APT35

[/ˌeɪ.piːˈtiː ˈθɜː(r).ti faɪv ˈtʃɑː(r).mɪŋ ˈkɪt.ən/]

APT35 (Charming Kitten) is an Iranian state-linked cyberespionage group active since 2011, conducting phishing, credential theft, and influence operations against political, academic, media, and NGO targets, with recent campaigns using more advanced and deceptive techniques.

IDENTITY

Attribution	: Iranian state-sponsored group linked to the Islamic Revolutionary Guard Corps (IRGC).
Active Since	: At least 2011
Aliases	: CharmingCypress, Group 83, TunnelVision, COBALT MIRAGE, TA455, Mint Sandstorm, Phosphorus, Smoke Sandstorm, NewsBeef, Charming Kitten, G0058, G0059, BOHRIUM, iKittens, Magic Hound, Newscaster, Newscaster Team, Parastoo, Yellow Dev13
Motivation	: Cyber-espionage, surveillance of dissidents, geopolitical intelligence collection, disinformation, and harassment operations.

TTPs

Initial Access	: Extensive use of spear-phishing, credential harvesting, fake news/media websites, and social engineering through platforms like LinkedIn and WhatsApp.
Persistence	: Custom malware families including POWERSTAR, Tickler, and CHAINSHOT; also use of legitimate cloud services (Google Drive, OneDrive) for command-and-control.
Malware & Tools	: POWERSTAR, DustySky, CHAINSHOT, HookStick, Tickler; exploitation of VPNs and unpatched vulnerabilities.
Techniques	: Credential phishing via fake login portals, watering-hole attacks, impersonation of journalists/academics, disinformation campaigns on social media, and occasional destructive attacks.

TARGET PROFILE

Target Sectors	: Government, defense, academia, NGOs, think tanks, technology, media, and human rights organizations.
Geographies Targeted	: Primarily United States, Israel, and Gulf States; also targets Europe and global dissident communities.

THREAT ASSESSMENT

Risk Level	: High – highly persistent, adaptable, and well-funded.
Most Recent Activity	: 2024–2025 operations included election-related phishing campaigns, credential theft from policy experts and journalists, and deployment of POWERSTAR malware in academic institutions.
Evolution	: Originally focused on simple phishing campaigns; expanded into supply-chain compromises, broader influence operations, and integration of AI-driven disinformation.

NOTABLE OPERATIONS

- **2014–2015:** “Newscaster” campaign – social engineering via fake online personas and news sites.
- **2018:** Large-scale phishing targeting U.S. and Middle Eastern universities, stealing academic credentials.
- **2020:** Phishing campaigns against pharmaceutical companies during COVID-19 pandemic.
- **2021:** Targeted Israeli defense and technology firms with DustySky and CHAINSHOT.
- **2022–2023:** Global spear-phishing linked to human rights activists and journalists.
- **2024:** Election-related influence and phishing campaigns tied to U.S. elections.
- **2025:** Continued operations against universities, think tanks, and policy groups with POWERSTAR and Tickler malware.