The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

August 18, 2026

# 17 Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps and Other Iranian Entities

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

WASHINGTON — A 14-count superseding (S2) indictment was unsealed today charging 17 members of the Mabna Institute, an Iran-based company that, since at least 2013, has conducted a coordinated campaign of cyber intrusions into computer systems for 144 U.S.-based universities, 178 foreign universities, at least 42 U.S.-based private sector companies, at least 11 foreign private sector companies, at least five U.S. federal and state government agencies, and at least two non-governmental organizations (NGOs). The Mabna Institute stole more than 31 terabytes of academic data and intellectual property from these universities, as well as the email accounts of employees at the private sector companies, government agencies, and NGOs. The defendants conducted many of these intrusions on behalf of the Islamic Republic of Iran's 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. Nine of the 17 defendants charged in the S2 indictment were previously charged in a 7-count indictment announced in March 2018. The case is assigned to U.S. District Judge Jesse M. Furman.

"The superseding indictment alleges that, at the behest of entities including the IRGC, these defendants hacked into universities and other research institutions worldwide, including the United States, stealing at least 31 terabytes of information and intellectual property of untold value," said Assistant Attorney General for National Security John A. Eisenberg. "The National Security Division is committed to protecting

the United States from such predators and will pursue those who perpetrate such crimes for as long as it takes to bring them to justice."

"Today's charges, which include eight additional defendants, reveal the broader network allegedly behind a sweeping, state-sponsored campaign to steal research and intellectual property from American universities, businesses, and government institutions," said U.S. Attorney Jamie McDonald for the Southern District of New York. "More than eight years after making the original indictment public, these charges make clear that the passage of time will not deter us from identifying and pursuing those who target the United States from abroad. Cyber operations have become a central instrument of national power, and attacks on American and allied institutions carry direct consequences for our security and economic strength. This office and our partners will continue to protect American innovation and pursue accountability for the individuals behind these attacks."

"These defendants allegedly built and profited from a sprawling hacking-for-hire operation that targeted the intellectual property of American and allied universities, companies, and government agencies for the benefit of the Iranian government," said Assistant Director Brett Leatherman of the FBI's Cyber Division. "Today's charges make clear to cyber adversaries everywhere: the FBI's memory is long, and time will not blunt our resolve to pursue justice. The FBI will continue working with law enforcement and private sector partners to identify malicious cyber actors, disrupt their operations, and impose real cost on them, wherever they operate."

According to the allegations contained in the S2 indictment:

Background on the Mabna Institute

Gholamreza Rafatnejad and Ehsan Mohammadi founded the Mabna Institute in approximately 2013 to assist Iranian universities and scientific and research organizations in stealing access to non-Iranian scientific resources. The Mabna Institute employed, contracted, and affiliated itself with hackers-for-hire and other contract personnel, including Abdollah Karima, also known as "Vahid Karima," Mostafa Sadeghi, Seyed Ali Mirkarmi, Mohammed Reza Sabahi, Roozbeh Sabahi, Abuzar Gohari Moqadam, Sajjad Tahmasebi, Saeid Houshyar, Behzad Mesri, also known as "Skote Vahshat," Manouchehr Hashemloo, Keyvan Fayaz, also known as "Achilles," also known as "The Joker," also known as "bc.monster," Amir Barati, Saber Shahbazi Ballojeh, Arman Kahzadian, and Mojtaba Galekuhi, also known as "Mojtaba Ghaleh Koui," to conduct cyber intrusions to steal academic data, intellectual property, email inboxes, and other proprietary data. 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.

Concurrent with the unsealing of the S2 indictment, the U.S. Department of State's Rewards for Justice program (RFJ) is offering a reward of up to $10 million for information leading to the location of defendants Mesri, Galekuhi, Kahzadian, Fayaz, and Ballojeh. The RFJ program seeks information on any person who, while acting at

the direction or under the control of a foreign government, engages in certain malicious cyber activities in violation of the Computer Fraud and Abuse Act.

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 178 universities located in foreign countries, including Australia, Canada, China, Denmark, Finland, Germany, Ireland, Israel, Italy, Japan, Malaysia, Netherlands, Norway, Poland, Saudi Arabia, 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, and Gigapaper was also 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.

Private Sector and Governmental and Non-Governmental Organization Hacking Campaigns

In addition to targeting and compromising universities, the defendants targeted and compromised and exfiltrated employee email accounts for at least five U.S. federal and state government agencies, at least 42 U.S. based private sector companies, at least approximately 11 foreign companies based in Germany, Italy, Switzerland, Sweden, and the United Kingdom, and various governmental and non-governmental organizations within the U.S., including 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.

Eight Additional Defendants Charged in the S2 Indictment

The S2 indictment charges eight additional defendants and describes continued efforts by the Mabna Institute to target American and international institutions. For example, the defendants targeted Home Box Office, Inc. (HBO), a media and entertainment company headquartered in New York, New York. Mesri was separately charged in *United States v. Behzad Mesri*, 17 Cr. 689 (AJN), with hacking into HBO's computer systems, stealing proprietary data, and then attempting to extort HBO for approximately $6 million worth of Bitcoin, a form of digital currency. Houshyar, Hashemloo, Fayaz, Ballojeh, and Kahzadian were also directly involved in the hack of HBO's systems along with Mesri.

Galekuhi, Fayaz, and Ballojeh participated in the Mabana Institute's efforts to hack into private sector companies and at least two governmental entities — including through password spray attacks, obtaining unauthorized access to victim systems, and exfiltrating data — causing victims to suffer an excess of $20 million in costs to investigate and remediate the intrusions. Barati moreover was involved in tracking the progress of the spearphishing campaigns, exchanging login credentials for compromised accounts with other co-conspirators, creating targeting lists, conducting computer network reconnaissance, and crafting phishing messages.

Anyone with information on these malicious cyber actors, or associated individuals or entities, please contact Rewards for Justice via the Tor-based tips-reporting channel at: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion. More information about this RFJ reward offer is located on the Rewards for Justice website.

A chart containing the names, charges, and maximum penalties for the defendants is set forth below.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the judge.

The National Security Division praised the outstanding investigative work of the FBI, the assistance of the United Kingdom's National Crime Agency (NCA), and thanked OFAC and the RFJ Program for their support. The Justice Department's Office of International Affairs is providing critical assistance.

Assistant U.S. Attorneys Nicholas W. Chiuchiolo, Connie L. Dang, and Adam Sowlati for the Southern District of New York lead the prosecution, with assistance provided by Trial Attorney Jacques Singer-Emery and former Trial Attorney Matthew Chang of the National Security Division's National Security Cyber Section.

*An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.*

| COUNT | CHARGE | DEFENDANTS | MAX. PENALTIES |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | Conspiracy to Commit Computer Intrusions (18 U.S.C. § 371) | RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, SABAHI, SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, FAYAZ, BARATI, BALLOJEH, and KAHZADIAN | Five years in prison |
| 2 | Conspiracy to Commit Wire Fraud (18 U.S.C. § 1349) | RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, SABAHI, SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, FAYAZ, BARATI, BALLOJEH, and KAHZADIAN | 20 years in prison |
| 3 | Computer Fraud – Unauthorized Access for Private Financial Gain (18 U.S.C. §§ 1030(a)(2), (c)(2)(B)(i), (c)(2)(B)(iii) and 2) | RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, SABAHI, SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, FAYAZ, BARATI, and KAHZADIAN | Five years in prison |
| 4 | Wire Fraud (18 U.S.C. §§ 1343 and 2) | RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, SABAHI, SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, BARATI, and KAHZADIAN | 20 years in prison |
| 5 | Computer Fraud – Unauthorized Access for Private Financial Gain (18 U.S.C. §§ 1030(a)(2), (c)(2)(B)(i), (c)(2)(B)(iii) and 2) | RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, SABAHI, SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, BARATI, and KAHZADIAN | Five years in prison |
| 6 | Wire Fraud (18 U.S.C. §§ 1343 and 2) | RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, SABAHI, SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, BARATI, and KAHZADIAN | 20 years in prison |

| | | | |
|---|---|---|---|
| 7 | Aggravated Identity Theft (18 U.S.C. §§ 1028A(a)(1), 1028A(b), and 2) | RAFATNEJAD, MOHAMMADI, KARIMA, SADEGHI, MIRKARIMI, SABAHI, SABAHI, MOQADAM, TAHMASEBI, HOUSHYAR, MESRI, HASHEMLOO, FAYAZ, BARATI, BALLOJEH, and KAHZADIAN | Mandatory sentence of two years in prison |
| 8 | Computer Fraud – Unauthorized Access for Private Financial Gain (18 U.S.C. §§ 1030(a)(2), (c)(2)(B)(i), (c)(2)(B)(iii), and 2; 18 U.S.C. § 3238) | HOUSHYAR, HASHEMLOO, FAYAZ, BALLOJEH, and KAHZADIAN | Five years in prison |
| 9 | Wire Fraud (18 U.S.C. §§ 1343 and 2; 18 U.S.C. § 3238) | HOUSHYAR, HASHEMLOO, FAYAZ, BALLOJEH, and KAHZADIAN | 20 years in prison |
| 10 | Aggravated Identity Theft (18 U.S.C. §§ 1028A(a)(1), 1028A(b), and 2; 18 U.S.C. § 3238) | HOUSHYAR, HASHEMLOO, FAYAZ, BALLOJEH, and KAHZADIAN | Mandatory sentence of two years in prison |
| 11 | Conspiracy to Commit Computer Intrusions (18 U.S.C. § 371; 18 U.S.C. § 3238) | FAYAZ, BALLOJEH, and MOJTABA GALEKUHI | Five years in prison |
| 12 | Computer Intrusion (18 U.S.C. §§ 1030(a)(2), (c)(2)(B)(i), and (c)(2)(B)(iii)) | FAYAZ, BALLOJEH, and MOJTABA GALEKUHI | Five years in prison |
| 13 | Conspiracy to Commit Wire Fraud (18 U.S.C. § 1349; 18 U.S.C. § 3238) | FAYAZ, BALLOJEH, and MOJTABA GALEKUHI | 20 years in prison |
| 14 | Aggravated Identity Theft (18 U.S.C. §§ 1028A(a)(1), 1028A(b), and 2; 18 U.S.C. § 3238) | FAYAZ, BALLOJEH, and MOJTABA GALEKUHI | Mandatory sentence of two years in prison |

###

NSD

26-940

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.