Experts: Software theft shows threat of mercenary hackers

July 26 2017, by Wilson Ring

This image released by the FBI shows a poster containing a photo of Mohammad Reza Rezakhah, who the agency is seeking to apprehend on charges of conspiring with others to hack into a Vermont defense contractor and to steal

sophisticated software, outlined in an indictment unsealed Monday, July 14, 2017. (FBI via AP)

On an October morning in 2012, the system administrator of a tiny Vermont defense contractor arrived at work to find the business' computers had been hacked and a sophisticated software program stolen. Prosecutors later concluded the thieves were a group of Iranians who sold the software to organizations within the Iranian government.

The hack, revealed in an indictment unsealed last week, shows that mercenary hackers who sell stolen data to friendly governments are a growing threat to defense contractors, experts say.

"They are essentially nonsanctioned espionage groups," said Brian Wallace, the lead security data scientist for the Irvine, California-based company computer security company Cylance Inc. "The government doesn't create them, they don't own them. They operate and get almost of their income from the government."

The South Burlington company, Arrow Tech Associates, makes software used to monitor projectiles in flight.

Arrow Tech President Charles Hillman said the firm was able to track the hackers' every keystroke, which helped the FBI trace the intrusion to three Iranians.

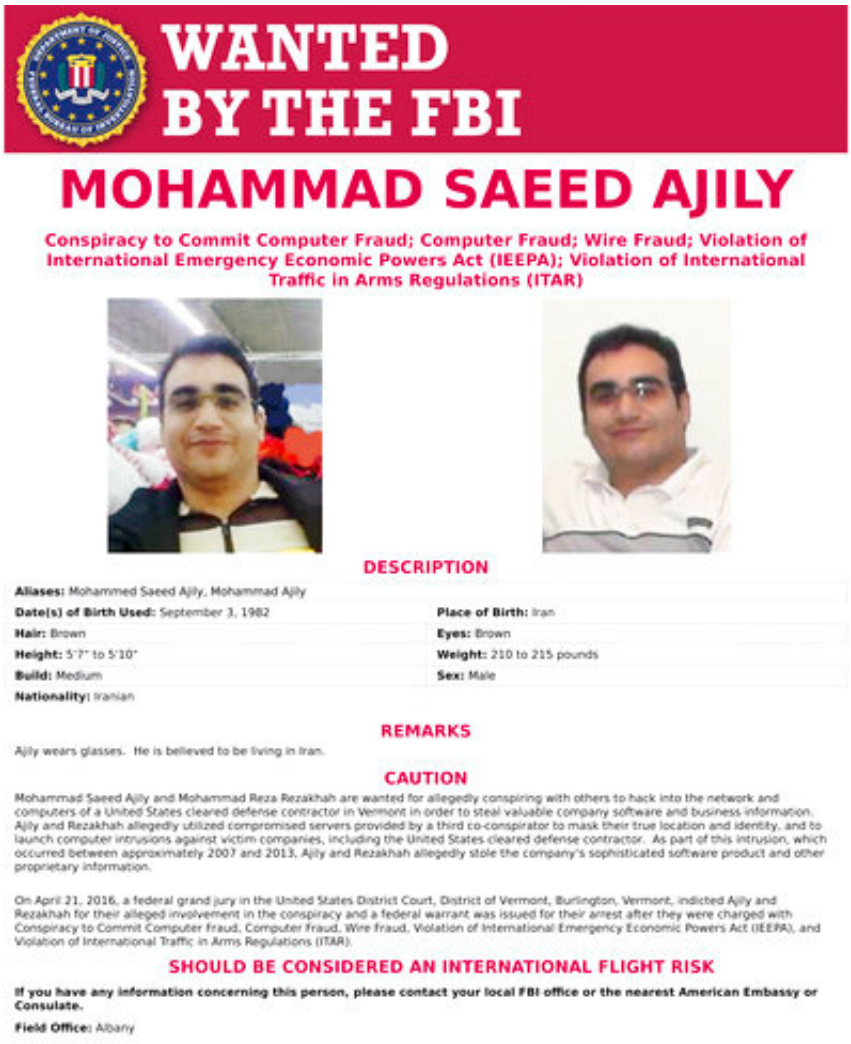
"We were very impressed with what they got done in just a few hours," he added.

Iranian officials in Washington referred an emailed question on the issue from The Associated Press to "the pertinent department." There was no

further reply.

The eight-count indictment released last week alleged that from at least 2007 through May 2013 the three men broke into computers in "Vermont and elsewhere." It said the group also stole software from an unidentified Western aerospace company in July 2012.

Arrest warrants were issued for two of the men: Mohammed Reza Rezakhah, 39, and Mohammed Saeed Ajily, 35. They were indicted in April 2016, and FBI wanted posters say the two men are believed to be in Iran.



This image released by the FBI shows a poster containing a photo of Mohammad Saeed Ajily, who the agency is seeking to apprehend on charges of conspiring with others to hack into a Vermont defense contractor and to steal sophisticated software, outlined in an indictment unsealed Monday, July 14, 2017. (FBI via AP)

The third man, Nima Golestaneh, had been indicted in 2013, but the case was sealed until February 2015, when he was brought to the U.S. from Turkey.

Golestaneh pleaded guilty in Vermont in December 2015. The next month, he was pardoned by then-President Barack Obama as part of a prisoner swap with Iran that included the release of Washington Post reporter Jason Rezaian and former U.S. Marine Amir Hekmati.

Such hacks are a growing threat for defense contractors, said Phil Sussman, the president of Norwich University Applied Research Institutes, which works on cyber security issues at the private Vermont military college.

"In the last five or six years anyways, it has been common knowledge that these kinds of services are readily available on the dark web and could be purchased," Sussman said.

Wallace said such arrangements are not exclusive to Iran.

"We can see a lot of similar activities coming out of Russia where you had independent hacking groups that don't work directly for the Russian government, but they do have very strong ties to the Russian government," he said.

Arrow Tech, which employs fewer than 10 people, sells software that measures the performance of projectiles. "Anything that comes out of a gun tube is in our wheelhouse," Hillman said.

It's unclear if the stolen ballistics software, used to analyze and design bullets and GPS-guided artillery shells, ever worked for the hackers. Hillman said he doubts the hackers could have even unlocked the software, because it requires a physical key, called a dongle, to operate.

Hillman said Arrow Tech has had to assure some of its 600 licensed customers in more than two dozen countries that their information is safe.

"Their information is not stored on these servers that are accessible from the outside," Hillman said. "I can't even access our servers from outside the building."