LAZARUS

[/ ˈlæz.ər.əs /]

Lazarus Group, a North Korea-linked APT active since 2009, conducts cyberattacks for finance, espionage, and political goals. Known for the Sony hack and WannaCry, it now focuses on bank and crypto theft, with recent operations like the Bybit hack targeting global finance and governments.

IDENTITY

Attribution	: North Korea (DPRK), specifically Bureau 121 / RGB.
Active Since	: At least 2009.
Aliases	: Andariel, Appleworm, Bluenoroff, Nickel Academy, Operation AppleJeus, ATK117, ATK3, Group 77, Dark Seoul, Operation DarkSeoul, Hastati Group, NICKEL GLADSTONE, TA404, Citrine Sleet, DEV-0139, DEV-1222, Diamond Sleet, Sapphire Sleet, ZINC, NewRomanic Cyber Army Team, Operation GhostSecret, Operation Troy, APT38, TEMP.Hermit, UNC2970, UNC4034, Bluenoroff subgroup, COPERNICIUM, COVELLITE, Labyrinth Chollima, Stardust Chollima, BeagleBoyz, Bureau 121, Hidden Cobra, Unit 121, G0032, G0082, APT-C-26, Whois Hacking Team.
Motivation	: Combination of financial gain to fund DPRK regime, strategic espionage, sabotage, and political influence.

TTPs

Initial Access	: Spearphishing, malicious documents, watering hole attacks, supply chain compromises, and exploitation of VPN and server vulnerabilities.
Persistence	: Custom malware families (DTrack, Manuscrypt, FALLCHILL, AppleJeus variants); use of stolen credentials and registry modifications.
C2 Infrastructure	: Infrastructure leveraging compromised servers, fast-flux DNS, and TOR-based communication.
Malware & Tools	: **Financial Theft:** FASTCash malware, ATM malware, crypto-targeting tools (AppleJeus, SnatchCrypto). **Espionage:** KEYMARBLE, LAZARUS RATs, NukeSped. **Destructive:** Wiper malware such as WannaCry (2017) and DarkSeoul campaigns.
Techniques	**:** Credential harvesting, lateral movement (via PsExec, RDP), exfiltration through cloud services, and data destruction/wiping.

TARGET PROFILE

Target Sectors	: Financial institutions & banking (SWIFT, ATMs, cryptocurrency), Government agencies and defense contractors, Energy, critical infrastructure, and media, Healthcare and technology.
Geographies Targeted	: Strong focus on **South Korea and Japan,** Significant activity **in U.S. and Europe,** Global targeting of **cryptocurrency exchanges and fintech firms.**

THREAT ASSESSMENT

Risk Level	: Critical (High Impact, Global Reach).
Most Recent Activity	: 2024–2025 activity includes large-scale cryptocurrency thefts (Bybit hack), persistent spearphishing in South Korea, and espionage against Western governments.
Evolution	: From early destructive ops (DarkSeoul, Sony Pictures) to global financial theft and espionage, with advanced use of AI-driven phishing and fake personas to infiltrate organizations.

NOTABLE OPERATIONS

- **2013 – Operation DarkSeoul:** Coordinated cyberattacks disrupting South Korean banks and broadcasters.
- **2014 – Sony Pictures Hack:** Data destruction and leaks tied to political motivations.
- **2016 – Bangladesh Bank Heist:** $81 million stolen via SWIFT manipulation.
- **2017 – WannaCry Ransomware:** Global ransomware worm impacting over 150 countries.
- **2018 – Operation AppleJeus:** Cryptocurrency exchange infiltration campaigns.
- **2020 – FASTCash 2.0:** ATM cash-out operations across Africa and Asia.
- **2023–2024:** AppleJeus and Bluenoroff subgroups heavily active in crypto thefts.
- **2025 – Bybit Hack & Continued Financial Ops:** Ongoing theft and espionage, spearphishing campaigns in South Korea, targeting global fintech and defense.