Department of Justice and Partner Departments and Agencies Conduct Coordinated Actions to Disrupt and Deter Iranian Malicious Cyber Activities Targeting the United States and the Broader International Community

Published: 2020-09-17 · Archived: 2026-04-02 12:24:20 UTC

Starting on Sept. 14, 2020 and continuing through today, the Department of Justice, the Federal Bureau of Investigation, the Department of Homeland Security, and the Department of the Treasury have engaged in a coordinated effort to disrupt and deter malicious cyber activities by actors associated with the Islamic Republic of Iran's (Iran) Ministry of Intelligence and Security (MOIS) and Islamic Revolutionary Guard Corps (IRGC), as well as other Iran-based individuals. These malicious cyber actors targeted victims in Australia, Europe, the Middle East, Southeast Asia, and the United States.

"This week's unsealing of indictments and other disruptive actions serves as another reminder of the breadth and depth of Iranian malicious cyber activities targeting not only the United States, but countries all over the world," said Assistant Attorney General for National Security John C. Demers. "Whether directing such hacking activities, or by offering a safe haven for Iranian criminal hackers, Iran is complicit in the targeting of innocent victims worldwide and is deepening its status as a rogue state. By contrast, the Department of Justice and its U.S. government partners stand with such victims, regardless of their location, and we will continue our cooperative efforts domestically and internationally to disrupt Iranian hacking activities."

"The FBI is using its unique partnerships and world-class capabilities to hold Iranian cyber actors publicly accountable for their actions," said Executive Assistant Director Terry Wade of the FBI's Criminal, Cyber, Response, and Services Branch. "Those malicious activities, as once again outlined this week, highlight Iran's persistent use of cyber methods to harm the citizens of the United States and its allies. No cyber actor should think they can compromise U.S. networks, steal our intellectual property, or hold our critical infrastructure at risk without incurring risk themselves. The FBI will continue to work with our partners to protect U.S. interests and to impose consequences on those cyber actors working on behalf of the Government of Iran in furtherance of their nefarious goals."

On Sept. 14, 2020, the FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency jointly published a Cybersecurity Advisory regarding tactics, techniques, and procedures (TTPs) of an Iran-based malicious cyber actor targeting several U.S. federal agencies and other U.S.-based networks.

On Sept. 15, 2020, in the District of Massachusetts, the Department announced the unsealing of a three-count indictment charging two hackers in relation to their intrusions into, and defacements of, websites hosted in the United States. The hackers, Behzad Mohammadzadeh, aka "Mrb3hz4d," a citizen and resident of the Iran, and Marwan Abusrour, aka "Mrwn007," a stateless national under the jurisdiction of the Palestinian Authority, conspired to and subsequently damaged computers in perceived retaliation for the January 2, 2020 U.S. military strike that killed Qasem Soleimani, the head of the IRGC-Quds Force, a U.S.-designated Foreign Terrorist

Organization. These defacements were a subset of the over 1,400 defacements around the world for which the defendants claimed responsibility between in or around June 2016 and July 2020.

On Sept. 16, 2020, in the District of New Jersey, the Department announced the unsealing of a 10-count indictment charging two hackers, who sometimes operated under the using the pseudonym "Sejeal," in relation to coordinated cyber intrusions and hacking campaigns targeted computer systems in Europe, the Middle East, and the United States. The defendants, Hooman Heidarian, aka "neo," and Medhi Farhadi, aka "Mehdi Mahdavi," both Iranian nationals residing in Iran, stole hundreds of terabytes of data, which typically included confidential communications pertaining to national security, foreign policy intelligence, non-military nuclear information, aerospace data, human rights activist information, victim financial information and personally identifiable information, and intellectual property, including unpublished scientific research. In some instances, the defendants' hacks were politically motivated or at the behest of the government of Iran, including instances where they obtained information regarding dissidents, human rights activists, and opposition leaders. In other instances, the defendants sold the hacked data and information on the black market for private financial gain.

On Sept. 17, 2020, in the Eastern District of Virginia, the Department announced the unsealing of a nine-count indictment charging three hackers in relation to an approximately four-year campaign to steal and attempt to steal critical information related to aerospace and satellite technology and resources, including sensitive commercial information, intellectual property, and personal data. The defendants, Said Pourkarim Arabi, Mohammad Reza Espargham, and Mohammad Bayati, all Iranian nationals residing in Iran, conducted their activity at the direction of the IRGC, of which Arabi was a member. The defendants primarily accomplished their intrusions through socially engineered spearphishing campaigns, using at least one target list of over 1,800 individuals in Australia, Israel, Singapore, the United States, and the United Kingdom. Upon successfully enticing a victim to click on a link in such a spearphishing e-mail, a member of the conspiracy would deploy malware that allowed the conspirators to gain access credentials, escalate their privileges, maintain their unauthorized access to victim networks, and ultimately steal the sought-after data. To accompany the unsealing of this indictment, and to aid potential targets in the identification of malicious activity, the FBI released a Private Industry Notification (PIN) that identified the conspiracy's TTPs and indicators of compromise.

Also on Sept. 17, 2020, the Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions against 45 individuals and one front company associated with the MOIS who comprised the cyber threat group known publicly as "Advanced Persistent Threat 39" (APT39), "Chafer," "Remexi," "Cadelspy," or "ITG07." According to OFAC, masked behind its front company, Rana Intelligence Computing Company (Rana), the MOIS employed a years-long malware campaign that targeted Iran's own citizens, the government networks of Iran's neighboring countries, and U.S.-based travel services companies. Concurrent with OFAC's action, and following a long-term FBI investigation, the FBI released technical indicators about Rana's malware in an FBI FLASH alert. This alert provides information to assist organizations and individuals in determining whether they were targeted by Rana.

The above disruptive actions targeting Iranian malicious cyber activities were the result of investigations conducted by the FBI's Boston, Newark, and Washington Field Offices and Cyber Division, the United States Attorney's Offices for the Eastern District of Virginia, District of Massachusetts, and District of New Jersey, and the National Security Division's Counterintelligence and Export Control Section. Several of the disruptive actions were the result of the close partnership between these Department of Justice components and the Department of

Homeland Security's Cybersecurity and Infrastructure Security Agency and Department of the Treasury's OFAC, and coordination through the National Cyber Investigative Joint Task Force.

The details contained in the above-described charging document are allegations. The defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.
