GALLIUM

[/ˈgæliəm /]

GALLIUM is a China state-sponsored APT group active since at least 2012, assessed as high risk for cyber espionage operations targeting telecommunications and government networks, with recent 2024–2025 campaigns using tools like SoftEther VPN and ShadowPad across Southeast Asia, Africa, and increasingly Europe and Latin America.

IDENTITY

Attribution	: China (PRC) state-sponsored APT group.
Active Since	: At least 2012.
Aliases	: Alloy Taurus, Granite Typhoon, Red Giant 4.
Motivation	: Cyber espionage supporting China's geopolitical, military, and economic intelligence priorities.

TTPs

Initial Access	- Exploitation of public-facing applications (notably telecom infrastructure). - Spear-phishing and watering-hole attacks. - Abuse of legitimate remote administration tools and VPN platforms (SoftEther VPN, AnyDesk). - Leveraging compromised supply chains and service providers.
Persistence	- Installation of ShadowPad and PlugX backdoors. - Use of legitimate VPN tunnels and RMM tools for continuous access. - Abuse of scheduled tasks and registry modifications for persistence.
Command & Control (C2)	- Custom C2 frameworks built into ShadowPad and PlugX. - Encrypted communications via TCP and HTTPS. - Utilization of proxy servers and legitimate cloud services for stealth.
Malware & Tools	- **ShadowPad:** Modular backdoor widely used by Chinese APTs for espionage and lateral movement. - **PlugX:** Used for data exfiltration and privilege escalation. - **SoftEther VPN:** Used to establish encrypted tunnels for C2. - QuasarRAT, Poison Ivy, and custom loaders for execution and persistence.
Techniques	- Living-off-the-land tactics using PowerShell, PsExec, and Windows Management Instrumentation (WMI). - Credential dumping via LSASS and registry hives. - Data exfiltration through encrypted channels and cloud storage abuse. - Lateral movement through RDP and VPN credential reuse.

TARGET PROFILE

Sectors	: Telecommunications, government, defense contractors, maritime communications, and critical infrastructure.
Geographies	: Southeast Asia, Middle East, Africa, Europe, and Latin America.
Notable Targets	: Telecom operators in Africa and Southeast Asia (2024–2025), European government networks, and satellite communication providers.

THREAT ASSESSMENT

Risk Level	: High.
Most Recent Activity	: 2024–2025 espionage operations targeting telecom and government sectors using SoftEther VPN and ShadowPad.
Evolution	: Demonstrated global expansion beyond APAC; refined TTPs with emphasis on covert operations using legitimate tools and encrypted channels.

NOTABLE OPERATIONS

- **2024 – Africa Telecom Campaign:** Deployment of SoftEther VPN servers in telecom networks for covert access and data exfiltration across multiple African nations.
- **2024 – Europe Expansion:** Use of ShadowPad and PlugX in EU-based government and diplomatic targets.
- **2023 – Middle East Intrusions:** Compromised telecom networks to intercept communications; linked to broader Chinese intelligence collection operations.
- **2018–2020 – Operation Soft Cell:** Long-term espionage targeting telecom providers in the Middle East and Southeast Asia for call metadata and subscriber data theft.