Subgroup: Operation Contagious Interview - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Subgroup: Operation Contagious Interview

Names	Operation Contagious Interview *(Palo Alto)* Wagemole *(Palo Alto)* Tenacious Pungsan *(Datadog Security Research)* Nickel Tapestry *(SecureWorks)* UNC5267 *(Mandiant)* WaterPlum *(NTT)* PurpleBravo *(Recorded Future)* Storm-0287 *(Microsoft)* Jasper Sleet *(Microsoft)*
Country	North Korea
Motivation	Information theft and espionage
First seen	2020
Description	A subgroup of Lazarus Group, Hidden Cobra, Labyrinth Chollima. (Palo Alto) Unit 42 researchers recently discovered two separate campaigns targeting job-seeking activities linked to state-sponsored threat actors associated with the Democratic People's Republic of Korea (DPRK), commonly known as North Korea. We call the first campaign "Contagious Interview," where threat actors pose as employers (often anonymously or with vague identities) to lure software developers into installing malware through the interview process. This malware creates the potential for various types of theft. We attribute with moderate confidence that Contagious Interview is run by a North Korea state-sponsored threat actor. We call the second campaign "Wagemole," where threat actors seek unauthorized employment with organizations based in the US and other parts of the world, with potential for both financial gain and espionage. We attribute with high confidence that Wagemole is a North Korea state-sponsored threat. Activity from both campaigns remains an ongoing active threat.

Observed		
Tools used	BeaverTail, InvisibleFerret, OtterCookie, PylangGhost.	
Operations performed	Jul 2024	How a North Korean Fake IT Worker Tried to Infiltrate Us <https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us>
	Sep 2024	Tenacious Pungsan: A DPRK threat actor linked to Contagious Interview <https://securitylabs.datadoghq.com/articles/tenacious-pungsan-dprk-threat-actor-contagious-interview/>
	Oct 2024	Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers to Install New Variants of BeaverTail and InvisibleFerret Malware <https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/>
	Oct 2024	DPRK IT Workers Expanding in Scope and Scale <https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale>
	Nov 2024	Fake North Korean IT Worker Linked to BeaverTail Video Conference App Phishing Attack <https://unit42.paloaltonetworks.com/fake-north-korean-it-worker-activity-cluster/>
	Nov 2024	New 'OtterCookie' malware used to backdoor devs in fake job offers <https://www.bleepingcomputer.com/news/security/new-ottercookie-malware-used-to-backdoor-devs-in-fake-job-offers/>
	Nov 2024	BeaverTail and Tropidoor Malware Distributed via Recruitment Emails <https://asec.ahnlab.com/en/87299/>
	Dec 2024	macOS FlexibleFerret | Further Variants of DPRK Malware Family Unearthed <https://www.sentinelone.com/blog/macos-flexibleferret-further-variants-of-dprk-malware-family-unearthed/>
	Jan 2025	North Korean APT Lazarus Targets Developers with Malicious npm Package <https://socket.dev/blog/north-korean-apt-lazarus-targets-developers-with-malicious-npm-package>
	Feb 2025	Lazarus Group Targets Organizations with Sophisticated LinkedIn Recruiting Scam

		<https://www.bitdefender.com/en-us/blog/labs/lazarus-group-targets-organizations-with-sophisticated-linkedin-recruiting-scam>
	Feb 2025	Additional Features of OtterCookie Malware Used by WaterPlum <https://jp.security.ntt/tech_blog/en-waterplum-ottercookie>
	Mar 2025	Lazarus Strikes npm Again with New Wave of Malicious Packages <https://socket.dev/blog/lazarus-strikes-npm-again-with-a-new-wave-of-malicious-packages>
	Mar 2025	From Contagious to ClickFake Interview: Lazarus leveraging the ClickFix tactic <https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/>
	Apr 2025	Lazarus Expands Malicious npm Campaign: 11 New Packages Add Malware Loaders and Bitbucket Payloads <https://socket.dev/blog/lazarus-expands-malicious-npm-campaign-11-new-packages-add-malware-loaders-and-bitbucket>
	Apr 2025	Contagious Interview (DPRK) Launches a New Campaign Creating Three Front Companies to Deliver a Trio of Malware: BeaverTail, InvisibleFerret, and OtterCookie <https://www.silentpush.com/blog/contagious-interview-front-companies/>
	May 2025	Famous Chollima deploying Python version of GolangGhost RAT <https://blog.talosintelligence.com/python-version-of-golangghost-rat/>
	Jun 2025	Another Wave: North Korean Contagious Interview Campaign Drops 35 New Malicious npm Packages <https://socket.dev/blog/north-korean-contagious-interview-campaign-drops-35-new-malicious-npm-packages>
	Jul 2025	Contagious Interview Campaign Escalates With 67 Malicious npm Packages and New Malware Loader <https://socket.dev/blog/contagious-interview-campaign-escalates-67-malicious-npm-packages>
Counter operations	May 2024	US woman allegedly aided North Korean IT workers infiltrate 300 firms <https://www.bleepingcomputer.com/news/security/five-arizona-ukraine-charged-for-cyber-schemes-infiltrating-over-300-companies-to-benefit-north-koreas-weapons-program/>

	Aug 2024	Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator <https://www.justice.gov/usao-mdtn/pr/department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and>
	Dec 2024	US offers $5 million for info on North Korean IT worker farms <https://www.bleepingcomputer.com/news/security/us-offers-5-million-for-info-on-north-korean-it-worker-farms/>
	Dec 2024	South Korea sanctions 15 North Koreans for IT worker scams, financial hacking schemes <https://cyberscoop.com/south-korea-sanctions-north-koreans-it-worker-scams/>
	Jan 2025	Two North Korean Nationals and Three Facilitators Indicted for Multi-Year Fraudulent Remote Information Technology Worker Scheme that Generated Revenue for the Democratic People's Republic of Korea <https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote>
	Jun 2025	DOJ moves to claim $7.74 million tied to North Korean IT worker scheme <https://therecord.media/north-korea-it-worker-scams-doj-civil-forfeiture-claim>
	Jun 2025	DOJ raids 29 'laptop farms' in operation against North Korean IT worker scheme <https://therecord.media/doj-raids-laptop-farms-crackdown>
	Jul 2025	Sanctions Imposed on DPRK IT Workers Generating Revenue for the Kim Regime <https://home.treasury.gov/news/press-releases/sb0190>
	Jul 2025	US hits senior North Korean officials with sanctions, $3 million bounties <https://therecord.media/us-sanctions-north-korean-officers-it-worker-scheme>
Information	<https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/> <https://www.knowbe4.com/hubfs/North-Korean-Fake-Employees-Are-Everywhere-WP_EN-us.pdf> <https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat/> <https://dd80b675424c132b90b3-	

	e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/2024-10-01-security-advisory.pdf> <https://www.secureworks.com/blog/fraudulent-north-korean-it-worker-schemes> <https://unit42.paloaltonetworks.com/north-korean-it-workers/> <https://www.sentinelone.com/labs/dprk-it-workers-a-network-of-active-front-companies-and-their-links-to-china/> <https://www.ic3.gov/PSA/2025/PSA250123> <https://nisos.com/research/dprk-github-employment-fraud/> <https://cyberscoop.com/north-korea-technical-workers-full-time-jobs/> <https://www.secureworks.com/blog/nickel-tapestry-infrastructure-associated-with-crowdfunding-scheme> <https://sec.okta.com/articles/2025/04/genaidprk/> <https://www.theregister.com/2025/04/29/north_korea_worker_interview_questions/> <https://therecord.media/north-korean-it-worker-scam-expands-rsa> <https://nisos.com/research/saja-dprk-employment-scam/> <https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
