WageMole

[/ˈweɪdʒˌmoʊl/]

WageMole is a North Korean APT group active since 2018, targeting cryptocurrency, fintech, defense, and tech sectors. They use social engineering, fake job offers, and AI-driven phishing to support North Korea's economic and weapons goals, focusing on regions like North America, Europe, and Asia.

IDENTITY

Attribution	: North Korea (DPRK) state-sponsored APT cluster.
Active Since	: Observed activity since at least 2018.
Aliases	: Nickel Tapestry, Storm-1877, UNC5267, Contagious Interview, Famous Chollima, WageMole.
Motivation	: Primarily financially motivated operations (cryptocurrency theft, heists) combined with strategic intelligence collection to support DPRK economic resilience and weapons programs.

TTPs

Initial Access	- Social-engineering via professional networks (LinkedIn), fake job postings and staged interview workflows delivering malicious documents or installers. - Spear-phishing with weaponized attachments (malicious ISO, LNK, or macro-enabled Office files) and credential-harvesting landing pages. - Supply-chain compromises targeting development toolchains and third-party vendors. - Exploitation of exposed RDP/SSH and poorly configured cloud management consoles.
Execution & Persistence	- Use of custom and off-the-shelf installers that drop loaders and backdoors. - Living-off-the-land techniques leveraging PowerShell, WMI, and scheduled tasks to execute payloads and survive reboots. - SSH key theft and insertion, web shells on dev/test infrastructure for durable access.
Privilege Escalation & Lateral Movement	- Credential dumping (LSASS, cached credentials) and reuse across services. - Abuse of remote management software and automation tools to move laterally within cloud and on-prem environments.
Command & Control (C2)	- Encrypted C2 over HTTPS and cloud-hosted platforms (object stores, CDN, SaaS) to blend with legitimate traffic. - Use of domain fronting and frequently changing infrastructure to evade blocklists.
Data Theft & Monetization	- Targeted exfiltration of wallet keys, exchange credentials, API keys and private repositories. - Direct manipulation of payment rails, SIM-swapping coordination, and use of money-laundering infrastructure (mixers, chain-hopping) to cash-out stolen assets.
Tools & Malware	- Custom loaders and backdoors tailored to avoid signature detection. - Cryptocurrency-focused tools for harvesting wallets and automating transfer transactions. - Common use of commodity RATs and remote administration tooling as fallbacks.

TARGET PROFILE

Target Sectors	: Cryptocurrency exchanges and custodians, fintech vendors, blockchain developers, financial services, defense contractors, and software supply-chain providers.
Geographies Targeted	: North America, Europe, South Korea, Japan, Singapore, and other APAC financial hubs.

THREAT ASSESSMENT

Risk Level	: High — combination of state sponsorship (providing resources, training and tolerance) and a financially driven ince: ntive model increases activity and resilience.
Most Recent Activity	: 2024–2025 surge in LinkedIn-based recruitment lures targeting crypto and fintech personnel; observed expansion into supply-chain compromise and more sophisticated credential-harvesting infrastructure.
Evolution	: Transitioned from opportunistic credential theft to organized campaigns aimed at high-value crypto targets, incorporating AI-assisted phishing content and more robust opsec.

NOTABLE OPERATIONS

- **2024 — Professional Recruiting Campaigns:** High-volume LinkedIn lures and fake hiring pipelines delivering malicious interview artifacts to engineers at crypto firms and exchanges.
- **2024–2025 — Supply-Chain Intrusions:** Compromise of third-party development or deployment tooling used to distribute malware to customers and partners.
- **Ongoing — Crypto Heists & Wallet Theft:** Targeted theft from custodial and individual wallets using harvested credentials and malware-assisted private key extraction.