Subgroup: Bluenoroff, APT 38, Stardust Chollima

Archived: 2026-04-05 22:37:42 UTC

APT group: Subgroup: Bluenoroff, APT 38, Stardust Chollima

Names	Bluenoroff *(Kaspersky)* APT 38 *(Mandiant)* Stardust Chollima *(CrowdStrike)* CTG-6459 *(SecureWorks)* Nickel Gladstone *(SecureWorks)* TEMP.Hermit *(FireEye)* T-APT-15 *(Tencent)* ATK 117 *(Thales)* Black Alicanto *(PWC)* Copernicium *(Microsoft)* TA444 *(Proofpoint)* Sapphire Sleet *(Microsoft)* TAG-71 *(Recorded Future)* Alluring Pisces *(Palo Alto)* Selective Pisces *(Palo Alto)* G0082 *(MITRE)*	
Country	North Korea	
Motivation	Financial crime	
First seen	2014	
Description	A subgroup of Lazarus Group, Hidden Cobra, Labyrinth Chollima. (Kaspersky) The Lazarus Group, a nation-state level of attacker tied to the 2014 attacks on Sony Pictures Entertainment, has splintered off a portion of its operation to concentrate on stealing money to fund itself.	
Observed		
Tools used		
Operations performed	Oct 2015	Duuzer backdoor Trojan targets South Korea to take over computers Symantec has found that South Korea is being impacted by an active

	back door Trojan, detected as Backdoor.Duuzer. While the malware attack has not been exclusively targeting the region, it has been focusing on the South Korean manufacturing industry. Duuzer is a well-designed threat that gives attackers remote access to the compromised computer, downloads additional files, and steals data. It's clearly the work of skilled attackers looking to obtain valuable information. <https://www.symantec.com/connect/blogs/duuzer-back-door-trojan-targets-south-korea-take-over-computers>
2015	SWIFT Attack on a bank in the Philippines <https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks>
Dec 2015	Attempted Vietnamese TPBank SWIFT Attack <https://www.bankinfosecurity.com/vietnamese-bank-blocks-1-million-online-heist-a-9105>
May 2016	SWIFT Attack on Banco del Austro in Ecuador <https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD>
Oct 2016	Mexican and Polish Financial Attack Organizations in 31 countries have been targeted in a new wave of attacks which has been underway since at least October 2016. The attackers used compromised websites or "watering holes" to infect pre-selected targets with previously unknown malware. There has been no evidence found yet that funds have been stolen from any infected banks. <https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0>
2017	In this campaign, the group sends spear-phishing emails containing an archived Windows shortcut file. The file names are disguised as security or cryptocurrency related files in order to entice users into executing them. <https://securelist.com/apt-trends-report-q2-2020/97937/>
Oct 2017	SWIFT Attack on Far Eastern International Bank (FEIB) in Taiwan <https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html>
Jan 2018	Attempted heist at Bancomext in Mexico <https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret>

May 2018	SWIFT attack on Banco de Chile in Chile <https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/>
Aug 2018	SWIFT attack on Cosmos Bank in India <https://www.darkreading.com/attacks-breaches/north-korean-hacking-group-steals-$135-million-from-indian-bank-/d/d-id/1332678>
Dec 2018	ATM breach of Redbanc in Chile <https://www.zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/>
Nov 2021	The BlueNoroff cryptocurrency hunt is still on <https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/>
2022	TA444: The APT Startup Aimed at Acquisition (of Your Funds) <https://www.proofpoint.com/us/blog/threat-insight/ta444-apt-startup-aimed-at-your-funds>
Sep 2022	North Korean hackers spoof venture capital firms in Japan, Vietnam and US <https://therecord.media/north-korean-hacking-group-spoofs-venture-capital-firms-finance-japan-vietnam>
Oct 2022	BlueNoroff introduces new methods bypassing MoTW <https://securelist.com/bluenoroff-methods-bypass-motw/108383/>
Dec 2022	Bluenoroff’s RustBucket campaign <https://blog.sekoia.io/bluenoroffs-rustbucket-campaign/>
Apr 2023	BlueNoroff Hidden Risk | Threat Actor Targets Macs with Fake Crypto News and Novel Persistence <https://www.sentinelone.com/labs/bluenoroff-hidden-risk-threat-actor-targets-macs-with-fake-crypto-news-and-novel-persistence/>
Jun 2023	The DPRK strikes using a new variant of RUSTBUCKET <https://www.elastic.co/security-labs/DPRK-strikes-using-a-new-variant-of-rustbucket>
Sep 2023	BlueNoroff strikes again with new macOS malware <https://www.jamf.com/blog/bluenoroff-strikes-again-with-new-macos-malware/>

	Oct 2023	BlueNoroff: new Trojan attacking macOS users <https://securelist.com/bluenoroff-new-macos-malware/111290/>
	Nov 2023	Microsoft: BlueNoroff hackers plan new crypto-theft attacks <https://www.bleepingcomputer.com/news/security/microsoft-bluenoroff-hackers-plan-new-crypto-theft-attacks/>
	Jun 2025	Feeling Blue(Noroff): Inside a Sophisticated DPRK Web3 Intrusion <https://www.huntress.com/blog/inside-bluenoroff-web3-intrusion-analysis>
Counter operations	Apr 2023	Prison Time for 11 Involved in India's Cosmos Bank Heist <https://www.bankinfosecurity.com/prison-time-for-11-involved-in-indias-cosmos-bank-heist-a-21854>
	Feb 2025	OpenAI bans ChatGPT accounts used by North Korean hackers <https://www.bleepingcomputer.com/news/security/openai-bans-chatgpt-accounts-used-by-north-korean-hackers/>
Information	<https://threatpost.com/lazarus-apt-spinoff-linked-to-banking-hacks/124746/> <https://www.microsoft.com/en-us/security/blog/2024/11/22/microsoft-shares-latest-intelligence-on-north-korean-and-chinese-threat-actors-at-cyberwarcon/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0082/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=a979f6ac-99b3-4810-9362-94187db06784