SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- Suits and Spooks

Security Experts:

WRITE FOR US

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe (Free)
- CISO Forum 2016
- ICS Cyber Security Conference
- Contact Us

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - White Papers
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
  - Whitepapers
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
  - Whitepapers
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - White Papers
  - Network Security
  - Application Security
- Management & Strategy

Iranian Hackers Targeted US Officials in Elaborate Social Media Attack Operation

By Mike Lennon on May 29, 2014

Share 80 G+1 1 Tweet Recommend 4 RSS

Iranian threat actors, using more than a dozen fake personas on popular social networking sites, have been running a wide-spanning cyber espionage operation since 2011, according to cyber intelligence firm iSIGHT Partners.

The recently uncovered activity, which iSIGHT Partners calls **NEWSCASTER**, was a “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.”

Using the fake personas, including at least two (falsified) legitimate identities from leading news organizations, and young, attractive women, the attackers were supported by a fictitious news organization called NewsOnAir.org (Do Not Visit) and were successful in connecting or victimizing over 2,000 individuals.

“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,” iSIGHT Partners said.

Podcast: Inside the 'NEWSCASTER' Cyber Espionage Campaign

The attackers used popular social media platforms such as Facebook, Twitter, LinkedIn, Google+, YouTube and Blogger as their attack platform.

While the attack method is not novel, the cyber intelligence firm says that what this group lacks in technical sophistication they make up for in brashness, creativity, and patience.

Working undetected since 2011, iSIGHT Partners said targets included 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.

Other victims targeted were in the U.K., Saudi Arabia, Iraq and also included vocal supporters of Israel.

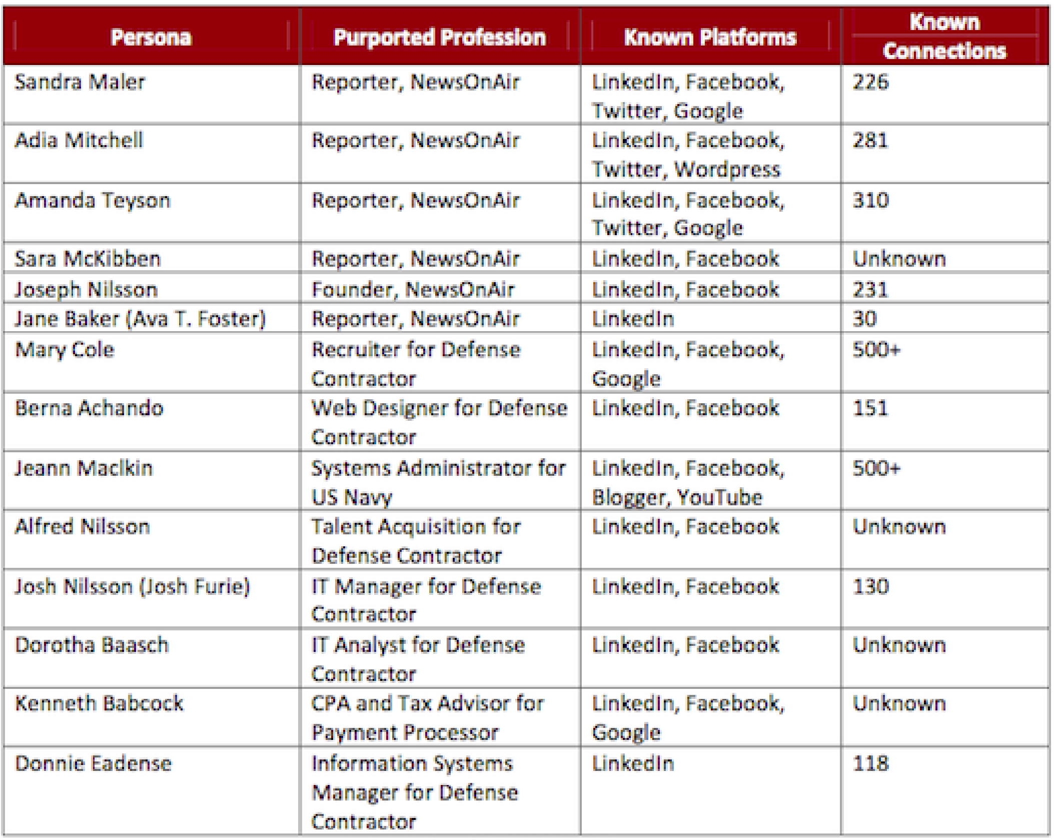
“Though it is possible anyone connected to the network was compromised, deliberate attempts to connect with certain entities suggest an interest in political, military, diplomatic and technical intelligence,” the closely held report said.

“Largely this campaign was about credential harvesting and recon,” Stephen Ward, Senior Director of Marketing at iSIGHT Partners, told *SecurityWeek*.

“They are using those connections to harvest connections to corporate email, harvest connections to personal email, and use those springboards for further lateral [movement], “ he said.

After making connections on social networks, targets were sent spear-phishing messages, often with links asking recipients to log-in to fake pages in order to capture credentials.

Below is a list of some of the accounts/fake personas allegedly used by the attackers.



Persona	Purported Profession	Known Platforms	Known Connections
Sandra Maler	Reporter, NewsOnAir	LinkedIn, Facebook, Twitter, Google	226
Adia Mitchell	Reporter, NewsOnAir	LinkedIn, Facebook, Twitter, Wordpress	281
Amanda Teyson	Reporter, NewsOnAir	LinkedIn, Facebook, Twitter, Google	310
Sara McKibben	Reporter, NewsOnAir	LinkedIn, Facebook	Unknown
Joseph Nilsson	Founder, NewsOnAir	LinkedIn, Facebook	231
Jane Baker (Ava T. Foster)	Reporter, NewsOnAir	LinkedIn	30
Mary Cole	Recruiter for Defense Contractor	LinkedIn, Facebook, Google	500+
Berna Achando	Web Designer for Defense Contractor	LinkedIn, Facebook	151
Jeann Maclkin	Systems Administrator for US Navy	LinkedIn, Facebook, Blogger, YouTube	500+
Alfred Nilsson	Talent Acquisition for Defense Contractor	LinkedIn, Facebook	Unknown
Josh Nilsson (Josh Furie)	IT Manager for Defense Contractor	LinkedIn, Facebook	130
Dorotha Baasch	IT Analyst for Defense Contractor	LinkedIn, Facebook	Unknown
Kenneth Babcock	CPA and Tax Advisor for Payment Processor	LinkedIn, Facebook, Google	Unknown
Donnie Eadense	Information Systems Manager for Defense Contractor	LinkedIn	118

Operational NEWSCASTER Personas

Source: iSIGHT Partners

The campaign also leveraged malware, and while the malware used was not particularly sophisticated, it does includes the capability to exfiltrate data.

“They are sort of disadvantaged from a technological advancement side of things,” Ward said, referring to assumed Irianian attackers. “They have taken to the cyber world the same way you can compare the impact of [improvised explosive devices]. The approach is low cost and does not really use a lot of sophistication from an exploit perspective, but is very effective and ultimately a bit more under the radar.”

“Adversaries such as these are increasingly adept at finding and exploiting opportunities to carry out cyber espionage, even when lacking sophisticated capability,” iSIGHT Partners concluded. “NEWSCASTER’s success is largely due to its patience, brazen nature, and innovative use of multiple social media platforms.”

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, iSIGHT Partners warned.

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.

Attribution to Iran

According to iSIGHT Partners, there is no direct information showing that the Iranian government is the ultimate sponsor of the campaign, but iSIGH researchers do believe the threat actors are located in Iran.

“[The attackers] maintained a regular schedule, including what appears to be a lengthy lunch break followed by the remainder of the work day,” the report said. “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.”

Additional clues, such as the targets the attackers selected, along with additional technical indicators, sparked iSIGHT to believe NEWSCASTER stems from Iran.

iSIGHT Partners said it did coordinate with the FBI to brief government agencies and also notified Facebook, LinkedIn and other social networks.

According to Ward, the identified malicious personas have been removed from Facebook and LinkedIn.

The report from iSIGHT Partners comes roughly two weeks after a report from FireEye, which suggested that Iranian attackers’ methodologies have “grown more consistent with other advanced persistent threat (APT) actors in and around Iran" following cyber attacks against Iran in the late 2000s.

“Iran has steadily increased their focus on cyber espionage over the years, placing significant emphasis on enhancing capabilities following the Stuxnet attacks,” Michael Sutton, VP of Security Research for Zscaler, told *SecurityWeek*. “The NEWSCASTER attacks, while not technically sophisticated were allegedly quite successful. Often social engineering can be the most powerful tool in an attacker's arsenal.”

Social networks are a significant challenge for security teams, Sutton says.

“They generally represent a personal communication medium which the organization does not have direct control over and yet can become a source of leaked data or a catalyst for attack as has been seen in the NEWSCASTER attacks. Moreover, due to password reuse, even if an attacker can gain access to credentials used by a victim on personal accounts, there is a string likelihood that the same credentials have also been used for more sensitive corporate accounts."

"The campaign reported by iSightPartners uncovers what we have known for the last decade -- that sophisticated hackers backed by nation states target the weakest link on networks -- the user with relatively unsophisticated techniques including spear phishing and social media," Anup Ghosh, founder and CEO of Invincea, told *SecurityWeek*.

"Using social media is both a way of establishing false bona fides while presenting a well accepted vector for reaching targets," Ghosh continued. "A simple LinkedIn or Twitter update with a link, or a timely email from a connection with embedded link or attachment is enough to compromise the intended target's machine, accounts, data, and enterprise network."

"This is not surprising as every major foreign adversary is leveraging social media as a cyber attack vector," added James C. Foster, CEO of ZeroFOX. "Our government realizes this threat is increasing and social media is being used for target reconnaissance and exploitation."

Listen to the Podcast: Inside the 'NEWSCASTER' Cyber Espionage Campaign

Related Reading: Social Media a Key Element for Terror Groups

Related Reading: News Junkies Make Great Targets

Share 80 G+1 1 Tweet Recommend 4 RSS

For more than 10 years, Mike Lennon has been closely monitoring and analyzing trends in the enterprise IT security space and the threat landscape. In his role at SecurityWeek he oversees the editorial direction of the publication and manages several leading security conferences.

Previous Columns by Mike Lennon:

Darktrace Raises $65 Million in Round Led By KKR
Hard Rock Hotel & Casino Hit By PoS Malware
Symantec to Acquire Blue Coat for $4.65 Billion
Symantec Wants to Protect Your Car From Zero-Day Attacks
Morgan Stanley to Pay $1 Million Penalty Over Customer Data Theft

Tags:
Cyberwarfare NEWS & INDUSTRY Malware Cybercrime

0 Comments SecurityWeek provides information security news and analysis. 1 Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

ALSO ON **SECURITYWEEK PROVIDES INFORMATION SECURITY NEWS AND ANALYSIS.**

Yahoo Rewards Researcher for ImageMagick Hack

1 comment • 2 months ago•

David Boccabella — I know of one major site that has been hit by this. It's forum source code (Proprietary) was downloaded and …

Mysteries of the Panama Papers

1 comment • 2 months ago•

Will Liu — ICIJ- look at the dns records! =)

Hacked WordPress Sites Target Random Users

1 comment • 2 months ago•

Dan Awontis — Wow, that's a huge number of attacks. Very informative article, worth reading.

New Tools Disguised as Old Malware in Hospital Attacks

1 comment • 10 days ago•

Mike Mastela — Patching and vulnerability remediation must move beyond the servers and traditional endpoints and include …

Subscribe Add Disqus to your site Add Disqus Add Privacy

Search

Subscribe to SecurityWeek

Enter Your Email Address Subscribe

Most Recent Most Read

- Neutrino, RIG Using Blackhat-TDS for Redirection
- Businesses in the Dark on Value of Corporate Data
- Israeli Ad Company Behind "Pirrit" OS X Adware: Report
- Hadoop Audit and Logging "Back in Time"
- OS X Backdoor Provides Unfettered Access to Mac Systems
- Darktrace Raises $65 Million in Round Led By KKR
- Microsoft Proposes Independent Body to Attribute Cyber Attacks
- Information-Collecting Android Keyboard Tops 50 Million Installs
- EU Invests €450 Million in Cybersecurity Partnership
- SBDH Espionage Toolkit Used to Target European Governments

Discussion

- People
- Recent
- Popular

Recent Comments

- Chuck Parks (OnesnZero's)

  Very good information & no shortage of these to be on guard for! Thank you

  Satana Ransomware Encrypts MBR and Files · 1 day ago

-
  Jeff Silverman

  David, This problem is nothing new. A friend of mine was working at a shop that still used SNMP v2 because some of their devices couldn't handle SNMP v3. They weren't willing to keep track of which...

  New X25519 Cipher Throws Enterprise Surveillance for a Loop · 2 days ago

-
  Crissa

  The needs and security measures - what devices are being integrated with - will differ substantially between employees and customers.

  The Great Analyst Debate Over Consumer IAM · 2 days ago

community on DISQUS

Popular Topics

- Information Security News
- IT Security News
- Risk Management
- Cybercrime
- Cloud Security
- Application Security
- Smart Device Security

Security Community

- IT Security Newsletters
- Suits and Spooks
- ICS Cyber Security Conference
- CISO Forum
- InfosecIsland.Com

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group

- Cyber Weapon Discussion Group
- RSS Feed
- Submit Tip
- Security Intelligence Group

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us

Wired Business Media