APT34 Cybersecurity Threat Intelligence Report

Prepared by: Gabriel Reis Santos
Role: Cybersecurity Consultant – Datacom
Date: 20 jun 25

Introduction

This report investigates the cyber threat group APT34 and outlines key findings based on open-source intelligence (OSINT) research. APT34, also known as OilRig or Helix Kitten, is a state-sponsored actor linked to several high-profile cyberattacks. The purpose of this report is to provide an overview of APT34's history, objectives, and techniques, and to recommend defensive strategies that the client can implement to reduce the risk of future intrusions.

APT34 History and Background

APT34 has been active since at least 2014 and is widely believed to be an Iranian cyber-espionage group. The group typically targets organizations in the Middle East but has also been observed conducting attacks against entities in Europe and North America. APT34 is known for using custom malware, social engineering, and credential harvesting to maintain long-term access to victim environments. Security firms such as FireEye (now part of Mandiant), Symantec, and CrowdStrike have extensively documented the group's activity. Their operations often align with the strategic interests of the Iranian government, especially in the fields of oil and gas, telecommunications, and critical infrastructure.

Nation-State Affiliation

APT34 is associated with the Islamic Republic of Iran. The group is suspected to operate under or in collaboration with Iran's Ministry of Intelligence and Security (MOIS). Its campaigns often support the country's geopolitical and intelligence-gathering objectives.

Targeted Industries

APT34 has primarily targeted organizations in the following sectors:

- Oil and gas
- Energy and utilities
- Telecommunications
- Financial services
- Government and public sector
- Critical infrastructure providers

Their targeting suggests a focus on both strategic intelligence and industrial disruption.

Motivations

The primary motivations behind APT34's campaigns appear to be:

- Intelligence gathering and espionage
- Surveillance of foreign governments and private industry
- Strategic disruption of adversarial infrastructure
- Gaining persistent access for potential future operations

Their attacks are carefully planned and often involve long dwell times within compromised networks.

Tactics, Techniques, and Procedures (TTPs)

Using the MITRE ATT&CK framework, APT34's known tactics and tools include:

Initial Access

- Spear phishing emails with malicious attachments or links
- Exploitation of public-facing applications

Execution

- PowerShell scripts
- Malicious Office macros

Persistence

- Registry run keys or startup folders
- Scheduled tasks

Credential Access

- Keylogging and credential dumping

Lateral Movement

- Remote Desktop Protocol (RDP) with stolen credentials
- Windows Admin Shares

Command and Control

- HTTP(S) and DNS-based communication

Exfiltration

- Data staging and transfer over command and control channels

Tools Used

- POWBAT
- QUADAGENT
- SEASHARPEE
- DNSpionage

APT34 has also been observed exploiting known vulnerabilities such as CVE-2017-0199 (Microsoft Office) and CVE-2018-6789 (Exim Mail Server).

Security Recommendations
To mitigate the risk of future attacks by APT34 or similar threat actors, the following measures are recommended:

Short-Term (0–30 Days)

- Enforce multi-factor authentication (MFA) across all user accounts
- Immediately patch vulnerable software and systems
- Conduct an organization-wide password reset
- Initiate a forensic review of logs, endpoints, and DNS activity
- Notify relevant stakeholders and regulators if necessary

Medium-Term (30–90 Days)

- Deploy endpoint detection and response (EDR) tools
- Implement stronger email filtering and attachment sandboxing
- Conduct mandatory phishing awareness training for employees
- Review and limit user access privileges

Long-Term (90+ Days)

- Adopt Zero Trust Architecture
- Regularly conduct red/purple team exercises simulating APT-style attacks
- Maintain up-to-date incident response plans
- Ensure segmented network architecture to contain lateral movement
- Subscribe to threat intelligence feeds from trusted sources

Conclusion

APT34 represents a persistent and well-resourced cyber threat. Their use of advanced techniques and alignment with state objectives means that organizations must adopt a proactive, defense-in-depth strategy. By applying the MITRE ATT&CK framework and implementing strong technical and procedural controls, the client can significantly improve their resilience against targeted cyberattacks.

References

MITRE ATT&CK – APT34: https://attack.mitre.org/groups/G0049/
Mandiant Threat Intelligence – https://www.mandiant.com/
CrowdStrike – https://www.crowdstrike.com/
Recorded Future – https://www.recordedfuture.com/
CISA – https://www.cisa.gov/