Kimsuky, Velvet Chollima - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Kimsuky, Velvet Chollima

Names	Kimsuky *(Kaspersky)* Velvet Chollima *(CrowdStrike)* Thallium *(Microsoft)* Black Banshee *(PWC)* SharpTongue *(Volexity)* ITG16 *(IBM)* TA406 *(Proofpoint)* TA427 *(Proofpoint)* APT 43 *(Mandiant)* ARCHIPELAGO *(Google)* Emerald Sleet *(Microsoft)* KTA082 *(Kroll)* UAT-5394 *(Talos)* Sparkling Pisces *(Palo Alto)* Springtail *(Symantec)* Larva-24005 *(AhnLab)* Larva-25004 *(AhnLab)* G0094 *(MITRE)* G0086 *(MITRE)*	
Country	North Korea	
Sponsor	State-sponsored	
Motivation	Information theft and espionage	
First seen	2012	
Description	(Kaspersky) For several months, we have been monitoring an ongoing cyber-espionage campaign against South Korean th are multiple reasons why this campaign is extraordinary in its execution and logistics. It all started one day when we enco somewhat unsophisticated spy program that communicated with its “master” via a public e-mail server. This approach is r many amateur virus-writers and these malware attacks are mostly ignored.	
Observed	Sectors: Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks and Ministry of Unification, and Korea Institute for Defense Analyses. Countries: Japan, South Korea, Thailand, Ukraine, USA, Vietnam and Europe.	
Tools used	AppleSeed, BabyShark, BITTERSWEET, CSPY Downloader, FlowerPower, Gh0st RAT, Gold Dragon, Grease, KGH_SP Kimsuky, KPortScan, MailPassView, Mechanical, Mimikatz, MoonPeak, MyDogs, Network Password Recovery, ProcDu ReconShark, Remote Desktop PassView, SHARPEXT, SmallTiger, SniffPass, SWEETDROP, TODDLERSHARK, TRAN Stealer, VENOMBITE, WebBrowserPassView, xRAT, Living off the Land.	
Operations performed	2013	For several months, we have been monitoring an ongoing cyber-espionage campaign against South Korean <https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/>
	2014	The South Korean government issued a report today blaming North Korea for network intrusions that stole Hydro and Nuclear Power (KHNP), the company that operates South Korea's 23 nuclear reactors. While th report stated that only 'non-critical' networks were affected, the attackers had demanded the shutdown of th after the intrusion. They also threatened 'destruction' in a message posted to Twitter. <https://arstechnica.com/information-technology/2015/03/south-korea-claims-north-hacked-nuclear-data/>
	Mar 2018	Operation “Baby Coin” <https://blog.alyac.co.kr/m/1963>

May 2018	Operation “Stolen Pencil” ASERT has learned of an APT campaign, possibly originating from DPRK, we are calling Stolen Pencil tha academic institutions since at least May 2018. <https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia>
Oct 2018	Operation “Mystery Baby” <https://blog.alyac.co.kr/m/1963>
Nov 2018	The spear phishing emails were written to appear as though they were sent from a nuclear security expert w works as a consultant for in the U.S. The emails were sent using a public email address with the expert’s na subject referencing North Korea’s nuclear issues. <https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/> <https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and
Jan 2019	Operation “Kabar Cobra” On January 7, 2019, a spear-phishing email with a malicious attachment was sent to members of the Minist press corps. <https://global.ahnlab.com/global/upload/download/techreport/[Analysis_Report]Operation%20Kabar%20
Apr 2019	Operation “Stealth Power” <https://blog.alyac.co.kr/2234>
Apr 2019	Operation “Smoke Screen” <https://blog.alyac.co.kr/attachment/cfile5.uf@99A0CD415CB67E210DCEB3.pdf>
Jul 2019	Operation “Red Salt” <https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.96_ENG.pdf>
Jul 2019	In what appears to be the first attack of its kind, a North Korean state-sponsored hacking group has been tar South Korean diplomats, government, and military officials. Targets of this recent campaign include former ambassadors, military generals, and retired members of Sou Ministry and Unification Ministry. <https://www.zdnet.com/article/north-korean-state-hackers-target-retired-diplomats-and-military-officials/>
Feb 2020	We decided to analyse the activity of the group after noticing a tweet of the user “@spider_girl22” in Febru <https://blog.yoroi.company/research/the-north-korean-kimsuky-apt-keeps-threatening-south-korea-evolvi
Feb 2020	North Korea has tried to hack 11 officials of the UN Security Council <https://www.zdnet.com/article/north-korea-has-tried-to-hack-11-officials-of-the-un-security-council/>
Mar 2020	According to a tweet shared by South Korean cyber-security firm IssueMakersLab, a group of North Korea malware inside documents detailing South Korea's response to the COVID-19 epidemic. The documents -- believed to have been sent to South Korean officials -- were boobytrapped with BabySha strain previously utilized by a North Korean hacker group known as Kimsuky. <https://twitter.com/issuemakerslab/status/1233010155018604545>
Dec 2020	We discovered that the Kimsuky group adopted a new method to deliver its malware in its latest campaign stock trading application. <https://securelist.com/apt-trends-report-q1-2021/101967/>
Dec 2020	Kimsuky APT continues to target South Korean government using AppleSeed backdoor <https://blog.malwarebytes.com/threat-analysis/2021/06/kimsuky-apt-continues-to-target-south-korean-gov appleseed-backdoor/>
2021	Triple Threat: North Korea-Aligned TA406 Steals, Scams and Spies <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-threat-insight-paper-triple-threat-N TA406-steals-scams-spies.pdf>
May 2021	South Korean officials said on Friday that hackers believed to be operating out of North Korea breached the of the South Korean Atomic Energy Research Institute (KAERI), the government organization that conduct nuclear power and nuclear fuel technology. <https://therecord.media/north-korean-hackers-breach-south-koreas-atomic-research-agency-through-vpn-b
May 2021	North Korean hackers breached major hospital in Seoul to steal data <https://www.bleepingcomputer.com/news/security/north-korean-hackers-breached-major-hospital-in-seou

Jun 2021	North Korean attackers use malicious blogs to deliver malware to high-profile South Korean targets <https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html>
Sep 2021	SharpTongue Deploys Clever Mail-Stealing Browser Extension “SHARPEXT” <https://www.volexity.com/blog/2022/07/28/sharptongue-deploys-clever-mail-stealing-browser-extension-
Jan 2022	On January 26th, 2022, the ASEC analysis team has discovered that the Kimsuky group was using the xRA based open-source RAT) malware. <https://asec.ahnlab.com/en/31089/>
Early 2022	Kimsuky’s GoldDragon cluster and its C2 operations <https://securelist.com/kimsukys-golddragon-cluster-and-its-c2-operations/107258/>
Apr 2022	Operation “Covert Stalker” <https://asec.ahnlab.com/en/58654/>
Oct 2022	Unveil the evolution of Kimsuky targeting Android devices with newly discovered mobile malware <https://medium.com/s2wblog/unveil-the-evolution-of-kimsuky-targeting-android-devices-with-newly-disc malware-280dae5a650f>
2023	Kimsuky Evolves Reconnaissance Capabilities in New Global Campaign <https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/
2023	From Social Engineering to DMARC Abuse: TA427’s Art of Information Gathering <https://www.proofpoint.com/us/blog/threat-insight/social-engineering-dmarc-abuse-ta427s-art-informatio
Feb 2023	Malware Disguised as Normal Documents <https://asec.ahnlab.com/en/47585/>
Mar 2023	CHM Malware Disguised as North Korea-related Questionnaire (Kimsuky) <https://asec.ahnlab.com/en/49295/>
Mar 2023	North Korean APT group ‘Kimsuky’ targeting experts with new spearphishing campaign <https://therecord.media/north-korea-apt-kimsuky-attacks>
Mar 2023	OneNote Malware Disguised as Compensation Form (Kimsuky) <https://asec.ahnlab.com/en/50303/>
Apr 2023	DPRK hacking groups breach South Korean defense contractors <https://www.bleepingcomputer.com/news/security/dprk-hacking-groups-breach-south-korean-defense-co
May 2023	Kimsuky Distributing CHM Malware Under Various Subjects <https://asec.ahnlab.com/en/54678/>
May 2023	Kimsuky Group Using Meterpreter to Attack Web Servers <https://asec.ahnlab.com/en/53046/>
May 2023	Kimsuky Group’s Phishing Attacks Targetting North Korea-Related Personnel <https://asec.ahnlab.com/en/52970/>
May 2023	Ongoing Campaign Using Tailored Reconnaissance Toolkit <https://www.sentinelone.com/labs/kimsuky-ongoing-campaign-using-tailored-reconnaissance-toolkit/>
May 2023	North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media <https://media.defense.gov/2023/Jun/01/2003234055/-1/-1/0/JOINT_CSA_DPRK_SOCIAL_ENGINEERI <https://www.sentinelone.com/labs/kimsuky-new-social-engineering-campaign-aims-to-steal-credentials-a strategic-intelligence/>
Jun 2023	Malware Disguised as HWP Document File (Kimsuky) <https://asec.ahnlab.com/en/54736/>
Jul 2023	Kimsuky Threat Group Using Chrome Remote Desktop <https://asec.ahnlab.com/en/55145/>
Jul 2023	Malicious Batch File (*.bat) Disguised as a Document Viewer Being Distributed (Kimsuky) <https://asec.ahnlab.com/en/55219/>
Aug 2023	North Korean hackers target U.S.-South Korea military drills, police say <https://www.reuters.com/world/north-korean-hackers-target-us-south-korea-military-drills-police-say-202

Oct 2023	Kimsuky Threat Group Uses RDP to Control Infected Systems <https://asec.ahnlab.com/en/57873/>
Nov 2023	Kimsuky Targets South Korean Research Institutes with Fake Import Declaration <https://asec.ahnlab.com/en/59387/>
Nov 2023	SmallTiger Malware Used in Attacks Against South Korean Businesses (Kimsuky and Andariel) <https://asec.ahnlab.com/en/66546/>
Dec 2023	Kimsuky Group Uses AutoIt to Create Malware (RftRAT, Amadey) <https://asec.ahnlab.com/en/59590/>
2024	Operation “DEEP#GOSU” Analysis of New DEEP#GOSU Attack Campaign Likely Associated with North Korean Kimsuky Targeting Stealthy Malware <https://www.securonix.com/blog/securonix-threat-research-security-advisory-new-deepgosu-attack-campa
Jan 2024	Kimsuky disguised as a Korean company signed with a valid certificate to distribute Troll Stealer <https://medium.com/s2wblog/kimsuky-disguised-as-a-korean-company-signed-with-a-valid-certificate-to-stealer-cfa5d54314e2>
Jan 2024	TrollAgent That Infects Systems Upon Security Program Installation Process (Kimsuky Group) <https://asec.ahnlab.com/en/61934/>
Jan 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-insta
Mar 2024	TODDLERSHARK: ScreenConnect Vulnerability Exploited to Deploy BABYSHARK Variant <https://www.kroll.com/en/insights/publications/cyber/screenconnect-vulnerability-exploited-to-deploy-bal
Mar 2024	Malware Disguised as Installer from Korean Public Institution (Kimsuky Group) <https://asec.ahnlab.com/en/63396/>
Mar 2024	Kimsuky deploys TRANSLATEXT to target South Korean academia <https://www.zscaler.com/blogs/security-research/kimsuky-deploys-translatext-target-south-korean-acaden
Mar 2024	Attack Activities by Kimsuky Targeting Japanese Organizations <https://blogs.jpcert.or.jp/en/2024/07/attack-activities-by-kimsuky-targeting-japanese-organizations.html>
May 2024	North Korean Hackers Exploit Facebook Messenger in Targeted Malware Campaign <https://thehackernews.com/2024/05/north-korean-hackers-exploit-facebook.html>
May 2024	Springtail: New Linux Backdoor Added to Toolkit <https://www.security.com/threat-intelligence/springtail-kimsuky-backdoor-espionage>
Jun 2024	Keylogger Installed Using MS Office Equation Editor Vulnerability (Kimsuky) <https://asec.ahnlab.com/en/66720/>
Jun 2024	MoonPeak malware from North Korean actors unveils new details on attacker infrastructure <https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/>
Jul 2024	APT Group Kimsuky Targets University Researchers <https://www.cyberresilience.com/threatintel/apt-group-kimsuky-targets-university-researchers/>
Sep 2024	North Korea Hackers Linked to Breach of German Missile Manufacturer <https://www.securityweek.com/north-korea-hackers-linked-to-breach-of-german-missile-manufacturer/>
Sep 2024	North Korean Kimsuky Hackers Use Russian Email Addresses for Credential Theft Attacks <https://thehackernews.com/2024/12/north-korean-kimsuky-hackers-use.html>
Sep 2024	How North Korean APT groups exploit DMARC misconfigurations — and what you can do about it <https://blog.barracuda.com/2024/10/02/north-korean-apt-groups-dmarc-misconfigurations>
Jan 2025	DPRK hackers dupe targets into typing PowerShell commands as admin <https://www.bleepingcomputer.com/news/security/dprk-hackers-dupe-targets-into-typing-powershell-com
Feb 2025	Persistent Threats from the Kimsuky Group Using RDP Wrapper <https://asec.ahnlab.com/en/86098/>

	Feb 2025	Operation “DEEP#DRIVE” Analyzing DEEP#DRIVE: North Korean Threat Actors Observed Exploiting Trusted Platforms for Targete <https://www.securonix.com/blog/analyzing-deepdrive-north-korean-threat-actors-observed-exploiting-trus targeted-attacks/>
	Feb 2025	Phishing Email Attacks by the Larva-24005 Group Targeting Japan <https://asec.ahnlab.com/en/86535/>
	Feb 2025	TA406 Pivots to the Front <https://www.proofpoint.com/us/blog/threat-insight/ta406-pivots-front>
	Mar 2025	Inside Kimsuky’s Latest Cyberattack: Analyzing Malicious Scripts and Payloads <https://labs.k7computing.com/index.php/inside-kimsukys-latest-cyberattack-analyzing-malicious-scripts-a
	May 2025	Case of Larva-25004 Group (Related to Kimsuky) Exploiting Additional Certificate – Malware Signed witl Certificate <https://asec.ahnlab.com/en/88132/>
	Jun 2025	Warning Against Distribution of Malware Disguised as Research Papers (Kimsuky Group) <https://asec.ahnlab.com/en/88465/>
Counter operations	Dec 2019	Microsoft takes court action against fourth nation-state cybercrime group <https://blogs.microsoft.com/on-the-issues/2019/12/30/microsoft-court-action-against-nation-state-cybercri
	Nov 2023	Treasury Targets DPRK’s International Agents and Illicit Cyber Intrusion Group <https://home.treasury.gov/news/press-releases/jy1938>
	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-ha
	Aug 2025	North Korean Kimsuky hackers exposed in alleged data breach <https://www.bleepingcomputer.com/news/security/north-korean-kimsuky-hackers-exposed-in-alleged-data
Information	<https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/> <https://securityintelligence.com/media/recent-activity-from-itg16-a-north-korean-threat-group/> <https://us-cert.cisa.gov/ncas/alerts/aa20-301a> <https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite> <https://www.darkreading.com/operations/how-north-korean-apt-kimsuky-is-evolving-its-tactics/d/d-id/1340956> <https://boho.or.kr/filedownload.do?attach_file_seq=2695&attach_file_id=EpF2695.pdf> <https://asec.ahnlab.com/en/30532/> <https://asec.ahnlab.com/en/60054/> <https://asec.ahnlab.com/wp-content/uploads/2023/03/2022-Threat-Trend-Report-on-Kimsuky.pdf> <https://asec.ahnlab.com/wp-content/uploads/2023/03/Unique-characteristics-of-Kimsuky-groups-spear-phishing-emails.p <https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report> <https://blog.google/threat-analysis-group/how-were-protecting-users-from-government-backed-attacks-from-north-korea <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/> <https://www.rapid7.com/blog/post/2024/03/20/the-updated-apt-playbook-tales-from-the-kimsuky-threat-actor-group/> <https://media.defense.gov/2024/May/02/2003455483/-1/-1/0/CSA-NORTH-KOREAN-ACTORS-EXPLOIT-WEAK-DM	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0094/> <https://attack.mitre.org/groups/G0086/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
