Subgroup: Andariel, Silent Chollima - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Subgroup: Andariel, Silent Chollima

Names	Andariel *(FSI)* Silent Chollima *(CrowdStrike)* Stonefly *(Symantec)* Plutonium *(Microsoft)* Onyx Sleet *(Microsoft)* APT 45 *(Mandiant)* Jumpy Pisces *(Palo Alto)* G0138 *(MITRE)*	
Country	North Korea	
Motivation	Information theft and espionage	
First seen	2009	
Description	A subgroup of Lazarus Group, Hidden Cobra, Labyrinth Chollima.	
Observed		
Tools used		
Operations performed	2014	Operation “BLACKMINE” Target: South Korean organizations. Method: Information theft and espionage.
	2014	Operation “GHOSTRAT” Target: Defense industry. Method: Information theft and espionage.
	2014	Operation “XEDA” Target: Foreign defense industries. Method: Information theft and espionage.
	2015	Operation “INITROY”/Phase 1 Target: South Korean organizations. Method: Information theft/early phase operation.

2015	Operation “DESERTWOLF”/Phase 3 Target: South Korean defense industry. Method: Information theft and espionage.
2015	Operation “BLACKSHEEP”/Phase 3. Target: Defense industry. Method: Information theft and espionage.
2016	Operation “INITROY”/Phase 2 Target: South Korean organizations. Method: Information theft/early phase operation.
2016	Operation “VANXATM” Target: ATM companies. Method: Financial theft/BPC.
2017	Operation “Mayday” Target: South Koran Financial Company. Method: Information theft and espionage.
Jun 2018	Operation “GoldenAxe” <https://blog.trendmicro.com/trendlabs-security-intelligence/new-andariel-reconnaissance-tactics-hint-at-next-targets/>
Apr 2021	Lazarus APT conceals malicious code within BMP image to drop its RAT <https://blog.malwarebytes.com/malwarebytes-news/2021/04/lazarus-apt-conceals-malicious-code-within-bmp-file-to-drop-its-rat/> <https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/>
Jun 2021	Andariel evolves to target South Korea with ransomware <https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/>
Feb 2022	Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage>
Aug 2022	Andariel deploys DTrack and Maui ransomware <https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/>
Oct 2022	DPRK hacking groups breach South Korean defense contractors <https://www.bleepingcomputer.com/news/security/dprk-hacking-groups-breach-south-korean-defense-contractors/>

Mar 2023	Operation “Blacksmith” Operation Blacksmith: Lazarus targets organizations worldwide using novel Telegram-based malware written in DLang <https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/>
Jun 2023	Andariel’s silly mistakes and a new malware family <https://securelist.com/lazarus-andariel-mistakes-and-easyrat/110119/>
Oct 2023	Multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability <https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/>
Nov 2023	Circumstances of an Attack Exploiting an Asset Management Program (Andariel Group) <https://asec.ahnlab.com/en/59073/>
Nov 2023	Circumstances of the Andariel Group Exploiting an Apache ActiveMQ Vulnerability (CVE-2023-46604) <https://asec.ahnlab.com/en/59318/>
Dec 2023	North Korean hackers stole anti-aircraft system data from South Korean firm <https://therecord.media/north-korea-hackers-stole-anti-aircraft-system-data>
Mar 2024	Andariel Group Exploiting Korean Asset Management Solutions (MeshAgent) <https://asec.ahnlab.com/en/63192/>
Apr 2024	North Korean hackers exploit VPN update flaw to install malware <https://www.bleepingcomputer.com/news/security/north-korean-hackers-exploit-vpn-update-flaw-to-install-malware/>
May 2024	Analysis of APT Attack Cases Using Dora RAT Against Korean Companies (Andariel Group) <https://asec.ahnlab.com/en/66088/>
Aug 2024	Stonefly: Extortion Attacks Continue Against U.S. Targets <https://www.security.com/threat-intelligence/stonefly-north-korea-extortion>
Mid 2024	Analysis of Attack Cases Against Korean Solutions by the Andariel Group (SmallTiger) <https://asec.ahnlab.com/en/85400/>

	Oct 2024	Jumpy Pisces Engages in Play Ransomware <https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/>
Counter operations	Jul 2024	Rewards for Justice – Reward Offer for Information on North Korean Malicious Cyber Actor Targeting U.S. Critical Infrastructure <https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-north-korean-malicious-cyber-actor-targeting-u-s-critical-infrastructure/>
Information	<https://asec.ahnlab.com/en/56405/> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a> <https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0138/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
