Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps

Published: 2018-03-23 · Archived: 2026-04-06 15:26:14 UTC

Rod J. Rosenstein, the Deputy Attorney General of the United States, Geoffrey S. Berman, the United States Attorney for the Southern District of New York, William F. Sweeney Jr., the Assistant Director-in-Charge of the New York Field Division of the Federal Bureau of Investigation ("FBI"), and John C. Demers, Assistant Attorney General for National Security, announced today the unsealing of an indictment charging GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, and SAJJAD TAHMASEBI. The defendants were each leaders, contractors, associates, hackers-for-hire, and affiliates of the Mabna Institute, an Iran-based company that was responsible for a coordinated campaign of cyber intrusions that began in at least 2013 into computer systems belonging to 144 U.S.-based universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the United States 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 activities of the defendants, the Mabna Institute conducted these intrusions to steal over 30 terabytes of academic data and intellectual property from universities, and email inboxes from employees of victim private sector companies, government victims, 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 clients. In addition to these criminal charges, today the Department of 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.

Deputy Attorney General Rod J. Rosenstein said: "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. 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."

Manhattan U.S. Attorney Geoffrey S. Berman said: "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. As alleged, this massive and brazen cyber-assault on the computer systems of hundreds of universities in 22 countries, including the United States, 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."

FBI Assistant Director William F. Sweeney Jr. said: "The numbers alone in this case are staggering, over 300 universities and 47 private sector companies both here in the United States and abroad were targeted to gain unauthorized access to online accounts and steal data. An estimated 30 terabytes was removed from universities' accounts since this attack began, which is roughly equivalent of 8 billion double-sided pages of text. It is hard to quantify the value on the research and information that was taken from victims but it is estimated to be in the billions of dollars. The nine Iranians indicted today now find themselves wanted by the FBI and our partner law enforcement agencies around the globe – and like other cyber criminals they will soon learn their ability to freely move was just limited to the virtual world only."

According to the allegations contained in the Indictment[1] 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, a/k/a "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 over 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, and has continued through at least December 2017, and broadly targeted all types of academic data and intellectual property from the systems of compromised universities, including, among other things, academic journals, theses, dissertations, and electronic books. Through the course of the conspiracy, U.S.-based universities spent over approximately $3.4 billion to procure and access such data and intellectual property.

The hacking campaign against universities was conducted across multiple stages. First, the defendants conducted online reconnaissance of university professors, including to determine these professors' research interests and the academic articles they had published. Second, using the information collected during the reconnaissance phase, the defendants created and sent spearphishing emails to targeted professors, which were personalized and created so as to appear to be sent from a professor at another university. In general, those spearphishing emails indicated

that the purported sender had read an article the victim professor had recently published, and expressed an interest in several other articles, with links to those additional articles included in the spearphishing email. If the targeted professor clicked on certain links in the email, the professor would be directed to a malicious Internet domain named to appear confusingly similar to the authentic domain of the recipient professor's university. The malicious domain contained a webpage designed to appear to be the login webpage for the victim professor's university. It was the defendants' intent that the victim professor would be led to believe that he or she had inadvertently been logged out of his or her university's computer system, prompting the victim professor for his or her login credentials. If a professor then entered his or her login credentials, those credentials were then logged and captured by the hackers.

Finally, the members of the conspiracy used stolen account credentials to obtain unauthorized access to victim professor accounts, through which they then exfiltrated intellectual property, research, and other academic data and documents from the systems of compromised universities, 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. At least approximately 31.5 terabytes of academic data and intellectual property from compromised universities were stolen and exfiltrated to servers under the control of members of the conspiracy located in countries outside the United States.

In addition to stealing academic data and login credentials for university professors 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 ("Falinoos"), a company controlled by ABDOLLAH KARIMA, a/k/a "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 United States-based and foreign universities.

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 so that foreign partners could assist in remediation efforts.

Private Sector Hacking Victims

In addition to targeting and compromising universities, the Mabna Institute defendants targeted and compromised employee email accounts for at least approximately 36 United States-based private companies, and at least approximately 11 private companies based in Germany, Italy, Switzerland, Sweden, and the United Kingdom, and exfiltrated entire email mailboxes from compromised employees' accounts. Among the United States-based private sector victims were three academic publishers, two media and entertainment companies, one law firm, 11 technology companies, five consulting firms, four marketing firms, two banking and/or investment firms, two online car sales companies, one healthcare company, one employee benefits company, one industrial machinery company, one biotechnology company, one food and beverage company, and one stock images company.

In order to compromise accounts of private sector victims, members of the conspiracy used a technique known as "password spraying," whereby they first collected lists of names and email accounts associated with the intended victim company through open source Internet searches. Then, they attempted to gain access to those accounts with commonly-used passwords, such as frequently used default passwords, in order to attempt to obtain unauthorized access to as many accounts as possible. Once they obtained access to the victim accounts, members of the conspiracy, among other things, exfiltrated entire email mailboxes from the victims. In addition, in many cases, the defendants established automated forwarding rules for compromised accounts that would prospectively forward new outgoing and incoming email messages from the compromised accounts to email accounts controlled by the conspiracy.

U.S. Government and NGO Hacking Victims

In the same time period as the university and private sector hacking campaigns described above, the Mabna Institute also conducted a computer hacking campaign against various governmental and non-governmental organizations within the United States. During the course of that campaign, employee login credentials were stolen by members of the conspiracy through password spraying. Among the victims were the following, all based in the United States: the United States Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the State of Indiana Department of Education, the United Nations, and the United Nations Children's Fund. As with private sector victims, the defendants targeted for theft email inboxes of employees of these organizations.

* * *

GHOLAMREZA RAFATNEJAD, EHSAN MOHAMMADI, ABDOLLAH KARIMA, a/k/a "Vahid Karima," MOSTAFA SADEGHI, SEYED ALI MIRKARIMI, MOHAMMED REZA SABAHI, ROOZBEH SABAHI, ABUZAR GOHARI MOQADAM, and SAJJAD TAHMASEBI, the defendants, are citizens and residents of Iran. 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. 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. The case is being handled by the Office's Complex Frauds and Cybercrime Unit. Assistant United States Attorneys Timothy T. Howard, Jonathan Cohen, and Richard Cooper are in charge of the prosecution, with assistance provided by 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.

[1] As the introductory phrase signifies, the entirety of the text of the Indictment, and the description of the Indictment set forth herein, constitute only allegations, and every fact described should be treated as an allegation.
