US charges Iranians in massive hacking scheme

March 23 2018

The US Treasury Department accuses Iran's Mabna Institute of cyber intrusions into the computer systems of 144 US universities, and 176 universities in 21 foreign countries

The United States unveiled charges on Friday against nine Iranians for

their alleged involvement in a massive state-sponsored hacking scheme which targeted hundreds of universities in the US and abroad and stole "valuable intellectual property and data."

Ten Iranians were also hit with sanctions along with an Iranian company, the Mabna Institute, which engaged in computer hacking on behalf of Iran's Revolutionary Guards, the US Treasury Department said.

The two founders of the Mabna Institute, Gholamreza Rafatnejad, 38, and Ehsan Mohammadi, 37, were among the nine Iranians indicted in New York and whose assets are subject to US seizure.

Since 2013, the Mabna Institute carried out cyber intrusions into the computer systems of 144 US universities, the Treasury Department said, and 176 universities in 21 foreign countries.

Mabna Institute employees and contractors "engaged in the theft of valuable intellectual property and data from hundreds of US and third-country universities... for private financial gain," it said.

"For many of these intrusions, the defendants acted at the behest of the Iranian government and, specifically, the Iranian Revolutionary Guard Corps," Deputy Attorney General Rod Rosenstein said.

The US Department of Labor, the US Federal Energy Regulatory Commission, dozens of private firms and non-governmental organizations such as the United Nations Children's Fund were also allegedly targeted.

Geoffrey Berman, US Attorney for the Southern District of New York, said the Iranians conducted spearphishing attacks designed to steal passwords from email accounts in one of the "largest state-sponsored" hacking schemes ever uncovered.

8,000 accounts compromised

The email accounts of more than 100,000 university professors worldwide were targeted, Berman said, and about 8,000 accounts were compromised.

He said 31 terabytes—about 15 billion pages—of academic data and intellectual property were stolen.

This included "research, and other academic data and documents, including, among other things, academic journals, theses, dissertations, and electronic books," the Justice Department said.

"The defendants targeted data across all fields of research and academic disciplines, including science and technology, engineering, social sciences, medical, and other professional fields," it said.

David Bowdich, deputy director of the FBI, said the defendants are in Iran and "apprehending these individuals presents a challenge."

"(But) the long arm of the law reaches worldwide," he said.

"You cannot hide behind a keyboard half way around the world and expect not to be held to account," Berman said.

One of the 10 Iranians subject to sanctions, Behzad Mesri, was already indicted in November 2017 in connection with the theft of scripts and plot summaries for HBO's "Game of Thrones," and for trying to extort $6 million in Bitcoin out of the network.

The Justice Department said that besides targeting university professors in the United States, the hackers also compromised accounts in 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.

Rafatnejad, Mohammadi and the seven other Mabna Institute employees or contractors were charged with identity theft, conspiracy to commit computer intrusions and other crimes.