CPA
Practice Advisor

TECHNOLOGY

Iranian Nationals Charged with Massive Hacking Scheme Targeting Accounting Firms, Other Companies

Investigators said some of the victims paid ransoms, while others contacted the FBI or local authorities.

Sep. 13, 2022

By Anthony G. Attrino, nj.com (TNS)

Three residents of Iran face federal charges for hacking computers in the United States, including in New Jersey and Pennsylvania where victims included a domestic violence shelter, a township in Union County, and an accounting firm in Morris County.

The suspects—who have remained in Iran—are charged with conspiracy to commit fraud, intentional damage to computers, and transmitting demands, according to an indictment unsealed on Wednesday.

The suspects were identified as Mansour Ahmadi, 34; Ahmad Khatibi Aghda, 45; and Amir Hossein Nickaein Ravari, 30. All are residents of Iran, prosecutors said.

"These defendants have been hacking and extorting victims—including critical infrastructure providers—for their personal gain, but the charges reflect how criminals can flourish in the safe haven that that the government of Iran has created and is responsible for," Assistant U.S. Attorney Matthew Olsen said in a statement.

According to court documents, the New Jersey victims included an unnamed municipality in Union County and an accounting firm in Morris County.

By launching an encryption attack of the Pennsylvania domestic violence shelter's computers, the hackers activated a program called "BitLocker," which denied shelter employees' access to data and some of its systems, court documents allege.

Another accounting firm in Illinois was hacked, as was a regional electric company in Mississippi, a housing authority in Washington state, a county government in Wyoming and others, including a Washington state construction company working on "critical infrastructure projects."

The hackers also obtained access to computers in use at a bar association in an unnamed state, according to court documents.

"(The suspects) were targeting known vulnerabilities in systems (with) ransomware," a spokesman for the U.S. Department of Justice said in a press briefing on Wednesday.

From October 2020 through August, the suspects conspired to transmit a damaging software program, encrypting users' software and causing thousands of dollars in damages.

“The goal of the conspiracy was for the defendants, acting from inside Iran, to obtain and maintain unauthorized access to victims’ computers,” the indictment states.

In Morris County, hackers in February and March launched an encryption attack, causing an accounting firm’s network to connect with their server.

“Are you ready to pay?” Aghda allegedly wrote in a March 8 email to a company representative, the indictment states. The next day, Aghda wrote again, stating that he had “locked more than 20 systems” and demanding $50,000, the indictment states.

“If you don’t want to pay, I can sell your data on the black market,” Aghda allegedly wrote the Morris County firm on March 16. “This choice is yours.”

In Union County, the hackers infiltrated a township government’s website in February, “gaining control and access to the township’s network and data,” the indictment states. It’s not clear from court records whether the hackers demanded money from township officials or if New Jersey residents’ private information was obtained by the hackers.

Investigators said some of the victims paid ransoms, while others contacted the FBI or local authorities.

The indictment states prosecutors obtained documented evidence of the conspiracy when Ahmadi sent an email to an unnamed person that included timesheets of hours worked by Ravari, Aghda and others.

The U.S. Department of Justice said Wednesday the suspects are believed to still be in Iran and have not been arrested. However, federal agents said they plan to arrest the men if they leave their country, and said the indictment was the result of a global effort to track down cyber criminals.

“I want the people of New Jersey, and across the country, to know that the FBI is working tirelessly every day to protect you from people and things you may never see,” Newark FBI Special Agent James Dennehy said in a statement.

—

Technology • News

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.