GHOSTEMPEROR

[/ ˈgoʊstˌɛm.pə.ər /]

GhostEmperor is a China-aligned APT active since 2019, conducting high-risk cyber-espionage against government, telecom, defense, and critical infrastructure in Southeast Asia, the Middle East, and Africa, using stealthy malware and rootkits for persistent access.

IDENTITY

Attribution	: China-aligned APT group, first exposed by Kaspersky in 2021.
Active Since	: At least 2019.
Aliases	: None widely confirmed beyond “GhostEmperor.”
Motivation	: Strategic cyber espionage focused on government, defense, and critical organizations to support Chinese state interests.

TTPs

Initial Access	: Exploitation of internet-facing servers and vulnerabilities in public applications, as well as spear-phishing emails.
Persistence	: Use of custom rootkits, particularly the “Demodex” rootkit, to maintain stealthy long-term access.
Command & Control (C2)	: Custom backdoors communicating over HTTPS and covert channels; rotating domains to evade detection.
Malware & Tools	: GhostEmperor backdoor framework, Demodex rootkit, custom loaders, privilege escalation tools.
Techniques	: Credential theft, lateral movement through compromised administrator accounts, stealth persistence via kernel-level implants, and data exfiltration with obfuscation.

TARGET PROFILE

Target Sectors	: Government, defense, telecom, critical infrastructure, and diplomatic organizations.
Geographies Targeted	: Southeast Asia, Middle East, and Africa, with a strong focus on ministries, embassies, and defense agencies.

THREAT ASSESSMENT

Risk Level	: High – advanced espionage actor with highly persistent and stealthy malware.
Most Recent Activity	: Active through 2024–2025, continuing espionage operations in Asia and the Middle East.
Evolution	: Known initially for deploying Demodex, one of the most advanced rootkits observed in the wild; continues to refine malware with stealth and persistence improvements.

NOTABLE OPERATIONS

- **2019:** Earliest identified operations targeting government organizations in Southeast Asia.
- **2020:** Expanded campaigns targeting telecom providers and diplomatic institutions with custom malware implants.
- **2021:** Publicly exposed by Kaspersky for use of the advanced Demodex rootkit; linked to high-profile espionage campaigns in Asia.
- **2022:** Continued long-term espionage campaigns against Middle Eastern governments, focusing on diplomatic and defense entities.
- **2023:** Shifted toward targeting African government agencies and infrastructure as part of broader Chinese strategic interests.
- **2024–2025:** Ongoing cyber espionage against governments and defense ministries in Asia and the Middle East, with refined persistence techniques and expanded infrastructure.