UNC4841

[/ /juː-ɛn-siː fɔːr ɛɪt fɔːr wʌn/ /]

UNC4841 is a China-linked APT tracked since 2021, conducting cyber-espionage for state interests. It targets government, defense, aerospace, telecom, and tech supply chains, mainly in the U.S., allied nations, and Asia-Pacific. Active through 2024–2025, it exploits zero-days, rapidly adopts new vulnerabilities, and maintains strong OPSEC, posing a high-risk threat.

IDENTITY

Attribution	: China-linked advanced persistent threat (APT) cluster.
Active Since	: Publicly tracked since at least 2021.
Aliases	: UNC4841, SLIME57. Sometimes overlaps in reporting with Storm-0558 and other China-nexus espionage groups, but tracked distinctly as UNC4841.
Motivation	: Cyber espionage in support of Chinese state interests, primarily targeting sensitive political, defense, and technology data.

TTPs

Initial Access	: Exploitation of zero-day vulnerabilities in widely deployed enterprise software; spear-phishing campaigns delivering malicious attachments.
Persistence	: Maintains footholds through web shells, compromised VPN credentials, scheduled tasks, and modified system registries.
C2 Infrastructure	: Custom malware families using HTTPS-based channels and DNS tunneling; dynamic domain switching to avoid detection.
Malware & Tools	: Custom implants, backdoors, credential stealers, and exploitation frameworks tailored to targeted environments.
Techniques	: Lateral movement via stolen credentials, privilege escalation, living-off-the-land binaries (LOLBins), and covert exfiltration of sensitive data.

TARGET PROFILE

Target Sectors	: Government, defense, aerospace, telecommunications, technology supply chains, and critical infrastructure.
Geographies Targeted	: Primarily North America, Europe, and Asia-Pacific, with a strong focus on the United States and allied nations.

THREAT ASSESSMENT

Risk Level	: High – highly capable state-backed espionage actor.
Most Recent Activity	: Active through 2024–2025, leveraging zero-day exploits and conducting sophisticated intrusions against government and defense networks.
Evolution	: Rapid adoption of emerging vulnerabilities, increased operational discipline, and expansion into supply chain compromise campaigns.

NOTABLE OPERATIONS

- **2021:** First public reporting of UNC4841/SLIME57 activity exploiting enterprise software vulnerabilities for espionage.
- **2022:** Conducted large-scale spear-phishing campaigns targeting defense contractors and government ministries in the Asia-Pacific region.
- **2023:** Exploited multiple zero-day vulnerabilities in collaboration platforms, enabling espionage against U.S. and European government agencies.
- **2024:** Expanded focus to include technology supply chains, targeting software vendors and telecom infrastructure providers.
- **2025:** Continued operations using zero-day exploits against critical enterprise applications; campaigns broadened to NATO-aligned countries and sensitive research institutions.