Three IRGC Cyber Actors Indicted for ‘Hack-and-Leak’ Operation Designed to Influence the 2024 U.S. Presidential Election

Published: 2024-09-27 · Archived: 2026-04-05 16:23:47 UTC

Note: View the indictment here and the FBI Wanted Poster here.

The Justice Department today announced the unsealing of an indictment charging Iranian nationals, and Islamic Revolutionary Guard Corps (IRGC) employees, Masoud Jalili, 36, also known as, مسعود جلیلی, Seyyed Ali Aghamiri, 34, also known as, سید علی آقامیری, and Yaser Balaghi, 37, also known as, یاسر بلاغی (the Conspirators), with a conspiracy with others known and unknown to hack into accounts of current and former U.S. officials, members of the media, nongovernmental organizations, and individuals associated with U.S. political campaigns. The activity was part of Iran’s continuing efforts to stoke discord, erode confidence in the U.S. electoral process, and unlawfully acquire information relating to current and former U.S. officials that could be used to advance the malign activities of the IRGC, including ongoing efforts to avenge the death of Qasem Soleimani, the former commander of the IRGC – Qods Force (IRGC-QF).

As alleged, in or around May, after several years of focusing on compromising the accounts of former U.S. government officials, the conspirators used some of the same hacking infrastructure from earlier in the conspiracy to begin targeting and successfully gaining unauthorized access to personal accounts belonging to persons associated with an identified U.S. Presidential campaign (U.S. Presidential Campaign 1), including campaign officials. The conspirators used their access to those accounts to steal, among other information, non-public campaign documents and emails (campaign material). The activity broadened in late June, when the conspirators engaged in a “hack-and-leak” operation, in which they sought to weaponize campaign material stolen from U.S. Presidential Campaign 1 by leaking such materials to members of the media and individuals associated with what was then another identified U.S. Presidential campaign (U.S. Presidential Campaign 2), in a deliberate effort to, as reflected in the conspirators’ own words and actions, undermine U.S. Presidential Campaign 1 in advance of the 2024 U.S. presidential election.

“The Justice Department is working relentlessly to uncover and counter Iran’s cyberattacks aimed at stoking discord, undermining confidence in our democratic institutions, and influencing our elections,” said Attorney General Merrick B. Garland. “The American people – not Iran, or any other foreign power – will decide the outcome of our country’s elections.”

“Today’s charges represent the culmination of a thorough and long-running FBI investigation that has resulted in the indictment of three Iranian nationals for their roles in a wide-ranging hacking campaign sponsored by the Government of Iran,” said FBI Director Christopher Wray. “The conduct laid out in the indictment is just the latest example of Iran’s brazen behavior. So today the FBI would like to send a message to the Government of Iran – you and your hackers can’t hide behind your keyboards.”

“These hack-and-leak efforts by Iran are a direct assault on the integrity of our democratic processes,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “Iranian government actors have long sought to use cyber-enabled means to harm U.S. interests. This case demonstrates our commitment to expose attempts by the Iranian regime or any other foreign actor to interfere with our free and open society.”

“This indictment alleges a serious and sustained effort by a state-sponsored terrorist organization to gather intelligence through hacking personal accounts so they can use the hacked materials to harm Americans and corruptly influence our election,” said U.S. Attorney Matthew Graves for the District of Columbia. “The detailed allegations in the indictment should make clear to anyone who might attempt to do the same that the Justice Department has the ability to gather evidence of such crimes from around the globe, will charge those who commit such crimes, and will do whatever we can to bring those charged to justice.”

As alleged in the indictment, beginning in or around January 2020, Jalili, Aghamiri, and Balaghi, working on behalf of the IRGC, commenced a wide-ranging hacking campaign that used spearphishing and social engineering techniques to target and compromise victims computers and accounts. Among the conspirators’ techniques were: using virtual private networks and virtual private servers to obscure their true location; creating fraudulent email accounts in the names of prominent U.S. persons and international institutions; creating spoofed login pages to harvest account credentials; sending spearphishing emails using compromised victim accounts; and using social engineering to obtain victims’ login information and multi-factor recovery/authentication codes. Some of the conspirators’ efforts were successful, while others were not.

In April 2019, the Department of State designated the IRGC as a foreign terrorist organization. Among the purposes of the conspiracy were for the conspirators to: (i) steal victims’ data, such as information related to U.S. government and foreign policy information concerning the Middle East; (ii) steal information relating to current and former U.S. officials that could be used to advance the IRGC’s malign activities; (iii) disrupt U.S. foreign policy in the Middle East; (iv) stoke discord and erode confidence in the U.S. electoral process; (v) steal personal and private information from persons who had access to information relating to U.S. Presidential Campaign 1, including non-public campaign material and information; and (vi) undermine U.S. Presidential Campaign 1 in advance of the 2024 U.S. presidential election by leaking stolen campaign material and information.

As reflected in the Sept. 18 joint statement released by the Office of the Director of National Intelligence, FBI, and Cybersecurity and Infrastructure Security Agency: “Iranian malicious cyber actors in late June and early July sent unsolicited emails to individuals then associated with President Biden’s campaign that contained an excerpt taken from stolen, non-public material from former Trump’s campaign as text in the emails. There is currently no information indicating those recipients replied. Furthermore, Iranian malicious cyber actors have continued their efforts since June to send stolen, non-public material associated with former President Trump’s campaign to U.S. media organizations.”

As alleged in further detail in the indictment, the conspirators’ hack-and-leak efforts involved the conspirators emailing stolen campaign material to individuals that the conspirators believed were associated with what was then U.S. Presidential Campaign 2 and members of the media.

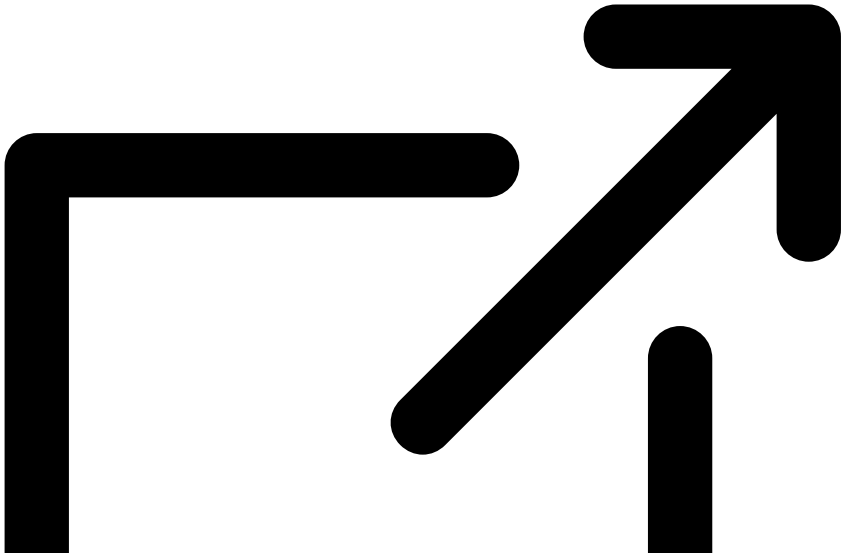
First, between on or about June 27 and July 3, the conspirators sent or forwarded an unsolicited email message to personal accounts of three persons that the conspirators believed were associated with U.S. Presidential Campaign 2. The June 27 email was sent to two recipients, and then forwarded the same day to another account for one of those recipients (due to the earlier email being sent to an invalid account for that recipient). This email chain contained campaign material stolen from an official for U.S. Presidential Campaign 1 (U.S. Victim 11). Neither of the recipients replied to the conspirators' email. In addition, the conspirators sent a follow up email on July 3rd to a third recipient's account, and the recipient similarly did not reply to the Conspirators.

Second, between on or about July 22 and on or about Aug. 31, the conspirators distributed other campaign material stolen from U.S. Victim 11 regarding U.S. Presidential Campaign 1's potential vice-presidential candidates to multiple members of the news media, in an attempt to induce the news media to publish the material. In one instance, for example, the conspirators' message stated "I think this information is worth a good [U.S. news publication] piece with your narration. Let me know your thoughts."

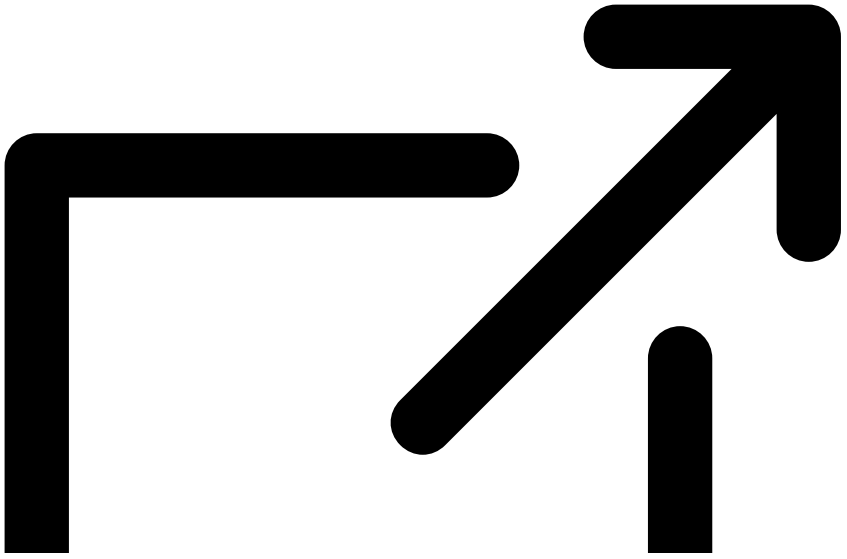
As alleged, these defendants also sought to promote the IRGC's goals and mission by compromising and maintaining unauthorized access to the email accounts of a number of former government officials, including U.S. Victim 1, who had served in a position with responsibility over U.S. Middle East policy at the time of Qasam Soleimani's death. Using this access, the defendants obtained information to assist the IRGC's efforts to target U.S. Victim 1 and others, including their means of identification, correspondence, travel information, lodging information and other information regarding their whereabouts and policy positions.

Jalili, Aghamiri, and Balaghi are charged with: conspiracy to commit identity theft, aggravated identity theft, access device fraud, unauthorized access to computers to obtain information from a protected computer, unauthorized access to computers to defraud and obtain a thing of value, and wire fraud, all while knowingly falsely registering domain names, which carries a maximum penalty of 12 years in prison; conspiracy to provide material support to a designated foreign terrorist organization, which carries a maximum penalty of 20 years in prison; eight counts of wire fraud while falsely registering domain names, each of which carries a maximum penalty of 27 years in prison; and eight counts of aggravated identity theft, each of which carries a mandatory minimum penalty of two years in prison. If convicted, a federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

Concurrent with today's announcement, the Department of State, through the Rewards for Justice Program, issued a reward



of up to $10 million for information on Jalili, Aghamiri, and Balaghi, the IRGC's interference in U.S. elections, or associated individuals and entities. Also, concurrent with today's announcement, the Department of the Treasury, Office of Foreign Asset Control (OFAC), pursuant to Executive Order (E.O.) 13694, as amended, and E.O. 13848 designated



Jalili for being responsible for or complicit in, or having engaged in, directly or indirectly, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

The FBI Washington Field Office is investigating this case. The FBI Cyber Division and Springfield and Minneapolis Field Offices provided substantial assistance in this matter. For more information on threat activity as

well as mitigation guidance, the FBI has released a Joint Cyber Security Advisory titled “Iranian Cyber Actors Targeting Personal Accounts to Support Operations.”

The Justice Department would like to thank the following private sector partners for their assistance with this case: Google, Microsoft, Yahoo, and Meta.

Assistant U.S. Attorneys Tejpal Chawla and Christopher Tortorice for the District of Columbia and Trial Attorney Greg Nicosia of the National Security Division’s National Security Cyber Section are prosecuting the case, with significant assistance from Paralegal Specialists Mariela Andrade and Kate Abrey. Joshua Champagne of the National Security Division’s Counterterrorism Section also provided valuable assistance.

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