Newscaster Group Compromises U.S. Media Company and Multiple U.S. Engineering Companies

Fusion (FS) | Cyber Espionage (CE)

April 03, 2017 10:29:00 AM, 17-00003220, Version: 1

Executive Summary

- FireEye iSIGHT Intelligence has detected active compromises and reconnaissance by Newscaster Group at multiple U.S.-based companies, including a media company, multiple engineering companies with ties to the U.S. defense industrial base (DIB), a military aerospace company, a transportation company, and an Egyptian technology services company.
- Circumstantial evidence indicates that Newscaster may have gained access to some systems by exploiting a vulnerability in Ektron CMS to upload webshell backdoors.
- The activity also leveraged a version of Mimikatz and PsExec to dump passwords, move laterally, and exfiltrate data.

Threat Detail

Newscaster Group has compromised least three U.S.-based companies, and reconnaissance has been observed at two other U.S. and one Egyptian company. At least one organization was likely compromised due to exploited vulnerabilities in an unpatched CMS platform. The activity has leveraged publicly available malware and legitimate windows tools to dump passwords and exfiltrate data.

- Newscaster Group has been detected operating inside a U.S. media company's network from March 2015 to the present and two U.S. engineering companies with ties to the U.S. DIB beginning in March 2017.
- Network reconnaissance and probing activity has been observed at a U.S. military aerospace company, a U.S. transportation company, and an Egyptian technology services company in March 2017

Initial Compromise Via Web Server Followed by Uploading Tools

At least one of the victims was initially infected via the placement of a webshell on a subdomain of a U.S. media company. Newscaster attempted to place webshells on this subdomain, likely to establish a foothold in the network.

- Newscaster likely gained access to the at least one network by exploiting CVE-2009-4473, a vulnerability in Ektron CMS that allows remote attackers to inject arbitrary code into the server.
- The actors were observed attempting to upload two webshells, ASPXSPY and Tunna, to the site from the IP address 5[.]45[.]117[.]151[.] Additional commands to these

webshells were observed originating from 5[.]101[.]122[.]222[.]
- The file m.zip (MD5: 02256910e217a146ab58b2016a934bae) was sent to the victim machine from 5[.]45[.]117[.]151[.] This ZIP file contained tools described below

Tools and Network Activity Indicate Password Stealing and Data Exfiltration

A ZIP file (MD5: 02256910e217a146ab58b2016a934bae) containing utilities to enable password stealing and exfiltration was uncovered at multiple victims. It contained a custom version of Mimikatz, the windows utility PsExec, and batch files for launching each of them and deleting the subsequent attacker files.

- MsMpEng.exe (MD5: 27552cd0d24cb1eb59259d2acd7181bf) is a custom version of the publicly available password dumping tool. It does not contain additional code, but is much smaller than the default build. A batch file, m.bat (MD5: 57195019972d4dcfb2e6ea8a3b4c3fca), would have likely been used to launch MsMpEng.exe.
- The Window's utility PsExec.exe (MD5: 27304b246c7d5b4e149124d5f93c5b01) was included with a batch file used to launch it, run.bat (MD5: faa41b1d027ebeabad1b6993a503f3b8). This would allow the attacker to remotely administer compromised systems.
- On one network, Mimikatz credential dumping was observed. A short time later, the attacker accessed an Outlook Web Access instance. Additionally, an RDP session leveraging plink/putty was detected attempting to connect with 45[.]76[.]81[.]117[.]

Indications of Wider Targeting

Additional, though more limited, network activity at a software company and open-source reporting indicate that Newscaster Group is targeting a wide array of Western-based companies, including the U.S. DIB.

- BROKEYOLK (HelpDesk4.exe, MD5: 3e372d38449971bbc64d9b99c087c7dc), a downloader used by Newscaster Group, was found calling out to msservice.site 185[.]73[.]37[.]81 at a company that provides navigation software. This incident also involved a launcher (flashplayer23ppxainstall.exe MD5: 638b74a712a7e45efc9bec126b0f2d87) and two reconnaissance tools (Network.bat MD5: 2a4c57d9f4b3101207cfef1f119b512e and info.bat MD5: 652ad9ed2bd452c14bea27b299b053c7).
- Public reporting discussed watering hole pages that leveraged BeEF, likely to target employees of U.S.-based defense contractors.

Tactics Reminiscent of Older Iranian Activity Not Previously Linked to Newscaster Group

The tactic of initially compromising web servers, then moving through the network was also leveraged in a series of compromises of U.S. entities that occurred between 2012 and 2013. These compromises included state governments in the U.S. and oil and tech companies.

- This older activity has not currently been tied to Newscaster Group, but leveraged two webshells, (MD5: a21e6576d8a6cc53c09cf56117753387 and MD5: e97cb786d7d9e7ef108b5e4a16afa850), observed at two of the U.S.-based companies in this wave of activity.

Attribution to Newscaster Group

We attribute this activity to Newscaster Group with high confidence due to the use of MsMpEng.exe (MD5:27552cd0d24cb1eb59259d2acd7181bf), m.bat (MD5: 57195019972d4dcfb2e6ea8a3b4c3fca), and the common use of file name m.bat. While Mimikatz is publicly available, this version has been customized, and we believe it is unique to Newscaster Group. Furthermore, m.bat (MD5: bd520343e2b07d810d20eec574331de9) has been observed in another Newscaster victim environment and is virtually identical to the m.bat version documented in this wave of activity.

Outlook and Implications

This activity demonstrates that Newscaster Group continues to be a threat to a wide range of U.S.-based industries. Its continued interest in media companies likely results from a desire to gain insight into coverage of Middle Eastern issues and potentially to use a compromise to spread to additional victims. Targeting engineering and DIB companies would allow Iran to potentially obtain sensitive intellectual property, which it could use to enhance its domestic military capabilities. Iran has an active ballistic missile program and may be attempting to gain information to support it.

In addition to the information gathering goals, it is possible that Newscaster Group is targeting these corporations in support of future operations designed to hurt or embarrass adversaries. Multiple organizations affected by the Shamoon malware have previously been compromised by Newscaster Group, creating the possibility that these intrusions are aimed to set the stage for a destructive attack. While we judge that such an attack would follow, rather than precede a deterioration in relations between the U.S. and Iran, the current bellicose rhetoric from both sides creates the possibility for escalation.

Please rate this product by taking a short four question survey

First Version Publish Date

April 03, 2017 10:29:00 AM

Threat Intelligence Tags

Motivation

- Financial or Economic
- Military/Security/Diplomatic

Affected System

- Enterprise/Network Systems
- Users/Application and Software

Source Geography

- Islamic Republic Of

Affected Industry

- Aerospace & Defense
- High Tech/Software/Hardware/Services
- Media/Entertainment/Publishing
- Transportation/Industrial Manufacturing/Automotive
- General Industrials
- Automobile & Parts
- Media
- Industrial Engineering
- Electronic & Electrical Equipment
- Industrial Transportation
- Industrial Support Services
- Technology

Intended Effect

- Military Advantage
- Destruction
- Embarrassment/Exposure/Brand Damage
- Competitive Advantage in Business or Economic Advantage
- Political Advantage
- IP or Confidential Business Information Theft

Tactics, Techniques And Procedures(TTPs)

- Network Reconnaissance
- Communications
- Malware Propagation and Deployment
- Enabling Infrastructures

Target Geography

- United States
- Egypt

Actor

- APT35

Targeted Information

- IT Information
- Intellectual Property

Malware Family

- Mimikatz
- Shamoon
- BROKEYOLK

Technical Indicators & Warnings

IP:	5[.]45[.]117[.]151
Identifier:	Related
Actor:	APT35
Network Type:	network
Domain:	msservice.site
IP:	185[.]73[.]37[.]81
Actor:	APT35
Network Type:	network
Identifier:	Attacker
IP:	45[.]76[.]81[.]117
Identifier:	Attacker
Actor:	APT35
Network Type:	network
IP:	5[.]101[.]122[.]222
Identifier:	Attacker
Actor:	APT35
Network Type:	network
SHA1:	08dcbb22947589537edb022eeea2532fdecfe174
Fuzzy Hash:	768:EpZjo8KBsTPVkhLG4vvv/+kdb5MHa25iBc:UZxjKhLdvvv/+kdbSHvim
Packer:	Microsoft Visual C# / Basic .NET
Actor:	APT35
File Name:	HelpDesk4.exe
SHA256:	7cdbf5c035a64cb6c7ee8c204ad42b4a507b1fde5e6708ea2486942d0d358823
File Size:	42496
File Compilation Date Time:	November 06, 2016 12:12:24 PM
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 Mono/.Net assembly
MD5:	3e372d38449971bbc64d9b99c087c7dc
SHA1:	8988b3c8372026853f5772b39c637456a7ca2d3a
Fuzzy Hash:	6144:W62iQw/qA8QI2vWSpMBRRtzThc10/QijLMbsBSMxO+TWJfPoedSRz5P:W62sV6+WSpWHtzThc1UQivMbmxO+TOAL
Identifier:	Attacker
Actor:	APT35

File Name:	m.zip
File Size:	335009
SHA256:	d3402d17d1ed7498be1f4098803861eeb189ff7976c2571b353582eceeb2c0a0
Type:	Zip archive data, at least v2.0 to extract
MD5:	02256910e217a146ab58b2016a934bae
SHA1:	6c1465c4a8e5c6c5b4fe0c19f8f3db8d37f89673
Fuzzy Hash:	3:koWoXLp0DBKbkvL6kgKCIW2o5iK79/AU4IdnOR/HOZsFWDBKbkvLN:ZmdqSgJRM09/WIdnCHFWdqSN
Identifier:	Attacker
Actor:	APT35
File Name:	run.bat
File Size:	172
SHA256:	4b58ce2a79ab179529c96d8193f905457463390efc37b3abc2acde74dd1c4354
Type:	ASCII text, with CRLF line terminators
MD5:	faa41b1d027ebeabad1b6993a503f3b8
SHA1:	b3557fc915398ec8bf6e17fc578399e4135127cd
Fuzzy Hash:	12:rVRfx9wxtTqEGnDSkpwVpSJ/T5/hk3eFSwMh5sRw2m0Cvn:rVF3w6ElkKpcT5/h8eFSwMhQwqs
Identifier:	Attacker
Actor:	APT35
File Name:	Unknown
File Size:	594
SHA256:	2e6c9a40286c7d81a927615b3c7f149e79b52038f85e9e6f1384720a2d60624b
Type:	ASCII text, with CRLF, LF line terminators
MD5:	a21e6576d8a6cc53c09cf56117753387
SHA1:	8516fca844ba1aa36a9268ab2d268250d42967e7
Fuzzy Hash:	6144:JqEm6RVbWS+KenROXrdeg1NzbAjDgLy5x3:TrRVbWWaEXrgg1NI0
Packer:	Microsoft Visual C++ 8.0 (DLL)
Actor:	APT35
File Name:	MsMpEng.exe
Malware Family:	Mimikatz
SHA256:	28290b9475c62039dda26b64e45f3e14815b6acd9ed49156a14e361df0524af8
File Size:	357376
File Compilation Date Time:	August 29, 2016 09:59:40 PM
Identifier:	Attacker
Type:	PE32+ executable for MS Windows (console) Mono/.Net assembly
MD5:	27552cd0d24cb1eb59259d2acd7181bf
SHA1:	5ef353ef57695a580ed73e4a3612ef69678ab580
Fuzzy Hash:	48:4FbrJErS4mBTiZT+TSTwTT+T+T6Tq9TeQ86P/XOj9+:4FbrJErS6Q8bc
Identifier:	Attacker
Actor:	APT35
File Name:	info.bat

File Size:	2233
SHA256:	1b3fafccb82c270bbdffec88b79c3893700f0a233d55c5b3bb394ca122a8fc8d
Type:	DOS batch file text
MD5:	652ad9ed2bd452c14bea27b299b053c7
SHA1:	923675c61f0b8d02c9412197b8ec20e646fb58a2
Fuzzy Hash:	48:Y5AoFsOERCniasZKRCesOKRCmBZuoRCkwRCTmRCkliRCcFRC3IRCqv7hSR3aKREH:YSoFsOE4n404FZ4mzuo4d4q4ks4A43I/
Identifier:	Attacker
Actor:	APT35
File Name:	Network.bat
File Size:	2473
SHA256:	a2c4dca0c6bd10c726aab687365b4fea818bca610c89cfb151e9c6b126b71cdf
Type:	DOS batch file text
MD5:	2a4c57d9f4b3101207cfef1f119b512e
SHA1:	3f024b6fe371c9b6cf609c800ae712ef11e99155
Fuzzy Hash:	3:oZBKQVtLF10BAw2/Xxhy1YR6nFk/1KbdnORn:o/9V5IV2vmYcwqdn+
Identifier:	Attacker
Actor:	APT35
File Name:	m.bat
File Size:	96
SHA256:	de3517a0678ea473598b1a291492ec87d5257acd500c2f286b04cfad77dfa707
Type:	ASCII text, with no line terminators
MD5:	bd520343e2b07d810d20eec574331de9
SHA1:	6ba78c34bd43edaad9b49090931cb221c7355300
Fuzzy Hash:	1536:gwRrdbBFb0ypL7FYDLsuXwvagSbtB54Ls4Oq4HqJuTNpatcc+IN2/AoYrLsHsKYV:n9Fb0ypL7FYDLsuXuvAtB54Ls4Oq4Hqn
Identifier:	Attacker
Actor:	APT35
File Name:	Unknown
File Size:	97568
SHA256:	45fbbdf7fec9a479281201c4150b1d7f0b87f87db8346d4cb89476b10644267d
Type:	UTF-8 Unicode (with BOM) English text, with very long lines, with CRLF line terminators
MD5:	e97cb786d7d9e7ef108b5e4a16afa850
SHA1:	1ba314dd2304d0359703aad6ddcf1e1a736003f5
Fuzzy Hash:	3:oZBKbkvLF10BAw2/Xxhy1YR6nFk/1KbdnORn:o/qSIV2vmYcwqdn+
Identifier:	Attacker
Actor:	APT35
File Name:	m.bat
File Size:	101

SHA256:	5c0ea62bb8b24ab84cf83925553803684fae52208afd652e41249ed131697c50
Type:	ASCII text, with no line terminators
MD5:	57195019972d4dcfb2e6ea8a3b4c3fca
SHA1:	ec9dd04d26ce1199712474657fbe55559d4421ab
Fuzzy Hash:	24576:78syW2MaF/aTwEjDhYnxhId1S52eAGuJwqexj1woiOPcwg:7OW9aixYnxhqU5Fxu6h4
Packer:	Nullsoft PiMP Stub -> SFX
Actor:	APT35
File Name:	flashplayer23ppxainstall.exe
SHA256:	8cebdb6c8102ac086d2ded28bb88547767943f30d0827271229f3a9731f3a078
File Size:	1278737
File Compilation Date Time:	November 12, 2005 02:55:26 PM
Identifier:	Attacker
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5:	638b74a712a7e45efc9bec126b0f2d87

Common Vulnerabilities and Exposures

CVE ID:	CVE-2009-4473(NVD Description)External Link

Version Information

Version:1.0, April 03, 2017 10:29:00 AM
Newscaster Group Compromises U.S. Media Company and Multiple U.S. Engineering Companies

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

For more information please visit: https://intelligence.fireeye.com/reports/17-00003220