FAMOUS CHOLLIMA

[/ ˈfeɪ.məs ʧoʊ.liː.mə /]

APT37 (FAMOUS CHOLLIMA) is a North Korea-aligned threat actor active since 2012, targeting government, defense, tech, academia, and finance. In 2025, it used spear-phishing, RokRat, and BeaverTail malware, evolving toward AI-driven social engineering and multi-stage attacks, primarily in South Korea and opportunistically worldwide.

IDENTITY

Attribution : Democratic People's Republic of Korea (DPRK) – state-sponsored

Active Since : -2012

Aliases : Reaper, Ricochet Chollima, ScarCruft, Group123, Temp.Reaper, InkySquid, Red Eyes, ATK4, Moldy Pisces, Storm-2077, G0067, Venus 121, TA-RedAnt, Reaper Group, Operation Erebus, Operation Daybreak

Motivation : Cyber espionage in support of DPRK's geopolitical and military goals; financial cybercrime to generate revenue for sanctions evasion

TTPs

Initial Access : Spear-phishing with malicious decoy documents (HWP, PDF, LNK); watering-hole attacks; malicious Node.js apps disguised as coding challenges; fraudulent job recruitment campaigns.

Persistence : Use of remote management tools, malicious browser extensions, scheduled tasks, registry modifications; insider access via fraudulent employment.

C2 Infrastructure : Custom RATs with encrypted comms; abuse of cloud services (Dropbox, Yandex, pCloud) for RokRat C2; compromised developer laptops ("laptop farms") to maintain remote access.

Malware & Tools : BeaverTail & InvisibleFerret malware families (2024–2025). - RokRat backdoor with PowerShell-based infection chain . - Kimsuky-linked malware and custom implants.

Techniques : Social engineering via LinkedIn, spear-phishing, and fake job interviews (often AI-assisted). - Deployment of trojanized apps and decoy files (e.g., "National Intelligence Research Society Newsletter"). - Use of fraudulent identities and genAI deepfakes to enhance credibility.

TARGET PROFILE

Target Sectors : Technology, Defense, Energy, Government, Media, Manufacturing, Consulting, Education, Financial Services, Healthcare, Research Institutes, Labor/Economic Policy Think Tanks.

Geographies Targeted : South Korea (primary), North America (U.S., Canada, Brazil), Europe (Germany, UK, Netherlands, Romania), East Asia (Japan, South Korea, Vietnam, China, India, Nepal), Middle East (Kuwait and others)

THREAT ASSESSMENT

Risk Level : High – one of the most active DPRK state-backed adversaries with global reach.

Most Recent Activity

- Conducted over 300 incidents in 2024, with ~40% involving malicious insider operations.
- Ongoing Operation HanKook Phantom (2025) spear-phishing campaign targeting South Korean academics, think tanks, and energy/security associations with LNK + PDF decoys .
- Deployed BeaverTail, InvisibleFerret, and RokRat malware widely.
- Leveraged genAI for social engineering and fraudulent recruitment.

Evolution : From traditional spear-phishing to sophisticated insider access campaigns, leveraging fraudulent recruitment, advanced malware infection chains, and cloud-based C2 infrastructure

NOTABLE OPERATIONS

2017–2019: Early Espionage Campaigns, Targeted South Korean gov/defense using spear-phishing and zero-day exploits.

2020–2021: COVID-19 Vaccine Espionage, Attempted theft of biomedical research from pharma and health orgs.

2022: ScarCruft Expansion, Broadened targeting across Europe & APAC.

2024: Fraudulent Job Recruitment, Insider campaign using fake developer interviews; malware disguised as coding challenges.

2024: BeaverTail & InvisibleFerret, Deployed new malware families during espionage and financial theft ops.

2025: Operation HanKook Phantom, Spear-phishing campaign using decoy PDF/LNK files (e.g., "National Intelligence Research Society Newsletter"), deploying RokRat to steal sensitive data and exfiltrate via cloud C2.

2025: Sustained Insider Ops, Continued malicious insider placement in tech, finance, and academic institutions globally.