PRESS RELEASE

Justice Department Charges Four Iranian Nationals for Multi-Year Cyber Campaign Targeting U.S. Companies

Tuesday, April 23, 2024
For Immediate Release
Office of Public Affairs

https://www.justice.gov/archives/opa/pr/justice-department-charges-four-iranian-nationals-multi-year-cyber-campaign-targeting-us

During the Course of the Conspiracy, One Defendant Also Worked for an IRGC Electronic Warfare and Cyber Defense Unit

An indictment was unsealed today in Manhattan federal court charging Iranian nationals Hossein Harooni (حسین هارونی), Reza Kazemifar (رضا کاظمی فر), Komeil Baradaran Salmani (کمیل برادران سلمانی), and Alireza Shafie Nasab (علیرضا شفیعی نسب) for their involvement in a cyber-enabled campaign to compromise U.S. government and private entities, including the U.S. Departments of Treasury and State, defense contractors, and two New York-based companies. Nasab was charged for the same conduct in a previous indictment that was unsealed on Feb. 29. The defendants remain at large.

Concurrent with today's unsealing, 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 identification or location of the group and the defendants. 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 (CFAA). Additionally, the Treasury Department announced sanctions against the four defendants, among other malicious cyber actors.

"Criminal activity originating from Iran poses a grave threat to America's national security and economic stability," said Attorney General Merrick B. Garland. "These defendants are alleged to have engaged in a coordinated, multi-year hacking campaign from Iran

targeting more than a dozen American companies and the U.S. Treasury and State Departments. This case represents just one part of the U.S. government's effort to counter the range of threats originating from Iran that endanger the American people."

"The FBI is constantly working to detect and counter cyber campaigns like the one described in today's indictment. From enabling lethal plots and repressing our citizens and residents to targeting our critical infrastructure, we've often seen the trail of dangerous cyber-criminal activity lead back to Iran," said FBI Director Christopher Wray. "Today's announcement demonstrates the FBI's commitment to using every lawful tool at our disposal, together with our domestic and international partners, to disrupt the threats posed from Iran to American businesses and citizens."

"Today's charges pull back the curtain on an Iran-based company that purported to provide 'cybersecurity services' while in actuality scheming to compromise U.S. private and public sector computer systems, including through spearphishing and social engineering attacks," said Assistant Attorney General Matthew G. Olsen of the Department of Justice's National Security Division. "The Department is committed to using a whole of government approach to disrupt such malicious activities and impose consequences on the individuals that carry them out. Employees that continue to work at these companies risk arrest and prosecution or a lifetime as an international fugitive from justice."

"As alleged, the defendants participated in a cyber campaign using spearphishing and other hacking techniques in an attempt to compromise private companies with access to defense-related information," said U.S. Attorney Damian Williams for the Southern District of New York. "Cyber intrusion schemes such as the one alleged threaten our national security, and I'm proud of our law enforcement partners and the career prosecutors of this office for continuing to use innovative technologies and investigative measures to disrupt and track down these cybercriminals. If you have information leading to the to the identification or location of Harooni, Kazemifar, Salmani, or Nasab, please reach out to the Department of State at rewardsforjustice.net."

According to court documents, from at least in or about 2016 through at least in or about April 2021, Harooni, Kazemifar, Salmani, Nasab, and other conspirators were members of a hacking organization that participated in a coordinated multi-year campaign to conduct and attempt to conduct computer intrusions. These intrusions targeted more than a dozen U.S. companies and the U.S. Departments of Treasury and State.

During the conspiracy, Kazemifar, Salmani, and Nasab were employed by Mahak Rayan Afraz (محک رایان افراز), an Iran-based company that purported to provide cybersecurity services, but which was, in fact, a front for the conspirators' operations.

The hacking group's private sector victims were primarily cleared defense contractors, which are companies that have been granted security clearances by the U.S. Department of Defense to access, receive, and store classified information for the purpose of conducting activities in support of U.S. Department of Defense programs. In addition, the group targeted a New York-based accounting firm and a New York-based hospitality company.

In conducting their hacking campaigns, the group used spearphishing — tricking an email recipient into clicking on a malicious link — to infect victim computers with malware. During their campaigns against one victim, the group compromised more than 200,000 employee accounts. In another campaign, the conspirators targeted 2,000 employee accounts. In order to manage their spearphishing operations, the group created and used a particular computer application that enabled the conspirators to organize and deploy their spearphishing attacks.

In the course of these spearphishing attacks, the conspirators compromised an administrator email account belonging to a defense contractor (Defense Contractor-1). Access to this administrator account empowered the conspirators to create unauthorized Defense Contractor-1 accounts, which the conspirators then used to send spearphishing campaigns to employees of a different defense contractor and a consulting firm.

In addition to spearphishing, the conspirators utilized social engineering, which involved impersonating others, generally women, to obtain the confidence of victims. These social engineering contacts were another means the conspiracy used to deploy malware onto victim computers and compromise those devices and accounts.

Kazemifar was responsible for testing the tools utilized by the conspiracy to execute its cyber campaigns. For example, Kazemifar was involved in testing spearphishing emails used to target victim companies and was involved in developing malware utilized by the conspiracy in social engineering initiatives. During the course of his involvement in the conspiracy, from at least in or about 2014 through at least in or about 2020, Kazemifar also worked for the Iranian Organization for Electronic Warfare and Cyber Defense (EWCD). EWCD is a component of the Islamic Revolutionary Guard Corps (IRGC), which is itself a component of the Iranian Armed Forces. Among other things, the IRGC is responsible for Iran's offensive cyber capabilities. The United States has designated the IRGC as a foreign terrorist organization.

Harooni was responsible for procuring, administering, and managing the online network infrastructure, including computer servers and customized software used to facilitate the computer intrusions. Harooni also fraudulently used the identity of a real person (Individual-1), including his use of a copy of Individual-1's true passport, to conceal his role in procuring online infrastructure used by the conspiracy to facilitate the computer intrusion campaign.

Salmani was responsible for testing tools utilized by the conspiracy to execute spearphishing campaigns, including the campaign against a hospitality company. Salmani was also involved in maintaining infrastructure used by the conspirators.

Nasab was responsible for procuring infrastructure used by the conspiracy, particularly infrastructure used in furtherance of social engineering campaigns. Nasab also used Individual-1's identity, including Individual-1's name and passport, to register server and email accounts that were used during malicious cyber campaigns.

The defendants are each charged with conspiracy to commit computer fraud, conspiracy to commit wire fraud, and wire fraud. If convicted, they face up to five years in prison for the computer fraud conspiracy, and up to 20 years in prison for each count of wire fraud and conspiracy to commit wire fraud. Harooni is additionally charged with knowingly damaging a protected computer, which carries a maximum penalty of 10 years in prison. Harooni, Salamani, and Nasab are additionally charged with aggravated identity theft, which carries a mandatory consecutive term of two years in prison. A federal district judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The FBI Cyber Division is investigating the case.

Assistant U.S. Attorneys Ryan B. Finkel, Dina McLeod, and Daniel G. Nessim for the Southern District of New York are prosecuting the case, with assistance from 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.