OilRig

[/ ˈɔɪl rɪg /]

OilRig (APT34 / Helix Kitten) is an Iran-linked cyber espionage group active since around 2014 and aligned with Iranian strategic intelligence objectives. In 2025, it focused on energy and defense targets across the Middle East and Europe, using spearphishing and cloud credential abuse.
The group poses a high risk due to its persistent operations, rapid adaptation, and collaboration with other Iran-nexus threat actors.

IDENTITY

Attribution / Origin : Iran-linked threat actor, associated with the Islamic Revolutionary Guard Corps (IRGC) Intelligence Organization.

Active Since : ~2014

Aliases : Earth Simnavaz, ATK40, Greenbug, TA452, APT34, CHRYSENE, G0049, Cobalt Gypsy, Crambus, EUROPIUM, Evasive Serpens, Hazel Sandstorm, Helix Kitten, IRN2, Twisted Kitten.

Motivation : Cyber-espionage, surveillance, and intelligence gathering to support Iranian political, military, and economic objectives.

TTPs

Initial Access : Spearphishing emails, supply chain compromise, credential harvesting via fake login portals, exploitation of VPN and email vulnerabilities.

Persistence : Custom PowerShell scripts, credential reuse across environments, and deployment of lightweight backdoors (e.g., Tonedeaf, Karkoff).

Command & Control (C2) : HTTPS, DNS tunneling, and cloud-based infrastructure for covert communications.

Malware & Tools : Tonedeaf, Helminth, Karkoff, PoisonFrog, BONDUPDATER, and DNSMessenger; frequent use of custom droppers and credential-stealing implants.

Techniques : Data exfiltration via cloud services, lateral movement through stolen credentials, and abuse of Microsoft 365 and Azure infrastructure for persistence and reconnaissance.

TARGET PROFILE

Target Sectors : Government, Energy, Defense, Telecommunications, Finance, and Academia.

Target Geographies : Middle East (UAE, Saudi Arabia, Israel), Europe (UK, France, Netherlands), and North America.

THREAT ASSESSMENT

Risk Level : High (Regional and Strategic)

Recent Activity : 2025 activity included campaigns targeting energy and defense industries using compromised Microsoft 365 credentials and cloud storage abuse.

Evolution : Shift from spearphishing-only operations to hybrid cloud intrusions and collaboration with other Iran-nexus actors (MuddyWater, Agrius, Peach Sandstorm). Increasing operational security and rapid adjustment to global sanctions-related geopolitics.

NOTABLE OPERATIONS

2017 – Greenbug Campaign: Compromised Middle Eastern telecom networks using custom Helminth backdoors.

2019 – DNSMessenger Operation: Leveraged DNS tunneling to exfiltrate data from oil and gas companies in the Gulf region.

2022 – Compromise of European Energy Firm: Used phishing and cloud-based persistence mechanisms via Azure infrastructure.

2024 – Cloud Credential Harvesting Campaign: Targeted Israeli and Emirati defense organizations with fake Microsoft 365 login portals.

2025 – Oil and Energy Espionage Drive: Coordinated campaign against European and Middle Eastern energy firms, exfiltrating sensitive industrial and financial data.