Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Iranian Hacking Charges Give US Cos. Cybersecurity Edge

By **Allison Grande**

Law360, New York (March 25, 2016, 9:49 PM ET) -- Federal prosecutors stepped up their efforts to name and shame foreign hackers who target U.S. companies by recently charging seven individuals with purported ties to the Iranian government with orchestrating cyberattacks against banks, stock exchanges and a New York dam, an escalation that provides businesses with valuable insights that can be used to better defend against future incidents.

In an indictment unsealed Thursday, the U.S. Department of Justice leveled computer hacking charges against seven individuals who were employed by two private security companies, ITSecTeam and Mersaud Co., that performed work on behalf of the Iranian government.

The charges stemmed from their alleged involvement in an extended campaign carried out between December 2011 and May 2013 to disable the operations of banks and stock exchanges, including Bank of America, ING Bank, PNC Bank, Nasdaq, the New York Stock Exchange, Capital One Bank, BB&T Bank, U.S. Bank and AT&T. One of the defendants was also accused of accessing a computer that controls the Bowman Dam in Rye, New York.

While the hackers remain at large, several former federal prosecutors told Law360 that the government's decision to go public with the allegations and provide a host of specifics about the motives and methods behind the attacks not only sends a strong message about the seriousness with which the Justice Department is pursuing such claims, but also provides assurance to U.S. companies struggling with how to fend off similar threats.

"Taking any mystery out of cyberhacking and these sorts of events for businesses across the spectrum is a positive thing because so much has been shrouded in secrecy or not publicly aired, so the more information that is available to folks, the more willing they are to come forward and the more steps they are going to be able to take to protect themselves given the experiences of their fellow businesses," said Rajesh De, a Mayer Brown LLP partner who most recently served as general counsel at the National Security Agency.

Because fighting well-funded and highly sophisticated nation-state actors is a lofty task for even the most prepared businesses, the ability and willingness of the DOJ to name the hackers and to disclose details about the duration, posture, and methods used to carry out the attack is becoming increasingly important in the battle to outwit the attackers, attorneys say.

"Attribution and the ability to put names and faces to online crimes is the hardest and one of the most critical steps to fighting state-sponsored activities," said Kimberly Peretti, an Alston & Bird LLP partner and

former senior litigator for the DOJ's Computer Crime and Intellectual Property Section. "It not only exposes actors to the sunlight and reduces their ability to operate in the shadows, but it advances the knowledge of this type of activity and gives companies more of an understanding of how they can be targeted."

The indictments also give businesses confidence in their ability to turn to and work with the government to fight the serious and growing threat to the security of their systems and data on the heels of the landmark passage of legislation in December intended to facilitate the sharing of information about cyberthreats between the sectors, attorneys say.

"These kind of indictments bring to the forefront the need to continue to have a public-private sector partnership in defending against activities, and if a company is targeted, to be prepared for how to respond and who they may need to work with in that response," Peretti said.

The federal government in recent years has made a point to make the investigation and prosecution of cybercrimes — especially those carried out by nation-states — a high priority.

In May 2014, prosecutors unsealed an indictment charging five member of the People's Liberation Army with conspiring to hack into the computers of Alcoa Inc., U.S. Steel Corp. and four other companies in the nuclear power, metals and solar power industries to steal sensitive information that would be "useful to their competitors" in China, including state-sponsored enterprises.

While the Chinese indictment involved the theft of trade secrets rather than the brute force attack meant to disrupt critical infrastructure operators that the government has tied to the Iranian defendants, the cases do share many similarities, including that they both send the message that no one is immune from the government's reach.

"These are the types of crimes where anonymity is so pervasive and criminals have thought to be outside the view of authorities, so the more they're exposed, the more that we can put that myth to bed," Peretti said.

The indictments also help to reinforce the government's position that companies who are infiltrated should be considered victims and should not be attacked for coming forward, attorneys say.

"It helps to remind people that this is a criminal act that in some ways in no different than someone walking into the bank and taking someone's money," said Grant Fondo, a Goodwin Procter LLP partner and former assistant U.S. attorney in the Northern District of California.

This attitude also has the potential to trickle down to the class actions and regulatory scrutiny that often follow such incidents, depending on the nature of the allegations being brought against the company, according to attorneys.

"There's an interesting dichotomy right now between very active regulators that are looking at companies' practices from a consumer standpoint to identify whether appropriate data protections are in place, and law enforcement being active on investigating the attacks that are occurring to steal that type of data," Peretti said. "I'm not sure what impact this type of indictment might have on that, but the fact that these attacks are well-orchestrated and very sophisticated is certainly not something to hide and is a fact that could be favorable."

But despite the benefits to be gained from publicly naming and shaming alleged nation-state actors, some

cautioned that the deterrent effect of such an approach may not be as sweeping as U.S. businesses may hope.

While he agreed that the public disclosure of new facts that could help the public gain a better sense of the facts surrounding the attacks and help decrease the likelihood of future incidents was a clear benefit of the indictment, David Hall, a Wiggin and Dana LLP partner and former assistant U.S. attorney, flagged the fact that no arrests were made as particularly troubling.

"This 'blame and shame' approach seems to be a new strategy of the DOJ," Hall said, noting that the indictment of the Chinese hackers nearly two years ago also was not accompanied by any arrests. "While I understand the degree of difficulty with making such arrests, it seems to me that a better approach across the board would be to actually follow through with the prosecution."

As evidence that it is possible for prosecutors to overcome the distance and foreign relations barriers to apprehending suspects in countries such as Iran and China, Hall cited a pair of cases from his more than 20-year career as a federal prosecutor: the apprehension of Chinese software pirate Xiang Li in 2011, and the arrest of Iranian military arms smuggler Amir Hossein Ardebili, who was lured to and captured in the Republic of Georgia in 2007.

"If deterrence were the ultimate point, then what they would really want to do is increase the cost to the hackers of undertaking this kind of illegal activity, and the way to do that is to arrest people and punishing them according to the law," Hall said.

But other former federal prosecutors say that despite the lack of arrests in connection with the last two high-profile indictments, they still severely hinder the future movements of the defendants, who range between 23 and 37 years old and risk arrest if they travel to an area with an extradition agreement with the U.S., a restriction that could make other potential recruits weary to follow in their footsteps.

"The indictments are a way to ratchet up concerns for people in Iran or other countries that may feel immune from government action by saying that if you do this, the government will charge you, which at a minimum may make people a little more nervous about leaving their country," Fondo said.

However the Iranian case ultimately plays out, attorneys predict that the Justice Department will have plenty more opportunities to further refine their approach to nation-state hackers in the months and years ahead.

"I think we're going to see the DOJ be very active on the national security side as well as the criminal side," Peretti said. "They're continuing to devote more resources and prosecutors to both sides and are dedicated to continuing to pursue this growing threat."

The government is represented in the Iranian hacker case by Assistant U.S. Attorney Timothy T. Howard of the Southern District of New York.

Counsel information for the defendants was not immediately available.

The case is USA v. Fathi et al., case number 1:16-cr-00048, in the U.S. District Court for the Southern District of New York.