Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps

justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

March 23, 2018

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Friday, March 23, 2018

Mabna Institute Hackers Penetrated Systems Belonging to Hundreds of Universities, Companies, and Other Victims to Steal Research, Academic and Proprietary Data, and Intellectual Property

An Indictment charging Gholamreza Rafatnejad, 38; Ehsan Mohammadi, 37; Abdollah Karima, aka Vahid Karima, 39; Mostafa Sadeghi, 28; Seyed Ali Mirkarimi, 34; Mohammed Reza Sabahi, 26; Roozbeh Sabahi, 24; Abuzar Gohari Moqadam, 37; and Sajjad Tahmasebi, 30, all citizens and residents of Iran, was unsealed today. The defendants were each leaders, contractors, associates, hackers-for-hire or affiliates of the Mabna Institute, an Iran-based company that, since at least 2013, conducted a coordinated campaign of cyber intrusions into computer systems belonging to 144 U.S. universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund. Through the defendants' activities, the Mabna Institute stole more than 31 terabytes of academic data and intellectual property from universities, and email accounts of employees at private sector

companies, government agencies, and non-governmental organizations. The defendants conducted many of these intrusions on behalf of the Islamic Republic of Iran's (Iran) Islamic Revolutionary Guard Corps (IRGC), one of several entities within the government of Iran responsible for gathering intelligence, as well as other Iranian government and university clients. In addition to these criminal charges, today the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated the Mabna Institute and the nine defendants for sanctions for the malicious cyber-enabled activity outlined in the Indictment.

The charges were announced by Deputy Attorney General Rod J. Rosenstein; Assistant Attorney General for National Security John C. Demers; U.S. Attorney Geoffrey S. Berman for the Southern District of New York; FBI Director Christopher A. Wray; Assistant Director in Charge William F. Sweeney Jr. of the FBI's New York Field Division; and Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker.

"These nine Iranian nationals allegedly stole more than 31 terabytes of documents and data from more than 140 American universities, 30 American companies, five American government agencies, and also more than 176 universities in 21 foreign countries," said Deputy Attorney General Rosenstein. "For many of these intrusions, the defendants acted at the behest of the Iranian government and, specifically, the Iranian Revolutionary Guard Corps. The Department of Justice will aggressively investigate and prosecute hostile actors who attempt to profit from America's ideas by infiltrating our computer systems and stealing intellectual property. This case is important because it will disrupt the defendants' hacking operations and deter similar crimes."

"Today, in one of the largest state-sponsored hacking campaigns ever prosecuted by the Department of Justice, we have unmasked criminals who normally hide behind the ones and zeros of computer code," said U.S. Attorney Berman. "As alleged, this massive and brazen cyber-assault on the computer systems of hundreds of universities in 22 countries and dozens of private sector companies and governmental organizations was conducted on behalf of Iran's Islamic Revolutionary Guard. The hackers targeted innovations and intellectual property from our country's greatest minds. These defendants are now fugitives from American justice, no longer free to travel outside Iran without risk of arrest. The only way they will see the outside world is through their computer screens, but stripped of their greatest asset – anonymity."

"This investigation involved a complex threat in a dynamic landscape, but today's announcement highlights the commitment of the FBI and our partners to vigorously pursue those that threaten U.S. property and security," said Director Wray. "Today, not only are we publicly identifying the foreign hackers who committed these malicious cyber intrusions, but we are also sending a powerful message to their backers, the Government of the Islamic Republic of Iran: your acts do not go unnoticed. We will protect our innovation, ideas and information, and we will use every tool in our toolbox to expose those who commit these cyber crimes. Our memory is long; we will hold them accountable under the law, no matter where they attempt to hide."

According to the allegations contained in the Indictment unsealed today in Manhattan federal court:

Background on the Mabna Institute

Gholamreza Rafatnejad and Ehsan Mohammadi, the defendants, founded the Mabna Institute in approximately 2013 to assist Iranian universities and scientific and research organizations in stealing access to non-Iranian scientific resources. In furtherance of its mission, the Mabna Institute employed, contracted, and affiliated itself with hackers-for-hire and other contract personnel to conduct cyber intrusions to steal academic data, intellectual property, email inboxes and other proprietary data, including Abdollah Karima, aka Vahid Karima, Mostafa Sadeghi, Seyed Ali Mirkarimi, Mohammed Reza Sabahi, Roozbeh Sabahi, Abuzar Gohari Moqadam, and Sajjad Tahmasebi. The Mabna Institute contracted with both Iranian governmental and private entities to conduct hacking activities on their behalf, and specifically conducted the university spearphishing campaign on behalf of the IRGC. The Mabna Institute is located at Tehran, Sheikh Bahaii Shomali, Koucheh Dawazdeh Metri Sevom, Plak 14, Vahed 2, Code Posti 1995873351.

University Hacking Campaign

The Mabna Institute, through the activities of the defendants, targeted more than 100,000 accounts of professors around the world. They successfully compromised approximately 8,000 professor email accounts across 144 U.S.-based universities, and 176 universities located in foreign countries, including Australia, Canada, China, Denmark, Finland, Germany, Ireland, Israel, Italy, Japan, Malaysia, Netherlands, Norway, Poland, Singapore, South Korea, Spain, Sweden, Switzerland, Turkey and the United Kingdom. The campaign started in approximately 2013, continued through at least December 2017, and broadly targeted all types of academic data and intellectual property from the systems of compromised universities. Through the course of the conspiracy, U.S.-based universities spent more than approximately $3.4 billion to procure and access such data and intellectual property.

The members of the conspiracy used stolen account credentials to obtain unauthorized access to victim professor accounts, which they used to steal research, and other academic data and documents, including, among other things, academic journals, theses, dissertations, and electronic books. The defendants targeted data across all fields of research and academic disciplines, including science and technology, engineering, social sciences, medical, and other professional fields. The defendants stole at least approximately 31.5 terabytes of academic data and intellectual property, which they exfiltrated to servers outside the United States that were under the control of members of the conspiracy.

In addition to stealing academic data and login credentials for the benefit of the Government of Iran, the defendants also sold the stolen data through two websites, Megapaper.ir (Megapaper) and Gigapaper.ir (Gigapaper). Megapaper was operated by Falinoos Company, a company controlled by Abdollah Karima, aka Vahid Karima, the defendant, and

Gigapaper was affiliated with Karima. Megapaper sold stolen academic resources to customers within Iran, including Iran-based public universities and institutions, and Gigapaper sold a service to customers within Iran whereby purchasing customers could use compromised university professor accounts to directly access the online library systems of particular U.S.-based and foreign universities.

Accompanying Mitigation Efforts

Prior to the unsealing of the Indictment, the FBI provided foreign law enforcement partners with detailed information regarding victims within their jurisdictions, so that victims in foreign countries could be notified and foreign partners could assist in remediation efforts.

Also, in connection with the unsealing of the Indictment, today the FBI provided private sector partners detailed information regarding the vulnerabilities targeted and the intrusion vectors used by the Mabna Institute in their campaign against private sector companies. This information will assist the public in its network defense and mitigation efforts.

* * *

Rafatnejad, Mohammadi, Karima, Sadeghi, Mirkarimi, Sabahi, Sabahi, Moqadam and Tahmasebi was each is charged with one count of conspiracy to commit computer intrusions, which carries a maximum sentence of five years in prison; one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison; two counts of unauthorized access of a computer, each of which carries a maximum sentence of five years in prison; two counts of wire fraud, each of which carries a maximum sentence of 20 years in prison; and one count of aggravated identity theft, which carries a mandatory sentence of two years in prison. The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencings of the defendants will be determined by the assigned judge.

Mr. Rosenstein and Mr. Berman praised the outstanding investigative work of the FBI, the assistance of the United Kingdom's National Crime Agency (NCA), and the support of the OFAC. Assistant U.S. Attorneys Timothy T. Howard, Jonathan Cohen and Richard Cooper are in charge of the prosecution, with assistance provided by Trial Attorneys Heather Alpino and Jason McCullough of the National Security Division's Counterintelligence and Export Control Section.

The charges contained in the Indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty.

For the U.S. Department of Treasury's press release announcing corresponding sanctions click here.