CRAFTY CAMEL

[/ˈkræfti ˈkæməl/]

Crafty Camel is an Iran-aligned cyber-espionage group active since 2017, focused on strategic intelligence and regional surveillance. They conduct high-risk, persistent operations using phishing, cloud credential theft, and supply-chain attacks. Their main targets include government, defense, energy, telecommunications, and policy sectors primarily in the Middle East, with some activity in the US, Europe, GCC states, and Israel.

IDENTITY

Attribution : Iran (state-aligned cyber-espionage operators).

Active Since : Approximately 2017.

Aliases : Operates within and alongside known Iranian APT clusters; overlaps observed with regional cyber-espionage infrastructure.

Motivation : Espionage, surveillance, and strategic intelligence collection supporting Iranian geopolitical and regional security priorities.

TTPs

Initial Access
- Spearphishing using geopolitical themes, defense-related lures, and impersonation of trusted organizations
- Exploitation of internet-facing infrastructure (VPN appliances, Microsoft Exchange, webmail portals)
- Compromise of cloud accounts through credential harvesting and MFA-bypass techniques

Persistence
- Deployment of custom loaders and lightweight backdoors
- Use of scheduled tasks, registry modifications, and covert administrative accounts
- Maintaining cloud persistence through OAuth token abuse and misconfigured identity platforms

Command & Control (C2)
- HTTPS-based communication blending with normal traffic
- Use of compromised Middle Eastern hosting providers for staging, C2, and data exfiltration
- DNS tunneling and cloud storage abuse for stealthy command channels

Malware & Tools
- Custom droppers and loaders used to deploy reconnaissance implants
- Credential harvesting utilities and email scraping tools
- Use of publicly available RATs and LOTL (Living-off-the-Land) techniques to evade detection

Techniques
- Credential theft from email platforms and cloud identity providers
- Lateral movement through SMB, RDP, and remote admin tooling
- Data staging in compressed encrypted archives prior to exfiltration
- Supply-chain targeting via third-party IT and telecom providers

TARGET PROFILE

Target Sectors
- Government ministries & diplomatic organizations
- Defense and aerospace contractors
- Energy, oil & gas, and transportation sectors
- IT service providers and telecommunications
- NGOs, academic institutions, and policy think tanks

Geographies Targeted
- Middle East (primary operational focus)
- United States (select defense contractors and policy organizations)
- Europe (research institutions and diplomatic targets)
- GCC states (government and energy networks)
- Israel

THREAT ASSESSMENT

Risk Level : High.

Most Recent Activity : 2023–2025 operations include credential harvesting campaigns, exploitation of perimeter vulnerabilities, and cloud-based infiltrations.

Evolution : Growing reliance on cloud intrusion techniques, blended social engineering, and modular malware; shifting from standalone intrusions to multi-layered campaigns aligned with Iranian intelligence requirements.

NOTABLE OPERATIONS

- **2018 – Government Credential Theft:** Phishing campaigns targeting regional government ministries across the Middle East.
- **2020 – Defense & Aerospace Reconnaissance:** Focused intrusions aimed at acquiring research, design files, and contractor communications.
- **2021 – Cloud Account Compromise:** Large-scale operations harvesting cloud credentials tied to policy researchers and NGOs