MOONLIGHT TIGER

[/ˈmuːnˌlaɪt ˈtaɪgər/]

Moonlight Tiger (APT-C-09) is an India-linked group targeting government and defense sectors in South and East Asia since 2015. They use advanced spearphishing and malware for espionage. Main targets are China, Pakistan, Sri Lanka, and some Southeast Asian and European entities.

IDENTITY

Attribution	: India-linked advanced persistent threat (APT) group associated with cyber-espionage operations targeting regional adversaries and geopolitical entities.
Active Since	: ~2015
Aliases	: APT-C-09, ATK11, Chinastrats, Dropping Elephant, Monsoon, Orange Athos, Patchwork, Sarit.
Motivation	: Intelligence gathering and surveillance in support of Indian strategic interests, particularly focused on defense, diplomatic, and research sectors in neighboring countries.

TTPs

Initial Access	: Spearphishing emails and watering-hole attacks using malicious documents (RTF, DOCX) exploiting Microsoft Office vulnerabilities; social engineering via LinkedIn and email.
Persistence	: Registry modifications, scheduled tasks, and DLL side-loading; reliance on open-source tools for persistence and lateral movement.
Command & Control (C2)	: HTTP/S-based C2 channels using compromised servers; sometimes employs encrypted PowerShell or Python scripts.
Malware & Tools	: BADNEWS (custom backdoor), Ragnatela, Meterpreter, and modified open-source RATs; occasional use of Java-based implants and PowerShell loaders.
Techniques	: Credential theft, information exfiltration, data staging via temporary cloud services, and reconnaissance within government or defense networks.

TARGET PROFILE

Target Sectors	: Government, Defense, Foreign Affairs, Think Tanks, and Academia.
Geographies	: Primarily China, Pakistan, Sri Lanka, Nepal, and selective European or Southeast Asian diplomatic missions.

THREAT ASSESSMENT

Risk Level	: High (Regional Intelligence Threat)
Most Recent Activity	: 2024–2025 campaigns delivering malware via fake conference invitations and policy research documents; evidence of custom loaders mimicking benign government templates.
Evolution	: Progressed from basic phishing to modular espionage operations with improved operational security and cloud-based data exfiltration. Demonstrates adaptive use of publicly available malware combined with custom Indian-developed implants.

NOTABLE OPERATIONS

- **2016 – Dropping Elephant Campaign:** Early public exposure targeting Chinese diplomatic and media organizations using spearphishing emails and malicious RTF files.
- **2018 – Patchwork Expansion:** Targeted Pakistani defense and foreign affairs institutions; introduced BADNEWS RAT and social engineering through fake academic research lures.
- **2020 – Operation Monsoon:** Conducted espionage against Southeast Asian defense ministries using modular PowerShell scripts and infected Office templates.
- **2023 – Orange Athos Operation:** Leveraged watering-hole attacks against South Asian think tanks to distribute updated Ragnatela backdoors.
- **2025 – Strategic Research Phishing Campaign:** Used counterfeit conference invitations to compromise Chinese and Sri Lankan defense research centers; improved C2 obfuscation observed in PowerShell loaders.