Reaper, APT 37, Ricochet Chollima, ScarCruft

Archived: 2026-04-05 21:13:57 UTC

APT group: Reaper, APT 37, Ricochet Chollima, ScarCruft

Names	Reaper *(FireEye)* TEMP.Reaper *(FireEye)* APT 37 *(Mandiant)* Ricochet Chollima *(CrowdStrike)* ScarCruft *(Kaspersky)* Cerium *(Microsoft)* Group 123 *(Talos)* Red Eyes *(AhnLab)* Geumseong121 *(ESRC)* Venus 121 *(ESRC)* Hermit *(Tencent)* InkySquid *(Volexity)* ATK 4 *(Thales)* ITG10 *(IBM)* Ruby Sleet *(Microsoft)* Crooked Pisces *(Palo Alto)* Moldy Pisces *(Palo Alto)* Osmium *(Microsoft)* Opal Sleet *(Microsoft)* TA-RedAnt *(AhnLab)* G0067 *(MITRE)*
Country	North Korea
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2012
Description	Some research organizations link this group to Lazarus Group, Hidden Cobra, Labyrinth Chollima. (FireEye) Read our report, APT37 (Reaper): The Overlooked North Korean Actor, to learn more about our assessment actor is working on behalf of the North Korean government, as well as various other details about their operations: • Targeting: Primarily South Korea – though also Japan, Vietnam and the Middle East – in various industry verticals, in chemicals, electronics, manufacturing, aerospace, automotive, and healthcare. • Initial Infection Tactics: Social engineering tactics tailored specifically to desired targets, strategic web compromises targeted cyberespionage operations, and the use of torrent file-sharing sites to distribute malware more indiscriminately • Exploited Vulnerabilities: Frequent exploitation of vulnerabilities in Hangul Word Processor (HWP), as well as Adob group has demonstrated access to zero-day vulnerabilities (CVE-2018-0802), and the ability to incorporate them into o • Command and Control Infrastructure: Compromised servers, messaging platforms, and cloud service providers to avo The group has shown increasing sophistication by improving their operational security over time. • Malware: A diverse suite of malware for initial intrusion and exfiltration. Along with custom malware used for espior APT37 also has access to destructive malware.
Observed	Sectors: Aerospace, Automotive, Chemical, Education, Financial, Government, Healthcare, High-Tech, Manufacturing Technology, Transportation. Countries: Cambodia, China, Czech, Hong Kong, India, Japan, Kuwait, Laos, Nepal, Poland, Romania, Russia, South I Thailand, UK, USA, Vietnam.

Tools used	BLUELIGHT, CARROTBALL, CARROTBAT, Cobalt Strike, CORALDECK, DOGCALL, Dolphin, Erebus, Final1st Loader, GELCAPSULE, GOLDBACKDOOR, GreezeBackdoor, HAPPYWORK, KARAE, KevDroid, Konni, MILKI N1stAgent, NavRAT, Nokki, Oceansalt, PoohMilk Loader, POORAIM, RokRAT, RICECURRY, RUHAPPY, ScarCruf SHUTTERSPEED, SLOWDRIFT, SOUNDWAVE, Syscon, VeilShell, WINERACK, ZUMKONG and several 0-day F Office exploits.	
Operations performed	2012	Spying on South Korean users.
	2016	Operation “Erebus” <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/erebus-linux-ransomware-impact-to-countermeasures>
	Mar 2016	Operation “Daybreak” Target: High profile victims. Method: Previously unknown (0-day) Adobe Flash Player exploit. It is also possible that the group deplo zero day exploit, CVE-2016-0147, which was patched in April. <https://securelist.com/operation-daybreak/75100/> Note: not the same operation as DarkHotel’s Operation “Daybreak”.
	Aug 2016	Operation “Golden Time” Target: South Korean users. Method: spear-phishing emails combined with malicious HWP documents created using Hancom Hangu
	Nov 2016	Operation “Evil New Year” Target: South Korean users. Method: spear-phishing emails combined with malicious HWP documents created using Hancom Hangu
	Mar 2017	Operation “Are You Happy?” Target: South Korean users. Method: Not only to gain access to the remote infected systems but to also wipe the first sectors of the de
	May 2017	Operation “FreeMilk” Target: Several non-Korean financial institutions. Method: A malicious Microsoft Office document, a deviation from their normal use of Hancom documer <https://unit42.paloaltonetworks.com/unit42-freemilk-highly-targeted-spear-phishing-campaign/>
	Nov 2017	Operation “North Korean Human Right” Target: South Korean users. Method: Spear-phishing emails combined with malicious HWP documents created using Hancom Hangu
	Dec 2017	Operation “Fractured Block” <https://unit42.paloaltonetworks.com/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-d malware-targeting-southeast-asia/>
	Jan 2018	Operation “Evil New Year 2018” Target: South Korean users. Method: Spear-phishing emails combined with malicious HWP documents created using Hancom Hangu
	Mar 2018	Operation “Battle Cruiser” <https://blog.alyac.co.kr/1625>
	Apr 2018	Operation “Star Cruiser” <http://blog.alyac.co.kr/1653>
	May 2018	Operation “Onezero” <https://brica.de/alerts/alert/public/1215993/analysis-of-apt-attack-on-operation-onezero-conducted-as-a panmunjom-declaration/>
	Aug 2018	Operation “Rocket Man” <https://brica.de/alerts/alert/public/1226363/the-latest-apt-campaign-of-venus-121-group-operation-rock
	Nov 2018	Operation “Korean Sword” <https://brica.de/alerts/alert/public/1252896/venus-121-apt-organization-operation-high-expert/>

Jan 2019	Operation “Holiday Wiper” <https://brica.de/alerts/alert/public/1252896/venus-121-apt-organization-operation-high-expert/>
Mar 2019	Operation “Golden Bird” <https://brica.de/alerts/alert/public/1252896/venus-121-apt-organization-operation-high-expert/>
Mar 2019	Operation “High Expert” <https://brica.de/alerts/alert/public/1252896/venus-121-apt-organization-operation-high-expert/>
Apr 2019	Operation “Black Banner” <https://brica.de/alerts/alert/public/1257351/venus-121-rocketman-campaign-operation-black-banner-apt
May 2019	We recently discovered some interesting telemetry on this actor, and decided to dig deeper into ScarCruf activity. This shows that the actor is still very active and constantly trying to elaborate its attack tools. Ba telemetry, we can reassemble ScarCruft’s binary infection procedure. It used a multi-stage binary infectio each module effectively and evade detection. <https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/>
Jul 2019	Operation “Fractured Statue” <https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-p attacks/>
Sep 2019	Operation “Dragon messenger” <https://blog.alyac.co.kr/attachment/cfile1.uf@99A46A405DC8E3031C9E2A.pdf>
Jan 2020	North Korean APT used VBA self decode technique to inject RokRat <https://blog.malwarebytes.com/threat-analysis/2021/01/retrohunting-apt37-north-korean-apt-used-vba-s technique-to-inject-rokrat/>
Mar 2020	Operation “Spy Cloud” <https://blog.alyac.co.kr/attachment/cfile8.uf@9977CF405E81A09B1C4CE2.pdf>
Dec 2020	North Korean software supply chain attack targets stock investors <https://www.bleepingcomputer.com/news/security/north-korean-software-supply-chain-attack-targets-s investors/> <https://blog.alyac.co.kr/3489>
Mar 2021	ScarCruft surveilling North Korean defectors and human rights activists <https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/>
Apr 2021	North Korean APT InkySquid Infects Victims Using Browser Exploits <https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser- <https://www.volexity.com/blog/2021/08/24/north-korean-bluelight-special-inkysquid-deploys-rokrat/>
Apr 2021	Who’s swimming in South Korean waters? Meet ScarCruft’s Dolphin <https://www.welivesecurity.com/2022/11/30/whos-swimming-south-korean-waters-meet-scarcrufts-dol
Jul 2021	New variant of Konni malware used in campaign targetting Russia <https://blog.malwarebytes.com/threat-intelligence/2021/08/new-variant-of-konni-malware-used-in-cam targetting-russia/>
Dec 2021	North Korean hackers target Russian diplomats using New Year greetings <https://therecord.media/north-korean-hackers-attack-russian-diplomats-using-new-year-greetings/> <https://blog.lumen.com/new-konni-campaign-targeting-russian-ministry-of-foreign-affairs/>
Jan 2022	KONNI evolves into stealthier RAT <https://blog.malwarebytes.com/threat-intelligence/2022/01/konni-evolves-into-stealthier-rat/>
Mar 2022	The ink-stained trail of GOLDBACKDOOR <https://stairwell.com/news/threat-research-the-ink-stained-trail-of-goldbackdoor/>
Mar 2022	Lookout Discovers New Spyware by North Korean APT37 <https://www.lookout.com/threat-intelligence/article/lookout-discovers-new-spyware-by-north-korean-a
May 2022	Comrades in Arms? | North Korea Compromises Sanctioned Russian Missile Engineering Company <https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-mis

	engineering-company/>
Jul 2022	Operation “STIFF#BIZON” The Securonix Threat Research (STR) team has been observing and investigating a new attack campaign high-value targets, including Czech Republic, Poland, and other countries. <https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/>
Sep 2022	Meeting the “Ministrer” <https://www.fortinet.com/blog/threat-research/konni-rat-phishing-email-deploying-malware>
Oct 2022	Internet Explorer 0-day exploited by North Korean actor APT37 <https://blog.google/threat-analysis-group/internet-explorer-0-day-exploited-by-north-korean-actor-apt3
Jan 2023	RedEyes hackers use new malware to steal data from Windows, phones <https://www.bleepingcomputer.com/news/security/redeyes-hackers-use-new-malware-to-steal-data-fror phones/>
Feb 2023	HWP Malware Using the Steganography Technique: RedEyes (ScarCruft) <https://asec.ahnlab.com/en/48063/>
Mar 2023	CHM Malware Disguised as Security Email from a Korean Financial Company: Redeyes (Scarcruft) <https://asec.ahnlab.com/en/49089/>
Apr 2023	RokRAT Malware Distributed Through LNK Files (*.lnk): RedEyes (ScarCruft) <https://asec.ahnlab.com/en/51751/>
Apr 2023	ITG10 Likely Targeting South Korean Entities of Interest to the Democratic People’s Republic of Korea <https://securityintelligence.com/posts/itg10-targeting-south-korean-entities/>
May 2023	Tracking Traces of Malware Disguised as Hancom Office Document File and Being Distributed (RedEy <https://asec.ahnlab.com/en/53377/>
May 2023	RedEyes Group Wiretapping Individuals (APT37) <https://asec.ahnlab.com/en/54349/>
Jul 2023	Operation “STARK#MULE” Detecting Ongoing STARK#MULE Attack Campaign Targeting Victims Using US Military Document L <https://www.securonix.com/blog/detecting-ongoing-starkmule-attack-campaign-targeting-victims-using document-lures/>
Sep 2023	Distribution of Backdoor via Malicious LNK: RedEyes (ScarCruft) <https://asec.ahnlab.com/en/56756/>
Sep 2023	RedEyes (ScarCruft)’s CHM Malware Using the Topic of Fukushima Wastewater Release <https://asec.ahnlab.com/en/56857/>
Dec 2023	Distribution of Phishing Email Under the Guise of Personal Data Leak (Konni) <https://asec.ahnlab.com/en/59763/>
Dec 2023	ScarCruft | Attackers Gather Strategic Intelligence and Target Cybersecurity Professionals <https://www.sentinelone.com/labs/a-glimpse-into-future-scarcruft-campaigns-attackers-gather-strategic and-target-cybersecurity-professionals/>
Aug 2024	AhnLab and NCSC Release Joint Report on Microsoft Zero-Day Browser Vulnerability (CVE-2024-381 <https://asec.ahnlab.com/en/83877/>
Sep 2024	Kimsuky-linked hackers use similar tactics to attack Russia and South Korea, researchers say <https://therecord.media/kimsuky-north-korea-hackers-targeting-russia-south-korea>
Sep 2024	Operation “SHROUDED#SLEEP” SHROUDED#SLEEP: A Deep Dive into North Korea’s Ongoing Campaign Against Southeast Asia <https://www.securonix.com/blog/shroudedsleep-a-deep-dive-into-north-koreas-ongoing-campaign-agai asia/>
Mar 2025	Operation “ToyBox Story” Analysis of APT37 Attack Case Disguised as a Think Tank for National Security Strategy in South Kore

		ToyBox Story) <https://www.genians.co.kr/en/blog/threat_intelligence/toybox-story>
Counter operations	Dec 2019	On December 27, a U.S. district court unsealed documents detailing work Microsoft has performed to di cyberattacks from a threat group we call Thallium, which is believed to operate from North Korea. Our c against Thallium, filed in the U.S. District Court for the Eastern District of Virginia, resulted in a court o Microsoft to take control of 50 domains that the group uses to conduct its operations. <https://blogs.microsoft.com/on-the-issues/2019/12/30/microsoft-court-action-against-nation-state-cyber
	Mar 2023	The Unintentional Leak: A glimpse into the attack vectors of APT37 <https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37>
Information	<https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf> <https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html> <https://threatpost.com/scarcruft-apt-group-used-latest-flash-zero-day-in-two-dozen-attacks/118642/> <https://global.ahnlab.com/global/upload/download/techreport/%5BAhnLab%5D%20Red_Eyes_Hacking_Group_Rep <https://exchange.xforce.ibmcloud.com/threat-group/guid:ebf490b366269368dda52acaf34e7d38> <https://thorcert.notion.site/TTPs-ScarCruft-Tracking-Note-67acee42e4ba47398183db9fc7792aff> <https://www.microsoft.com/en-us/security/blog/2024/11/22/microsoft-shares-latest-intelligence-on-north-korean-and-actors-at-cyberwarcon/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0067/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=crooked-pisces> <https://pan-unit42.github.io/playbook_viewer/?pb=moldypisces>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
