APT35 Threat Group Profile

Fusion (FS) | Cyber Espionage (CE)

December 15, 2017 02:24:00 PM, 17-00014595, Version: 1

Executive Summary

- APT35 (Newscaster Team) engages in cyber operations where the goal appears to be strategic intelligence collection.
- APT35 primarily targets organizations throughout the Middle East, U.S., and Europe.
- Based on currently available data, we assess with moderate confidence that APT35 works on behalf of the Iranian Government.

Threat Detail

FireEye iSIGHT Intelligence assesses with moderate confidence that APT35 (Newscaster Team) is an Iranian Government-sponsored cyber espionage threat actor that conducts long-term, resource-intensive operations to collect strategic intelligence. APT35 has historically relied on marginally sophisticated tools during operations, including publicly available webshells and penetration testing tools, suggesting a relatively nascent development capability. However, the breadth and scope of APT35's operations, particularly as it relates to its complex social engineering efforts, likely indicates that the group is well resourced in other areas.

- APT35 targets include military, diplomatic, and government personnel from the U.S. and the Middle East, as well as organizations in the media, energy, and defense industrial base (DIB) sectors within those regions.
- From August 2016 to August 2017, APT35 engaged in multiple operations against a broad range of victims, including telecommunications, business services, technology, energy, chemical, construction and engineering, government, aerospace and defense, and media entities in the Middle East, U.S., and Europe.
- APT35 sought information related to organizations' network information, credentials, user emails, and host information from compromised systems.
- APT35 has also demonstrated efforts to hide their tracks likely to ensure continued access to victim environments by taking actions such as deleting log files, clearing evidence of search queries, and searching for evidence of previous computer intrusion-related investigations.

Affected Industries

- Aerospace/Military
- Business Services
- Chemical
- Construction/Engineering
- Consulting Services

- Energy
- Financial
- Government
- High Tech
- Media/Entertainment
- Telecommunications

Affected Countries

- Egypt
- Germany
- Iraq
- Netherlands
- Saudi Arabia
- Switzerland
- United States

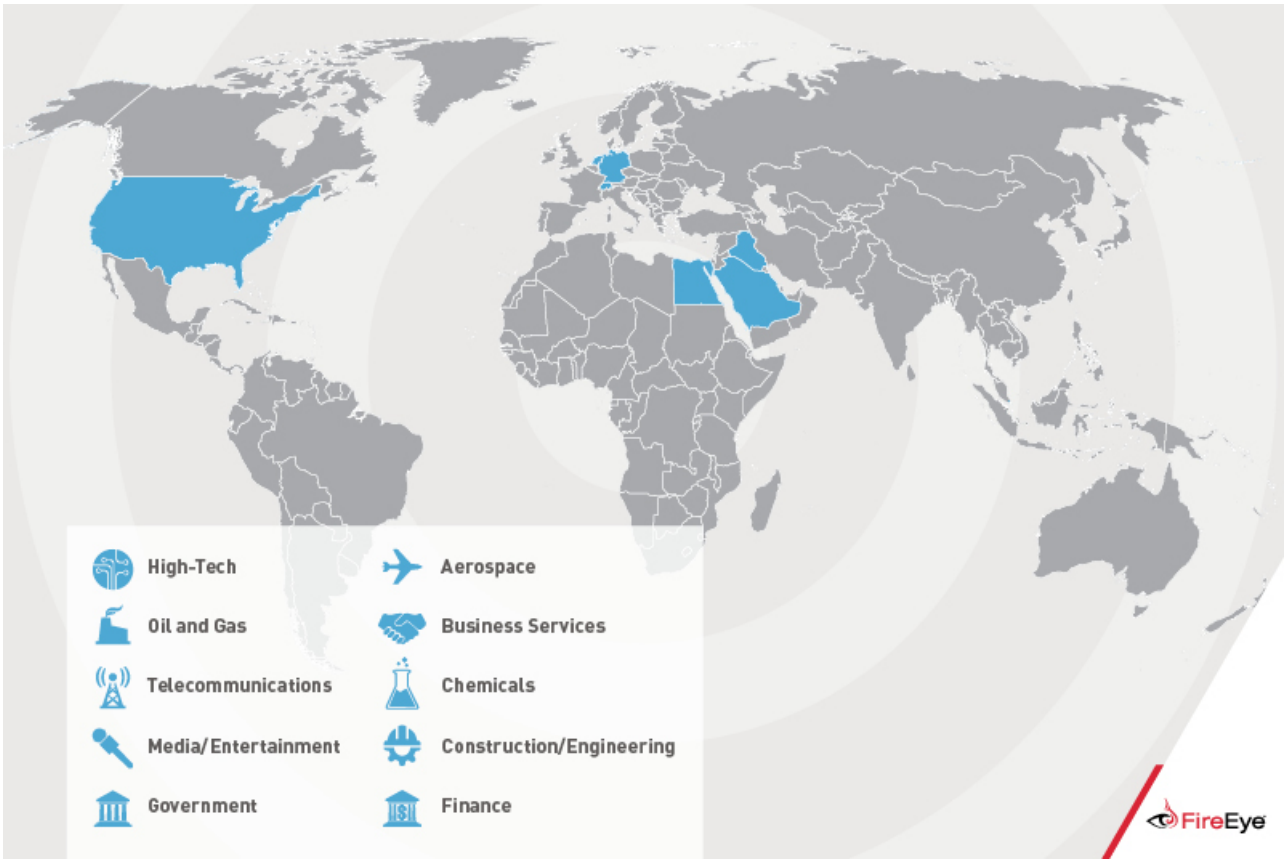

Figure 1: Scope of APT35 targeting

Previously Reported Activity

FireEye has observed APT35 operations as early as 2014. Historically, the group leveraged social engineering techniques through large networks of online personas across multiple social media platforms. Many of these personas claimed to be part of news organizations or employees for defense contractors. The necessary effort required to establish these networks and online front organizations suggests that the group is well resourced. More recent operations suggest that APT35 has expanded their targeting both in scope and

employed toolset.

- Research in May 2014 uncovered multiple suspected APT35 online personas with collective connections to thousands of individuals across LinkedIn, Facebook, Twitter, Google, WordPress, and Blogger. This network used pictures and information of real people. Many of these personas purported to be media professionals and defense contractors.
- In April 2015, APT35 registered a news-themed domain as part of the command and control (C&C) infrastructure for DRUBOT malware. In one instance, an early persona masqueraded as a representative of a media organization that would be targeted a few years later.
- In May 2015, the group expanded its toolset with weaponized Android Package Kits (APKs) to target Android mobile devices.
- In August 2016, APT35 continued to target Middle East organizations in the commerce and oil and gas industries using elaborate social engineering schemes. In one example, APT35 attempted to entice a victim by sending a spear-phishing email with a link to a "funny video." When that effort failed, APT35 persisted and sent a second spear-phishing email threatening to deactivate the user's Outlook Web Apps (OWA) account.
- In March 2017, APT35 performed network reconnaissance and probing activity at a U.S. military aerospace company, a U.S. transportation company, and an Egyptian technology services company. APT35 also targeted a company that provides software to the defense industry during the same month.

APT35 Tactics, Techniques, and Procedures (TTPs)

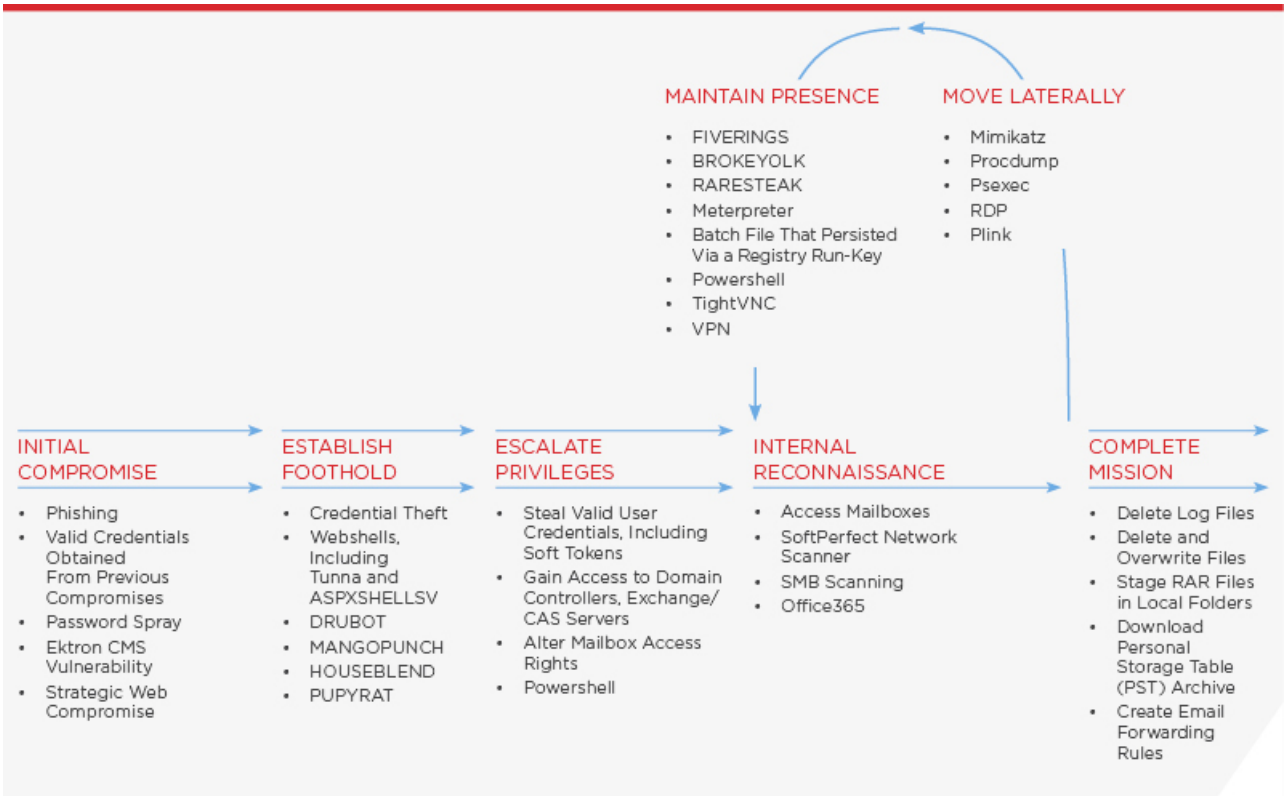

Figure 2: APT35 attack lifecycle

Initial Compromise

APT35 typically relies on spearphishing to initially compromise an organization, often using lures related to health care, job postings, resumes, or password policies. However, we have also observed the group using compromised accounts with credentials harvested from prior operations, strategic web compromises, and password spray attacks against externally facing web applications as additional techniques to gain initial access. Password spray is a technique that attempts to guess username password combinations using a small number of passwords against a large volume of users.

- In one instance, the group leveraged a malicious macro-enabled .doc file masquerading as a resume associated with an energy company.
- APT35 leveraged truncated links (briefl.ink) in spear-phishing emails, likely attempting to appear as a legitimate service. These links would redirect victims to domains hosting malicious macro-enabled documents.
- APT35 appears to use valid credentials obtained from previous compromises to access victim environments in some cases. In one example, there was no evidence that APT35 circumvented or exploited a vulnerability to gain access to a target's web application, suggesting that the group already had access to valid user credentials. In other cases, APT35 used previously harvested legitimate credentials to access VPN and webmail accounts at victim organizations.
- APT35 targeted an organization with a macro-enabled weaponized version of an internal document. We discovered the group storing this .doc file on the victim's SharePoint page, suggesting an attempt to create a strategic web compromise within the environment.
- In one instance, APT35 gained initial access by leveraging a vulnerability in the Ektron CMS that was installed on the company's web server.
- In late 2016, APT35 engaged in a password spray attack against an organization's OWA interface. The group generated millions of authentication attempts on the organization's accounts.

Establish Foothold

APT35 frequently uses publicly available tools, such as Mimikatz and PupyRAT, to establish a foothold on compromised systems.

- Using the publicly available Mimikatz credential harvester, APT35 attempts to remotely gather credentials on compromised machines. In at least one operation, PsExec was used to deploy a batch script that executed a Windows-compiled variant of Mimikatz.
- APT35 also employed malicious macro-enabled documents that installed an in-memory PupyRAT payload, an open-source Python-based backdoor, to establish a foothold on victims' systems.
- APT35 uses a variety of webshells to establish a foothold on internet-facing servers. The two most common ones used are ASPXSHELLSV and TUNNA.
- APT35 uses the HOUSEBLEND downloader and the DRUBOT and MANGOPUNCH backdoors that are unique to the group to establish a foothold on victims' systems.

Malware Family	Description	Availability
ASPXSHELLSV	Webshell	Public
PUPYRAT	Backdoor	Public
TUNNA	Webshell	Public
MANGOPUNCH	.Net Backdoor	Non-Public
DRUBOT	Backdoor	Non-Public
HOUSEBLEND	Downloader	Non-Public

Table 1: APT35 tools used to establish foothold

Privilege Escalation

The group primarily uses publicly available or Windows-native utilities to escalate privileges on victims' systems in addition to PowerShell commands.

- APT35 frequently deploys the publicly available Mimikatz credential harvester to systems, often using a batch file named "m.bat" to execute it. This technique is commonly used amongst other suspected Iranian groups, with the filename "m.bat" frequently used by APT35.
- APT35 uses the ProcDump utility to dump the memory of lsass.exe to enable credential scraping. These memory dumps are typically archived in .zip files.
- During multiple operations, APT35 altered mailbox access rights to gain privileged access to multiple other users' or group's mailbox accounts. APT35 used PowerShell cmdlets to add a delegate to each of the targeted accounts, likely to reduce the overhead associated with accessing multiple accounts. Instead of having to separately log in to each targeted account, APT35 used the single delegate account to access the mailboxes for all of the targeted accounts.
- Once inside the victim's network, APT35 also searched for RSA SecureID soft tokens to subsequently authenticate to the target's VPN using valid credentials.

Internal Recon

- On multiple occasions, APT35 used the publicly available SoftPerfect Network Scanner to identify potential victim hosts and network segments.
- APT35 accesses OWA mailboxes with Full Access permissions and searches for account credentials.
- During at least one operation, APT35 used the Office 365 eDiscovery console, an administrator tool to search for content in Exchange Online mailboxes, SharePoint Online, and OneDrive.

Lateral Movement

The group frequently leverages publicly available tools to move across victims' systems and relies on RDP and SMB sessions.

- During multiple operations, the group used Mimikatz to gather credentials across multiple systems on victims' networks.

- APT35 frequently uses the ProcDump utility to extract a copy of lsass.exe process memory on multiple systems.
- APT35 often uses stolen credentials and RDP sessions to connect to multiple other systems and connect to attacker-controlled infrastructure to download further tools.
- The group uses the publicly available PsExec utility to run commands on remote hosts.
- After compromising systems, the group heavily relies upon SMB to move laterally to other systems using stolen credentials.

Maintain Presence

APT35 leverages several malware families, some that are unique to the group and others that are publicly available, to maintain presence on compromised machines.

- APT35 deployed BROKEYOLK, a .NET downloader that downloads and executes a file from a hard-coded C&C server, as a service to execute automatically on system start.
- The group leveraged a publicly available Metasploit payload, Meterpreter, to maintain persistence on machines.
- APT35 created a batch file that persisted via a registry Run key. The file was later deleted and replaced with another batch file.
- The group frequently uses Plink to create reverse-SSH tunnels to tunnel RDP connections into victims' networks from attacker-controlled hosts on the internet. APT35 often delivers Plink to externally facing servers alongside webshells.
- During operations, the group deployed the non-public FIVERINGS data miner to gather system information and screenshots that were uploaded to its C&C server via HTTP Simple Object Access Protocol (SOAP) webservices.
- We observed the group using the non-public BROKEYOLK downloader to download files from hard-coded C&C servers via HTTP SOAP requests.
- APT35 used two batch-scripts that executed PowerShell code that connected to a public IP address and downloaded malware on the system.
- In one operation, APT35 used an executable copy of TightVNC, a legitimate tool for remote access.
- During some operations, the group connected to victims' VPNs from multiple compromised accounts.
- APT35 will also create new Windows user accounts and groups to facilitate access.

Malware Family	Description	Availability
BROKEYOLK	.Net Downloader	Non-Public
FIVERINGS	Data Mining Backdoor	Non-Public
RARESTEAK	Uploader	Non-Public

Table 2: APT35 tools used to maintain presence

Network Infrastructure

APT35's domain names, domain registration information, and infrastructure provider selection for C&C is reflective of attempts to masquerade as legitimate services and hide its true identity.

- APT35 commonly uses domains masquerading as legitimate services or entities such as the BBC, Chrome, Microsoft, Mozilla, and government portals (see Table 3).
- While early APT35 domain registrations used pseudonyms, more recent activity suggests a reliance on privacy protection services.
- APT35 commonly uses well-known VPS providers, including Hertzner, Digital Ocean, and LeaseWeb.

Domain	Registrant Email	Registrant Name
com-adm.in	gdetorres46@yahoo.com	Gleen Torrs
local-news.org	gdetorres46@yahoo.com	Glenn Torres
bbconline.net	gdetorres46@yahoo.com	Glenn Torres
maildelivery5.com	gdetorres46@yahoo.com	Gleen Torres
sitesynchronization.info	gdetorres46@yahoo.com	Glenn Torres

Table 3: Sample domains

Mission Complete

Typically, APT35 takes steps to remove indicators of some activity within systems and networks as part of its operational security. The group is known to delete system log files as well as Volume Shadow Copies created on compromised systems.

- During at least one operation, APT35 staged data archived in a RAR folder on the local machine before exfiltration.
- APT35 typically deletes log files to remove evidence of their presence on systems.
- The group deletes all attacker-created Volume Shadow Copies, which create a backup of key system files that are not locked or protected by the operating system. APT35 used this technique to retrieve a copy of the ntds.dit database of all user credentials from the Active Directory server.

Data Theft

To exfiltrate sought-after data, APT35 uses built-in utilities and email forwarding rules, in addition to uploading RAR archives by leveraging the non-public RARESTEAK uploader.

- APT35 has used CSVDE, a built-in command-line tool, to export information from a victim organizations' Active Directory.
- The group frequently compromises a target's Office 365 environment to exfiltrate data.
- During at least one operation, we found APT35 forwarding emails from a victim's email address to an attacker-owned email address.
- APT35 uses the non-public RARESTEAK uploader to upload RAR archives to an attacker-owned C&C IP address.

Operational Security

APT35 frequently works to minimize evidence of activity on victims' systems, likely to maintain access to compromised environments and complicate victims' remediation efforts. Notably, during an ongoing compromise, the group searched for reports relating to current intrusions, likely to collect intelligence on the victim's investigative and remediation efforts. This type of data regarding how the victim reacted to previous compromises provides APT35 with a better understanding on how to avoid future discovery.

- The group deletes log files, including Security and System Windows event logs. In at least one instance, APT35 deleted all Volume Shadow Copies that the group previously created.
- In at least one compromise, APT35 used the Sysinternals ProcDump utility to extract a copy of the lsass.exe process memory. By acquiring a copy of the lsass.exe process memory, an attacker can extract credentials offline without executing utilities on the local system that may generate an alert by an anti-virus or host intrusion prevention system (HIPS).
- After using the Office 365 eDiscovery console to perform searches on a victim network, APT35 removed several of their queries from the application's search history.
- During an intrusion, APT35 used features in the Office 365 eDiscovery console to preview search results, which allowed the group to view the search results within the application without having to download any files locally to the system.

Information Targeted Aligns with Nation-State Intelligence Interests

Similar to other suspected Iranian cyber threat groups, APT35's activity suggests an interest in gathering intelligence about government, military, and energy entities. Unlike the regional focus of APT34, APT35 appears to have a broader operational reach, suggesting that it has a large-scale mission to gather strategic intelligence to benefit the Iranian Government.

- APT35 has targeted military and diplomatic personnel, as well as several defense contracting firms in the U.S. and the Middle East.
- In at least one operation, the group searched for and viewed data relating to government, military, technology, energy, telecommunications, finance, and consulting organizations using the Office 365 eDiscovery console.
- APT35 has also targeted information relating to the Middle East Government, oil and gas industries, as well as military and aviation organizations.
- APT35 frequently targets credential information, including targeting the mailboxes of organizations' IT teams to potentially further access to victim environments.

Iranian Attribution

We assess with moderate confidence that APT35 is an Iranian cyber espionage threat group based on the group's use of Iranian infrastructure, hours of operation, as well as its targeting of entities and data that align with government interests.

- APT35's targeting of military, government, and energy entities, with particular focus on Middle East organizations, aligns with previous targeting by Iranian threat groups.
- Previous APT35 operations have aligned with working hours in Tehran. While more recent APT35 activity has varied in terms of operational hours, this may be due to potential expansion of scope in targeting efforts.
- APT35 has logged in to organizations' VPNs from IP addresses originating from Iran. These IP addresses are assigned to Iran Cell Service and Communication Company and Mobile Communications Company of Iran, respectively, both of which are headquartered in Tehran (Table 4).

IP Address	ASN	NETBLOCK
31.2.187.16	Mobile Communications Company of Iran	Notrino
31.2.210.242	Mobile Communications Company of Iran	Mobile Communication Company of Iran
5.106.154.254	Mobile Communications Company of Iran	Mobile Communication Company of Iran
5.112.141.58	Iran Cell Service and Communication Company	Iran Cell Service and Communication Company
5.114.216.155	Iran Cell Service and Communication Company	Iran Cell Service and Communication Company
5.121.30.161	Iran Cell Service and Communication Company	Iran Cell Service and Communication Company
5.122.193.155	Iran Cell Service and Communication Company	Iran Cell Service and Communication Company
5.122.86.127	Iran Cell Service and Communication Company of Iran	Iran Cell Service and Communication Company of Iran
5.210.250.79	Mobile Communications Company of Iran	Mobile Communication Company of Iran

Table 4: Iranian IP addresses that attempted to log on to target organization's VPN

Please rate this product by taking a short four question survey

First Version Publish Date

December 15, 2017 02:24:00 PM

Threat Intelligence Tags

Motivation

- Military/Security/Diplomatic

Affected System

- Enterprise/Application Layer
- Users/Application and Software

Source Geography

- Iran

Affected Industry

- Aerospace & Defense
- Governments
- Energy & Utilities
- Financial Services
- Governments → Security/Military/Law Enforcement
- Business and Professional Services/Legal/Accounting/Consulting
- High Tech/Software/Hardware/Services
- Telecommunications
- Construction & Engineering
- Media/Entertainment/Publishing
- Electricity
- Media
- Government - Subnational
- Legal
- Construction & Materials
- Government - National
- Technology

Intended Effect

- Military Advantage
- Credential Theft/Account Takeover
- Political Advantage

Tactics, Techniques And Procedures(TTPs)

- Social Engineering
- Network Reconnaissance
- Malware Propagation and Deployment
- Domain Registration/DNS Abuse and Manipulation

Target Geography

- Saudi Arabia
- Afghanistan
- Netherlands
- Syrian Arab Republic

- United States
- Egypt
- United Kingdom
- Israel
- Iraq
- Switzerland
- Germany

Actor

- APT35

Targeted Information

- Government Information
- IT Information
- Sales/Marketing Data
- Credentials

Technical Indicators & Warnings

Network Type:	network
Domain:	sitesynchronization.info
Identifier:	Attacker
IP:	5.121.30.161
Identifier:	Related
Network Type:	network
Network Type:	network
Domain:	bbconline.net
Identifier:	Attacker
IP:	5.210.250.79
Identifier:	Attacker
Network Type:	network
Network Type:	network
Domain:	briefl.ink
Identifier:	Attacker
IP:	5.112.141.58
Identifier:	Attacker
Network Type:	network
Network Type:	network
Domain:	bbconline.net
Identifier:	Attacker

Network Type:	network
Domain:	maildelivery5.com
Identifier:	Attacker
IP:	31.2.187.16
Identifier:	Related
Network Type:	network
IP:	5.122.86.127
Identifier:	Related
Network Type:	network
Network Type:	network
Domain:	com-adm.in
Identifier:	Attacker
IP:	5.106.154.254
Identifier:	Attacker
Network Type:	network
IP:	31.2.210.242
Identifier:	Related
Network Type:	network
IP:	5.122.193.155
Identifier:	Related
Network Type:	network
IP:	5.114.216.155
Identifier:	Attacker
Network Type:	network
Network Type:	network
Domain:	local-news.org
Identifier:	Attacker

Version Information

Version:1.0, December 15, 2017 02:24:00 PM
APT35 Threat Group Profile

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

For more information please visit: https://intelligence.fireeye.com/reports/17-00014595