monday its systems "are almost fully back online," just over a week after the March 28 hacking. The company hired experts from Symantec Corp. to help investigate.

Nickles said Tuesday there was no evidence that patient or employee records were compromised.

MedStar said in a statement Friday evening to the AP that it would not provide details about how the attack occurred, and it criticized further media coverage of the case as perpetuating "the infamy of malicious attacks for airtime and publicity" and encouraging copycat hackers.

The MedStar hackers employed virus-like software known as Samas, or "samsam," that scours the Internet searching for accessible and vulnerable JBoss application servers, especially ones used by hospitals. It's the real-world equivalent of rattling doorknobs in a neighborhood to find unlocked homes. When it finds one, the software breaks in using the old vulnerabilities, then can spread across the company's network by stealing passwords. Along the way, it encrypts scores of digital files and prevents access to them until victims pay the hackers a ransom, usually between $10,000 and $15,000.

If a victim hasn't made safe backups of files, there may be little choice except to pay, although MedStar has said it paid nothing. The hospital

chain shut down its systems quickly after discovering the attack, limiting its impact to archives, some imaging and lab files and other duplicate records, according to the person with inside knowledge of the attack.

"This old issue is still somehow spread across Internet-facing servers," said Stefano Di Paola and Giorgio Fedon of Minded Security, an Italian security firm, in a joint statement to the AP. They discovered a related vulnerability in the servers in 2010 that Red Hat designated its highest priority to fix.

The FBI issued a flash message to companies days after the MedStar hacking, describing the dangers of samsam and asking for help detecting it and improving defenses against it. Days later, the Homeland Security Department issued a separate warning about samsam and another common ransomware strain, Locky, which tricks victims into opening email attachments to infect computers.

Cisco Systems Inc., which has studied the attacks, estimated there were about 2.1 million servers around the world vulnerable to samsam, although some may be additionally protected by other layers of security. It described the ransomware campaign as "proving to be a profitable affair."

"If you haven't patched your server, you're vulnerable, and it can compromise your server at 3 a.m. in the morning when no one's watching," said Craig Williams, a senior technical leader at Talos, Cisco's security research organization. "This is simply a case of people not following best practices and not applying patches for people to correct their systems."

Identifying the hackers and arresting them can be difficult. Tracing the scanning activity preceding an attack typically leads to other hacked computers; logs that might yield identifying clues can be manipulated or

deleted and the samsam software is unusually self-sufficient and doesn't require hackers to control it after an infection. Ransoms are paid using hard-to-trace digital currency.