# NEWSCASTER – An Iranian Threat Inside Social Media

By Stephen Ward May 28, 2014 iSIGHT Partners


On May 29th, iSIGHT Partners released a report focused on a new threat – dubbed NEWSCASTER – targeting the public and private sector in the U.S., Israel, UK and beyond using social media. We believe the threat originates from Iran.

Below you will find key details related to this disclosure. A full copy of the iSIGHT Partners report is available upon request by registering here.

For any media related inquires on the NEWSCASTER Threat please contact Adrienne Reitz, newscaster@okco.com

## Here is what you need to know…

**WHAT IS THE NEWS?**

iSIGHT Partners believes Iranian threat actors are using more than a dozen fake personas on social networking sites (Facebook, Twitter, LinkedIn, Google+, YouTube, Blogger) in a coordinated, long-term cyber espionage campaign. At least 2,000 people/targets are, or have been, caught in the snare and are connected to the false personas.

This campaign, working undetected since 2011, targets senior U.S. military and diplomatic personnel, congressional personnel, Washington D.C. area journalists, U.S. think tanks, defense contractors in the U.S. and Israel, as well as others who are vocal supporters of Israel to covertly obtain log-in credentials to the email systems of their victims. Additional victims in the U.K. as well as Saudi Arabia and Iraq were targeted.

The targeting, operational schedule, and infrastructure used in this campaign is consistent with Iranian origins.

**HOW DOES IT WORK?**

The fake personas claim to work in journalism, government, and defense contracting. 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.

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.

Accounts were then targeted with "spear-phishing" messages. Links which appeared to be legitimate asked recipients to log-in to false pages, thus capturing credential information. It is not clear at this time how many credentials the attack has captured to date.

Additionally, this campaign is linked to malware. While the malware is not particularly sophisticated it includes capability that can be used for data exfiltration.

**WHAT DOES THIS MEAN?**

The discovery and investigation of the attack reveals three critical insights:

1. Social media offers a powerful and covert pathway for targeting key government and industry leadership through a third-party platform potentially outside of existing security measures.
2. Given targeting associated with this campaign, Iranian actors may have used accesses gained through this activity to 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. Furthermore, it is possible that any access or knowledge could be used as reconnaissance-for-attack in advance of disruptive or destructive activity.
3. Adversaries such as these are increasingly adept at finding and exploiting opportunities to carry out cyber espionage, even when lacking sophisticated capability. NEWSCASTER's success is largely due to its patience, brazen nature, and innovative use of multiple social media platforms.

**WHAT KIND OF DATA WAS TAKEN?**

We are unable to say with complete visibility. However, it is reasonable to assume that a vast amount of social content was compromised in addition to some number of log-in credentials that can be used to access additional systems and information.

As users often maintain the same credentials for multiple sites, it is impossible to determine the scope, scale, and duration of data loss.

**WHO SHOULD BE WORRIED ABOUT THIS THREAT?**

Given the covert nature of cyber espionage, its impacts are often difficult to forecast or measure; however, in this instance, we expect any access obtained by the NEWSCASTER network will be ultimately exploited for intelligence value.

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.

It is also possible that the compromise of such high-ranking and influential people could be used to access the senior levels of as-of-yet unidentified organizations in the U.S., Israel, and elsewhere. Furthermore, we surmise that access could be leveraged as reconnaissance-for-attack, supporting eventual disruptive or destructive attacks against targeted entities. Though there is no evidence indicating the NEWSCASTER network was

created to support such activity, previous incidents publicly attributed to Iran, such as Operation Ababil and the attacks on Saudi Aramco underscore this possibility.

The NEWSCASTER network appears to be primarily focused on targeting senior military and policymakers, firms associated with defense technology, and the U.S.-Israel lobby, however, we found victims in the financial and energy sectors, as well as elsewhere, and we recognize that we could only see a portion of the accounts connected to this network. Organizations involved in critical infrastructure, or who have information that may be of strategic or tactical interest to a nation-state adversary should be concerned about a threat such as this.

**WHY DOES ISIGHT PARTNERS THINK THIS ORIGINATES IN IRAN?**

Though the timing of the social network attack may seem irregular at first, over multiple years the schedule behind the activity becomes apparent. They maintained a regular schedule, including what appears to be a lengthy lunch break followed by the remainder of the work day. These hours conform to work hours in Tehran. Furthermore, the operators work half the day on Thursday and rarely work on Friday, the Iranian weekend. Other clues, such as the targets on which the operators have chosen to focus and additional technical indicators, lead us to believe NEWSCASTER originates in Iran.

**WHAT IS THE NEWSCASTER NETWORK AFTER?**

Without seeing how the information stolen by the NEWSCASTER network is used, it is difficult to make a definitive assessment of their ultimate motivation. However, the actors have intimated their interest in specific defense technology as well as military and diplomatic information by their targeting. This type of targeting is inconsistent with cyber-criminal behavior.

It remains possible that the actors could selectively reveal information gained through this campaign to embarrass those who were targeted, or already have, but we have seen no evidence of this at this time. Ultimately, we believe the sponsors of the activity are seeking information advantage over rival military forces, defense industries, diplomats, and others.

**IS THIS TYPE OF ACTIVITY COMMON ON SOCIAL NETWORKS?**

We have previously identified cyber espionage campaigns which originate from China using social network accounts to propagate, but never a campaign of such complexity working across so many platforms. NEWSCASTER is unprecedented in complexity, scale, and longevity.

**HOW DID ISIGHT PARTNERS UNCOVER THIS ACTIVITY?**

We are protective of sources and methods, but we can confirm that these actors did not go unnoticed by some targeted entities and they left significant evidence of their activity throughout the Internet. As with many other threats, iSIGHT Partners combined malware analysis, open source research, and research from our global collection network to create our assessment of the NEWSCASTER network.

**IS NEWSONAIR.COM ALSO PART OF THE FAKE NEWS RUSE?**

Newsonair.COM, a legitimate Indian news operation, is not the same as newsonair.ORG. We have no indication that newsonair.COM was in anyway linked to faux newsonair.ORG site that was part of this campaign.

**IS THIS THE GOVERNMENT OF IRAN?**

We can't be certain. We have no information implicating the ultimate sponsor. In the past we've seen cyber espionage operations carried out by government organizations, corporate intermediaries, and other third parties.

**WHAT STEP CAN AN ENTERPRISE TAKE TO PROTECT ITSELF?**

In addition to blocking known NEWSCASTER infrastructure, an enterprise can protect itself by taking steps to mitigate the human elements of the NEWSCASTER threat. Though the actors took pains to create a complex

social engineering capability, they made many mistakes and were detected by potential victims. Personnel can learn from these mistakes to better recognize similar incidents.

NEWSCASTER was brazen, complex multi-year cyber-espionage that used a low-tech approach to avoid traditional security defenses –exploiting social media and people who are often the "weakest link" in the security chain. This underscores the importance of cyber threat intelligence that enables enterprises to proactively tune defenses to combat a determined and persistent adversary utilizing constantly evolving tactics.

**WHAT DOES THIS MEAN FOR THE GENERAL PUBLIC?**

Don't be worried, but do be vigilant. As always, do not create trusted connections with unknown organizations and/or individuals. Never provide login credentials with any site or person who contacts to you (rather than you contacting it), use strong passwords and regularly change them.

**HAVE YOU COORDINATED WITH THE FBI ON THIS REPORT?**

The intelligence development and analysis was completed independently by iSIGHT Partners.

iSIGHT Partners did coordinate with the FBI to:

- Brief government agencies and our commercial clients
- Coordinate on the release of the report
- Identify the relevance/possible impact of the threat to critical infrastructure entities and agencies

**WHY ARE YOU MAKING THIS AVAILABLE TO THE PUBLIC?**

The complexity, scale, and longevity of this campaign leads us to believe that there may be additional victims that do not yet realize they are at risk. We hope that by making this information public, we can deter further incidents. If you determine you are a victim, immediately contact the Federal Bureau of Investigation at either your local FBI Cyber Task Force or FBI CYWATCH (email: cywatch@ic.fbi.gov or phone: +1-855-292-3937)

**WHO IS ISIGHT PARTNERS?**

Dallas-based iSIGHT Partners is a global cyber intelligence firm that delivers cyber threat intelligence and insight to leading enterprises in business and government. With 200+ experts in 16 countries and expertise in 24 languages, only iSIGHT can deliver the full context and intent of our clients' most damaging cyber threats, allowing security organizations to respond faster, defend proactively, and invest smarter. With iSIGHT Partners, enterprises can deploy their defenses more efficiently and effectively, and internal security professionals can more accurately quantify the return on security investments for senior management.

## iSIGHT Partners Contact Info:

**Media Inquiries:** iSIGHT Partners, Adrienne Reitz, newscaster@okco.com

**Existing iSIGHT Partner customers contact:** Chris Usserman, cusserman@isightpartners.com

**FBI suspected victims:** cywatch@ic.fbi.gov or Voice: +1-855-292-3937

**Twitter:** @iSIGHT_Partners

**LinkedIn:** iSIGHT Partners

Tags cyber crime cyber data cyber espionage cyber espionage facebook cyber experts cyber intelligence cyber threat intelligence data feeds hacktivism incident response iranian cyber espionage threat feeds

## Want to learn more?

**Request a Consultation >**

**Interested in a FREE Trial? >**

**Download a Datasheet >**


## Recent Posts

ThreatScape Media Highlights Update – Week Of June 8th

ThreatScape Media Highlights Update – Week Of May 25th

Threat Intelligence & the C-Suite: Defining Risk for the Board Room

### John P. Watters

Chairman / CEO, iSIGHT Partners

If you do not understand the motivation, intent and capability of your adversaries, then you cannot understand the associated risk to your enterprise. Without this threat context, there is no way to accurately assess the risk, determine the most effective strategy to counter the threat or calculate the ROI for your security investments.

+1-214-731-4585 info@isightpartners.com