Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses

justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public

November 28, 2018

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, November 28, 2018

A federal grand jury returned an indictment unsealed today in Newark, New Jersey charging Faramarz Shahi Savandi, 34, and Mohammad Mehdi Shah Mansouri, 27, both of Iran, in a 34-month-long international computer hacking and extortion scheme involving the deployment of sophisticated ransomware, announced Deputy Attorney General Rod J. Rosenstein, Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney Craig Carpenito for the District of New Jersey and Executive Assistant Director Amy S. Hess of the FBI.

The six-count indictment alleges that Savandi and Mansouri, acting from inside Iran, authored malware, known as "SamSam Ransomware," capable of forcibly encrypting data on the computers of victims. According to the indictment, beginning in December 2015, Savandi and Mansouri would then allegedly access the computers of victim entities without authorization through security vulnerabilities, and install and execute the SamSam Ransomware on the computers, resulting in the encryption of data on the victims' computers. These more than 200 victims included hospitals, municipalities, and public institutions, according to the indictment, including the City of Atlanta, Georgia; the City of Newark, New Jersey; the Port of San Diego, California; the Colorado Department of

Transportation; the University of Calgary in Calgary, Alberta, Canada; and six health care-related entities: Hollywood Presbyterian Medical Center in Los Angeles, California; Kansas Heart Hospital in Wichita, Kansas; Laboratory Corporation of America Holdings, more commonly known as LabCorp, headquartered in Burlington, North Carolina; MedStar Health, headquartered in Columbia, Maryland; Nebraska Orthopedic Hospital now known as OrthoNebraska Hospital, in Omaha, Nebraska and Allscripts Healthcare Solutions Inc., headquartered in Chicago, Illinois.

According to the indictment, Savandi and Mansouri would then extort victim entities by demanding a ransom paid in the virtual currency Bitcoin in exchange for decryption keys for the encrypted data, collecting ransom payments from victim entities that paid the ransom, and exchanging the Bitcoin proceeds into Iranian rial using Iran-based Bitcoin exchangers. The indictment alleges that, as a result of their conduct, Savandi and Mansouri have collected over $6 million USD in ransom payments to date, and caused over $30 million USD in losses to victims.

“The Iranian defendants allegedly used hacking and malware to cause more than $30 million in losses to more than 200 victims,” said Deputy Attorney General Rosenstein. “According to the indictment, the hackers infiltrated computer systems in 10 states and Canada and then demanded payment. The criminal activity harmed state agencies, city governments, hospitals, and countless innocent victims.”

“The allegations in the indictment unsealed today—the first of its kind—outline an Iran-based international computer hacking and extortion scheme that engaged in 21st-century digital blackmail,” said Assistant Attorney General Benczkowski. “These defendants allegedly used ransomware to infect the computer networks of municipalities, hospitals, and other key public institutions, locking out the computer owners, and then demanded millions of dollars in payments from them. As today’s charges demonstrate, the Criminal Division and its law enforcement partners will relentlessly pursue cybercriminals who harm American citizens, businesses, and institutions, regardless of where those criminals may reside.”

“The defendants in this case developed and deployed the SamSam Ransomware in order to hold public and private entities hostage and then extort money from them,” said U.S. Attorney Carpenito. “As the indictment in this case details, they started with a business in Mercer County and then moved on to major public entities, like the City of Newark, and healthcare providers, like the Hollywood Presbyterian Medical Center in Los Angeles and the Kansas Heart Hospital in Wichita—cravenly taking advantage of the fact that these victims depend on their computer networks to serve the public, the sick, and the injured without interruption. The charges announced today show that the U.S. Attorney’s Office for the District of New Jersey will continue to act to disrupt such criminal acts, and identify those who are responsible for them, no matter where in the world they may seek to hide.”

“This indictment demonstrates the FBI’s continuous commitment to unmasking malicious actors behind the world’s most egregious cyberattacks,” said Executive Assistant Director Hess. “By calling out those who threaten American systems, we expose criminals who hide behind their computer and launch attacks that threaten our public safety and national security. The actions highlighted today, which represent a continuing trend of cyber criminal activity emanating from Iran, were particularly threatening, as they targeted public safety institutions, including U.S. hospital systems and governmental entities. The FBI, with the assistance of our private sector and U.S. government partners, are sending a strong message that we will work together to investigate and hold all criminals accountable.”

Savandi and Mansouri are charged with one count of conspiracy to commit wire fraud, one count of conspiracy to commit fraud and related activity in connection with computers, two substantive counts of intentional damage to a protected computer and two substantive counts of transmitting a demand in relation to damaging a protected computer.

According to the indictment, Savandi and Mansouri created the first version of the SamSam Ransomware in December 2015, and created further refined versions in June and October 2017. In addition to employing Iran-based Bitcoin exchangers, the indictment alleges that the defendants also utilized overseas computer infrastructure to commit their attacks. Savandi and Mansouri would also use sophisticated online reconnaissance techniques (such as scanning for computer network vulnerabilities) and conduct online research in order to select and target potential victims, according to the indictment. According to the indictment, the defendants would also disguise their attacks to appear like legitimate network activity.

To carry out their scheme, the indictment alleges that the defendants also employed the use of Tor, a computer network designed to facilitate anonymous communication over the internet. According to the indictment, the defendants maximized the damage caused to victims by launching attacks outside regular business hours, when a victim would find it more difficult to mitigate the attack, and by encrypting backups of the victims’ computers. This was intended to—and often did—cripple the regular business operations of the victims, according to the indictment. The most recent ransomware attack against a victim alleged in the indictment took place on Sept. 25, 2018.

This case was investigated by the FBI’s Newark Field Office. Senior Counsel William A. Hall Jr. of the Criminal Division’s Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorney and Chief of the Cybercrimes Unit Justin S. Herring of the District of New Jersey are prosecuting the case. The Department thanks its law enforcement colleagues at the National Crime Agency (UK), West Yorkshire Police (UK), Calgary Police Service (Canada), and the Royal Canadian Mounted Police. Significant assistance was provided by the Justice Department’s National Security Division and the Criminal Division’s Office of International Affairs.

Victims are encouraged to contact their local FBI field office and file a complaint online with the Internet Crime Complaint Center (IC3). The IC3 staff reviews complaints, looking for patterns or other indicators of significant criminal activity, and refers investigative packages of complaints to the appropriate law enforcement authorities in a particular city or region. The FBI provides a variety of resources relating to ransomware through the IC3, which can be reached at www.ic3.gov. For more information on ransomware prevention, visit: https://www.ic3.gov/media/2016/160915.aspx

Charges contained in an indictment are merely allegations, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.