MedStar says 2007, 2010 software flaws were not part of hack

April 6 2016, by Tami Abdollah

In this March 28, 2016 file photo, a sign covers the door to MedStar Georgetown University Hospital in Washington. MedStar Health Inc. said April 6 that hackers who seriously disrupted its operations and held some data hostage did not exploit software vulnerabilities that were the subjects of warnings in 2007 and 2010 to break into its corporate network. (AP Photo/Molly Riley, File)

MedStar Health Inc. said Wednesday that hackers who seriously disrupted its operations and held some data hostage did not exploit

software vulnerabilities that were the subjects of warnings in 2007 and 2010 to break into its corporate network.

The hospital chain released a new statement after The Associated Press reported Tuesday that hackers broke into a corporate computer server exploiting flaws that had persisted for years on the network. The AP's report was attributed to a person familiar with the investigation who was not authorized to discuss the findings publicly. MedStar said the new information came from Symantec Corp., which it hired to investigate.

The vulnerabilities were in a JBoss application server, supported by Red Hat Inc. and other organizations, which were the subject of public warnings in 2007 and 2010.

MedStar said, "The 2007 and 2010 fixes referenced in the article were not contributing factors in this event."

MedStar assistant vice president Ann Nickels declined to clarify or elaborate. It's unclear whether MedStar was trying to convey that the two vulnerabilities had been already resolved or that hackers had found another method of breaking into the JBoss server.

The MedStar hackers employed virus-like software known as Samas, or "samsam," that scours the Internet searching for accessible JBoss application servers that are vulnerable to those flaws. It's the virtual 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.

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