HAFNIUM (Silk Typhoon)

[/ˈhæfniəm (sɪlk taɪˈfuːn)/]

HAFNIUM (Silk Typhoon) is a high-risk, China-aligned APT active since 2019, focused on global espionage via exploitation of internet-facing enterprise systems, with continued activity through 2024–2025 targeting unpatched infrastructure.

IDENTITY

Attribution : Commonly assessed as a China-linked advanced persistent threat actor supporting strategic intelligence collection.

Active Since : ~2019 (earliest publicly attributed campaigns); peak visibility during 2020–2021.

Aliases : ATK233; G0125; MURKY PANDA; Operation Exchange Marauder; Red Dev 13; Silk Typhoon

Motivation : Espionage-focused — acquisition of sensitive communications, policy data, and intellectual property.

TTPs

Initial Access

- Exploitation of zero-day and n-day vulnerabilities in internet-facing enterprise software.
- Mass scanning and compromise of on-premise email and collaboration servers.
- Opportunistic access without reliance on user interaction.

Execution

- Remote code execution via server-side vulnerabilities.
- Deployment of web shells for command execution.
- Abuse of application-level permissions rather than local privilege escalation.

Persistence

- Multiple web shells placed in different directories.
- Use of legitimate server functionality to maintain access.
- Reliance on redundancy rather than stealthy persistence mechanisms.

Command & Control (C2)

- HTTP/HTTPS-based C2 communication.
- Use of compromised servers as staging and relay nodes.
- Dynamic domain usage and occasional cloud-hosted infrastructure.

Lateral Movement & Collection

- Selective mailbox access and document harvesting.
- Credential extraction from server memory and configuration files.
- Opportunistic lateral movement using stolen credentials.

Exfiltration & Impact

- Data exfiltration via encrypted web traffic.
- Focused on intelligence theft; no ransomware or destructive payloads observed.

Malware & Tools Observed

- Web shells (primary access mechanism).
- Simple loaders and scripts for automation.
- Minimal reliance on complex custom malware families.

TARGET PROFILE

Primary Sectors : Government institutions, defense and policy organizations, universities and research bodies, NGOs, private enterprises.

Secondary Sectors : Legal services, healthcare, professional services with exposed enterprise servers.

Geographic Focus : Global — North America, Europe, East Asia, Middle East.

THREAT ASSESSMENT

Risk Level : HIGH — rapid exploitation capability, global reach, and systemic impact.

Recent Activity : Continued infrastructure-focused campaigns observed through 2024–2025.

Evolution : Transitioned from headline zero-day exploitation to diversified enterprise platform targeting with sustained opportunistic access.

NOTABLE OPERATIONS

2020–2021: Operation Exchange Marauder — mass exploitation of Microsoft Exchange Server zero-day vulnerabilities worldwide.

2021–2022: Follow-on intrusions leveraging unpatched Exchange environments and web shell persistence.

2023–2024: Reduced but persistent activity targeting exposed enterprise infrastructure beyond Exchange.

2024–2025: Continued selective exploitation of internet-facing systems with lower visibility but sustained intelligence objectives.