Los Angeles hospital attack concerns cybersecurity experts

February 19 2016, by Justin Pritchard

Cybersecurity experts worry that the $17,000 a Los Angeles hospital paid hackers to regain control of its computers could signal a troubling escalation of the growing "ransomware" threat.

Though patient care was not "compromised in any way," Hollywood Presbyterian Medical Center paid the bounty "in the best interest of restoring normal operations," President Allen Stefanek said in a written statement.

A typical attack starts when a person opens an emailed link or attachment. Malicious code locks the computer—or, worse, an entire network. Victims pay hackers for a "key" to unlock their machines—and may be desperate to do so if they have not diligently backed up their data and networks.

Many ransomware victims pay quietly, or abandon infected machines. It was unusual that Hollywood Presbyterian, which has more than 400 beds and is owned by CHA Medical Center of South Korea, both revealed the attack publicly and disclosed its cost.

Computer security experts said hospitals are particularly vulnerable because some medical equipment runs on old operating systems that cannot easily be safeguarded. If an employee opens an infected file from a computer that also connects with a patient monitoring station or insulin pump, those devices also could be locked.

Hospitals have not been as diligent in combating cyber threats such as ransomware as other sectors, according to several experts, despite the life-and-death nature of their operations, their tight control over patient information and mandates that they move toward electronic record keeping.

Hospitals are "about 10 to 15 years behind the banking industry" in combatting cyber threats, said Lysa Myers, a researcher with the computer security firm ESET.

The math behind whether to pay a ransom demand can be simple.

Paying thousands of dollars to resolve a serious attack that has penetrated a multimillion dollar business such as a large hospital would be "a no brainer," said James Carder, chief information security officer of LogRhythm, a security intelligence and analytics firm.

Several companies have told Carder that the FBI suggested they pay ransom, he said. Jason Haddix, the director of technical operations at the information security firm Bugcrowd, said companies also have told him the same.

"If you're at a point where you can't do anything," said Haddix, "sometimes the only option is to pay."

An FBI spokeswoman did not immediately respond when asked whether the FBI has in some cases suggested that a company pay. The agency said it is investigating the Hollywood Presbyterian case.

"Ransomware has been around for several years, but there's been a definite uptick lately in its use by cyber criminals," the FBI wrote in a 2015 post on its website. The agency said that it is "targeting these offenders and their scams."

Hollywood Presbyterian paid 40 bitcoins, a digital currency of floating value that on Thursday was worth about $420 each. The problem was first noticed Feb. 5, hospital president Stefanek said, and its system was fully functioning 10 days later.

One reason hackers are attracted to ransomware is that it can be created with relative ease—do-it-yourself ransomware kits are available—and the return on investment can be strong.

To launch a ransomware campaign that lasts one month might cost $5,900, and generate about $90,000 in revenue, according to projections by the cyber security firm Trustwave.

A report from Intel Corp.'s McAfee Labs released in November said the number of ransomware attacks is expected to grow in 2016 because of increased sophistication in the software used to do it. The company estimates that on average, 3 percent of users with infected machines pay a ransom.

While a hacker may get several hundred dollars to unlock many individual computers, getting $17,000 is a decent payday. Based on the public confirmation of that figure, hackers are "going to begin to test the price," said Jack Danahy, chief technology officer at cyber security firm Barkly.

The best defense against a ransomware attack is not to click on unknown links and attachments. Intrusion detection systems and firewalls can help if a person does click—but once the ransomware is entrenched, if the system does not have good system backup practices, the choices boil down to paying or never regaining control.