# APT 42

[ /ˌeɪ.piːˈtiː ˌfɔː(r).ti ˈtuː/ ]

APT42 is an Iran-linked espionage group active since at least 2015, targeting diplomats, NGOs, journalists, and civil society through phishing, credential theft, and mobile/cloud surveillance. Operating primarily in the Middle East but also against Western entities, the group conducts intelligence-focused campaigns that pose a high risk to political and civil organizations.

## IDENTITY

| | |
|---|---|
| Attribution | : Iran-linked advanced persistent threat (APT) group. |
| Active Since | : At least 2015. |
| Aliases | : UNC788, CALANQUE. |
| Motivation | : State-aligned cyber espionage and surveillance supporting Iranian strategic intelligence objectives |

## TTPs

| | |
|---|---|
| Initial Access | : Highly tailored spear-phishing (persona-based outreach), cloud account takeover (OAuth consent phishing), watering-hole pages, credential harvesting portals, MFA fatigue / push bombing. |
| Persistence | : OAuth token abuse, mailbox rules, app passwords/legacy protocols, SSO refresh tokens, scheduled tasks and startup entries on compromised endpoints. |
| Command & Control (C2) | : HTTPS over cloud and shared hosting providers, domain fronting/redirectors, dynamic DNS. |
| Malware & Tools | : Lightweight custom downloaders, PowerShell/HTA loaders, web shells, credential harvesters; occasional mobile surveillance apps distributed via links. |
| Techniques | - Social engineering posing as academics/journalists to establish trust<br>- HTML/Office attachment lures, link-based phishing to fake login portals<br>- Account discovery and data collection in cloud email (search/export), exfil via APIs<br>- Living-off-the-land (PowerShell, curl, certutil) and LOLBins for staging |

## TARGET PROFILE

| | |
|---|---|
| Target Sectors | : Government and diplomacy, NGOs and civil society, media and academia, healthcare and policy think tanks. |
| Geographies Targeted | : Middle East (primary), North America, and Europe. |

## THREAT ASSESSMENT

| | |
|---|---|
| Risk Level | : High – persistent credential theft and cloud-centric espionage against policy-relevant targets. |
| Most Recent Activity | : Continued persona-driven phishing and cloud account takeovers (2024–2025); emphasis on OAuth consent and mailbox data collection. |
| Evolution | : Shift from attachment-heavy phishing to cloud/OAuth abuse and long-lived access in mail and collaboration suites. |

## NOTABLE OPERATIONS

- **2017–2019:** Campaigns against regional researchers and policy experts using journalist/academic personas and credential harvesters.
- **2020–2021:** Focus on cloud email takeovers of NGOs and healthcare policy stakeholders; increased use of OAuth consent phishing.
- **2022–2023:** Expanded infrastructure with redirectors and look-alike domains; refined social engineering with multi-touch outreach before delivery of phishing links.
- **2024–2025:** Sustained targeting of Middle East and Western think-tank/government adjacencies; short-lived infrastructure and mailbox rule abuse for stealthy exfiltration.