

Treasury Sanctions Iranian Cyber Actors for Malicious Cyber-Enabled Activities Targeting Hundreds of Universities

March 23, 2018

Washington – Today, in a coordinated action with the U.S. Department of Justice, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) designated one Iranian entity and 10 Iranian individuals under Executive Order (E.O.) 13694, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” as amended. The entity and individuals designated today engaged in the theft of valuable intellectual property and data from hundreds of U.S. and third-country universities and a media company for private financial gain.

“Iran is engaged in an ongoing campaign of malicious cyber activity against the United States and our allies. The IRGC outsourced cyber intrusions to The Mabna Institute, a hacker network that infiltrated hundreds of universities to steal sensitive data,” said Treasury Under Secretary Sigal Mandelker. “We will not tolerate the theft of U.S. intellectual property, or intrusions into our research institutions and universities. Treasury will continue to systematically use our sanctions authorities to shine a light on the Iranian regime’s malicious cyber practices, and hold it accountable for criminal cyber-attacks.”

As a result of today’s action, all property and interests in property of the designated persons subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

OFAC DESIGNATIONS

Today’s action designates one Iranian entity and 10 Iranian nationals pursuant to E.O. 13694, as amended, which targets malicious cyber activities, including those related to the significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for private financial gain.

The **Mabna Institute** is an Iran-based company that engaged in the theft of personal identifiers and economic resources for private financial gain. The organization was founded in or about

2013 to assist Iranian universities and scientific and research organizations in obtaining access to non-Iranian scientific resources. The Mabna Institute also contracted with Iranian governmental and private entities to conduct hacking activities on its behalf.

The Mabna Institute conducted massive, coordinated cyber intrusions into computer systems belonging to at least approximately 144 United States-based universities, in addition to at least 176 universities located in 21 foreign countries: Australia, Canada, China, Denmark, Finland, Germany, Ireland, Israel, Italy, Japan, Malaysia, the Netherlands, Norway, Poland, Singapore, South Korea, Spain, Sweden, Switzerland, Turkey, and the United Kingdom. The exfiltrated data and stolen login credentials acquired through these malicious cyber-enabled activities were used for the benefit of Iran's Islamic Revolutionary Guard Corps (IRGC), and were also sold within Iran through at least two websites. The stolen login credentials belonging to university professors were used to directly access online university library systems.

Today, OFAC is also designating nine Iran-based individuals who were leaders, contractors, associates, hackers for hire, and affiliates of the Mabna Institute for engaging in malicious cyber-enabled activities related to the significant misappropriation of economic resources or personal identifiers for private financial gain.

Gholamreza Rafatnejad (Rafatnejad) was a founding member of the Mabna Institute and organized the Mabna Institute hacking campaign.

Ehsan Mohammadi (Mohammadi) was also a founding member of the Mabna Institute. Along with Rafatnejad, Mohammadi also helped organize Mabna's university hacking campaign and received from others compromised account credentials belonging to university professors.

Seyed Ali Mirkarimi (Mirkarimi) was a hacker and Mabna Institute contractor. Mirkarimi engaged in a variety of phases of Mabna's university hacking campaign, including the crafting and testing of malicious, spearphishing emails and organizing of stolen credentials.

Mostafa Sadeghi (Sadeghi) was a hacker and affiliate of the Mabna Institute. Sadeghi compromised more than 1,000 university professor accounts. Sadeghi exchanged credentials for compromised professor accounts with other Mabna-affiliated actors. Sadeghi was also involved in the operation of, and maintained a financial interest in, one of the websites selling access to the stolen university data.

Sajjad Tahmasebi (Tahmasebi) was a Mabna Institute contractor. He helped facilitate the spearphishing campaign targeting universities by, among other things, conducting online

network surveillance of victim university computer systems and maintaining lists of credentials stolen from victim professors.

Abdollah Karima (Karima) was a businessman who owned and operated a company that sold, through a website, access to stolen academic materials obtained through computer intrusions. Karima contracted with the Mabna Institute to direct hacking activities. Mabna affiliates regularly provided compromised university professor login credentials to Karima.

Abuzar Gohari Moqadam (Gohari Moqadam) was a professor and affiliate of the Mabna Institute. Gohari Moqadam exchanged stolen credentials for compromised accounts with Mabna Institute founders Rafatnejad and Mohammadi.

Roozbeh Sabahi (Sabahi) was a contractor for the Mabna Institute. Roozbeh Sabahi assisted in the execution of the various Mabna hacking activities, including its university campaign by, among other things, organizing stolen credentials obtained by Mabna Institute hackers.

Mohammed Reza Sabahi (Sabahi) was a Mabna Institute contractor. Sabahi assisted in the carrying out of Mabna's spearphishing campaign targeting universities. Among his activities, Mohammed Reza Sabahi created targeting lists of university professors and catalogued academic databases at targeted universities.

In addition to the designations above related to the activities of the Mabna Institute, OFAC today designated an additional Iranian national pursuant to E.O. 13694, as amended, for engaging in significant malicious cyber-enabled misappropriation of economic resources, personal identifiers, and financial information for private financial gain for activities targeting a U.S. media company.

Behzad Mesri (Mesri) compromised multiple user accounts belonging to a U.S. media and entertainment company in order to repeatedly gain unauthorized access to the company's computer servers and steal valuable stolen data including confidential and proprietary information, financial documents, and employee contact information. Mesri then engaged in an attempt to extort the victim company for \$6 million.

Mesri is the subject of an indictment announced by the U.S. District Court for the Southern District of New York on November 21, 2017.

[Identifying information on the individuals and entity designated today.](#)

DEPARTMENT OF JUSTICE ACTION

OFAC closely coordinated its action with the Department of Justice, which today released details regarding its law enforcement action against the nine leaders, contractors, associates, hackers for hire, and affiliates of the Mabna Institutedesignated today.

[The Department of Justice press release.](#)

####