Iran cyberspies created fake news website, researchers say (Update)

May 29 2014, by Rob Lever

Spies based in Iran created a bogus news organization used for espionage since 2011 against US and Israeli military targets, security researchers said

Spies based in Iran created a bogus news organization used for espionage since 2011 against US and Israeli military targets, security researchers said.

A report released this week by iSight Partners says that more than 2,000

people are or have been targeted in the operation dubbed Newscaster, which uses a "front media outlet" called NewsOnAir.org.

The operation appears to be "carried out by Iranian actors, though there is a dearth of information implicating its ultimate sponsor," the report said. It is believed to still be ongoing.

Under the program, spies plagiarized the work of real media outlets "to legitimize their personas as journalists," the report added.

Some of the news organizations whose work was misappropriated included the Associated Press, Reuters and the BBC.

'Brash and complex'

The documents from iSight called the operation "brash and complex," and the analysts found at least two legitimate identities falsified from news organizations including Fox News and Reuters.

The effort is part of a campaign that also used social media and "spear-phishing" to connect with officials and contractors in order to gain access to secret networks and steal data.

In addition to the fake news operation, the network uses its made-up personas to establish connections on Facebook and other social networks, with the aim of stealing email logins and other credentials.

"What this group lacks in technical sophistication, they make up for in brashness, creativity and patience," the iSight report said.

The length of the operation "is indicative of at least marginal success" it added.

In addition to the US and Israel, the report said that the operation may have targeted "high- and low-ranking personnel in multiple countries," including Britain, Iraq and Saudi Arabia.

Specific targets included members of the US military, congressional personnel, Washington area journalists and diplomats, US and Israeli defense contractors and members of the "US/Israeli lobby."

Of particular interest to the network were people involved in nuclear non-proliferation and sanctions that could affect Tehran.

"We are aware that hackers in Iran and elsewhere often use social media to gain information or make connections with targets of interest, including US government and private entities," US State Department spokeswoman Jen Psaki said.

"To defend against these threats, the United States is committed to helping the public and private sector protect itself in cyberspace by sharing actionable information."

'Alternative approach'

The operation suggests a stealth effort to steal data, unlike some of the more overt cyberattacks, said iSight's John Hultquist.

"In many ways, these operators have escaped the malware arms race in lieu of an alternative approach," Hultquist said in a blog post.

"Newscaster focuses on human factors and third-party platforms, weak spots for many of the most sophisticated enterprise defenses."

The report said the news site was registered in Iran and that the IP addresses used by the site also appear to be Iranian.

Other evidence, including the use of a Persian password, bolster suspicions the operation came from Iran.

"The network of personas is especially complex, including dozens of accounts with fictitious personal and professional material, many of whom claim to work for the news provider NewsOnAir.org," the report said.

The researchers said the impact is hard to assess, but warned that "successful compromises could be leveraged for diplomatic, military and other strategic advantages, and possibly even used as reconnaissance for attack."