

U.S. DEPARTMENT OF THE TREASURY

Treasury Sanctions IRGC–Affiliated Cyber Actors for Roles in Ransomware Activity

September 14, 2022

*Action Part of U.S. Government Response to the Continuous Malicious Cyber Activities
Conducted by Iranian Actors*

WASHINGTON — Today, the Department of the Treasury’s Office of Foreign Assets Control (OFAC) sanctioned ten individuals and two entities for their roles in conducting malicious cyber acts, including ransomware activity. Today’s designations are part of a joint action with the Department of Justice, Department of State, Federal Bureau of Investigation, U.S. Cyber Command, National Security Agency, and Cybersecurity and Infrastructure Security Agency. The individuals and entities designated today are all affiliated with Iran’s Islamic Revolutionary Guard Corps (IRGC). This action continues the series of OFAC designations that aim to protect U.S. persons from [ransomware activity](#), [facilitators of ransomware activity](#), and [other cybercrime](#).

“Ransomware actors and other cybercriminals, regardless of their national origin or base of operations, have targeted businesses and critical infrastructure across the board—directly threatening the physical security and economy of the United States and other nations,” said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. “We will continue to take coordination action with our global partners to combat and deter ransomware threats, including those associated with the IRGC.”

Ransomware incidents have disrupted critical services and businesses globally, including schools, government offices, hospitals and emergency services, transportation, energy, and food companies. Reported ransomware payments in the United States reached over \$590 million in 2021, compared to a total of \$416 million in 2020. The U.S. government estimates that these payments represent just a fraction of the economic harm caused by malicious cyber activities. In addition to the millions of dollars directly paid in ransoms and allocated to response and recovery, the disruption to critical sectors underscores the objectives of those who seek to weaponize technology for personal gain, disrupting our economy and damaging the companies, families, and individuals who depend on it for their livelihoods, savings, and

futures. The perpetrators behind these ransomware incidents seek to harm the United States and extort the American people and our allies, and those who provide financial services to, or facilitate money laundering for, ransomware actors enable this illegal activity.

Today's action demonstrates the U.S. government's commitment to disrupting ransomware infrastructure and actors. The United States will not tolerate malicious cyber activities, including disruptive cybercrime activities, victimizing the backbone of the U.S. economy and critical infrastructure.

IRGC-AFFILIATED MALICIOUS CYBER ACTORS

Today, OFAC, as part of a whole-of-government response, took action against a group of Iran-based malicious cyber actors who have been compromising networks based in the United States and other nations since at least 2020. This IRGC-affiliated group is known to exploit software vulnerabilities in order to carry out their ransomware activities, as well as engage in unauthorized computer access, data exfiltration, and other malicious cyber activities. Private cybersecurity firms routinely give monikers to specific cyber campaigns, and while the individuals sanctioned today do not directly align with a named advanced persistent threat group, some of their malicious cyber activity can be partially attributable to several named intrusion sets, such as "APT 35," "Charming Kitten," "Nemesis Kitten," "Phosphorus," and "Tunnel Vision." Several cybersecurity firms have determined these intrusion sets as being associated with the Government of Iran, and have identified them as having conducted a varied range of malicious cyber-enabled activities, including ransomware and cyber-espionage.

This group has launched extensive campaigns against organizations and officials across the globe, particularly targeting U.S. and Middle Eastern defense, diplomatic, and government personnel, as well as private industries including media, energy, business services, and telecommunications.

In February 2021, this group of malicious cyber actors victimized a New Jersey municipality through a computer network using a specific Fortinet vulnerability. These actors used their access to create unauthorized accounts, escalate their privileges, and conduct lateral movement to other parts of the network. They also used a fast reverse proxy on one of the municipality's servers in order to establish persistent remote access to a particular domain that was registered by **Mansour Ahmadi** (Mansour). The group also deployed tools such as Mimikatz and Filezilla in furtherance of their malicious activity.

In March and April 2021, this malicious cyber group launched the first known set of their encryption activities by compromising networks, activating Microsoft BitLocker without authorization, and holding the decryption keys for ransom. During this time, a number of small businesses were impacted, including a law firm, an accounting firm, and a construction contractor.

In June 2021, the group gained unauthorized access to supervisory control and data acquisition systems associated with a U.S.-based children's hospital. Once the group compromised the network, they created unauthorized accounts, escalated privileges, moved laterally through the network, established persistent access, exfiltrated data, and encrypted at least one device with BitLocker. U.S. government law enforcement partners provided a notification to the children's hospital before there were any impacts to patient care or medical services.

From June through August 2021, the group accelerated their malicious activity by targeting a wide range of U.S.-based victims, including transportation providers, healthcare practices, emergency service providers, and educational institutions. U.S. government agencies were able to warn potential victims of this activity and prevented or mitigated harm to or the compromise of computer networks in many cases.

From September 2021 through the present, this group primarily gained unauthorized access to victim networks by exploiting Microsoft Exchange and related ProxyShell vulnerabilities, including an incident in October 2021 when they compromised the network of an electric utility company serving a rural area of the United States, and maliciously used BitLocker to disrupt operations.

This IRGC-affiliated group is comprised of employees and associates of **Najee Technology Hooshmand Fater LLC** (Najee Technology) and **Afkar System Yazd Company** (Afkar System). Mansour is the owner, managing director, and chairman of the board of Najee Technology. **Ahmad Khatibi Aghda** (Khatibi) is managing director and member of the board of Afkar System. Additional employees and associates of Najee Technology and/or Afkar System include: **Ali Agha-Ahmadi** (Ali Ahmadi); **Mohammad Agha Ahmadi** (Mohammad Ahmadi); **Mo'in Mahdavi** (Mahdavi); **Aliakbar Rashidi-Barjini** (Rashidi); **Amir Hossein Nikaeen Ravari** (Nikaeen); **Mostafa Haji Hosseini** (Mostafa); **Mojtaba Haji Hosseini** (Mojtaba); and, **Mohammad Shakeri-Ashtijeh** (Shakeri).

Khatibi has been associated with Afkar System since at least 2007 and serves as its managing director and is a member of the board. Khatibi is among the cyber actors who gained

unauthorized access to victim networks to encrypt the network with BitLocker and demand a ransom for the decryption keys. He leased network infrastructure used in furtherance of this malicious cyber group's activities, he participated in compromising victims' networks, and he engaged in ransom negotiations with victims.

Nikaeen was an employee of Afkar System from 2015 to at least 2019. Nikaeen leased and registered network infrastructure used in furtherance of this malicious cyber group's activities and participated in compromising victims' networks.

Ali Ahmadi has been a Najee Technology employee since at least 2019. Rashidi has worked for Mansour since at least February 2021.

The IRGC-affiliated employees—Mansour, Ali Ahmadi, Mohammad Ahmadi, Mahdavi, Rashidi, Khatibi, Nikaeen, Mostafa, Mojtaba, and Shakeri— of the IRGC-affiliated companies, Najee Technology and Afkar System, are responsible for or complicit in, or have engaged in, directly or indirectly, global targeting of various networks, including critical infrastructure, by exploiting well-known vulnerabilities to gain initial access in furtherance of malicious activities, including ransom operations.

Mansour, Ali Ahmadi, Mohammad Ahmadi, Mahdavi, Rashidi, Khatibi, Nikaeen, Mostafa, Mojtaba, and Shakeri were designated pursuant to Executive Order (E.O.) 13694, as amended, for being responsible for or complicit in, or having engaged in, directly or indirectly, a cyber-enabled activity identified pursuant to E.O. 13694, as amended.

Najee Technology was designated pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity identified pursuant to E.O. 13694, as amended.

Afkar System was designated pursuant to E.O. 13694, as amended, for being owned or controlled by, or for having acted for or on behalf of, directly or indirectly, Khatibi, a person whose property and interests in property are blocked pursuant to E.O. 13694, as amended.

In addition to being designated for sanctions, the U.S. Attorney's Office for the District of New Jersey unsealed an indictment charging Mansour, Khatibi, and Nikaeen with violating the Computer Fraud and Abuse Act (CFAA) and conspiring to violate the CFAA.

State's Rewards for Justice (RFJ) program [is offering a reward](#) of up to \$10 million for information leading to the identification or location of Mansour, Khatibi, Nikaeen, or any other person who, while acting at the direction or under the control of a foreign government,

participates in malicious cyber activities against U.S. critical infrastructure in violation of the CFAA.

Additionally, a joint cyber security advisory (CSA)—the result of an analytical effort among the Department of the Treasury, FBI, NSA, USCYBERCOM, Australia’s Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), and the United Kingdom’s National Cyber Security Centre (NCSC)—has been published to highlight continued malicious cyber activity by advanced persistent threat (APT) actors that the authoring agencies assess are affiliated with IRGC.


SANCTIONS IMPLICATIONS

As a result of today’s action, all property and interests in property of the designated persons described above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person, or the receipt of any contribution or provision of funds, goods, or services from any such person. In addition, financial institutions and other persons that engage in certain transactions or activities with the sanctioned entities and individuals may expose themselves to sanctions or be subject to an enforcement action.

The power and integrity of OFAC sanctions derive not only from OFAC’s ability to designate and add persons to the SDN List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to [OFAC’s Frequently Asked Question 897 here](#). For detailed information on the process to [submit a request for removal from an OFAC sanctions list](#).

[Click here for more information on the individuals and entities designated today.](#)

See [OFAC’s Updated Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments here](#) , for information on the actions that OFAC would consider to be mitigating

factors in any related enforcement action involving ransomware payments with a potential sanctions risk. For information on complying with sanctions applicable to virtual currency, see [OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry here](#) .

FOR MORE INFORMATION ON RANSOMWARE

Please visit [StopRansomware.gov](https://stopransomware.gov), a one-stop resource for individuals and organizations of all sizes to reduce their risk of ransomware incidents and improve their cybersecurity resilience.

This webpage brings together tools and resources from multiple federal government agencies under one platform. Learn more about how ransomware works, how to protect yourself, how to report an incident, and how to request technical assistance.

###