APT34 (OilRig) Investigation Report

APT34, also known as OilRig. They were once considered to be separate entities until more reports show further overlap they have together. They're a persistent cyber espionage group widely believed to be operating on behalf of the **Iranian** government. They're notorious for stealing information and executing cyber espionage campaigns in alignment with Iran's national interests.

Targeted industries:

APT34 has targeted a broad scope of sectors focused on economic development and geopolitical influence. Their targets include:

- Technology services
- Oil and Gas Industries
- Telecommunications
- Financials industries
- Aerospace & Defense
- Government and Critical Infrastructure.

Motivations:

APT34's primary objective is information gathering tied to Iran's geopolitical interest. They have focused on Espionage as a practice of spying on foreign governments or competing companies that are political, military, business, and financial for obtaining their plans and activities. The attacks can be damaging as data breaches, intellectual property theft, operational threats etc.

Tactics, Techniques, Procedures:

APT34 conducted a wide range of Tactics, Techniques, Procedures (TTPs) that are consistent with long-term, stealth espionage campaigns. Common techniques include:

Tactic	**Technique**	**MITRE ATT&CK ID**	**Technique**
Initial Access	Phishing	T1566	Spearphishing emails with malicious attachments. They are also spread to job offers in websites like Linkedin.
Command and Control	Encrypted Channel: Asymmetric Cryptography	T1573.002	They used the PowerExchanged utility to create c2 channels.
Command & Control	Drive-by-Compromise	T0817	Utilized Watering hole attacks to collect credentials that could

			be used to gain access to ICS networks.
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001	Credential dumping tools such as Mimikatz to steal credentials to log into the compromised system and Outlook web access.

Mitigation Strategies

Organizations can protect against APT34 and similar threats by implementing a layered defense strategy:

Migration	**ID**	**Description**
User training	M1017	Users can be trained to identify social engineering techniques and phishing emails.
Restrict Web-Based Content	M1021	Determine if certain website attachment extensions can be used for phishing to block content for business operations.
Network Intrusion Prevention	M1031	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity.
Valid Accounts	T1078	Require MFA as another critical layer of defense even when the user's credentials are compromised.
Application Isolation and sandboxing	M0948	Built-in browser sandboxes