TraderTraitor

[/ˈtreɪ.dər ˈtreɪ.tər/]

TRADERTRAITOR (Jade Sleet / UNC4899) is a North Korea–linked Lazarus subgroup active since 2018, responsible for major crypto thefts—including the $1.5B ByBit attack—and targeting crypto, blockchain, and fintech firms worldwide.

IDENTITY

Attribution	: North Korea–aligned advanced persistent threat group, assessed to be a subunit of the Lazarus Group.
Active Since	: At least 2018
Aliases	: Jade Sleet, UNC4899, Pukchong.
Motivation	: Financial gain through cryptocurrency theft, blockchain exploitation, and software supply-chain compromise.

TTPs

Initial Access	: Social engineering campaigns targeting blockchain and fintech developers, phishing emails impersonating recruiters or partners, and compromised open-source repositories.
Persistence	: Modified application updates, trojanized developer tools, and backdoored npm or PyPI packages.
Command & Control (C2)	: Encrypted HTTPS communication via DPRK-controlled or compromised infrastructure, often disguised as legitimate API traffic.
Malware & Tools	: AppleJeus, Signed macOS and Windows malware, fake wallet apps, custom loaders, and downloader frameworks.
Techniques	: Credential harvesting, digital signature abuse, cryptocurrency wallet theft, data exfiltration, and lateral movement via developer environments

TARGET PROFILE

Target Sectors	: Cryptocurrency exchanges, blockchain platforms, fintech organizations, and software supply-chain providers.
Geographies Targeted	: United States, South Korea, Japan, Singapore, and European Union member states.

THREAT ASSESSMENT

Risk Level	: Critical, representing one of the most financially impactful APT clusters globally.
Most Recent Activity	: Active throughout 2024–2025, including the ByBit exchange compromise and blockchain infrastructure supply-chain attacks.
Evolution	: Expanded from direct phishing campaigns to sophisticated multi-stage supply-chain compromises and cross-platform payload delivery.

NOTABLE OPERATIONS

- **2017–2019:** Campaigns against regional researchers and policy experts using journalist/academic personas and credential harvesters.
- **2020–2021 AppleJeus Series:** Deployment of fake cryptocurrency applications to compromise exchange employees and wallet developers.
- **2022 Trojanized Developer Tools:** Infiltration of GitHub repositories distributing compromised open-source packages.
- **2023 Social Engineering Surge:** Targeting cryptocurrency startup employees via LinkedIn and Telegram.
- **2024–2025 Blockchain Exploitation:** Multi-vector operations compromising software suppliers and exchanges, leading to major cryptocurrency thefts exceeding $1 billion.