HAZY TIGER

[/ ˈheɪ.zi ˈtaɪgər /]

HAZY TIGER is a South Asia-linked APT active since 2013, conducting cyber espionage against government, defense, energy, and critical infrastructure. By 2024–2025, it used spear-phishing, custom malware, and Android spyware, mainly targeting South and Southeast Asia.

IDENTITY

Attribution / Origin	: South Asia-linked APT (attribution varies; often associated with regional intelligence operations).
Active Since	: At least 2013.
Aliases	: TA397, APT-C-08, Bitter, Orange Yali, T-APT-17.
Motivation	: Strategic cyber espionage to collect intelligence on political, military, and energy-related targets.

TTPs

Initial Access	: Spear-phishing with localized lures, watering-hole sites, malicious Android APKs posing as utility or communication apps.
Persistence	: Custom backdoors, web shells, scheduled tasks, registry modifications, abuse of legitimate remote administration tools.
Command & Control (C2)	: HTTPS/TLS over bespoke domains, dynamic DNS, and cloud-hosted infrastructure to blend with normal traffic.
Malware & Tools	: Custom Windows backdoors, Android surveillance implants, credential harvesters, PowerShell loaders, encrypted exfiltration utilities.
Techniques	- Highly localized social engineering focused on regional geopolitics - Use of multi-stage loaders to avoid detection - Living-off-the-land binaries (LOLbins) for lateral movement - Short-lived infrastructure and fast pivoting to reduce exposure

TARGET PROFILE

Target Sectors	: Government (ministries, foreign affairs), defense & military, energy (utilities and oil & gas), critical national infrastructure, research institutions.
Geographies Targeted	: Primarily South Asia (India, Pakistan, Bangladesh, Sri Lanka); opportunistic activity in Southeast Asia and the Middle East.

THREAT ASSESSMENT

Risk Level	: High focused regional espionage actor with sustained campaigns against sensitive targets.
Most Recent Activity	: 2024–2025 spear-phishing and Android surveillance campaigns against government and energy sector targets (short, focused operations).
Evolution	: From traditional phishing and desktop backdoors to multi-platform operations including mobile surveillance and cloud-based exfiltration

NOTABLE OPERATIONS

- **2013–2016:** Early spear-phishing campaigns against regional government email accounts; deployment of custom backdoors for long-term access.
- **2017–2019:** Increased targeting of energy sector and critical infrastructure; introduction of Android-based surveillance implants.
- **2020–2021:** Use of watering-hole sites and localized lures to target diplomatic and policy researchers.
- **2022–2025:** Short, high-stealth campaigns using short-lived C2, targeted Android lures, and multi-stage loaders aimed at minimizing forensic footprints.