RAZOR TIGER

[/ ˈreɪˌzɔːr ˈtaɪgər /]

SideWinder (APT-C-17) is an India-linked cyber espionage group active since 2012, targeting political and military institutions across South Asia. By 2024–2025, it expanded operations using advanced malware and information operations, primarily against Pakistan and China.

IDENTITY

Attribution / Origin	: Assessed as India-linked advanced persistent actor (open-source and industry reporting).
Active Since	: ~2012 (earliest observed campaign reporting and cluster activity).
Aliases	: APT-C-17; SideWinder; Rattlesnake; T-APT-04.
Motivation	: Strategic intelligence collection and political/military espionage; regional influence operations.

TTPs

Initial Access

- Highly targeted spear-phishing (malicious Office/HTML attachments, weaponized documents).
- Credential harvesting via phishing portals and cloud-hosted decoys (SharePoint, Google Drive lures).
- Exploitation of internet-facing enterprise services and one-day vulnerabilities when available.

Execution & Privilege Escalation

- Use of macros, malicious RTF/Office exploit chains, and staged PowerShell loaders.
- Living-off-the-land (LOTL) techniques: PowerShell, WMI, scheduled tasks and signed system utilities to evade detect.

Persistence

- Custom backdoors and implants deployed as persistent services and DLL side-loading.
- Abuse of VPN/remote-access services and legitimate remote-management tools for long-lived access.

Command & Control (C2)

- Multi-stage C2 with encrypted HTTP(S) beacons and domain-fronting through legitimate cloud services.
- Use of proxying (VPN/SoftEther-like infrastructure) and ephemeral domains to frustrate takedown.

Lateral Movement & Collection

- Credential dumping and reuse, remote management tools, RDP and SMB abuse for lateral movement.
- Targeted reconnaissance focused on defense, diplomatic and critical infrastructure systems; selective data exfiltration.

Exfiltration & Impact

- Small, targeted exfiltration of documents and credentials to minimize detection.
- Occasional use of secondary channels (cloud storage, multipart uploads) to conceal transfer.

Malware & Tools Observed (Representative)

- Custom implants / loaders (staged payload model).
- PowerShell-based loaders, custom C2 implants, DLL side-loaders.
- Use of commodity tooling selectively (RMM tools, Cobalt Strike/Beacon only when needed).

TARGET PROFILE

Target Sectors

- **Primary Sectors:** Government (diplomatic and foreign affairs), defense & military, telecommunications, critical national infrastructure, maritime/logistics (regional strategic interest).
- **Secondary Sectors:** Research & higher education, non-profit (policy/strategic programs).
- **Geographic Focus:** South Asia (Pakistan, Afghanistan, Nepal, Bangladesh, Sri Lanka, Maldives), expanding activity into Southeast Asia and select Middle East targets.

THREAT ASSESSMENT

Risk Level	: HIGH — capable, patient, and focused on high-value intelligence collection.
Most Recent Activity	: Continued campaigns through 2024–2025 with updated implants and broadened sector scope.
Evolution	: Shift from commodity malware and mass phishing toward highly tailored social engineering, LOTL techniques, and cloud-facilitated C2. Increased interest in maritime/logistics and infrastructure-adjacent targets in recent years.

NOTABLE OPERATIONS

- 2012–2016 — *Early espionage campaigns:* Long-term credential harvesting and targeted spear-phishing against regional diplomatic and defense targets; initial use of custom loaders.
- 2017–2019 — *Tooling maturation:* Adoption of staged implants and more robust persistence techniques (DLL side-loading, service implants); targeted against military and telecom infrastructure.
- 2020–2022 — *Infrastructure & cloud abuse:* Increased use of cloud-hosted decoys (SharePoint/Drive) and exploitation of internet-facing applications for access; selective lateral movement and credential theft.
- 2023–2025 — *Re-tooling & expansion:* Broadened sector targeting (maritime, port logistics, nuclear-adjacent supply chains in some reporting), renewed custom implant families, and greater use of living-off-the-land tactics to evade detection.