Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry

home.treasury.gov/news/press-releases/sm1127

September 17, 2020

Washington – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on Iranian cyber threat group **Advanced Persistent Threat 39** (**APT39**), 45 associated individuals, and one front company. Masked behind its front company, **Rana Intelligence Computing Company** (**Rana**), the Government of Iran (GOI) employed a years-long malware campaign that targeted Iranian dissidents, journalists, and international companies in the travel sector. Concurrent with OFAC's action, the U.S. Federal Bureau of Investigation (FBI) released detailed information about APT39 in a public intelligence alert.

"The Iranian regime uses its Intelligence Ministry as a tool to target innocent civilians and companies, and advance its destabilizing agenda around the world," said Treasury Secretary Steven T. Mnuchin. "The United States is determined to counter offensive cyber campaigns designed to jeopardize security and inflict damage on the international travel sector."

These individuals and entities were designated pursuant to Executive Order (E.O.) 13553.

Rana advances Iranian national security objectives and the strategic goals of Iran's Ministry of Intelligence and Security (MOIS) by conducting computer intrusions and malware campaigns against perceived adversaries, including foreign governments and other individuals the MOIS considers a threat. APT39 is being designated pursuant to E.O. 13553

for being owned or controlled by the MOIS, which was previously designated on February 16, 2012 pursuant to Executive Orders 13224, 13553, and 13572, which target terrorists and those responsible for human rights abuses in Iran and Syria, respectively.

Rana is being designated pursuant to E.O. 13553 for being owned or controlled by MOIS. Forty-five cyber actors are also being designated pursuant to E.O. 13553 for having materially assisted, sponsored, or providing financial, material, or technological support for, or goods or services to or in support of the MOIS. The identification of these individuals and their roles related to MOIS and APT39 comes as the result of a long-term investigation conducted by the FBI Boston Division.

The 45 designated individuals served in various capacities while employed at Rana, including as managers, programmers, and hacking experts. These individuals provided support for ongoing MOIS cyber intrusions targeting the networks of international businesses, institutions, air carriers, and other targets that the MOIS considered a threat.

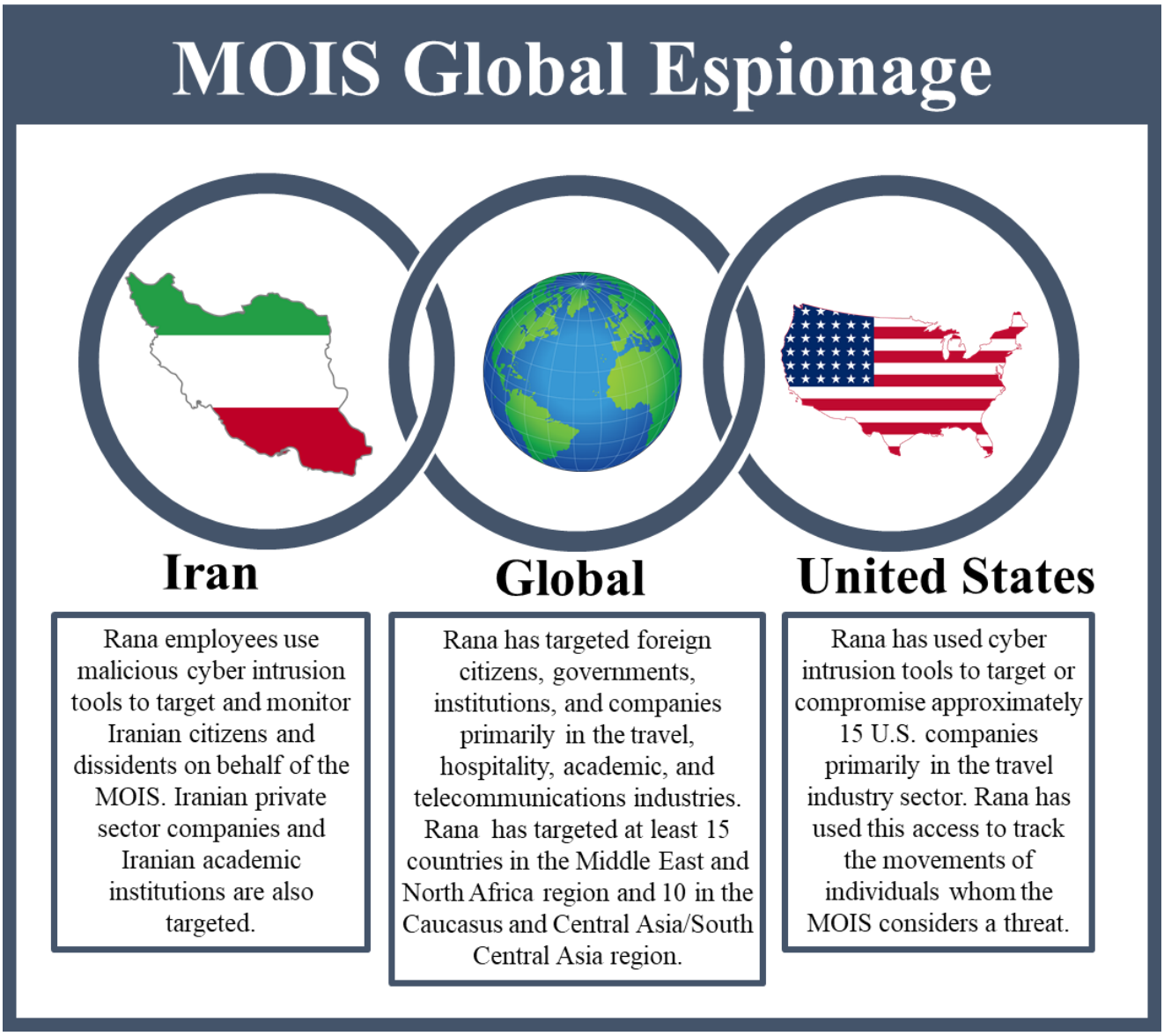
The FBI advisory, also being released today, details eight separate and distinct sets of malware used by MOIS through Rana to conduct their computer intrusion activities. This is the first time most of these technical indicators have been publicly discussed and attributed to MOIS by the U.S. government. By making the code public, the FBI is hindering MOIS's ability to continue their campaign, ending the victimization of thousands of individuals and organizations around the world.

"The FBI, through our Cyber Division, is committed to investigating and disrupting malicious cyber campaigns, and collaborating with our U.S. government partners to impose risks and consequences on our cyber adversaries. Today, the FBI is releasing indicators of compromise attributed to Iran's MOIS to help computer security professionals everywhere protect their networks from the malign actions of this nation state," said FBI Director Christopher Wray. "Iran's MOIS, through their front company Rana, recruited highly educated people and turned their cyber talents into tools to exploit, harass, and repress their fellow citizens and others deemed a threat to the regime. We are proud to join our partners at the Department of Treasury in calling out these actions. The sanctions announced today hold these 45 individuals accountable for stealing data not just from dozens of networks here in the United States, but from networks in Iran's neighboring countries and around the world."

Rana Intelligence Computing Company: MOIS and APT39's Disguise

On the left, Rana's logo is detailed. Rana is a front company for APT39 actors working for the Iranian MOIS, the logo for which is detailed on the right.

The MOIS, camouflaged as Rana, has played a key role in the GOI's abuse and surveillance of its own citizens. Through Rana, on behalf of the MOIS, the cyber actors designated today used malicious cyber intrusion tools to target and monitor Iranian citizens, particularly dissidents, Iranian journalists, former government employees, environmentalists, refugees, university students and faculty, and employees at international nongovernmental organizations. Some of these individuals were subjected to arrest and physical and psychological intimidation by the MOIS. APT39 actors have also victimized Iranian private sector companies and Iranian academic institutions, including domestic and international Persian language and cultural centers. Rana has also targeted at least 15 countries in the Middle East and North Africa region.



Rana's targeting has been both internal to Iran and global in scale, including hundreds of individuals and entities from more than 30 different countries across Asia, Africa, Europe, and North America. Rana has used malicious cyber intrusion tools to target or compromise approximately 15 U.S. companies primarily in the travel sector. MOIS cyber actors targeted a wide range of victims, including global airlines and foreign intelligence services. The unauthorized access obtained by the individuals designated today allow the MOIS to track individuals whom it considers a threat.

As a result of today's action, all property and interests in property of the individuals and entities above, and of any entities that are owned, directly or indirectly, 50 percent or more by them, individually, or with other blocked persons, that are in the United States or in the possession or control of U.S. persons, are blocked and must be reported to OFAC. Unless authorized by a general or specific license issued by OFAC or otherwise exempt, OFAC's regulations generally prohibit 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. 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.

View identifying information on the entites and individuals designated today.

View the FBI’s Public Intelligence Alert on APT39.

####

Use featured image

Off