Cybersecurity firm: More Iran hacks as US sanctions loomed

September 18 2018, by Jon Gambrell

Alister Shepherd, the director of a subsidiary of the cybersecurity firm FireEye, gestures during a presentation about the APT33 hacking group, which his firm suspects are Iranian government-aligned hackers, in Dubai, United Arab Emirates, Tuesday, Sept. 18, 2018. FireEye warned Tuesday that Iranian government-aligned hackers have stepped up their efforts in the wake of President Donald Trump pulling America from the nuclear deal. (AP Photo/Jon Gambrell)

An Iranian government-aligned group of hackers launched a major campaign targeting Mideast energy firms and others ahead of U.S. sanctions on Iran, a cybersecurity firm said Tuesday, warning further attacks remain possible as America re-imposes others on Tehran.

While the firm FireEye says the so-called "spear-phishing" email campaign only involves hackers stealing information from infected computers, it involves a similar type of malware previously used to inject a program that destroyed tens of thousands of terminals in Saudi Arabia.

The firm warns that raises the danger level ahead of America re-imposing crushing sanctions on Iran's oil industry in early November.

"Whenever we see Iranian threat groups active in this region, particularly in line with geopolitical events, we have to be concerned they might either be engaged in or pre-positioning for a disruptive attack," Alister Shepherd, a director for a FireEye subsidiary, told The Associated Press.

Iran's mission to the United Nations did not immediately respond to a request for comment on FireEye's report.

FireEye, which often works with governments and large corporations, refers to the group of Iranian hackers as APT33, an acronym for "advanced persistent threat." APT33 used phishing email attacks with fake job opportunities to gain access to the companies affected, faking domain names to make the messages look legitimate. Analysts described the emails as "spear-phishing" as they appear targeted in nature.

FireEye first discussed the group last year around the same time. This year, the company briefed journalists after offering presentations to potential government clients in Dubai at a luxury hotel and yacht club on the man-made, sea-horse-shaped Daria Island.

While acknowledging their sales pitch, FireEye warned of the danger such Iranian government-aligned hacking groups pose. Iran is believed to be behind the spread of Shamoon in 2012, which hit Saudi Arabian Oil Co. and Qatari natural gas producer RasGas. The virus deleted hard drives and then displayed a picture of a burning American flag on computer screens. Saudi Aramco ultimately shut down its network and destroyed over 30,000 computers.

A second version of Shamoon raced through Saudi government computers in late 2016, this time making the destroyed computers display a photograph of the body of 3-year-old Syrian boy Aylan Kurdi, who drowned fleeing his country's civil war.

But Iran first found itself as a victim of a cyberattack. Iran developed its cyber capabilities in 2011 after the Stuxnet computer virus destroyed thousands of centrifuges involved in Iran's contested nuclear program. Stuxnet is widely believed to be an American and Israeli creation.

APT33's emails haven't been destructive. However, from July 2 through July 29, FireEye saw "a by-factors-of-10 increase" in the number of emails the group sent targeting their clients, Shepherd said. The actual number of attacks likely was even larger as FireEye's figures only include their own clients.

The emails, pretending to be from a Mideast oil and gas company, targeted organizations in the Mideast, North America and Japan. The recipients included companies involved in the oil and gas industry, utilities, insurance, manufacturing and education, FireEye said.

Several clues lead FireEye to believe APT33 has the backing of Iran's government. The hackers uses Farsi, work an Iranian workweek of Saturday through Wednesday and correspond during Iranian office hours, FireEye said. Its list of targets also includes American firms in

petrochemicals and aviation, as well as allied nations, like members of the six-nation Gulf Cooperation Council, Shepherd said. The GCC encompasses Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates.

"Since we started tracking APT33 in 2013, their sophistication has definitely improved. . We wouldn't put them on the same level as some of the more-sophisticated Russian groups, for instance, in terms of capability," Shepherd told the AP. "But they are a very capable group and they manage to meet their objectives, which is to compromise institutions in both the government and private sector and steal data."