Newscaster Threat Uses Social Media for Intelligence Gathering

By Sean Michael Kerner

Published: 2014-05-29 · Archived: 2026-04-05 16:57:23 UTC

A report published on May 28 by iSight Partners alleges that a widespread social media attack campaign has been undertaken by Iran against organizations in the United States, the United Kingdom and Israel.

Dubbed "Newscaster" by iSight Partners, a global provider of cyber-threat intelligence, the social media campaign involves multiple layers of deception, as attackers are creating fake identities with careers in the defense industry, journalism and government.

"These accounts are elaborate and have created credibility using, among other tactics, a fictitious journalism website, newsonair.org, that plagiarizes news content from other legitimate media outlets," iSight states. "These credible personas then connected, linked, followed, and 'friended' target victims, giving them access to information on location, activities, and relationships from updates and other common content."

The Newscaster campaign also involves the use of targeted messages to victims in a bid to steal log-in credential information. According to iSight Partners, the impact of Newscaster extends to at least 2,000 people who are connected to the fake online identities. Going a step further, the report points the finger at Iran for being the source of Newscaster.

The purpose of Newscaster is likely for intelligence gathering.

"We infer, from our limited knowledge of Newscaster targeting, that such intelligence could ultimately support the development of weapon systems, provide insight into the disposition of the U.S. military or the U.S. alliance with Israel, or impart an advantage in negotiations between Iran and the U.S., especially with regards to sanctions and proliferation issues," iSight stated.

While iSight Partners is officially ringing the warning bell on the Newscaster threat now, it is not an unknown threat to others in the information security industry.

"We have been tracking this activity for some time," Adam Meyers, vice president of intelligence at CrowdStrike, told *eWEEK*. "We designate it using the cryptonym Charming Kitten."

Eric Cowperthwaite, vice president of advanced security and strategy at Core Security, told *eWEEK* that anyone involved in media reporting, foreign affairs and defense should consider themselves to always be a target for cyber-attack.

From a protection standpoint, there are a number of things that individuals and organizations can do to limit the risk of being a victim of Newscaster. Especially when it comes to social media, all individuals need a much higher

degree of awareness and they need to be much more paranoid and less trusting, Cowperthwaite said.

Meyers noted that the Newscaster/Charming Kitten attackers are using social engineering both through direct contact and social networks. He suggests that users be wary of social media requests from unknown individuals.

“It’s safer to not accept a request than to be compromised,” Meyers said. “If unknown people, no matter how interesting or attractive they may seem, send a request or a link, say no—this is a targeted attacker’s honey trap.”

Sean Michael Kerner is a senior editor at eWEEK *and* InternetNews.com. *Follow him on Twitter @TechJournalist.*
