KONNI

(Vedalia / TA406 / Koni APT / Opal Sleet / OSMIUM)

[/ˈkɒni/]

A North Korea-aligned APT active since 2016, **Konni** conducts persistent espionage against South Korean government and diplomatic targets via spearphishing lures, LNK payloads, and lightweight loaders — prioritizing credential harvesting and intelligence collection.

IDENTITY

Attribution	: North Korea–linked APT cluster associated with the Reconnaissance General Bureau (RGB).
Active Since	: -2016
Aliases	: Vedalia, TA406, Koni APT, Opal Sleet, OSMIUM
Motivation	: Strategic cyber-espionage targeting South Korean and international diplomatic, defense, and policy entities in support of DPRK intelligence priorities.

TTPs

Initial Access	: Spearphishing emails with malicious attachments or links; weaponized Office documents and LNK shortcut payloads.
Persistence	: Scheduled tasks, PowerShell scripts, and registry-based persistence; use of compromised servers as staging points.
Command & Control (C2)	: HTTP/S and FTP-based C2 channels; frequent use of legitimate but compromised domains.
Tools & Malware	: KONNI RAT, CARROTBAT, BabyShark, and custom PowerShell-based loaders; deployment of secondary payloads for credential theft and surveillance.
Techniques	: Social engineering with government or diplomatic lures, credential harvesting, data exfiltration, and system reconnaissance.

TARGET PROFILE

Target Sectors	: Government, Diplomatic Missions, Defense Contractors, Telecommunications, and Academia.
Geographies Targeted	: Primarily South Korea, with secondary activity in Japan, Russia, and Southeast Asia.

THREAT ASSESSMENT

Risk Level	: High (Regional Intelligence Threat)
Most Recent Activity	: 2024–2025 spearphishing waves impersonating South Korean ministries and think tanks; continued use of lightweight RATs and cloud-hosted C2 infrastructure.
Evolution	: Transition from basic remote-access malware to modular espionage frameworks; increasing overlap with other DPRK clusters such as Kimsuky and Andariel, suggesting coordinated collection efforts under RGB command.

NOTABLE OPERATIONS

- **2017 – KONNI RAT Campaign:** Targeted South Korean government personnel with spearphishing attachments disguised as diplomatic correspondence.
- **2020 – BabyShark Variant Deployment:** Expanded espionage toolkit used to monitor policy and defense networks in Seoul.
- **2022 – Credential Harvesting Campaign:** Large-scale phishing operation using malicious LNK files and decoy PDFs themed around inter-Korean relations.
- **2024 – Opal Sleet Overlaps:** Detected collaboration indicators with DPRK-linked APTs focusing on defense sector entities in South Korea and Japan.
- **2025 – Diplomatic Espionage:** Renewed KONNI RAT distribution campaigns via fake government documents, targeting South Korean embassies and policy research institutes.