National Security

Iranian hackers are targeting U.S. officials through social networks, report says

Central to the cyber-espionage campaign is a fake news site called NewsOnAir.org, which features foreign policy and defense stories. (Kacper Pempel/Reuters)

By **Ellen Nakashima** May 29 Follow @nakashimae

A group of Iranian hackers has waged a creative campaign of cyber-espionage, targeting hundreds of high-ranking U.S. defense, diplomatic and other officials who are lured to fake Web sites through an elaborate social media network that features a bogus online news site, according to a new report.

Since at least 2011, the hackers have targeted current and former senior military officials, including a four-star admiral; current and former foreign policy officials who work on nonproliferation issues; as well as personnel from more than 10 U.S. and Israeli

defense contractors, according to iSight Partners, a cybersecurity research firm.

The operation, which the firm dubbed Newscaster, uses sites such as Twitter, Facebook and LinkedIn to draw in the hackers' targets, iSight Partners researchers said. Its centerpiece is a fake news site called NewsOnAir.org, which features foreign policy and defense stories.

"They're very brash," said Tiffany Jones, iSight Partners senior vice president. "What they lack in technical sophistication they make up for in creativity and persistence."

The hackers appear to be after intelligence that could support weapon systems development, or provide insight into the U.S. military, the U.S.-Israel alliance or nuclear negotiations between Iran and the United States and other powers, the report said.

The researchers could not determine, however, what data might have been stolen.

The NewsOnAir.org site is registered in Tehran and was located on a server that hosted mostly Iranian Web sites, they said.

"The social networking is so elaborate they've got connections to the highest levels of American policy,'' said John Hultquist, iSight Partners' head of intelligence on cyber-

espionage.

Iranian dissidents and journalists have been targeted using the same techniques for years by state-sponsored hackers, said Collin Anderson, an expert on Iranian censorship and hacker groups who is affiliated with the University of Pennsylvania's Annenberg School of Communication, and who was shown a copy of the report.

"The defense industry is just catching up with what's been going on to Iranian civil society for a long time," he said.

The hacker group, which maintained hours consistent with the Iranian workweek, taking Thursday and Friday off, created more than a dozen fake personas or identities. In one case, though, it used a real Reuters reporter's name and professional bio, and in another it used a Fox TV reporter's photo. Other fake identities involved defense contractor employees and, in one case, a systems administrator for the U.S. Navy.

Using these personas, the hackers established online relationships with friends, relatives and colleagues of their targets through sites such as LinkedIn and Facebook. Having established those social links, they sought to "friend" or create online relationships with their targets.

Once connected to their targets, they established their bona fides by, for instance, sending friendly messages with links to fake sites such as NewsOnAir.org. That site contained legitimate articles first published elsewhere, but with the bylines replaced by fake reporters' names. New stories were tweeted out through the account @NewsOnAir2.

As the ruse went on, they would send their targets links to, for instance, a YouTube video of a weapons system. When the target clicked on the link, he would be redirected to a spoof page — maybe a Gmail log-in or company e-mail log-in page — designed to steal his log-in and password information.

In all, the hackers established connections with more than 2,000 people, including targets and their friends, family and co-workers, iSight Partners said.

"This is the most elaborate social engineering scheme we've seen associated with cyber-espionage," Hultquist said.

The Newscaster campaign also targeted journalists, lobbyists for Israeli interests and members of Congress, iSight Partners researchers said.

The Iranians are not among the elite or most

sophisticated of hackers. The United States, Russia, Israel and China still are leagues ahead. But the Iranians are working hard to catch up, experts say.

ISight Partners researchers said one concern is that the type of access obtained through operations such as Newscaster could be exploited in support of disruptive or destructive attacks on U.S. companies or government networks.

U.S. intelligence analysts have linked Iran to cyberattacks in 2012 on oil and gas companies in Saudi Arabia and Qatar, which are allied with Western powers that have tightened economic and oil sanctions against Iran in an effort to slow Iran's nuclear program. The attack on state-owned oil company Saudi Aramco resulted in damage to 30,000 computers, which had to be replaced.

In 2010, a sophisticated cyberattack against Iran's nuclear program was revealed when security researchers discovered a computer worm dubbed Stuxnet. That campaign, which damaged 1,000 uranium-enrichment centrifuges at the Natanz nuclear facility, eventually was linked to the United States and Israel. The two governments have never officially acknowledged responsibility.