


[Unnamed groups: North Korea] - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:14:02 UTC

↪ APT group: [Unnamed groups: North Korea]

Names	[Unnamed groups: North Korea] (?)	
Country	 North Korea	
Motivation	Information theft and espionage	
First seen	2019	
Description	These are reported APT activities attributed to a country, but not to an individual threat group.	
Observed	Countries: Worldwide.	
Tools used		
Operations performed	Aug 2019	Suspected North Korean Cyber Espionage Campaign Targets Multiple Foreign Ministries and Think Tanks < https://www.anomali.com/blog/suspected-north-korean-cyber-espionage-campaign-targets-multiple-foreign-ministries-and-think-tanks#When:14:00:00Z >
	Apr 2024	Operation “DEV#POPPER” Analysis of DEV#POPPER: New Attack Campaign Targeting Software Developers Likely Associated With North Korean Threat Actors < https://www.securonix.com/blog/analysis-of-devpopper-new-attack-campaign-targeting-software-developers-likely-associated-with-north-korean-threat-actors/ >
	Jul 2024	Research Update: Threat Actors Behind the DEV#POPPER Campaign Have Retooled and are Continuing to Target Software Developers via Social Engineering < https://www.securonix.com/blog/research-update-threat-actors-behind-the-devpopper-campaign-have-retooled-and-are-continuing-to-target-software-developers-via-social-engineering/ >

	Aug 2024	South Korea says DPRK hackers stole spy plane technical data < https://www.bleepingcomputer.com/news/security/south-korea-says-dprk-hackers-stole-spy-plane-technical-data/ >
	Oct 2024	APT Actors Embed Malware within macOS Flutter Applications < https://www.jamf.com/blog/jamf-threat-labs-apt-actors-embed-malware-within-macos-flutter-applications/ >
Counter operations	Jan 2019	Justice Department Announces Court-Authorized Efforts to Map and Disrupt Botnet Used by North Korean Hackers < https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-efforts-map-and-disrupt-botnet-used-north >
Information		<p><https://www.us-cert.gov/ncas/current-activity/2020/02/14/north-korean-malicious-cyber-activity></p> <p><https://www.us-cert.gov/ncas/alerts/aa20-106a></p> <p><https://www.us-cert.gov/ncas/current-activity/2020/05/12/north-korean-malicious-cyber-activity></p> <p><https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a></p> <p><https://www.us-cert.gov/ncas/current-activity/2018/08/09/North-Korean-Malicious-Cyber-Activity></p> <p><https://www.us-cert.gov/ncas/current-activity/2019/09/09/north-korean-malicious-cyber-activity></p> <p><https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf></p> <p><https://unit42.paloaltonetworks.com/threat-assessment-north-korean-threat-groups-2024/></p> <p><https://www.ic3.gov/PSA/2024/PSA240903></p> <p><https://www.jamf.com/blog/jamf-threat-labs-observes-targeted-attacks-amid-fbi-warnings/></p> <p><https://blog.barracuda.com/2024/10/02/north-korean-apt-groups-dmarc-misconfigurations></p> <p><https://unit42.paloaltonetworks.com/mac-os-malware-targets-crypto-sector/></p> <p><https://www.trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html></p> <p><https://reports.dtexsystems.com/DTEX-Exposing+DPRK+Cyber+Syndicate+and+Hidden+IT+Workforce.pdf></p>

Last change to this card: 27 June 2025

Download this actor card in [PDF](#) or [JSON](#) format

[↑](#)

Source: <https://apt.eta.or.th/cgi-bin/showcard.cgi?u=42a46962-999d-4cd2-bde5-c842e3efdd22>