Iranian hacking spree hit hospitals, other entities in 43 US states

November 29 2018, by Tim Johnson, Mcclatchy Washington Bureau

Credit: CC0 Public Domain

Two Iranian hackers charged Wednesday in a federal indictment were accused of attacking the computer networks of hospitals and other targets in 43 states, a broad criminal extortion campaign that walloped a

heart hospital in Kansas and disrupted one of the nation's largest diagnostic blood testing companies in North Carolina.

Federal prosecutors said the three-year cybercrime spree caused tens of millions of dollars in damage from coast to coast. It marked the first U.S. indictment against foreign hackers engaged in a for-profit ransomware and extortion scheme.

The two hackers developed unique tools to hold U.S. computer networks hostage from Iran, prosecutors said. The two Iranians, Faramarz Shahi Savandi, 34, and Mohammad Mehdi Shah Mansouri, 27, remain at large, presumably in their homeland, officials said.

Assistant Attorney General Brian A. Benczkowski sidestepped a question about whether Iran's government sponsored the two, saying only that the indictment contains no such allegation.

The three-year ransomware campaign hit at least 200 victims in the United States, collecting more than $6 million in extortion payments and causing more than $30 million in losses, Deputy Attorney General Rod J. Rosenstein said.

Ransomware is computer code that encrypts targeted systems and cripples networks until victims pay a ransom, usually in a digital currency like Bitcoin.

The Iranian ransomware, called SamSam, has been in use since early 2016.

In one of the Iranian team's first alleged actions in 2016, it hit the computers of the 54-bed Kansas Heart Hospital in Wichita, which provides specialized cardiovascular care for patients throughout Kansas and northern Oklahoma.

Press reports at the time said Kansas Heart Hospital paid an undisclosed ransom, then faced new demands from the hackers. Hospital spokeswoman Joyce Heismeyer could not be reached immediately.

The hackers breached the networks of at least six health care-related entities, including Hollywood Presbyterian Hospital of Los Angeles and MedStar Health of Columbia, Md.

Other targets of the Iranians' campaign included the networks of the cities of Atlanta (encrypted in March) and Newark, N.J. (April 2017), the Colorado Department of Transportation (Feb. 19, 2018) and the Port of San Diego (Sept. 25, 2018).

Officials said the hackers were intent on creating disruption and inflicting physical harm as much as in collecting ransom, deliberately targeting health care facilities and hospitals.

"Many of the victims were public agencies with missions that involve saving lives and performing other critical functions for the American people," Deputy Attorney General Rod Rosenstein said.

States suffering six or more attacks from SamSam include California, Texas, Florida, Georgia, North Carolina, Missouri and Illinois, according to the Justice Department. Only seven states escaped any attacks at all. The Justice Department did not provide a complete list of all the known victims, or say which victims paid a ransom.

Some security researchers questioned whether the indictment would put any dent in ransomware attacks.

"The impact that these indictments will have is unclear since the individuals are purportedly located in Iran and remain at large," said Kimberly Goody, a cybercrime analyst at FireEye, a major cybersecurity

firm.

One of the most recent attacks occurred July 14 against Laboratory Corporation of America, or LabCorp, a Burlington, N.C., diagnostic company that processes more than 2.5 million tests per week, and holds a patient database of nearly half the U.S. population. Its global footprint reaches 127 countries.

A company spokesman, Donald R. Von Hagen, declined to say how many computers were disabled when hackers penetrated the network on July 14.

"There is no evidence that any LabCorp data was removed from our systems," LabCorp said in an Oct. 26 statement. It said the attack affected access to test results for a limited period but that "operations were returned to normal within a few days."

Many victims of SamSam may have kept the attacks to themselves, paying the hackers and praying that a key would be offered in return to decrypt their networks.

While an increasing number of victims of cybercrime are going to authorities, FBI Executive Assistant Director Amy S. Hess said, " I would surmise that it is not the majority yet."

Sophos, a United Kingdom-based security software company, which has followed SamSam for nearly three years, said this month that a SamSam attack occurs on average once a day. It says ransom demands routinely top $50,000.

What is unique about the SamSam ransomware, experts say, is that it is tailored to allow a cybercriminal to map out and move through a targeted network, unlike other ransomware that spreads haphazardly in

campaigns largely visible to software engineers.

The Iranian hackers set up customized websites on underground networks to offer victims technical support in making their Bitcoin ransom payments.

In separate but coordinated action, the Treasury Department slapped sanctions on two other Iranians that it said facilitated the exchange of Bitcoin ransom payments into Iranian currency. Treasury's Office of Foreign Assets Control, or OFAC, took the unusual move of publishing the digital currency addresses the two Iranians used and said that they conducted at least 7,000 transactions.

Prosecutors alleged that the Iranians used Bitcoin transactions and communicated through TOR, a dark web browser that cybercriminals believe protects anonymity.

But Hess said the FBI was able to crack through the digital barriers.

"Anonymizers might not make you as anonymous as you think you are," she said.

An expert on digital currencies, Yaya J. Fanusie, said the sanctions against the two additional Iranians, Ali Khorashadizadeh and Mohammad Ghorbaniyan, was aimed at the broader cybercriminal world.

"These actions are a signal," said Fanusie, a former CIA analyst, adding that law enforcement officials are adapting to "emerging financial technologies like cryptocurrency."

Fanusie said that while criminals can store Bitcoin in anonymous digital wallets stored at digital currency addresses, the movement of digital

coins leaves "a public trail for anyone to follow and analyze."