

Treasury Targets Supporters of Iran's Islamic Revolutionary Guard Corps and Networks Responsible for Cyber-Attacks Against the United States

9/14/2017

Washington – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated 11 entities and individuals for engaging in support of designated Iranian actors or malicious cyber-enabled activity. The persons sanctioned in today's actions include one entity engaging in activities in support of Iran's Islamic Revolutionary Guard Corps (IRGC) ballistic missile program; two Ukraine-based entities providing support to designated airlines, including one affiliated with the IRGC-Qods Force (IRGC-QF); and two Iran-based networks responsible for malicious cyber-enabled attacks against the U.S. financial system. Today's actions were taken pursuant to Executive Order (E.O.) 13382, which targets proliferators of weapons of mass destruction and their means of delivery and their supporters; E.O. 13224, which targets terrorists and those providing support to terrorists and acts of terrorism; and E.O. 13694, which targets persons engaging in significant malicious cyber-enabled activities.

"Treasury will continue to take strong actions to counter Iran's provocations, including support for the IRGC-Qods Force and terrorist extremists, the ongoing campaign of violence in Syria, and cyber-attacks meant to destabilize the U.S. financial system," said Treasury Secretary Steven T. Mnuchin. "These sanctions target an Iranian company providing material support to the IRGC's ballistic missile program, airlines that support the transport of fighters and weapons into Syria, and hackers who execute cyber-attacks on American financial institutions."

As a result of today's actions, all property and interests in property of those designated subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them. In addition, foreign financial institutions that facilitate significant transactions for, or persons that provide material or certain other support to, the entities and individuals designated today risk exposure to sanctions that could sever their access to the U.S. financial system or block their property and interests in property under U.S. jurisdiction.

Sadid Caran Saba Engineering Company (SABA)

Today, OFAC sanctioned Iran-based SABA for proliferation activities related to Iran's ballistic missile program. SABA has provided, or attempted to provide, financial, material, technological, or other support for, or goods or services in support of, the IRGC. The IRGC was designated pursuant to E.O. 13382 on October 25, 2007, for being a key Iranian entity of proliferation concern. The IRGC has been outspoken about its willingness to proliferate ballistic missiles.

Since at least 2014, SABA has entered into contracts to procure and install numerous, multi-ton explosion-proof crane systems for the IRGC Research and Self-Sufficiency Jihad Organization (RSSJO). The RSSJO, which is responsible for researching and developing ballistic missiles on behalf of the IRGC, was designated pursuant to E.O. 13382 on July 18, 2017.

Khors Aircompany and Dart Airlines

OFAC also designated Ukraine-based Khors Aircompany and Dart Airlines pursuant to the global terrorism E.O. 13224 for aiding designated Iranian and Iraqi airlines through the provision of aircraft and services. Both Khors Aircompany and Dart Airlines help Iran's Caspian Air and Iraq's Al-Naser Airlines procure U.S.-origin aircraft, as well as crew and services.

Iran-based Caspian Air was designated pursuant to E.O. 13224 on August 29, 2014, for providing support to IRGC elements by transporting personnel and illicit material, including weapons, from Iran to Syria. Al-Naser Airlines was designated pursuant to E.O. 13224 on May 21, 2015, for transferring at least eight Airbus A340 and one Airbus A320 aircraft to Mahan Air in Iran. Iranian airline Mahan Air was designated pursuant to E.O. 13224 on October 12, 2011, for providing financial, material, and technological support to the IRGC-QF.

Khors Aircompany provides material support and services to Caspian Air through a sub-wet-lease of a U.S.-origin aircraft. As recently as late 2016, Khors Aircompany provided material support and services to Al-Naser Airlines through the sub-wet-lease of a separate aircraft. A wet lease is any leasing arrangement whereby a person agrees to provide an entire aircraft and at least one crew member.

Dart Airlines is being designated for providing material support and services to Caspian Air through sub-wet-leases of U.S.-origin aircraft. Dart Airlines has also previously provided the sub-wet-lease of separate U.S.-origin aircraft to Al-Naser Airlines. Additionally, Khors Aircompany provided the wet lease and sale of multiple aircraft worth millions of dollars and services related to aircraft leases to Mahan Air. Dart Airlines has also provided to Mahan Air U.S.-origin aircraft and parts, which Dart Airlines procured through front companies.

ITSec Team and Mersad Co. Associated Individuals

OFAC designated private Iranian computer security company ITSec Team pursuant to E.O. 13694 for causing a significant disruption to the availability of a computer or network of computers. Between approximately December 2011 and December 2012, ITSec Team planned and executed distributed denial of service (DDoS) attacks against at least nine large U.S. financial institutions, including top U.S. banks and U.S. stock exchanges. During that time, ITSec Team performed work on behalf of the Iranian Government, including the IRGC.

OFAC also designated three Iranian nationals for acting for or on behalf of ITSec Team. Ahmad Fathi was responsible for supervising and coordinating ITSec Team's DDoS attacks against the U.S. financial sector. Amin Shokohi, a computer hacker who worked for ITSec Team, helped build the botnet that ITSec Team used in its DDoS attacks against U.S. financial institutions. Hamid Firoozi, a network manager at ITSec Team, procured computer servers for the botnet that ITSec Team used in its DDoS activities targeting the U.S. financial sector.

Additionally, OFAC today designated four Iranian nationals pursuant to E.O. 13694 for causing a significant disruption to the availability of a computer or network of computers while working for Mersad Co., a private computer security company based in Iran that was affiliated with the IRGC.

Sadegh Ahmadzadegan was responsible for managing the Mersad Co. botnet, which was used to target 24 corporations in the U.S. financial sector during DDoS attacks in 2012 and 2013. Sina Keissar, along with others at Mersad Co., placed malicious computer scripts on compromised computers and computer servers within the Mersad Co. botnet that performed several functions during those DDoS attacks against the U.S. financial sector. Keissar also procured U.S.-based computer servers used by Mersad Co. to access and manipulate the Mersad Co. botnet and performed preliminary testing of the same botnet prior to its use in the DDoS attacks. Omid Ghaffarinia, along with others at Mersad Co., developed malware and computer scripts, which they installed on the compromised computers and computer servers that constituted the Mersad Co. botnet, which allowed for remote access and control of the compromised computers. Nader Saedi, along with others at Mersad Co., planned and

Iran Designations; Non-proliferation Designations; Counter Terrorism Designations; Cyber-related Designations;

9/14/2017

OFFICE OF FOREIGN ASSETS CONTROL

Specially Designated Nationals List Update

The following individuals have been added to OFAC's SDN List:

AHMADZADEGAN, Sadegh (a.k.a. "el_nitr0jen"; a.k.a. "Nitr0jen"; a.k.a. "Nitr0jen26"); DOB 27 Oct 1992; nationality Iran; Additional Sanctions Information - Subject to Secondary Sanctions (individual) [CYBER2].

FATHI, Ahmad (a.k.a. "M3HRAN"; a.k.a. "M3S3C3"; a.k.a. "MOHAMMADI, Farhad"), No. 12, Saremi Street, Nejatollahi Street, Tehran, Iran; Gharani St., Besharat St., Saremi Alley, No. 12, Tehran, Tehran, Iran; DOB 11 Sep 1978; nationality Iran; Additional Sanctions Information - Subject to Secondary Sanctions; Identification Number 5725729366035 (Iran) (individual) [CYBER2] (Linked To: ITSEC TEAM).

FIROOZI, Hamid (a.k.a. "H4mid@Tm3l"); DOB 06 Aug 1981; alt. DOB 23 Jun 1981; alt. DOB 01 Jan 1980; nationality Iran; Additional Sanctions Information - Subject to Secondary Sanctions (individual) [CYBER2] (Linked To: ITSEC TEAM).

GHAFFARINIA, Omid; DOB 24 Jun 1990; nationality Iran; Additional Sanctions Information - Subject to Secondary Sanctions (individual) [CYBER2].

KEISSAR, Sina (a.k.a. "sina_molove"); DOB 20 May 1990; nationality Iran; Additional Sanctions Information - Subject to Secondary Sanctions (individual) [CYBER2].

SAEDI, Nader (a.k.a. "tahersaedi"; a.k.a. "turk_server"; a.k.a. "turkserver"); DOB 22 Feb 1990; nationality Iran; Additional Sanctions Information - Subject to Secondary Sanctions (individual) [CYBER2].

SHOKOHI, Amin (a.k.a. "Pejvak"); DOB 11 Jul 1990; alt. DOB 11 Jul 1989; alt. DOB 05 Aug 1981; POB Karaj, Iran; Additional Sanctions Information - Subject to Secondary Sanctions (individual) [CYBER2] (Linked To: ITSEC TEAM).

The following entities have been added to OFAC's SDN List:

DART AIRLINES (a.k.a. DART AIRCOMPANY; a.k.a. DART UKRAINIAN AIRLINES; a.k.a. TOVARYSTVO Z OBMEZHENOYU VIDPOVIDALNISTYU 'DART'; a.k.a. "DART, LLC"; a.k.a. "DART, TOV"), 26a, Narodnogo Opolchenyia Street, Kiev 03151, Ukraine; Kv. 107, Bud. 15/2 Vul.Shuliavska, Kyiv 01054, Ukraine; Ave. Vozdukhoflostsky 90, Kiev 03036, Ukraine; Additional Sanctions Information - Subject to Secondary Sanctions; Tax ID No. 252030326052 (Ukraine); Government Gazette Number 25203037 (Ukraine) [SDGT] [IFSR].

assisted in the same DDoS attacks. Saedi wrote computer scripts used to locate and exploit vulnerable servers to help build the Mersad Co. botnet used in the attacks.

On March 24, 2016, the Department of Justice announced that a grand jury in the Southern District of New York indicted the seven ITSec Team and Mersad Co. associated individuals being designated today.

ITSEC TEAM (a.k.a. AMN PARDAZESH KHARAZMI; a.k.a. "IT SECURITY & PENETRATION TESTING TEAM"; a.k.a. "POOYA DIGITAL SECURITY GROUP"), Unit 2, No. 129, Mir Ali Akbari St, Motahari Avenue, Tehran, Iran; Additional Sanctions Information - Subject to Secondary Sanctions [CYBER2].

KHORS AIRCOMPANY (a.k.a. AVIAKOMPANIYA KHORS, TOV; a.k.a. KHORS AIR; a.k.a. TOVARYSTVO Z OBMEZHENOYU VIDPOVIDALNISTYU 'AVIAKOMPANIYA 'KHORS'; a.k.a. "HORS AIRLINES LTD."), 60 Volunska Street, Kiev 03151, Ukraine; Bud. 34 Bul.Lesi Ukrainky, Kyiv 01133, Ukraine; Lesi Ukraini Bulvar 34, Kiev 252133, Ukraine; Additional Sanctions Information - Subject to Secondary Sanctions; Government Gazette Number 04937956 (Ukraine) [SDGT] [IFSR].

SADID CARAN SABA ENGINEERING COMPANY (a.k.a. SADID CARAN SABA COMPANY; a.k.a. SADID CARAN SABA ENG. CO.; a.k.a. "S.C. SABA ENG CO."; a.k.a. "SABA CRANE"), Unit 501, No. 17, Beside Samen Drugstore, Hakim West Highway, Tehran, Iran; No. 1401, Cross 5th Golazin and 2nd Golara, Eshtehard Industrial Zone, Eshtehard, Alborz, Iran; Additional Sanctions Information - Subject to Secondary Sanctions [NPWMD] [IFSR].