Department of Justice

U.S. Attorney's Office

Eastern District of Virginia

SHARE

FOR IMMEDIATE RELEASE Thursday, September 17, 2020

Iranian Hackers Indicted for Stealing Data from Aerospace and Satellite Tracking Companies

ALEXANDRIA, Va. – An indictment was unsealed today charging three computer hackers, all of whom were residents and nationals of the Islamic Republic of Iran (Iran), with engaging in a coordinated campaign of identity theft and hacking on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC), a designated foreign terrorist organization, in order to steal critical information related to United States aerospace and satellite technology and resources.

"We will relentlessly pursue and expose those who seek to harm American companies and individuals wherever they reside in the world," said G. Zachary Terwilliger, U.S. Attorney for the Eastern District of Virginia. "The use of malware, the theft of commercial data and intellectual property, and the use of social engineering to steal the identities of United States citizens to accomplish unlawful acts will not be tolerated. Along with our incredible and steadfast law enforcement partners, the Eastern District of Virginia continues to lead efforts to combat serious cybercrime globally and the charges outlined in the indictment exposing IRGC linked hacking operations in the United States are just another example of the fruits of our seamless teamwork."

Charged in the indictment are defendants Said Pourkarim Arabi, 34, Mohammad Reza Espargham, 25, and Mohammad Bayati, 34, all Iranian nationals residing in Iran.

"For the third time in three days, the Department has charged Iranian hackers," said John C. Demers, Assistant Attorney General for National Security. "This case highlights the Islamic Revolutionary Guard

Corps' efforts to infiltrate the networks of American companies in search of valuable commercial information and intellectual property. It is yet another effort by a rogue foreign nation to steal the fruits of this country's hard work and expertise."

According to allegations in the indictment, the defendants' hacking campaign, which targeted numerous companies and organizations in the United States and abroad, began in approximately July 2015 and continued until at least February 2019. The defendants at one time possessed a target list of over 1,800 online accounts, including accounts belonging to organizations and companies involved in aerospace or satellite technology and international government organizations in Australia, Israel, Singapore, the United States, and the United Kingdom.

"Today's charges are yet another example of the FBI's dedication to investigating those who target and attempt to steal data and proprietary information from the United States," said James A. Dawson, Assistant Director in Charge of the FBI's Washington Field Office. "Today's charges allege that these individuals conspired in a coordinated campaign with known IRGC members and acted at their direction. The defendants targeted thousands of individuals in an attempt to steal critical information related to United States aerospace and satellite technology. The FBI remains dedicated to protecting the United States, and we continue to impose risk and consequences on cyber adversaries through our unique authorities, world-class capabilities, and enduring partnerships."

To facilitate their victimization of these targets, the defendants engaged in a coordinated campaign of social engineering to identify real United States citizens working in the satellite and aerospace fields whose identities the defendants could assume online. The defendants then impersonated those individuals and used their stolen identities to register email addresses and fraudulently purchase domains and hacking tools for use in the scheme. The defendants then created customized spear phishing emails that purported to be from the individuals whose identities the defendants had stolen, in an attempt to entice the recipients to click on malicious links embedded in the emails. Once a recipient clicked on a malicious link, malware would be downloaded to the individual's computer, giving the defendants unauthorized access to the recipient's computer and network. The defendants then used additional hacking tools to maintain unauthorized access, escalate their privileges, and steal data sought by the IRGC. Using these methods, the defendants successfully compromised multiple victim networks, resulting in the theft of sensitive commercial information, intellectual property, and personal data from victim companies, including a satellite-tracking company and a satellite voice and data communication company.

Arabi is charged with conspiracy to commit computer intrusions, obtaining information by unauthorized access to protected computers, intentional damage to protected computers, aggravated identity theft, and conspiracy to commit wire fraud. If convicted, Arabi faces a maximum penalty of 20 years in prison.

Espharghamis charged with conspiracy to commit computer intrusions, obtaining information by unauthorized access to protected computers, intentional damage to protected computers, and conspiracy to commit wire fraud. If convicted, Espharghamfaces a maximum penalty of 20 years in prison.

Bayati is charged with conspiracy to commit computer intrusions, and conspiracy to commit wire fraud. If convicted, Bayati faces a maximum penalty of 20 years in prison.

U.S. V. JAVAID PERWAIZ

U.S. V. ALEKSEI BURKOV

Actual sentences for federal crimes are typically less than the maximum penalties. A federal district court judge will determine any sentence after taking into account the U.S. Sentencing Guidelines and other statutory factors.

Assistant U.S. Attorneys Nathaniel Smith III, Jay V. Prabhu, and Danya Atiyeh are prosecuting the case with assistance from Trial Attorney Evan Turgeon of the Justice Department's National Security Division.

A copy of this press release is located on the website of the U.S. Attorney's Office for the Eastern District of Virginia. Related court documents and information are located on the website of the District Court for the Eastern District of Virginia or on PACER by searching for Case No. 1:20-cr-217.

Attachment(s):
Download us_v_arabi_et_al_0.pdf

Topic(s):
National Security

Component(s):
USAO - Virginia, Eastern

Contact:
Joshua Stueve
Director of Public Affairs
joshua.stueve@usdoj.gov

Updated September 17, 2020