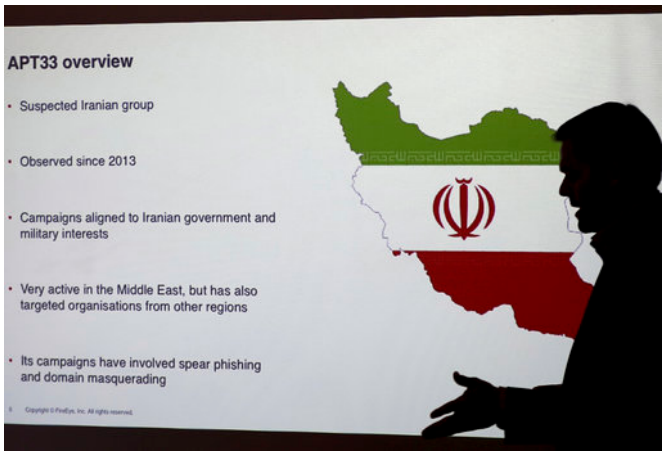
Report: Iran group hacks aviation, petrochemical industries

20 September 2017, by Jon Gambrell



Stuart Davis, a director at one of FireEye's subsidiaries speaks to journalists about the techniques of Iranian hacking, Wednesday, Sept. 20, 2017, in Dubai, United Arab Emirates. A new report by FireEye, a cybersecurity firm, warned that a suspected group of hackers in Iran are targeting the aviation and petrochemical industries in Saudi Arabia, the U.S. and South Korea. (AP Photo/Kamran Jebreili)

A group of hackers suspected of working in Iran for its government is targeting the aviation and petrochemical industries in Saudi Arabia, the U.S. and South Korea, a cybersecurity firm warned Wednesday.

The report by FireEye also said the suspected Iranian hackers left behind a new type of malware that could have been used to destroy the computers it infected, an echo of two other Iran-attributed cyberattacks targeting Saudi Arabia in 2012 and 2016 that destroyed systems.

Iran's office at the United Nations did not immediately respond to a request for comment Wednesday and its state media did not report on the claims. However, suspected Iranian hackers long have operated without caring if people found it was them or if there would be consequences, making them incredibly dangerous, said Stuart Davis, a director at one of FireEye's subsidiaries.

"Today, without any repercussions, a neighboring country can compromise and wipe out 20 institutions," Davis said.

FireEye, which often works with governments and large corporations, refers to the group 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 it look like the messages came from Boeing Co. or defense contractors.

Stuart Davis, a director at one of FireEye's subsidiaries, stands in front of a map of Iran as he speaks to journalists about the techniques of Iranian hacking, Wednesday, Sept. 20, 2017, in Dubai, United Arab Emirates. A new report by FireEye, a cybersecurity firm, warned that a suspected group of hackers in Iran are targeting the aviation and petrochemical industries in Saudi Arabia, the U.S. and South Korea. (AP Photo/Kamran Jebreili)

The hackers remained inside of the systems of those affected for "four to six months" at a time, able to steal data and leaving behind the malware that FireEye refers to as Shapeshifter. The coding contains Farsi-language references, the official language of Iran, FireEye said.

Timestamps in the code also correspond to hackers working from Saturday to Wednesday, the Iranian workweek, Davis said. The programs used in the campaign are popular with Iranian coders, servers were registered via Iranian companies and one of the spies appears to have accidentally left his online handle, "xman_1365_x," in part of the code.

That name "shows up all over Iranian hacker forums," FireEye's John Hultquist said. "I don't think they're worried about being caught. ... They just don't feel like they have to bother."

The Associated Press was able to find other clues pointing to an Iranian nexus.

One of the malicious websites used in the operation was registered in February 2016 via an Iranian company called Server Pars, the firm's chief executive, Ali Mehrabian, said. Mehrabian declined to make the customer's name available publicly, citing his company's privacy policy, but said they had a Tehran address.

Stuart Davis, a director at one of FireEye's subsidiaries, blocks part of a projection as he speaks to journalists about the techniques of Iranian hacking, Wednesday, Sept. 20, 2017, in Dubai, United Arab Emirates. A new report by FireEye, a cybersecurity firm, warned that a suspected group of hackers in Iran are targeting the aviation and petrochemical industries in Saudi Arabia, the U.S. and South Korea. (AP Photo/Kamran Jebreili)

The hacker known as "xman" did not return emails seeking comment.

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.

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 having 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. Suspicion again fell on Iran.

FireEye's report said it believed APT33 "is likely in search of strategic intelligence capable of benefiting a government or a military sponsor."

High on the list of any potential suspects within Iran would be its paramilitary Revolutionary Guard. U.S. prosecutors in March 2016 accused hackers associated to Guard-linked companies of attacking dozens of banks and a small dam near New York City. Hackers linked to the Guard also have been suspected of targeting the email and social-media accounts of Obama administration officials.