West Texas Cyber Security Consortium

Iranians Caught Cyber Snooping on High-Value US Targets

By John P. Mello Jr.
TechNewsWorld
05/29/14 4:18 PM PT

Through an elaborate social engineering ruse that involved setting up a fake news organization, Iranian spies were able to convince thousands of valuable U.S. and Israeli targets to connect with them on social media. "The Iranians use a relatively low level of technological sophistication, but what they lacked in sophistication, they made up in creativity," said iSight's Stephen Ward.

A cyberespionage campaign with links to Iran for at least three years has been targeting U.S. military and congressional personnel, journalists and diplomats, as well as U.S. and Israeli defense contractors and members of the U.S./Israel lobby, according to a report released Thursday by iSight Partners.

Using more than a dozen phony identities on online social networks, the spy ring managed to rope into its web of deceit more than 2,000 high-value targets, harvesting credentials or planting malware capable of stealing data from infected systems, the firm found.

"Two years ago, Iran said it wanted to develop cyberespionage capability," Stephen Ward, senior marketing director for iSight Partners, told TechNewsWorld. "They meant it -- and we're seeing that."

Ironically, the Iranian bogus persona campaign began around the time it was reported that the U.S. Central Command had awarded a contract to a California company to develop software for creating fake online personalities to spread pro-American propaganda on the Internet.

In an elaborate scheme, the Iranian cyberspies established a fake news outlet, the Newscaster Network, on major social networks -- Facebook, Google+, Twitter and LinkedIn -- and populated it with fake personas.

The personas probed high-value targets on the social media, making requests to connect. After joining a person's circle of contacts, they sent the target a link to a fake portal to the social network. When the target entered their credentials at the phony portal, the spies then could harvest them.

The credentials enabled them to enter the target's network.

"They can move from machine to machine, collecting intelligence and information on what assets are on the network and how they can be accessed, and escalate their privileges to access more sensitive information," Andrey Dulkin, senior director of cyber innovation atCyberArk, told TechNewsWorld.

9 to 5 in Tehran

At least one of the networks, Facebook, dismantled Newscaster before the release of the iSight report.

"We discovered this group while investigating suspicious friend requests and other activity on our site," the company said in a statement provided to TechNewsWorld by Facebook Communications Manager Jay Nancarrow.

"Creating fake profiles and distributing malware are clear violations of our policies," it continued. "We removed all of the offending profiles we found to be associated with the fake NewsOnAir organization, and we have used this case to further refine our systems that catch fake accounts at various points of interaction on the site and block malware from spreading."

The Iranian operation isn't as sophisticated as some launched by Chinese hackers, but it was just as potent. "The Iranians use a relatively low level of technological sophistication, but what they lacked in sophistication, they made up in creativity," iSight's Ward said.

"There's no designer malware or Zero Day kernel exploit," he continued. "Does it mean this wasn't an effective campaign? No. This was a multiyear campaign to establish a false sense of trust in the minds of a lot of high-value targets. They used lower-tech weapons for high-end results."

Smoking Keyboards?

In the past, Iran has denied involvement in cyberwarfare activity, but iSight cited a number of ties from the Newscaster network to Iran. For example, one Newscaster persona tried to get Facebook friends to participate in a poll on Iranian diplomacy. In addition, the password for some malware used by the spies was the Persian word "Parastoo." Moreover, Facebook activity by the network corresponded to working hours in Tehran.

"I don't know if the Iranians did this or not, but I've taken a look at some of the connections and personalities that they created, and there's a lot of work in there," Vincent Berk, CEO ofFlowTraq, told TechNewsWorld.

"If you're a company and are trying to get that kind of social media outreach," he continued, "it would take a full marketing department to do that, so someone is investing some serious money here."

Iranian hackers have grabbed headlines in the past with massive Distributed Denial of Service attacks on U.S. banks and a data destruction rampage at Saudi Aramco.

"The bank attacks were significantly disruptive, although they only attacked the websites of the banks, not their infrastructure," Richard Stiennon, chief research analyst at IT Harvest, told TechNewsWorld.

"The attack on Saudi Aramco was extremely destructive. They had to rebuild 30,000 Windows PCs after the attack," he said.

"To date, this is the first time anyone has accused the Iranians of something that looks like nation-state spying," Stiennon added, "as opposed to hacktivist-type attacks." ECT

John Mello is a freelance technology writer and contributor to *Chief Security Officer* magazine. You can connect with him on Google+.

http://www.technewsworld.com/story/80528.html