TechXplore

US sanctions on Iranian hackers highlight growing concern about the Islamic Republic's cyberwarriors

May 1 2024, by Vasileios Karagiannopoulos and Iain Reid

Credit: CC0 Public Domain

A feature of the simmering tensions between the US, Israel and Iran has been not just the tit-for-tat missile and drone strikes and assassinations, but accusations of cyberwarfare waged by Iran.

On April 23, the US Treasury announced it was sanctioning two Iranian companies and four Iranian individuals for conducting malicious cyberattacks against more than a dozen US companies and government organizations. The Treasury alleged that these organizations and individuals had conducted spear phishing, malware and ransomware attacks, which it said aimed to destabilize important national infrastructure in the US.

This followed an announcement in February that it was sanctioning a group of Iranian hackers linked to the country's military for what it described as "unconscionable and dangerous" attacks on water and wastewater systems in the US.

Identifying the people behind these attacks can often be challenging. But the US is claiming the hacks are perpetrated by "front companies" and hackers operating for Iran's Islamic Revolutionary Guard Corps Cyber Electronic Command (IRG-CEC).

The main sanctioned company, Mehrsam Andisheh Saz Nik (MASN) is identified as regularly launching what is known in the cyber world as advanced persistent threat (APT) attacks.

APTs are long-term attacks on high-value targets such as large companies and government organizations.

MASN was linked in 2019 by cybersecurity giant Symantec (now Gen Digital Inc) with a group it called Tortoiseshell. Symantec said

Tortoiseshell had been active in the Middle East since at least July 2018. It was linked with cyberattacks against Saudi Arabian IT providers and Israeli shipping, logistics and financial services companies.

Much less is known about the actions of the second sanctioned company, Dadeh Afzar Arman. But from information available online, it claims to be a software and web development company based in Tehran.

Alongside the sanctions, the US government is offering a reward of US$10 million (£8 million) and a "plane ticket to somewhere new" for anyone having more information about the hackers in question.

The recent announcement follows a wider pattern of the US naming and shaming cybercrime groups it has identified and linked to rogue activity.

By publicly naming these groups, in this instance, the US says it wants to inform the Iranian public that the IRG-CEC is using these companies for launching illegal cyber-attacks against international targets. But efforts by the US government to deter state-backed hackers working for governments including Iran, China and Russia have yet to bear fruit.

To date, no such suspects have ever been apprehended to stand trial in the US.

War in all but name

Washington and Tehran have been at loggerheads since the 1979 revolution. The US imposed sanctions against the Islamic Republic when militant students overran the US embassy in the Iranian capital in November 1979 sparking the 400-day hostage crisis.

They have endured since with various levels of intensity. This, despite efforts by the Obama administration to move towards normalization, with the signing in 2015 of an agreement under which Iran agreed to limit its nuclear program in return for an easing of sanctions.

Donald Trump pulled the US out of the agreement in 2018.

The first major act of cyberwar between the two countries was, in fact, the Stuxnet "worm", a joint venture between the US and Israel. Stuxnet drove a wrecking ball through Iran's nuclear facilities in 2010. The virus manipulated control systems and caused centrifuges to overheat. This caused serious damage and set Iran's nuclear program back by years.

This incident marked the beginning of an on-again, off-again conflict between the two countries. In 2016, the US Justice Department indicted seven Iranian computer specialists. It accused the group of hacking into dozens of American banks as well as trying to take over the controls of a small dam in a suburb of New York.

This was the first time the US had publicly accused the Iranian Revolutionary Guard Corps (IRGC) of involvement in cyber-attacks. But it is thought Iran had been targeting the US financial systems with what the FBI called a "systematic campaign of distributed denial of service (DDoS) attacks" since 2011.

After the US assassinated top Iranian general, Qasem Soleimani, in 2020, the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency published an official guidance, warning US companies to prepare for a possible wave of cyber-attacks from Iran.

At the time the threat was talked down. One expert wrote in the New York Times that: "Tehran is a capable and prolific actor in the realm of cyberwarfare, but it has no proven ability to create large-scale physical damage through cyberoperations."

Growing threat

However, in recent years Iran seems to have further developed its cyber capabilities. In 2023, the Office of the Director of National Intelligence's annual threat assessment declared that: "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of US and allied networks and data."

Meanwhile, the National Cyber Power Index ranked Iran as tenth among the 30 countries it investigated in 2022 (up from 23rd in 2020). Additionally, in a peer-reviewed article published recently that offers a new global metric for cybercriminality, Iran is ranked 11th in relation to the impact, professionalism and technical skills of cybercriminals operating in the country.

In the increasingly murky margins of a world where cybercriminals and governments can overlap, Iran's increasing sophistication in this field cannot be ignored.

Provided by The Conversation

Citation: US sanctions on Iranian hackers highlight growing concern about the Islamic Republic's cyberwarriors (2024, May 1) retrieved 17 May 2024 from https://techxplore.com/news/2024-05-sanctions-iranian-hackers-highlight-islamic.html