EARTH ESTRIES

[/ɜːrθ ˈɛstriz/]

Earth Estries is a China-linked APT group active since the early 2020s, conducting cyber-espionage in support of state interests. It targets governments, defense, telecom, research, and international organizations worldwide, exploiting server vulnerabilities and spear-phishing. Active through 2024–2025, the group shows increasing sophistication and alignment with Beijing's strategic priorities, posing a high-risk threat.

IDENTITY

Attribution	: China-linked advanced persistent threat (APT) group.
Active Since	: At least early 2020s.
Aliases	: Sometimes associated with broader Chinese espionage clusters (related to Earth Krahang and others, but distinct).
Motivation	: Cyber espionage in support of Chinese state interests, primarily focused on intelligence collection from governments, critical infrastructure, and research institutions.

TTPs

Initial Access	: Exploitation of unpatched vulnerabilities in internet-facing applications; spear-phishing with malicious attachments.
Persistence	: Use of web shells, scheduled tasks, and compromised VPN credentials to maintain long-term access.
C2 Infrastructure	: Employs custom malware families with HTTP/S and DNS tunneling-based C2 channels.
Malware & Tools	: Known to deploy multiple custom implants, loaders, and web shells for espionage operations.
Techniques	: Living-off-the-land techniques, credential dumping, lateral movement within compromised networks, and data exfiltration using covert channels.

TARGET PROFILE

Target Sectors	: Government, defense, telecommunications, research, technology, and international organizations.
Geographies Targeted	: Global – more than 70 government entities compromised across Europe, Asia, Africa, and the Americas.

THREAT ASSESSMENT

Risk Level	: High – persistent, state-backed, and capable of global-scale cyber-espionage.
Most Recent Activity	: Active in 2024–2025, with campaigns exploiting vulnerabilities in public-facing servers and deploying advanced phishing campaigns.
Evolution	: Demonstrates increasing operational maturity, including improved obfuscation, diverse intrusion methods, and alignment with Chinese geopolitical goals.

NOTABLE OPERATIONS

- **2021–2022:** Initial discovery of Earth Estries campaigns targeting government institutions in Asia through spear-phishing.
- **2023:** Expansion of operations to European and African government agencies, including telecommunications entities.
- **2024:** Coordinated campaigns against over 70 global government organizations, exploiting server vulnerabilities and delivering custom malware.
- **2025:** Ongoing espionage campaigns against critical infrastructure and international bodies, aligning with Beijing's intelligence priorities.