ThreatScape®

NEWSCASTER:
An Iranian Threat Within Social Networks

iSIGHTPARTNERS®
Security beyond the edge®

ThreatScape® Intelligence Report – May 28, 2014

Contents

Executive Summary

Key Points:

- More than 2000 people are connected to the NEWSCASTER network of false personas, which has existed since at least 2011.
- The personas are supported by fictitious personal content, family relationships and the front media outlet NewsOnAir.org.
- Operators have intimated an interest in specifically targeted defense contractors and senior military and government officials.
- Malicious activity is tied to personas and the NewsOnAir.org website, and victims were sent links to credential collection websites that appear to be web portals.
- A review of the adversary's activities suggests they operate on Tehran's professional schedule.

Since at least 2011, a network of fake personas we have dubbed NEWSCASTER has been sending social engineering content to senior military and government officials and the private sector in the US and Israel. Many of the personas are linked to the fictitious news agency NewsOnAir.org, which reposts and credits themselves with the work of other media outlets to legitimize personas as journalists. While the ultimate sponsor of this activity is unknown, several indicators suggest it originates in Iran. This incident underscores the threats posed by social networking platforms and affirms that enterprises must take steps to control the human factors that may place them at risk. Though the covert nature of this campaign obscures its impact, successful compromises could be leveraged for diplomatic, military and other strategic advantages and possibly even used as reconnaissance for attack.

The NEWSCASTER Threat

We believe NEWSCASTER is a long-term, resource intensive cyber espionage operation motivated by the prospect of strategic intelligence. Targeting, professional operational schedule and complexity suggest this activity is carried out by Iranian actors, though there is a dearth of information implicating its ultimate sponsor.

- Personas are used to directly target several current and former senior US military and diplomatic personnel and several specific defense contracting firms in the US and Israel. Though targeting of organizational senior leadership and those associated with the defense industrial base (DIB) are tactics that have been used in hacktivist activity, long-term persistent reconnaissance and exploitation of specific targets is inconsistent with actors who intend to ultimately expose their operations.
- The activity is carried out from infrastructure previously registered in Tehran and co-hosted with other Iranian websites. The activity also appears to occur in line with a professional schedule feasible for actors located in Tehran.
- The network of personas is exceptionally complex, including dozens of accounts with fictitious personal and professional material, many of whom claim to work for the news provider NewsOnAir.org.

Personas Across Multiple Platforms

iSIGHT Partners has uncovered multiple social networking accounts leveraged in a coordinated, long-term cyber espionage campaign since at least 2011. The network of personas is interconnected and supported by an extensive social engineering regimen that crosses multiple social networking platforms and websites.

- iSIGHT Partners has uncovered more than a dozen operational fictitious personas residing on Facebook, LinkedIn, Twitter and other platforms connected to more than 2000 accounts.

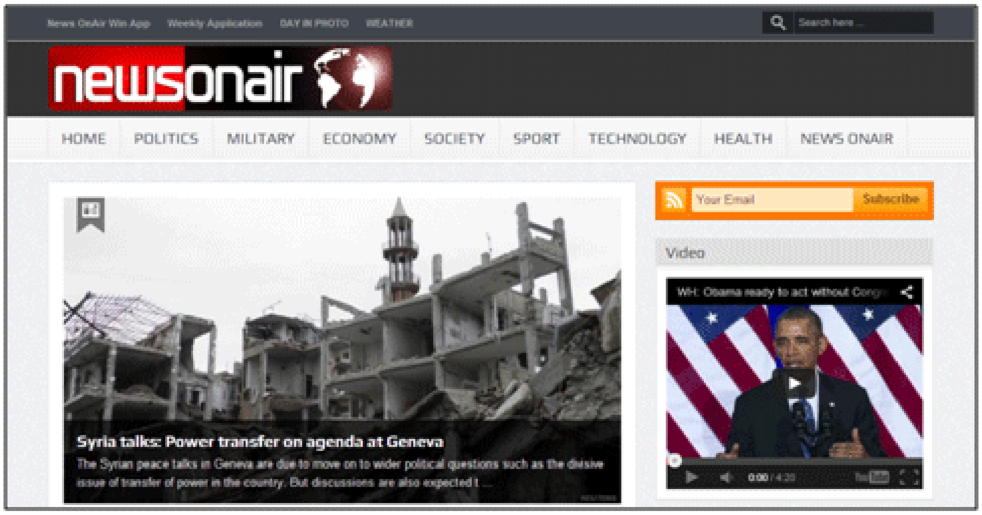
Persona	Purported Profession	Known Platforms	Known Connections
Sandra Maler	Reporter, NewsOnAir	LinkedIn, Facebook, Twitter, Google	226
Adia Mitchell	Reporter, NewsOnAir	LinkedIn, Facebook, Twitter, Wordpress	281
Amanda Teyson	Reporter, NewsOnAir	LinkedIn, Facebook, Twitter, Google	310
Sara McKibben	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

- All profiles are fictitious and use the pictures or information of real individuals, both public and otherwise.
  - Several personas used the names of real people while displaying alternative profile images, while others used images of real people, to include the moderately famous, paired with completely fabricated personas. For example, profiles purporting to be associated with the journalist Sandra Maler of Thompson Reuters used identifying profile images that clearly do not depict the known journalist. In addition, the Alfred

Nilsson persona uses images of Michael Mirisch, the founder of Los Angeles-based charity Hollywood Knights.

  - Multiple personas used the photographs of others connected to the network. The fabricated NewsOnAir persona of Amanda Teyson used pictures of an Italian national reenacting a World War II combat cameraman. The Italian national is friends with the Adia Mitchell persona. Pictures used in the Dorotha Baash persona are taken from a profile who is friends with the persona of Jeann Maclkin.
- Several personas are linked via claims of employment by the fictitious journalism organization NewsOnAir. The NewsOnAir.org website uses news from other sources and credits it to the affiliated personas.



Syria talks: Power transfer on agenda at Geneva

The Syrian peace talks in Geneva are due to move on to wider political questions such as the divisive issue of transfer of power in the country. But discussions are also expected t ...

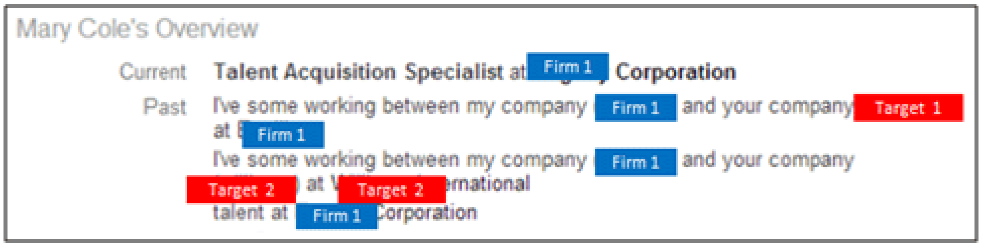
NewsOnAir.org website

- Still others indicate they are members of a Nilsson family, whose patriarch is ostensibly Joseph Nilsson, the persona who claims to have founded NewsOnAir.
- Additional ties include active social networking connections such as sharing and endorsements and the reuse of distinctive language in profiles. For instance, several profiles intimated they worked with targeted companies using the phrase, "I've some working between my company [company they claim to work for] and your company [targeted company]."

Targeting

The network was principally leveraged against US and Israeli targets in public and private sectors, though additional targeting included personnel from the United Kingdom, Saudi Arabia, Syria, Iraq, Afghanistan and elsewhere. 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. With the exception of personas that appear to be solely used to support the bonafides of others, the majority of personas purport to be journalists, members of the military or defense contractors.

- Several accounts intimated the targeting interest of the actors by creating profiles tailored to targeted organizations. In passages in several profiles, the actors defined a relationship between the company for which they claimed to work and the profile's reader, whom they referred to in the first person and whose company they identified. These profiles intimated an interest in US and Israeli defense contractors working in aerospace.



Mary Cole's Overview

Current Talent Acquisition Specialist at Firm 1 Corporation

Past I've some working between my company Firm 1 and your company Target 1 at Firm 1

I've some working between my company Firm 1 and your company Target 2 at Target 2 ernational talent at Firm 1 Corporation

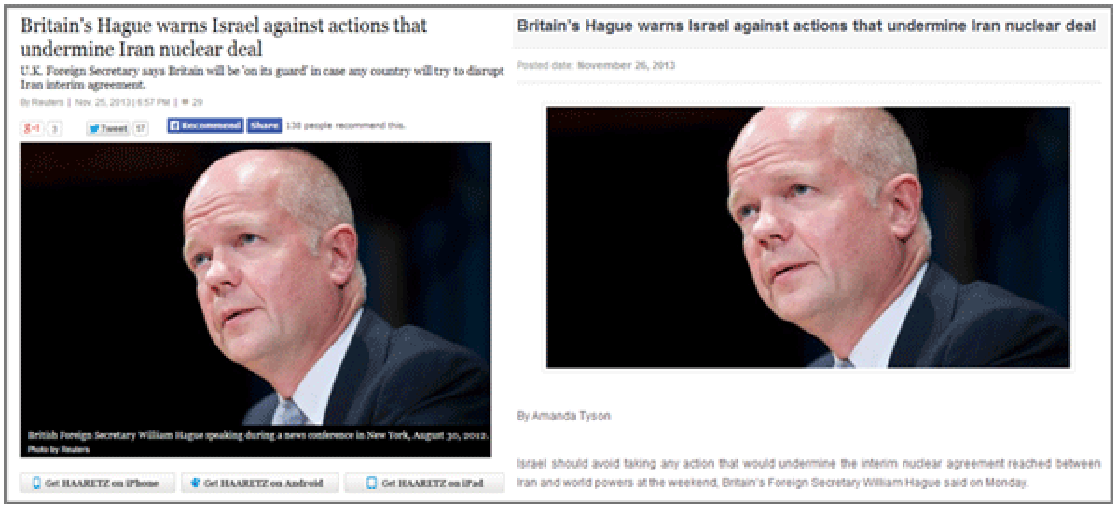
LinkedIn profiles indicated, in first person, which companies were specifically targeted

- Social networking accounts were found with extensive relationships to several current and former flag officers of the US military and senior government officials. The deliberate nature of their targeting was indicated by a long-term process of "friending"(or connecting their profiles to) people with whom the target is familiar or intimately related, building bona fides prior to ultimately friending the targeted person.
- Entities connected to the network included, but were not limited to:
    - Several current and former senior members of the military
    - Current and former senior foreign policy leaders, to includes those associated with nuclear non-proliferation and sanctions
    - Politicians and bureaucrats at the state and federal level with a particular concentration around the state of North Carolina
    - The US-Israel lobby
    - Personnel from at least ten separate US and Israeli defense contractors
    - Several other accounts that have no apparent connection to geopolitics or organizations typically targeted in espionage activity
- Of note, a persona using the name Kendrick Babson is inconsistent with the aforementioned targeting motivation demonstrated by the choice of associated occupation. While others leverage military, DIB or journalist profiles, Kendrick Babson is purportedly an accountant working for a payment processor.

NewsOnAir.org, the Nilsson Family and Supporting Personas

Many of the personas claim to belong to the fictitious news organization NewsOnAir, which has its own Facebook and LinkedIn presence and a content-rich webpage setup at NewsOnAir.org designed to further legitimize the personas. Additionally, several of the personas are members of a fictitious "Nilsson" family, which includes NewsOnAir's so-called founder. We anticipate that there are several supporting personas that we have not yet identified that were created solely to legitimize other personas.

- NewsOnAir.org is a website that features news stories updated several times weekly. The stories' content is not original and is taken from other sources such as CNN, Reuters and the BBC. Stories are frequently reposted with the bylines of the NewsOnAir personas and reposted to their social networking sites.



Britain's Hague warns Israel against actions that undermine Iran nuclear deal

U.K. Foreign Secretary says Britain will be 'on its guard' in case any country will try to disrupt Iran interim agreement.

By Reuters | Nov. 25, 2013 | 6:57 PM | 29

British Foreign Secretary William Hague speaking during a news conference in New York, August 30, 2012. Photo by Reuters

Britain's Hague warns Israel against actions that undermine Iran nuclear deal

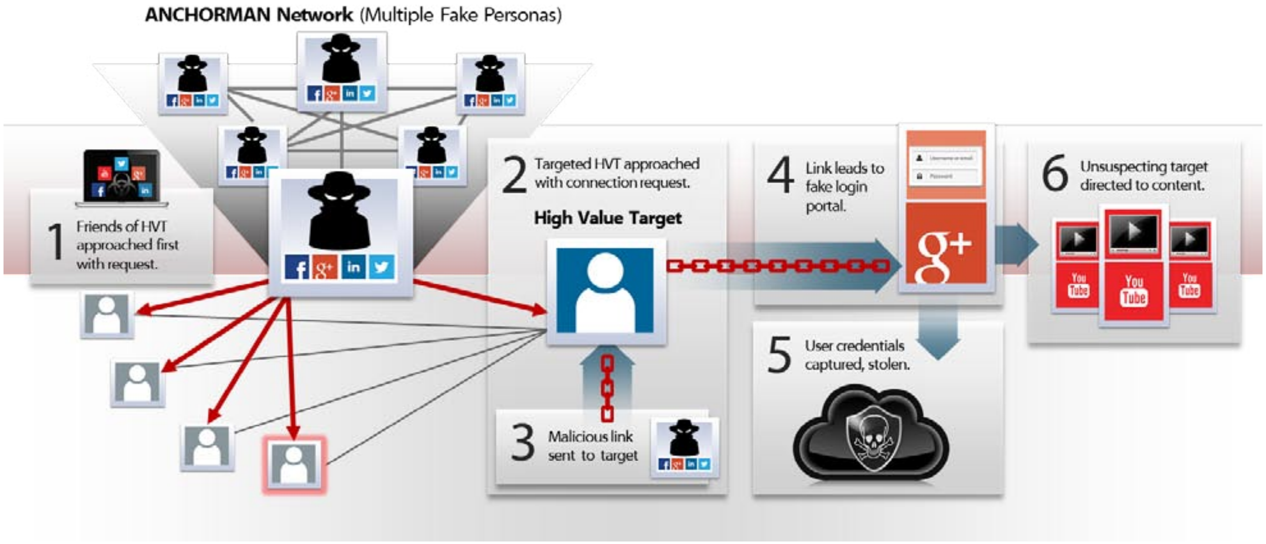
Posted date: November 26, 2013

By Amanda Tyson

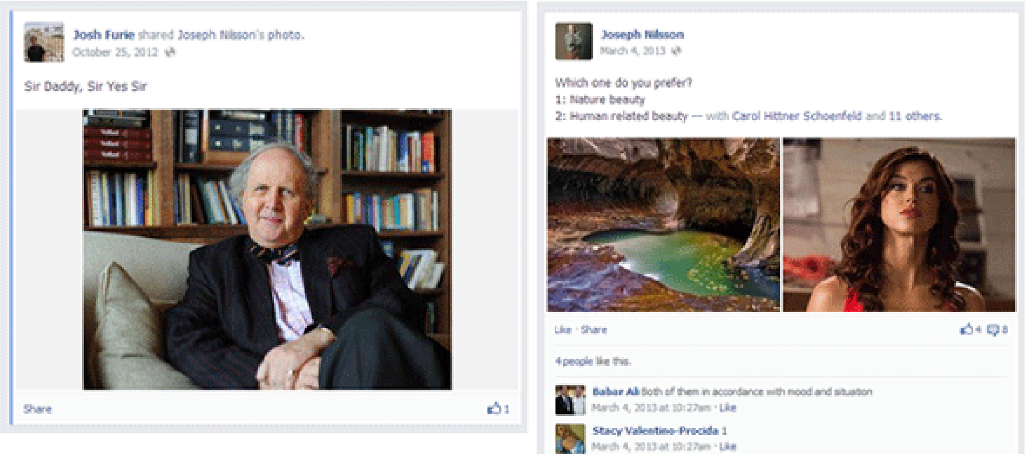
Israel should avoid taking any action that would undermine the interim nuclear agreement reached between Iran and world powers at the weekend, Britain's Foreign Secretary William Hague said on Monday.

Reuters article, reposted one day later to NewsOnAir.org and credited to Amanda Teyson (her name is misspelled, a common mistake)

- After new stories are posted to the NewsOnAir site, links to the stories are shared through the NewsOnAir Twitter account "@NewsOnAir2."
- In addition to Twitter, NewsOnAir maintains a presence on LinkedIn and Facebook.
- In addition to news content, the NewsOnAir website offers apps for download. A weather application, a radio application and an application that reminds users to rest their eyes are offered through the site. The applications are modified to call back to a server controlled by the operators with user details, but no additional functionality was found.
- Several personas claim to be members of the Nilsson family or use the surname Nilsson. Joseph Nilsson, Alfred Nilsson and Josh Nilsson appear to be actively associated with direct targeting, while additional accounts with the Nilsson name appear to have been created to support the bonafides of others.


ANCHORMAN Network (Multiple Fake Personas)
1 Friends of HVT approached first with request.
2 Targeted HVT approached with connection request.
High Value Target
3 Malicious link sent to target
4 Link leads to fake login portal.
5 User credentials captured, stolen.
6 Unsuspecting target directed to content.

High Value Targets (HVT) and Malicious Links



Josh Furie shared Joseph Nilsson's photo.
October 25, 2012

Sir Daddy, Sir Yes Sir

Share 1

Joseph Nilsson
March 4, 2013

Which one do you prefer?
1: Nature beauty
2: Human related beauty — with Carol Hittner Schoenfeld and 11 others.

Like · Share 4 8

4 people like this.

Babar Ali Both of them in accordance with mood and situation
March 4, 2013 at 10:27am · Like

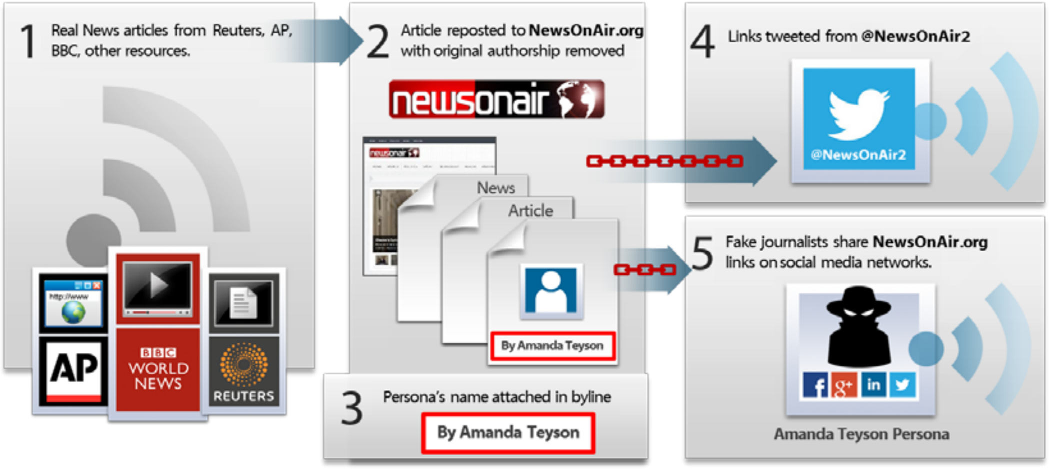
Stacy Valentino-Procida 1
March 4, 2013 at 10:27am · Like

In Facebook posts, personas intimated their fictitious familial relationships

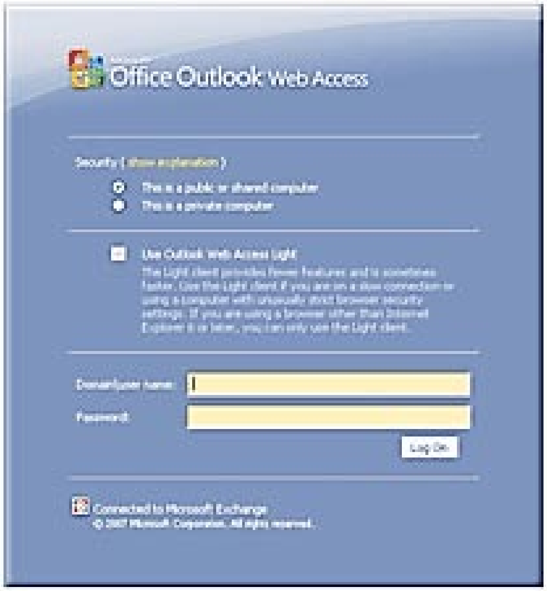
Malicious Activity

Personas are linked through infrastructure to a number of credential collection sites, which we believe are being leveraged to gain access to accounts of targeted personnel. These sites, which at first glance appear to be the banal login pages for Yahoo, Google and Outlook Web Access, are linked to the NewsOnAir.org infrastructure and can be leveraged to gain covert access to sensitive accounts. Furthermore, other connected activity suggests additional, possibly nascent malicious capabilities that are being deployed or have previously been used.

- NewsOnAir.org is connected to credential phishing sites associated with domain com-login.mobi through links to eyeleo.com-login.mobi, offered as an App of the Week through the website. Other sites hosted on the domain include:
    - youtube.com-login.mobi
    - login.yahoo.com-login.mobi
    - accounts.google.com-login.mobi
    - m.login.live.com-login.mobi


1 Real News articles from Reuters, AP, BBC, other resources.
http://www
AP
BBC WORLD NEWS
REUTERS
2 Article reposted to NewsOnAir.org with original authorship removed
newsonair
News
Article
By Amanda Teyson
3 Persona's name attached in byline
By Amanda Teyson
4 Links tweeted from @NewsOnAir2
@NewsOnAir2
5 Fake journalists share NewsOnAir.org links on social media networks.
Amanda Teyson Persona

NewsOnAir.Org: A Front News Agency



Office Outlook Web Access

Security (show explanation)

◉ This is a public or shared computer
○ This is a private computer

□ Use Outlook Web Access Light
The Light client provides fewer features and is sometimes faster. Use the Light client if you are on a slow connection or using a computer with unusually strict browser security settings. If you are using a browser other than Internet Explorer 6 or later, you can only use the Light client.

Domain\user name:
Password:

Connected to Microsoft Exchange
© 2007 Microsoft Corporation. All rights reserved.

Credential collection site that resembles an Outlook Web Access portal

- Several of the sites hosted on com-login.mobi are fictitious login sites used to surreptitiously collect unsuspecting visitors' credentials. The sites, which appear to be Outlook Web Access, Yahoo and Google login pages, have been leveraged in spear-phishing messages containing links that appear to be banal. The following link was used to send users to a credential collection page prior to redirecting them to a YouTube clip posted by the persona Jeann Maclkin:

  http://youtube.com-login.mobi/watch.aspx?v=uYvYJtzT8js&feature=youtu.be&f=g&h=http://youtu.be/kxXA2_4Yv2A

- EyeLeo and at least two other apps offered for download through the NewsOnAir.org website are modified to send victim system information back to IP address 198.20.182.55. However, they do not appear to have any additional functionality.
- An embedded and broken iFrame on NewsOnAir.org pointed to the domain internetexplorers.org. The iFrame had an extraneous double quotation mark rendering the tag invalid.
- Multiple IRC malware samples were discovered that communicate with internetexplorers.org, updatexplore.com and mcaffeea.com, domains associated through registrants and other connections to NewsOnAir.org. All of the samples used the Persian term "parastoo" as a password. Of the IRC malware analyzed, samples were configured to communicate with four channels: "weather," "radio," "albert" and "tistani." Notably, two of the apps offered on the website are radio and weather related.
- iSIGHT Partners linked the following infrastructure to the activity:

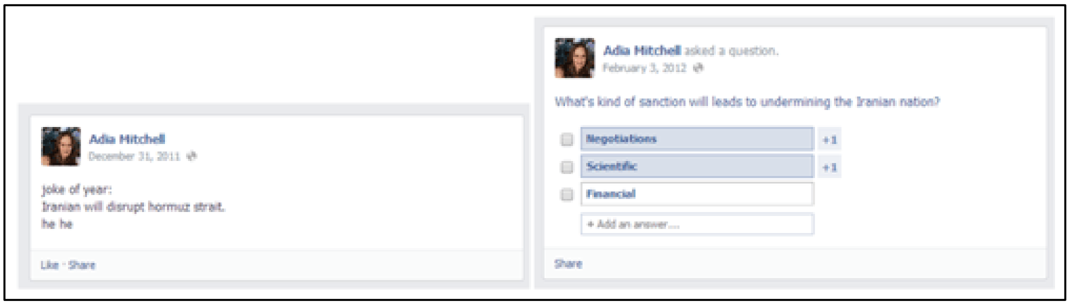
Domain	IP Address
com-login.mobi	198.20.182.55
internetexplorers.org	213.152.173.147
updatexplore.com	70.168.71.240
mcafeea.com	184.82.202.248
mediaplayercodec.net	192.69.208.213
fun4us.us	192.69.204.57
	46.4.149.236

Domain	IP Address
	199.26.84.143

Iranian Origins

Targeting, social engineering ploys, adversary operational schedule and technical indicators suggest this activity has an Iranian origin.

- In 2011 and 2012, the Adia Mitchell Facebook account "friended" multiple accounts associated with conservative and North Carolina state politics. The persona proceeded to post awkward attempts to engage Facebook friends in conversation regarding Iranian diplomacy, culminating in the posting of an online poll in which friends of the account could participate.



Adia Mitchell
December 31, 2011

joke of year:
Iranian will disrupt hormuz strait.
he he

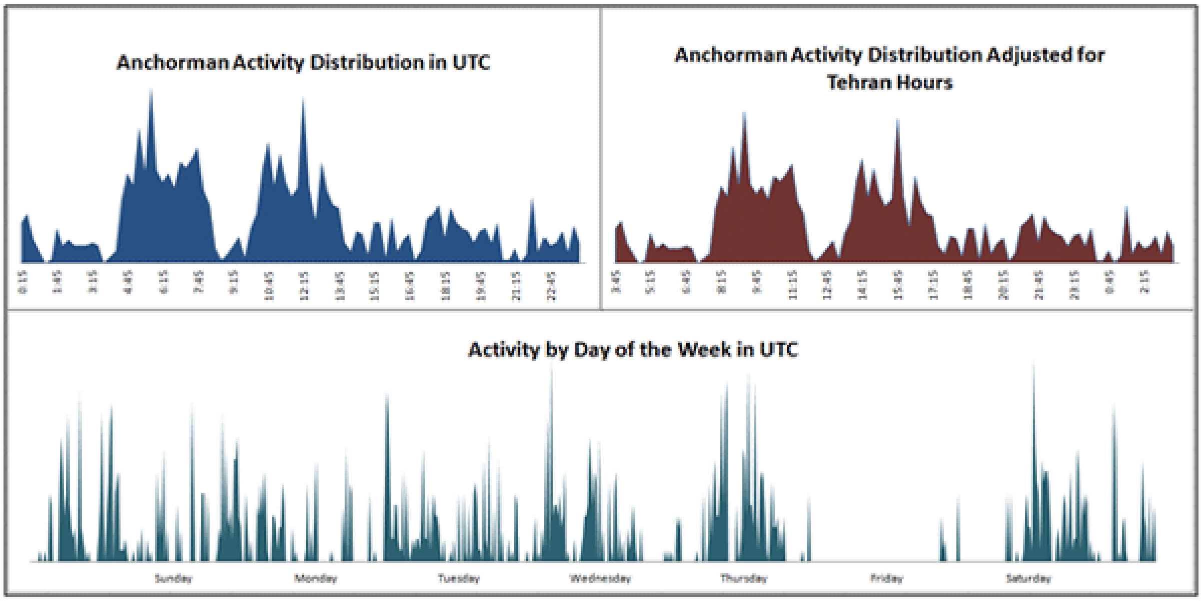
Adia Mitchell asked a question.
February 3, 2012

What's kind of sanction will leads to undermining the Iranian nation?

□ Negotiations +1
□ Scientific +1
□ Financial

Early Facebook activity included attempts to engage others on Iranian topics

- The distinctly Persian term "Parastoo" was used as a password for IRC malware associated through infrastructure to this activity. While the term is not distinct to any operator (such as the hacktivist Parastoo) it is distinctly Persian.
- NewsOnAir.org was previously registered in Tehran, and IP addresses used in infrastructure almost exclusively host Iranian content, suggesting hosting was obtained from an Iranian provider or intermediary.
- An analysis of Facebook activity indicates operators maintain regular hours that coincide with the professional workday in Tehran, Iran. Furthermore, activity drops off midday Thursday and resumes on Saturday, coinciding with the professional workweek.



Activity closely correlated with Tehran professional hours

Outlook and Implications

Cyber espionage activity with origins in Iran is not unprecedented. The Mahdi campaign, which largely focused on targets in Iran, the Gulf States and Israel, was attributed by iSIGHT Partners to an Iranian actor in 2012. Since then, iSIGHT Partners has tracked additional activity that appears to target Iran's dissident population and the US defense industrial base, such as activity attributed to members of the Ajax Security Team. International pressure and strategic uncertainty have almost certainly created an exigent need for intelligence in the country, which has been recently publicly implicated in several offensive cyber actions.

Given the covert nature of cyber espionage, its impacts are often difficult to forecast or measure; however, in this instance, we expect any accesses 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 US military or the US alliance with Israel, or impart an advantage in negotiations between Iran and the US, 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 US, 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.

Methods used in this campaign are not novel, but they are brazen, especially when compared with short-term considerably less resource intensive efforts used by other cyber espionage actors. The personal nature of this campaign sets it apart from others and raises concerns that threats to organizations and personnel are not limited to enterprise systems or the office—social networking sites, personal accounts and even family members can be a vector for compromise by an adversary who compensates for sophistication with audacious, long-term actions.

Mitigation

We advise that victims and potential victims of this campaign consider the following course of actions:

- If you suspect you may be a victim:
    - Check for communications between enterprise system and known NEWSCASTER domains and IPs.
    - Check for communications to URLs associated with NEWSCASTER social network accounts.

- If you determine you are victim:
    - Immediately contact the Federal Bureau of Investigation at either your local FBI Cyber Task Force or FBI CYWATCH:

      E-Mail: cywatch@ic.fbi.gov
      Voice: +1-855-292-3937

- Above all:
    - Never directly engage social network accounts.
    - Never visit the Newsonair.org website or any other associated sites.
    - Never disclose sensitive personally identifiable information on public social network sites.
    - Only "friend" or "accept" invites on social network sites from people who you know.
    - Be wary of unsolicited links and confirm their veracity whenever possible.

Technical Annex

Analysis of IRC Bot

Key Points:

- Analysis was performed on a binary and was found to be an IRC bot.
- Command and control (C&C) servers associated with the bot family include internetexplorers.org, update.mcafeea.com and download.updatexplore.com.

  Channels the bot attempts to join include #tistani, #Weather, #albert and #Radio. Each channel uses the same password: "Parastoo."
- Victim usernames follow consistent naming convention, such "t__" followed by three digits.

Summary

iSIGHT Partners analyzed a malicious IRC bot. Several samples of the bot were found, all connecting to shared infrastructure and using the same password to join channels on the network. From past data, it is clear the IRC bot is intended for targeted operations, as the number of simultaneous users (8) allowed onto the IRC server at a given time is extremely small.

In our search, we uncovered samples that communicated with internetexplorers.org, update.macafeea.com and download.updateexplore.com. The channels the bots attempted to join varied, but the most commonly seen channel was #tistani. Others observed were #Weather, #Radio and #albert. Each used the same password for joining the channel "Parastoo."

Technical Details

Execution

When executed, the malware first writes a configuration file to a folder in the TEMP directory. This configuration file contains a version number, the channel to join, two possible IRC nicks to use, a date and an unknown number field. The IRC bot is then copied and executed; a batch file is also written that sets the IRC bot's persistence mechanisms via registry.

After a period of sleeping, the bot attempts to join the IRC server, join the channel and await further commands. Several of the strings in the bot are encrypted with a simple substitution cipher.

Some possible commands include:

- !DCC
- !SHLNV
- !SHLV
- !CMD
- !MSF
- !DSF
- !DWN
- !DWNEXE
- SETCUR
- EXE
- SETVER
- !INI
- DRIVE
- VIEW
- REN
- MOVE
- COPY
- DEL
- MKDIR
- DIR
- EXEC
- HELp
- /start
- RESET
- KILL
- DELREG
- ISAC
- VER

The bot appears to be written to use a hard-coded boundary value for file transfers:

```
---------------------------7b4a6d158c9
```

This string appears in multiple Chinese-language forums regarding coding for file transfers.

The malware also uses the mutex "afOneCopyMutex" to ensure only one instance of the malware runs at a time.

While the bot's full functionality was not tested, it appears capable of downloading remote files, file execution and searching infected victims' disks.

Files Dropped

After successful execution, the malware drops the following files to victims' systems:

- [TEMP]\System\Configuration.ini
  - IRC Bot configuration
- [ALLUSERSPROFILE]\WindowsUpdate\System\isass.exe
  - IRC Bot
- [TEMP]\lpt1\driver.bat
  - Sets registry keys for malware persistence.

Persistence Method

While it was not observed during dynamic analysis, evidence indicates it is possible of maintaining persistence via the following registry key:

- **Key**: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\System
- **Value**: [ALLUSERSPROFILE]\WindowsUpdate\System\isass.exe

Network Communications

After successful installation/initialization, the malware proceeds to make the following callback to the C&C server over port (80/tcp):

Note: Victim to C&C in Red, C&C to Victim in Blue

```
USER AS_ # # :des
NICK t__516
JOIN :#tistani Parastoo
```

Network Intelligence

Passive DNS

According to Passive DNS, other host names in the domain (updatexplore.com) include:

- download.updatexplore.com

According to Passive DNS, other host names in the domain (mcafeea.com) include:

- downloadcenter.mcafeea.com
- update.mcafeea.com

According to Passive DNS, other host names in the domain (com-login.mobi) include:

- login.yahoo.com-login.mobi
- youtube.com-login.mobi
- www.com-login.mobi
- accounts.google.com-login.mobi
- eyeleo.com-login.mobi

Passive DNS was queried for the domain (internetexplorers.org):

- 184.82.202.248
- 141.255.161.171
- 199.26.84.169

Passive DNS was queried for the domain (update.mcafeea.com):

- 192.69.204.57
- 46.4.149.236
- 213.152.173.147

Passive DNS was queried for the domain (download.updatexplore.com):

- 192.69.208.213

Passive DNS was queried for the following IP address (199.26.84.169):

- eyeleo.com-login.mobi
- internetexplorers.org

IP Information

```
IP Location:     Switzerland Switzerland  Zurich    Private Layer Inc
ASN:     Switzerland AS51852 PLI-AS Private Layer INC (registered Nov 15, 2010)
Resolve Host:    customer9.orypt.info
IP Address:      141.255.161.171
inetnum:      141.255.160.0 - 141.255.167.255
netname:      EU-PRIVATELAYER-20110706
descr:        Private Layer INC

IP Location:     United States United States       Dallas    Dfw Datacenter
ASN:     United States AS30496 COLO4 - Colo4, LLC (registered Oct 21, 2003)
Resolve Host:    win13-169.wsp.c4d.privatedns.biz
IP Address:      199.26.84.169
Reverse IP:      507      websites use this address. (examples: 00000000.ir 1064.ir 1179.ir
1446.ir)
```

```
 NetRange:      199.26.84.0 - 199.26.87.255
NetName:       DFW-DATACENTER
```

Domain Information

This section includes a standard Whois on the domain(s) directly related to the malware, but only includes the following data:

```
Domain Name:INTERNETEXPLORERS.ORG
Created On:18-Aug-2012 09:38:08 UTC
Last Updated On:20-Dec-2013 13:27:58 UTC
Expiration Date:18-Aug-2014 09:38:08 UTC
Sponsoring Registrar:Realtime Register B.V. (R1336-LROR)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:t96dohz5wb
Registrant Name:john cortez
Registrant Organization:LLC
Registrant Street1:Lockheed Blvd
Registrant Street2:
Registrant Street3:
Registrant City:palm
Registrant State/Province:California
Registrant Postal Code:92274
Registrant Country:US
Registrant Phone:+001.4084733000
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant E-mail:john-cortez@llc.com

Domain Name:updatexplore.com
Name Server:ns03.hostcontrol.org
Name Server:ns02.hostcontrol.com
Name Server:ns01.hostcontrol.com
Created On:2012-11-29 10:34:03.0
Last Updated On:2014-01-13 11:34:03.0
Expiration Date:2014-11-29 11:34:03.0
Sponsoring Registrar:REALTIME REGISTER B.V.
Reseller:Realtime Register B.V.
Status:CLIENT_TRANSFER_PROHIBITED
Status:REDEMPTION_PERIOD
Status:CLIENT_HOLD
Status:PENDING_DELETE
Registrant ID:RC_22222159
Registrant Name:john cortez
Registrant Organization:LLC
Registrant Street1:Lockheed Blvd
Registrant City:palm
Registrant State:California
Registrant Postal Code:92274
Registrant Country:US
Registrant Phone:+001.4084733000
Registrant Fax:
Registrant E-mail:john-cortez@llc.com

Domain Name:mcafeea.com
Name Server:ns03.hostcontrol.org
Name Server:ns02.hostcontrol.com
Name Server:ns01.hostcontrol.com
Created On:2012-12-24 12:39:40.0
Last Updated On:2013-12-26 00:08:02.0
Expiration Date:2014-12-24 13:39:40.0
Sponsoring Registrar:REALTIME REGISTER B.V.
Reseller:Realtime Register B.V.
Status:CLIENT_TRANSFER_PROHIBITED
Status:CLIENT_HOLD
Status:OK
Status:AUTO_RENEW_PERIOD
Registrant ID:RC_22222159
Registrant Name:john cortez
Registrant Organization:LLC
Registrant Street1:Lockheed Blvd
Registrant City:palm
Registrant State:California
Registrant Postal Code:92274
Registrant Country:US
Registrant Phone:+001.4084733000
Registrant Fax:
Registrant E-mail:john-cortez@llc.com
```

Related Samples

- b08e84277e0f2221f187dd97273ee643
  - download.updatexplore.com.
  - internetexplorers.org
  - update.mcafeea.com
  - #albert
- f5d4f59b2cb6a98bfeadf595a29f9ca2
  - update.mcafeea.com
  - #Weather
- 994a376df0f799725fd609e125ea8efe
  - update.mcafeea.com
- c30d0f1b6f8c25ec49bbca32beb6513b
  - mcafeea.com
  - update.mcafeea.com
  - #Radio
- 7224d82bcbed0663afd1a296c587f6bf
  - Internetexplorers.org
  - #tistani
- faeb660d03beec1abfb960b1bfab2211
  - Internetexplorers.org
  - #tistani
- baa6d4d60d77dc120cf545df5d755eaf
  - internetexplorers.org
  - #tistani
- dfa72a90fdaf914756cd1f860a45f35b
  - internetexplorers.org
  - #tistani
- 4e7a9a58ceb07d111fd57174b9fc29e5
  - Internetexplorers.org
  - #tistani
- b2e6de2255946219e02872e3fc330e60
  - Data profiling tool
  - From http://eyeleo.com-login.mobi/EyeLeo_Installer_1.1.exe
  - 198.20.182.55
- 0c66db47cae6950e78a76fcacc7f5b8b
  - Data profiling tool
  - From http://newsonair.org/application/RadioTunaSetup1.exe
  - 198.20.182.55
- 4f064b3a9b230e18cbd3745a49592d26
  - Data profiling tool
  - From http://newsonair.org/application/weathersp3_StubInstaller.exe
  - 198.20.182.55

File Information

Name: driver.bat
Identifier: attacker Extension: bat
Type: ASCII text, with no line terminators
Size: 176

Packer: None detected
MD5sum: d1d457876a373b022a6afca718c71cab
Sha1: fdc4b6ba87ab8349490878a7a97eb60bce813442
Sha256: 8491c741674ca0c73dbf49d16386722d8cf21569bb85d766f562ee6083347ea3
Fuzzy:
3:iV5t/NyfrZfyM1K7eB/k+UZaYW52gidJfCdlH1MARm5IDfAuCHcHZlKDn:zH1jhRUTgidJqdEARm5IDezDn
MIME: text/plain
Compiled: NA Description: Installs persistence for bot.

Name: lsass.exe
Identifier: attacker Extension: exe
Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Size: 192512
Packer: ['Armadillo v1.71']
MD5sum: de1fbaf90f18a382289e996590d0b76d
Sha1: 4daa50171005c12cc371e80db7569b781917e2b2
Sha256: e72c0330360e4dcffb0771ca167274279cbadc7742b2dc70ffcbfc471ef62bf6
Fuzzy: 3072:nkXhoQH9FeIaAH2vBWIdaUXRrk5B2DlcgclpjguW/8/0sOKEtA:qikIUoBkGu7XX/h/2A
MIME: application/octet-stream
Compiled: 2012-08-27 01:42:15 Description: IRC Bot

Name: Configurations.ini
Identifier: attacker Extension: ini
Type: ASCII text, with CRLF line terminators
Size: 98
Packer: None detected
MD5sum: 90af5ea2c44cd57f983af552a6097b41
Sha1: a7017bc6586a8de2d42a41ec072be0c5fd236607
Sha256: dbd4fe1bd942b77376fff1b3500606bdcaa725a2dccfc5d49ed4560af816bfe6
Fuzzy: 3:3qyATWGxU8rWPPkvejyVc5DVyIXxov:avy8rVvejyQpw
MIME: text/plain
Compiled: NA Description: Configuration file for the bot.