SILENT CHOLLIMA

[/ ˈsaɪ.lənt tʃoʊˈliː.mə /]

Silent Chollima (APT45 / Onyx Sleet) is a North Korea–linked threat actor focused on cyber espionage and revenue generation. Active since around 2013, it has recently targeted U.S. healthcare, defense, and critical infrastructure using stealthy, credential-based techniques.

IDENTITY

Attribution : North Korea (DPRK).

Active Since : Approximately 2013.

Aliases : APT45, Onyx Sleet.

Motivation : Espionage and financial gain in support of North Korea's military and economic strategies.

TTPs

Initial Access : Spearphishing with malicious attachments and fake job lures; exploitation of public-facing applications and VPN vulnerabilities.

Persistence : Use of scheduled tasks, registry modifications, and installation of custom malware for long-term access.

Command & Control (C2) : HTTPS-based communication and use of legitimate cloud services (Dropbox, OneDrive) to mask traffic.

Malware & Tools : DTrack, Maui ransomware, KEYMARBLE, and other DPRK-linked implants for credential harvesting and data exfiltration.

Techniques : Living-off-the-land binaries (PowerShell, CertUtil), credential dumping (LSASS), and lateral movement via SMB and RDP.

TARGET PROFILE

Target Sectors

- Government and defense contractors
- Healthcare and pharmaceuticals
- Critical infrastructure (energy, logistics, transportation)
- Financial and cryptocurrency platforms

Geographies Targeted

- United States
- South Korea
- Japan
- Europe (Select defense and diplomatic entities)

THREAT ASSESSMENT

Risk Level : High

Recent Activity : 2024–2025 operations targeting U.S. healthcare networks and cryptocurrency firms; continued use of ransomware for financial generation.

Evolution : Expanding beyond espionage to hybrid operations combining financial theft and disruptive campaigns using cloud-based persistence mechanisms.

NOTABLE OPERATIONS

2018 – DTrack Campaign: Espionage operation against financial institutions and ATMs in India, part of the wider Lazarus ecosystem.

2021 – Healthcare Sector Breaches: Attacks on hospitals and research laboratories during COVID-19 vaccine research initiatives.

2023 – Maui Ransomware: Deployment of Maui ransomware across U.S. healthcare systems, confirmed attribution to APT45.

2024 – Credential Theft Operations: Phishing and VPN exploitation campaigns targeting U.S. and South Korean defense contractors.

2025 – Cryptocurrency Targeting: Large-scale theft of digital assets from exchanges and fintech companies to support DPRK state programs.