An official website of the United States government
Here's how you know

THE UNITED STATES DEPARTMENT of JUSTICE
STICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, September 16, 2020

Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and the Middle East

Two Iranian nationals have been charged in connection with a coordinated cyber intrusion campaign – sometimes at the behest of the government of the Islamic Republic of Iran (Iran) – targeting computers in New Jersey, elsewhere in the United States, Europe and the Middle East, the Department of Justice announced today.

According to a 10-count indictment returned on Sept. 15, 2020, Hooman Heidarian, a/k/a "neo," 30, and Mehdi Farhadi, a/k/a "Mehdi Mahdavi" and "Mohammad Mehdi Farhadi Ramin," 34, both of Hamedan, Iran, stole hundreds of terabytes of data, which typically included confidential communications pertaining to national security, foreign policy intelligence, non-military nuclear information, aerospace data, human rights activist information, victim financial information and personally identifiable information, and intellectual property, including unpublished scientific research. In some instances, the defendants' hacks were politically motivated or at the behest of Iran, including instances where they obtained information regarding dissidents, human rights activists, and opposition leaders. In other instances, the defendants sold the hacked data and information on the black market for private financial gain.

"We will not bring the rule of law to cyberspace until governments refuse to provide safe harbor for criminal hacking within their borders," said Assistant Attorney General for National Security John C. Demers. "Unfortunately, our cases demonstrate that at least four nations — Iran, China, Russia and North Korea — will allow criminal hackers to victimize individuals and companies from around the world, as long as these hackers will also work for that country's government — gathering information on human rights activists, dissidents and others of intelligence interest. Today's defendants will now learn that such service to the Iranian regime is not an asset, but a criminal yoke that they will now carry until the day they are brought to justice."

"These Iranian nationals allegedly conducted a wide-ranging campaign on computers here in New Jersey and around the world," said U.S. Attorney Carpenito for the District of New Jersey. "They brazenly infiltrated computer systems and targeted intellectual property and often sought to intimidate perceived enemies of Iran, including dissidents fighting for human rights in Iran and around the world. This conduct threatens our national security, and as a result, these defendants are wanted by the FBI and are considered fugitives from justice."

"The indictment of two Iranian nationals charged with computer hacking, fraud, and aggravated identity theft demonstrates how the FBI continues to work relentlessly with our law enforcement partners to identify cybercriminals who seek to do harm to American citizens, businesses, and universities, regardless of where those criminals may reside and hold them accountable," said George M. Crouch Jr., Special Agent in Charge of the FBI Newark Division. "Mehdi Farhadi and Hooman Heidarian are now fugitives and have been added to the FBI website for charges in connection with a massive, coordinated cyber intrusion campaign. These actions demonstrate how imposing risks and consequences on our cyber adversaries will continue to be a top priority for the FBI."

According to the indictment:

Beginning in at least 2013, the defendants were responsible for a coordinated campaign of cyber intrusions into computer systems in New Jersey and around the world. The victims included several American and foreign universities, a Washington, D.C.-based think tank, a defense contractor, an aerospace company, a foreign policy organization, non-governmental organizations (NGOs), non-profits, and foreign government and other entities the defendants identified as rivals or adversaries to Iran. In addition to the theft of highly protected and sensitive data, the defendants also vandalized websites, often under the pseudonym "Sejeal" and posted messages that appeared to signal the demise of Iran's internal opposition, foreign adversaries, and countries identified as rivals to Iran, including Israel and Saudi Arabia.

To select their victims, the defendants conducted online reconnaissance, including gathering public data and intelligence to determine a victim's areas of expertise, and using vulnerability scanning tools and other means to assess computer networks. The defendants gained and maintained unauthorized access to victim networks using various tools, including: session hijacking, where a valid computer session was exploited to gain unauthorized access to information or services in a computer system; SQL injection, in which they used malicious code to access information that was not intended to be displayed, such as sensitive government data, user details, and personal identifiers; and malicious programs installations, which allowed the defendants to maintain unauthorized access to computers.

The defendants then used key-loggers and "remote access Trojans" to maintain access and monitor the actions of users of the victim networks. They also developed a botnet tool, which facilitated the spread of malware, denial of service attacks, and spamming to victim networks. In some instances, the defendants used their unauthorized access to victim networks or accounts to establish automated forwarding rules for compromised victim accounts, whereby new outgoing and incoming emails were automatically forwarded from the compromised accounts to accounts controlled by defendants.

Assistant Attorney General Demers and U.S. Attorney Carpenito credited special agents of the FBI, under the direction of Special Agent in Charge Crouch in Newark, with the investigation leading to the charges.

Each defendant is charged with: one count of conspiracy to commit fraud and related activity in connection with computers and access devices; unauthorized access to protected computers; unauthorized damage to protected computers; conspiracy to commit wire fraud; and access device fraud; and five counts of aggravated identity theft.

The counts of conspiracy to commit computer fraud and related activity in connection with computers and access devices, and unauthorized access to protected computers, each carry a maximum sentence of five years in prison. The counts of unauthorized damage to protected computers and access device fraud each carry a maximum sentence of ten years in prison. The count of conspiracy to commit wire fraud carries a maximum sentence of 20 years in prison. The counts of aggravated identity theft each carry a mandatory sentence of two years in prison.

The government is represented by Assistant U.S. Attorney Dean C. Sovolos of the U.S. Attorney's Office National Security Unit, Daniel V. Shapiro, Deputy Chief of the U.S. Attorney's Office Criminal Division, and Trial Attorney Scott McCulloch of the National Security Division's Counterintelligence and Export Control Section.

The charges and allegations contained in the indictment are merely accusations and the defendants are considered innocent unless and until proven guilty.

Topic(s):
Counterintelligence and Export Control
National Security

Component(s):
National Security Division (NSD)
USAO - New Jersey

Press Release Number:
20-945

Updated September 16, 2020