US indicts seven Iranians over hacking banks, dam (Update)

March 24 2016

The United States on Thursday announced computer hacking charges against seven Iranians working for firms linked to the Iranian government, accusing them of infiltrating dozens of American banks and a major New York dam.

The hacking of nearly 50 banks and financial institutions from 2011 to 2013 saw the organizations lose tens of millions of dollars in remediation costs and the dam attack could have imperiled public health, prosecutors said.

It came as the US Treasury named three outfits involved in Iran's ballistic missile program to its sanctions blacklist and one day after a consultant to the Iranian mission at the United Nations was released on a $3 million bond after being charged with conspiracy and money laundering.

The developments cut through hopes eight months ago that the nuclear deal reached between Iran, the United States and five other nations would put Tehran and Washington relations on a firmer footing.

The hacking suspects were employed by two private computer security companies in Iran, named as ITSec Team and Mersad Co., that performed work on behalf of the government, including the powerful Revolutionary Guard Corps, the US said.

In what prosecutors called "a frightening new frontier for cybercrime,"

one suspect allegedly hacked into the system that controls the Bowman Avenue Dam in Rye, New York, less than 30 miles (50 kilometers) north of Manhattan.

"Although no actual harm resulted from that infiltration, the potential havoc of such a hack of American infrastructure could wreak is scary to think about," Manhattan chief prosecutor Preet Bharara told reporters.

Attorney General Loretta Lynch announced the charges after an unsealed three-count indictment from a New York grand jury detailed how the defendants allegedly disabled servers to stop businesses from working online.

The New York Stock Exchange, NASDAQ, American Express, Bank of America, J.P. Morgan Chase, Citibank and HSBC were among those affected, according to the 17-page indictment.

Damaging free markets

Thursday's announcement comes one month after President Barack Obama unveiled a $19 billion cybersecurity action plan as his intelligence chief warned of the growing risks from new technologies that open more doors to hackers.

"Today we have unsealed an indictment against seven alleged experienced hackers employed by computer security companies working on behalf of the Iranian government, including the Revolutionary Guard Corps," Lynch said.

Founded in the aftermath of the 1979 revolution, the Revolutionary Guards is a hugely powerful and influential security institution in Iran responsible for defending the Islamic republic against domestic and foreign threats.

"Online services were disrupted. Hundreds of thousands of Americans were unable to access bank accounts online. These attacks were relentless, systematic and widespread," Lynch told reporters.

"We believe they were conducted with the sole purpose of undermining the companies and damaging America's free markets."

US prosecutors did not specify whether the Iranian government or the Revolutionary Guards had ordered the attacks. The defendants live in Iran and it is difficult to foresee when or how they could appear in a US court.

Prosecutors said the hacking took place between December 2011 and May 2013.

The defendants were named as Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan (who went by the name "Nitr0jen26"), Omid Ghaffarinia (also known as "PLuS"), Sina Keissar and Nader Saedi, whose moniker was "Turk Server."

Bowman Dam hack

Firoozi was also charged with using a computer in Iran to hack into the controls of the Bowman Dam, causing more than $30,000 in remediation costs, between August and September 2013.

It would have allowed him to operate the sluice gates—which regulate the water stored—had the gates not been disconnected for maintenance, prosecutors said.

"But for that fact, that access would have given the defendant the access to control water levels, flow rates, an outcome that could have posed a clear and present danger to the public health and safety of Americans,"

said Lynch.

On Thursday, the US Treasury also named units involved in Iran's ballistic missile program to its sanctions blacklist, two weeks after the country ran missile tests that Washington labeled "provocative and destabilizing."

Among those sanctioned were the Al-Ghadir Missile Command of the Revolutionary Guard—the corps that manages the country's ballistic missiles.

Meanwhile, in New York Wednesday, US citizen Ahmad Sheikhzadeh, a consultant to the Iranian mission to the United Nations, was freed from custody on a $3 million bond.

He is charged with five counts of falsifying income tax returns, as well as conspiring to violate laws about doing business with Iran and money laundering.

Cyber security company Norse and the American Enterprise Institute think tank warned last year that Iran has launched increasingly sophisticated digital attacks and spying on US targets.