Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election

justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed

November 18, 2021

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, November 18, 2021

An indictment was unsealed in New York today charging two Iranian nationals for their involvement in a cyber-enabled campaign to intimidate and influence American voters, and otherwise undermine voter confidence and sow discord, in connection with the 2020 U.S. presidential election.

According to court documents, Seyyed Mohammad Hosein Musa Kazemi (سید محمد حسین موسی کاظمی), aka Mohammad Hosein Musa Kazem, aka Hosein Zamani, 24, and Sajjad Kashian (سجاد کاشیان), aka Kiarash Nabavi, 27, both of Iran, obtained confidential U.S. voter information from at least one state election website; sent threatening email messages to intimidate and interfere with voters; created and disseminated a video containing disinformation about purported election infrastructure vulnerabilities; attempted to access, without authorization, several states' voting-related websites; and successfully gained unauthorized access to a U.S. media company's computer network that, if not for successful FBI and victim company efforts to mitigate, would have provided the conspirators another vehicle to disseminate false claims after the election.

“This indictment details how two Iran-based actors waged a targeted, coordinated campaign to erode confidence in the integrity of the U.S. electoral system and to sow discord among Americans,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “The allegations illustrate how foreign disinformation campaigns operate and seek to influence the American public. The Department is committed to exposing and disrupting malign foreign influence efforts using all available tools, including criminal charges.”

“As alleged, Kazemi and Kashian were part of a coordinated conspiracy in which Iranian hackers sought to undermine faith and confidence in the U.S. presidential election,” said U.S. Attorney Damian Williams for the Southern District of New York. “Working with others, Kazemi and Kashian accessed voter information from at least one state’s voter database, threatened U.S. voters via email, and even disseminated a fictitious video that purported to depict actors fabricating overseas ballots. The United States will never tolerate any foreign actors’ attempts to undermine our free and democratic elections. As a result of the charges unsealed today, and the concurrent efforts of our U.S. government partners, Kazemi and Kashian will forever look over their shoulders as we strive to bring them to justice.”

“The FBI remains committed to countering malicious cyber activity targeting our democratic process,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “Working rapidly with our private sector and U.S. government partners and ahead of the election, we were able to disrupt and mitigate this malicious activity – and then to enable today’s joint, sequenced operations against the adversary. Today’s announcement shows what we can accomplish as a community and a country when we work together, and the FBI will continue to do its part to keep our democracy safe.”

According to the allegations contained in the indictment unsealed today:

The Voter Intimidation and Influence Campaign

Starting in approximately August 2020, and proceeding until November 2020, Kazemi, Kashian, and other co-conspirators began a coordinated, campaign to undermine faith and confidence in the 2020 presidential election (the “Voter Intimidation and Influence Campaign”) and otherwise sow discord within U.S. society. The Campaign had four components:

- In September and October 2020, members of the conspiracy conducted reconnaissance on, and attempted to compromise, approximately 11 state voter websites, including state voter registration websites and state voter information websites. Those efforts resulted in the successful exploitation of a misconfigured computer system of a particular U.S. state (“State-1”), and the resulting unauthorized downloading of information concerning more than 100,000 of State-1’s voters.

- In October 2020, members of the conspiracy, claiming to be a “group of Proud Boys volunteers,” sent Facebook messages and emails (the “False Election Messages”) to Republican Senators, Republican members of Congress, individuals associated with the presidential campaign of Donald J. Trump, White House advisors, and members of the media. The False Election Messages claimed that the Democratic Party was planning to exploit “serious security vulnerabilities” in state voter registration websites to “edit mail-in ballots or even register non-existent voters.” The False Election Messages were accompanied by a video (the “False Election Video”) carrying the Proud Boys logo, which purported, via simulated intrusions and the use of State-1 voter data, to depict an individual hacking into state voter websites and using stolen voter information to create fraudulent absentee ballots through the Federal Voting Assistance Program (FVAP) for military and overseas voters.[1]
- Also in October 2020, the conspirators engaged in an online voter intimidation campaign involving the dissemination of a threatening message (the “Voter Threat Emails”), purporting to be from the Proud Boys, to tens of thousands of registered voters, including some voters whose information the conspiracy had obtained from State-1’s website. The emails were sent to registered Democrats and threatened the recipients with physical injury if they did not change their party affiliation and vote for President Trump.
- On Nov. 4, 2020, the day after the 2020 U.S. presidential election, the conspirators sought to leverage earlier September and October 2020 intrusions into an American media company’s (Media Company-1) computer networks. Specifically, on that day, the conspirators attempted to use stolen credentials to again access Media Company-1’s network, which would have provided them another vehicle for further disseminating false claims concerning the election through conspirator-modified or created content. However, because of an earlier FBI victim notification, Media Company-1 had by that time mitigated the conspirators’ unauthorized access and these log-in attempts failed.

Background on Kazemi and Kashian

Kazemi and Kashian are experienced Iran-based computer hackers who worked as contractors for an Iran-based company formerly known as Eeleyanet Gostar, and now known as Emennet Pasargad. Eeleyanet Gostar purported to provide cybersecurity services within Iran. Among other things, Eeleyanet Gostar is known to have provided services to the Iranian government, including to the Guardian Council.

As part of his role in the Voter Intimidation and Influence Campaign, Kazemi compromised computer servers that were used to send the Voter Threat Emails, drafted those emails, and compromised the systems of Media Company-1. Kashian managed the conspirators’ computer infrastructure used to carry out the Voter Threat Emails campaign and he purchased social media accounts in furtherance of the Voter Intimidation and Influence Campaign.

Kazemi and Kashian are both charged with one count of conspiracy to commit computer fraud and abuse, intimidate voters, and transmit interstate threats, which carries a maximum sentence of five years in prison; one count of voter intimidation, which carries a maximum sentence of one year in prison; and one count of transmission of interstate threats, which carries a maximum sentence of five years in prison. Kazemi is additionally charged with one count of unauthorized computer intrusion, which carries a maximum sentence of five years in prison; and one count of computer fraud, namely, knowingly damaging a protected computer, which carries a maximum sentence of 10 years in prison. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

Concurrent with the unsealing of the indictment, the Department of the Treasury Office of Foreign Assets Control (OFAC) designated Emennet Pasargad, Kazemi, Kashian, and four other Iranian nationals comprising Emennet Pasargad leadership pursuant to Executive Order 13848, “Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election.” Additionally, the Department of State’s Rewards for Justice Program, is offering a reward of up to $10 million for information on or about the Kazemi and Kashian’s activities.

The FBI’s Cyber Division and Cleveland Field Office are investigating the case.

Assistant U.S. Attorneys Dina McLeod and Louis A. Pellegrino and Trial Attorney Adam Small of the National Security Division’s Counterintelligence and Export Control Section are prosecuting the case.

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

---

[1] In actuality, the computer intrusions depicted in the False Election Video were simulated intrusions created by members of the conspiracy using their own server and data obtained during the State-1 exploitation. Further, the FVAP could not actually be leveraged in the manner implied by the False Election Video.

Attachment(s):

Download Kazemi Indictment
Topic(s):

Cybercrime

National Security