Suspected Adversary: APT34 (OilRig)(HelixKitten), Iranian-Aligned Intelligence Collection Group

History

APT34 — also known as OilRig — is a cyber-espionage group that has been active since at least 2014.

Based on information gathered from sources like Mandiant, CrowdStrike,

Recorded Future, and Mitre.

Nation/state are they associated with?

Iran

Targeted industries:
Middle Eastern sectors such as,
Energy (especially oil and gas),
Government,
Finance, Telecommunications
and Chemical industries

APT34 Motives

Category	Details
Primary Objective	**Intelligence gathering** — stealing confidential government, corporate, and energy sector data.
Targets	- **Government ministries** (especially foreign affairs, defense, energy). - **Financial institutions**. - **Energy companies** (especially **oil and gas**, critical to Iran's regional interests). - **Telecommunications firms**. - **Chemical and engineering firms**.
Political Motivation	Support **Iran's national interests**, particularly in regional influence across the Middle East. Their activity often coincides with geopolitical tensions (e.g., sanctions, nuclear negotiations).
Economic Motivation	Obtain commercial secrets that can **boost Iran's domestic industries** (especially oil and technology sectors).

Strategic Motivation	Maintain **surveillance over rivals** (both regional rivals like Saudi Arabia, UAE, Israel, and Western countries). Gain long-term access to networks to **anticipate political moves** and **negotiation strategies**.
Tactical Motivation	Create **persistence within critical infrastructure** so that they could, if needed, pivot to sabotage (though APT34 itself tends to focus more on espionage).

APT34 TTPs

Tactic	Technique	Description
Initial Access	T1566.001 – Spearphishing Attachment	Sends emails with malicious attachments to compromise victims.
	T1566.002 – Spearphishing Link	Emails contain links to credential harvesting sites (e.g., fake Outlook logins).
Execution	T1059 – Command and Scripting Interpreter	Uses PowerShell scripts to execute malicious payloads post-infection.

Persistence	T1505.003 – Web Shell	Installs web shells on compromised servers for persistent remote access.
	T1078 – Valid Accounts	Harvests and abuses legitimate user credentials to maintain long-term access.
Privilege Escalation	T1055 – Process Injection	Injects code into legitimate processes to evade detection and elevate privileges.
Defense Evasion	T1070.004 – File Deletion	Deletes artifacts and malware after use to avoid detection.
	T1027 – Obfuscated Files or Information	Obfuscates payloads and scripts to bypass security solutions.
Credential Access	T1110.001 – Password Guessing	Tries weak passwords for remote access and lateral movement.
	T1556.001 – Credentials from Password Stores	Targets saved credentials from browsers or password vaults.
Discovery	T1083 – File and Directory Discovery	Searches the filesystem for sensitive files and folders.

	T1016 – System Network Configuration Discovery	Gathers information about the network topology and configurations.
Lateral Movement	T1021.002 – SMB/Windows Admin Shares	Moves laterally within networks via SMB and shared admin accounts.
Collection	T1114.002 – Email Collection via Mail Client	Steals emails using direct access to mail clients like Outlook.
	T1560.001 – Archive Collected Data	Archives stolen data for easier exfiltration.
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols	Uses HTTPS and HTTP to communicate with command-and-control servers.
	T1105 – Ingress Tool Transfer	Downloads additional malware/tools into compromised environments.
Exfiltration	T1048.002 – Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Uses secure channels like HTTPS to exfiltrate stolen data without detection.