Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses

November 28, 2018

WASHINGTON – The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) took action today against two Iran-based individuals, **Ali Khorashadizadeh** and **Mohammad Ghorbaniyan**, who helped exchange digital currency (bitcoin) ransom payments into Iranian rial on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims. Also today, OFAC identified two digital currency addresses associated with these two financial facilitators. Over 7,000 transactions in bitcoin, worth millions of U.S. dollars, have processed through these two addresses - some of which involved SamSam ransomware derived bitcoin. In a related action, the U.S. Department of Justice today indicted two Iranian criminal actors for infecting numerous data networks with SamSam ransomware in the United States, United Kingdom, and Canada since 2015.

"Treasury is targeting digital currency exchangers who have enabled Iranian cyber actors to profit from extorting digital ransom payments from their victims. As Iran becomes increasingly isolated and desperate for access to U.S. dollars, it is vital that virtual currency exchanges, peer-to-peer exchangers, and other providers of digital currency services harden their networks against these illicit schemes," said Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker. "We are publishing digital currency addresses to identify illicit actors operating in the digital currency space. Treasury will aggressively pursue Iran and other rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards to further their nefarious objectives."

Today's action focuses on a ransomware scheme known as "SamSam" that has victimized numerous corporations, hospitals, universities, and government agencies and held over 200 known victims' data hostage for financial gain. To execute the SamSam ransomware attack, cyber actors exploit computer network vulnerabilities to gain access and copy the SamSam ransomware into the network. Once in the network, these cyber actors use the SamSam ransomware to gain administrator rights that allow them to take control of a victim's servers

and files, without the victim's authorization. The cyber actors then demand a ransom be paid in bitcoin in order for a victim to regain access and control of its own network.

Central to the SamSam ransomware scheme's success were **Khorashadizadeh** and **Ghorbaniyan**, who helped the cyber actors exchange digital currency derived from ransom payments into Iranian rial and also deposited the rial into Iranian banks. To help convert the digital currency ransom payments into rial, **Khorashadizadeh** and **Ghorbaniyan** used the following two digital currency addresses: 149w62rY42aZBox8fGcmqNsXUzSStKeq8C and 1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V. Since 2013, **Khorashadizadeh** and **Ghorbaniyan** have used these two digital currency addresses to process over 7,000 transactions, to interact with over 40 exchangers—including some US-based exchangers—and to send approximately 6,000 bitcoin worth millions of USD, some of which involved bitcoin derived from SamSam ransomware.

While OFAC routinely provides identifiers for designated persons, today's action marks the first time OFAC is publicly attributing digital currency addresses to designated individuals. Like traditional identifiers, these digital currency addresses should assist those in the compliance and digital currency communities in identifying transactions and funds that must be blocked and investigating any connections to these addresses. As a result of today's action, persons that engage in transactions with **Khorashadizadeh** and **Ghorbaniyan** could be subject to secondary sanctions. Regardless of whether a transaction is denominated in a digital currency or traditional fiat currency, OFAC compliance obligations are the same. See OFAC's updated FAQ's for additional information on compliance requirements for digital currencies.

OFAC designated Iran-based **Khorashadizadeh** and **Ghorbaniyan** pursuant to Executive Order 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, the SamSam ransomware attacks. The SamSam ransomware attacks are cyber-enabled activities originating from, or directed by, persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States that have the purpose or effect of harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector, causing a significant disruption to the availability of a computer or network of computers, and 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.

As a result of today's action, all property and interests in property of the designated persons that are in the possession or control of U.S. persons or within or transiting the United States are blocked, and U.S. persons generally are prohibited from dealing with them.

Today's action marks the fourth round of U.S. sanctions targeting the Iranian regime this month. Under this Administration, in less than two years, OFAC has sanctioned more than 900 individuals, entities, aircraft, and vessels, including for a range of activities related to Iran's support for terrorism, ballistic missile program, weapons proliferation, cyberattacks, transnational criminal activity, censorship, and human rights abuses. This marks the highest-ever level of U.S. economic pressure targeting the Iranian regime. This sanctions pressure campaign is designed to blunt the broad spectrum of the Iranian regime's malign activities and compel the regime to change its behavior.

OFAC closely coordinated its action with the Department of Justice and the Federal Bureau of Investigation, which released details regarding its law enforcement action against the two Iranian criminal cyber actors.

Identifying information on the entities designated today.

####