Lazarus Group, Hidden Cobra, Labyrinth Chollima

Archived: 2026-04-05 23:19:53 UTC

NamesLazarus Group *(Kaspersky)*
Labyrinth Chollima *(CrowdStrike)*
Group 77 *(Talos)*
Hastati Group *(SecureWorks)*
Whois Hacking Team *(McAfee)*
NewRomanic Cyber Army Team *(McAfee)*
Zinc *(Microsoft)*
Hidden Cobra *(Trend Micro)*
Appleworm *(Symantec)*
APT-C-26 *(Qihoo 360)*
ATK 3 *(Thales)*
SectorA01 *(ThreatRecon)*
ITG03 *(IBM)*
TA404 *(Proofpoint)*
DEV-0139 *(Microsoft)*
Guardians of Peace *(self given)*
Gods Apostles *(self given)*
Gods Disciples *(self given)*
UNC577 *(Mandiant)*
UNC2970 *(Mandiant)*
UNC4034 *(Mandiant)*
UNC4736 *(Mandiant)*
UNC4899 *(Mandiant)*
Diamond Sleet *(Microsoft)*
Citrine Sleet *(Microsoft)*
Jade Sleet *(Microsoft)*
TraderTraitor *(CISA)*
Gleaming Pisces *(Palo Alto)*
Slow Pisces *(Palo Alto)*
G0032 *(MITRE)* Country North Korea SponsorState-sponsored, Bureau/Unit 211 MotivationInformation theft and espionage, Sabotage and destruction, Financial crime First seen2007 Description(Malwarebytes) Lazarus Group is commonly believed to be run by the North Korean government, motivated primarily by financial gain as a method of circumventing long-standing sanctions against the regime. They first came to substantial media notice in 2013 with a series of coordinated attacks against an assortment of South Korean broadcasters and financial institutions using DarkSeoul, a wiper program that overwrites sections of the victims' master boot record.

In November 2014, a large scale breach of Sony Pictures was attributed to Lazarus. The attack was notable due to its substantial penetration across Sony networks, the extensive amount of data exfiltrated and leaked, as well of use of a wiper in a possible attempt to erase forensic evidence. Attribution on the attacks was largely hazy, but the FBI released a statement tying the Sony breach to the earlier DarkSeoul attack, and officially attributed both incidents to North Korea.

Fast forward to May 2017 with the widespread outbreak of WannaCry, a piece of ransomware that used an SMB exploit as an attack vector. Attribution to North Korea rested largely on code reuse between WannaCry and previous North Korean attacks, but this was considered to be thin grounds given the common practice of tool sharing between regional threat groups. Western intelligence agencies released official statements to the public reaffirming the attribution, and on September 6, 2018, the US Department of Justice charged a North Korean national with involvement in both WannaCry and the Sony breach.

Lazarus Group has 3 subgroups:
1. Subgroup: Andariel, Silent Chollima
2. Subgroup: BeagleBoyz
3. Subgroup: Bluenoroff, APT 38, Stardust Chollima
4. Subgroup: Operation Contagious Interview

The following groups may be associated with the Lazarus Group: Covellite, Reaper, APT 37, Ricochet Chollima, ScarCruft, Wassonite and Moonstone Sleet.

ObservedSectors: Aerospace, Defense, Energy, Engineering, Financial, Government, Healthcare, Media, Shipping and Logistics, Technology and BitCoin exchanges.
Countries: Australia, Bangladesh, Belgium, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Netherlands, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam and Worldwide (WannaCry). Tools used3proxy, 3Rat Client, Andaratm, AppleJeus, ARTFULPIE, Aryan, ATMDtrack, AuditCred, BADCALL, Bankshot, BanSwift, BISTROMATH, Bitsran, BLINDINGCAN, BlindToad, Bookcode, BootWreck, BottomLoader, Brambul, BTC Changer, BUFFETLINE, Castov, CheeseTray, CleanToad, ClientTraficForwarder, COLDCAT, CollectionRAT, Concealment Troy, Contopee, CookieTime, Dacls RAT, DarkComet, DAVESHELL, DBLL Dropper, DeltaCharlie, Destover, DLRAT, Dozer, DoublePulsar, DRATzarus, Dtrack, Duuzer, DyePack, ELECTRICFISH, EternalBlue, FALLCHILL, Fimlis, FudModule, Gh0st RAT, Gopuram, HARDRAIN, Hawup, Hermes, HLOADER, HOOKSHOT, HOPLIGHT, HotelAlfa, HOTCROISSANT, Hotwax, HtDnDownLoader, Http Dr0pper, HTTP Troy, ICONICSTEALER, Joanap, Jokra, KANDYKORN, KEYMARBLE, KillDisk, Koredos, Lazarus, LightlessCan, LIGHTSHIFT, LIGHTSHOW, MagicRAT, MATA, Mimikatz, Mydoom, NachoCheese, NestEgg, NickelLoader, NineRAT, NukeSped, OpBlockBuster, PEBBLEDASH, PhanDoor, PLANKWALK, Plink, PondRAT, POOLRAT, PowerBrace, PowerRatankba, PowerShell RAT, PowerSpritz, PowerTask, ProcDump, Proxysvc, PSLogger, Quickcafe, QuiteRAT, Ratankba, RatankbaPOS, RawDisk, Recon, RedShawl, Rifdoor, Rising Sun, Romeos, RomeoAlfa, RomeoBravo, RomeoCharlie, RomeoDelta, RomeoEcho, RomeoFoxtrot, RomeoGolf, RomeoHotel, RomeoMike, RomeoNovember, RomeoWhiskey, RustBucket, Scout, SHARPKNOT, SheepRAT, SIDESHOW, SierraAlfa, SierraCharlie, SIGFLIP, SLICKSHOES, SmallTiger, Stunnel, SUDDENICON, SUGARLOADER, TAINTEDSCRIBE, TAXHAUL, Tdrop, Tdrop2, TFlower, ThreatNeedle, TigerRAT, TOUCHKEY, TOUCHMOVE, TOUCHSHIFT, TOUCHSHOT, Troy, TYPEFRAME, ValeforBeta, VEILEDSIGNAL, VHD, Volgmer, VSingle, Vyveva, WannaCry, WbBot, WinorDLL64, WolfRAT, Wormhole, YamaBot, Yort, Living off the Land. Operations performed2007Operation “Flame”
Target: South Korean government.
Method: Disruption and sabotage. Jul 2009Operation “Troy”
North Korean hackers are suspected of launching a cyber-attack on some of the most important government offices in the US and South Korea in recent days, including the White House, the Pentagon, the New York Stock Exchange and the presidential Blue House in Seoul.
The attack took out some of South Korea’s most important websites, including those of the Blue House, the defense ministry, the national assembly, Shinhan bank, Korea Exchange bank and the top internet portal Naver.
Target: Government, financial and media institutions in South Korea and USA.
Method: DdoS attacks.

<https://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack> Mar 2011Attack on South Korean banks and media

Recent Distributed Denial of Service (DdoS) attacks on a number South Korean websites have been in news for the past week. The threat responsible for carrying out these attacks is Trojan.Koredos.

Target: South Korean organizations.

Method: DdoS attacks and destruction of infected machines.

<https://www.symantec.com/connect/blogs/trojankoredos-comes-unwelcomed-surprise> Mar 2013Operation “Ten Days of Rain” / ”DarkSeoul”

Computer networks running three major South Korean banks and the country’s two largest broadcasters were paralyzed Wednesday in attacks that some experts suspected originated in North Korea, which has consistently threatened to cripple its far richer neighbor.

The attacks, which left many South Koreans unable to withdraw money from A.T.M.’s and news broadcasting crews staring at blank computer screens, came as the North’s official Korean Central News Agency quoted the country’s leader, Kim Jong-un, as threatening to destroy government installations in the South, along with American bases in the Pacific.

Target: Three broadcasting stations and a bank in South Korea.

Method: Infecting with viruses, stealing and wiping information.

<https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html> May 2013South Korean Financial Companies Targeted by Castov

In the past few months we have been actively monitoring an exploit kit, called Gongda, which is mainly targeting South Korea. Interestingly, we have come across a piece of malware, known as Castov, being delivered by this exploit kit that targets specific South Korean financial companies and their customers. The cybercriminals in this case have done their research on the South Korean online financial landscape.

<https://www.symantec.com/connect/blogs/south-korean-financial-companies-targeted-castov> Jun 2013DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War

Yesterday, June 25, the Korean peninsula observed a series of cyberattacks coinciding with the 63rd anniversary of the start of the Korean War. While multiple attacks were conducted by multiple perpetrators, one of the distributed denial-of-service (DdoS) attacks observed yesterday against South Korean government websites can be directly linked to the DarkSeoul gang and Trojan.Castov.

<https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war> Nov 2014Operation “Blockbuster”: Breach of Sony Pictures Entertainment

The attack on Sony Pictures became public knowledge on November 24, 2014, when Sony employees turned on their computers to be greeted with the sight of a neon red skeleton and the words “Hacked by GOP”, which stood for “Guardians of the Peace”. The message also threatened to release data later that day if an unspecified request was not met. Over the following weeks, huge swathes of information stolen from Sony were released, including: personal information about employees and their families; email correspondence between employees at the company; information about company salaries, unreleased Sony films, and other information.

Target: Sony Pictures Entertainment (released the “Interview” movie, ridiculing the North Korean leader).

Method: Infecting with malware, stealing and wiping data of the company’s employees, correspondence, copies of unreleased films.

<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know>

<https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf> Jun 2015Using the Palo Alto Networks AutoFocus threat intelligence platform, we identified several samples of malicious code with behavior similar to the aforementioned Operation Troy campaign dating back to June 2015, over two years after the original attacks in South Korea. Session data revealed a live attack targeting the transportation and logistics sector in Europe.

<https://unit42.paloaltonetworks.com/tdrop2-attacks-suggest-dark-seoul-attackers-return/> Mar 2017The Blockbuster Sequel

This recently identified activity is targeting Korean speaking individuals, while the threat actors behind the attack likely speak both Korean and English. This blog will detail the recently discovered samples, their functionality, and their ties to the threat group behind Operation Blockbuster.
<https://unit42.paloaltonetworks.com/unit42-the-blockbuster-sequel/> May 2017WannaCry ransomware
ThaiCERT's whitepaper:
<https://www.dropbox.com/s/hpr9fas9xbzo2uz/Whitepaper WannaCry Ransomware.pdf?dl=0> Jun 2017We analyzed a new RATANKBA variant (BKDR_RATANKBA.ZAEL–A), discovered in June 2017, that uses a PowerShell script instead of its more traditional PE executable form—a version that other researchers also recently identified.
<https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba/> Aug 2017The Blockbuster Saga Continues
Unit 42 researchers at Palo Alto Networks have discovered new attack activity targeting individuals involved with United States defense contractors.
<https://unit42.paloaltonetworks.com/unit42-blockbuster-saga-continues/> Late 2017Several financial sector and a casino breaches using KillDisk wiping malware in Latin America and USA.
<https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/>
<https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/> 2017/2018Cryptocurrency attacks on South Korean exchanges.
<https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf>
<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/> Jan 2018F-Secure’s investigation revealed that a system administrator from the target organization received a phishing document via their personal LinkedIn account. The document masqueraded as a legitimate job advert for a role in a blockchain technology company that matched the employee’s skills.
<https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf> Mar 2018APT attack on Turkish Financial Sector.
Target: Turkish Financial Sector.
Method: Spear-phishing with Bankshot implant.
<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/> Apr 2018Operation “GhostSecret”
Target: The impacted organizations are in industries such as telecommunications, health, finance, critical infrastructure, and entertainment.
Method: Spear-phishing with Destover-like implant.
<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/> Apr 2018The first artefacts we found relating to MATA were used around April 2018. After that, the actor behind this advanced malware framework used it aggressively to infiltrate corporate entities around the world.
<https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/> Aug 2018Operation “AppleJeus”
Target: Cryptocurrency exchange.
Method: Fake installer and macOS malware.
<https://securelist.com/operation-applejeus/87553/> Jul 2018Operation “CryptoCore”
Operation “Dangerous Password”
Operation “Leery Turtle”
<https://www.clearskysec.com/wp-content/uploads/2020/06/CryptoCore_Group.pdf>
<https://www.clearskysec.com/wp-content/uploads/2021/05/CryptoCore-Lazarus-Clearsky.pdf> Summer 2018Our investigation into the Dtrack RAT actually began with a different activity. In the late summer of 2018, we discovered ATMDtrack, a piece of banking malware targeting Indian banks. Further analysis showed that the malware was designed to be planted on the victim’s ATMs, where it could read and store the data of cards that were inserted into the machines.

<https://securelist.com/my-name-is-dtrack/93338/> Oct 2018Operation “Sharpshooter”
Target: 87 organizations in many different sectors (majority Government and Defense) across the globe, predominantly in the United States.
Method: Rising Sun implant to gather intelligence.
<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/> Nov 2018More Attacks on Cryptocurrency Businesses
Target: Some of the documents (for instance one entitled “sample document for business plan evaluation of venture company”) were prepared in Korean, presumably to target South Korean businesses. Another contains a business overview of what seems to be a Chinese technology consulting group named LAFIZ (“we couldn’t confirm if it’s a legitimate business or another fake company made up by Lazarus,” Kaspersky Lab researchers said). Yet another provided information for coin listings with a translation in Korean, researchers said.
Method: Documents containing weaponized macros, “carefully prepared to attract the attention of cryptocurrency professionals.” It utilizes PowerShell to control Windows systems and macOS malware for Apple users.
<https://securelist.com/cryptocurrency-businesses-still-being-targeted-by-lazarus/90019/> Mar 2019The infamous Lazarus threat actor group has been found targeting an Israeli defense company, according to new research outlined by a cybersecurity firm ClearSky. The campaign is carried out with an intention to steal military and commercial secrets.
<https://cyware.com/news/lazarus-hacking-group-expand-their-attack-horizon-by-targeting-an-israeli-defense-company-02e2ec77> Mar 2019Operation “AppleJeus sequel”
As a result of our ongoing efforts, we identified significant changes to the group’s attack methodology.
<https://securelist.com/operation-applejeus-sequel/95596/> Apr 2019“Hoplight” Malware Campaign
Known as “Hoplight,” the malware is a collection of nine files, though most of those are designed to work as obfuscation layers to keep admins and security software from spotting the attack.
<https://www.theregister.co.uk/2019/04/10/lazarus_group_malware/> May 2019North Korean Tunneling Tool: ELECTRICFISH
This report provides analysis of one malicious 32-bit Windows executable file. The malware implements a custom protocol that allows traffic to be funneled between a source and a destination Internet Protocol (IP) address. The malware continuously attempts to reach out to the source and the designation system, which allows either side to initiate a funneling session. The malware can be configured with a proxy server/port and proxy username and password. This feature allows connectivity to a system sitting inside of a proxy server, which allows the actor to bypass the compromised system’s required authentication to reach outside of the network.
<https://www.us-cert.gov/ncas/analysis-reports/AR19-129A> May 2019Hackers associated with the APT Lazarus/HIDDEN COBRA group were found to be breaking into online stores of large US retailers and planting payment skimmers as early as May 2019.
<https://sansec.io/research/north-korea-magecart> Sep 2019Operation “In(ter)caption”
Operation “In(ter)caption”
At the end of last year, we discovered targeted attacks against aerospace and military companies in Europe and the Middle East, active from September to December 2019. A collaborative investigation with two of the affected European companies allowed us to gain insight into the operation and uncover previously undocumented malware.
<https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf> Sep 2019Lazarus Group’s MATA Framework Leveraged to Deploy TFlower Ransomware
<https://www.sygnia.co/mata-framework> Oct 2019Dacls, the Dual platform RAT
<https://blog.netlab.360.com/dacls-the-dual-platform-rat-en/> Dec 2019The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT
<https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/> 2020Operation “North Star”
In this 2020 campaign McAfee ATR discovered a series of malicious documents containing job postings taken from leading

defense contractors to be used as lures, in a very targeted fashion.
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/>
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-summary-of-our-latest-analysis/>
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-behind-the-scenes/> 2020Operation “Dream Job”
Upon infection, the attackers collected intelligence regarding the company’s activity, and also its financial affairs, probably in order to try and steal some money from it.
<https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf> Feb 2020Lazarus BTC Changer
<https://www.group-ib.com/blog/btc_changer> Mar 2020Lazarus on the hunt for big game
<https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/> Apr 2020New Mac variant of Lazarus Dacls RAT distributed via Trojanized 2FA app
<https://blog.malwarebytes.com/threat-analysis/2020/05/new-mac-variant-of-lazarus-dacls-rat-distributed-via-trojanized-2fa-app/> Apr 2020We discovered another malware cluster named CookieTime used in a campaign mainly focused on the defense industry.
<https://securelist.com/apt-trends-report-q1-2021/101967/> Jun 2020Covid-19 Relief: North Korea Hackers Lazarus Planning Massive Attack on US, UK, Japan, Singapore, India, South Korea?
<https://www.ibtimes.sg/covid-19-relief-north-korea-hackers-lazarus-planning-massive-attack-us-uk-japan-singapore-47072> Jun 2020ESET researchers have discovered a previously undocumented Lazarus backdoor, which they have dubbed Vyveva, being used to attack a freight logistics company in South Africa.
<https://www.welivesecurity.com/2021/04/08/are-you-afreight-dark-watch-out-vyveva-new-lazarus-backdoor/> Mid 2020Lazarus targets defense industry with ThreatNeedle
<https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Lazarus-targets-defense-industry-with-Threatneedle-En.pdf> Aug 2020North Korean hackers are targeting Israel's defense sector, Israel Ministry of Defense claims
<https://www.cyberscoop.com/north-korea-hackers-lazarus-group-israel-defense/> Nov 2020ESET researchers uncover a novel Lazarus supply-chain attack leveraging WIZVERA VeraPort software
<https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/> Dec 2020As the COVID-19 crisis grinds on, some threat actors are trying to speed up vaccine development by any means available. We have found evidence that actors, such as the Lazarus group, are going after intelligence that could help these efforts by attacking entities related to COVID-19 research.
<https://securelist.com/lazarus-covets-covid-19-related-intelligence/99906/> Jan 2021New campaign targeting security researchers
<https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/>
<https://www.zdnet.com/article/google-north-korean-hackers-have-targeted-security-researchers-via-social-media/>
<https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/> Mar 2021Lazarus Attack Activities Targeting Japan (VSingle/ValeforBeta)
<https://blogs.jpcert.or.jp/en/2021/03/Lazarus_malware3.html> Mar 2021Update on campaign targeting security researchers
<https://blog.google/threat-analysis-group/update-campaign-targeting-security-researchers/> Spring 2021Lazarus campaign TTPs and evolution
<https://cybersecurity.att.com/blogs/labs-research/lazarus-campaign-ttps-and-evolution> Autumn 2021Amazon-themed campaigns of Lazarus in the Netherlands and Belgium
<https://www.welivesecurity.com/2022/09/30/amazon-themed-campaigns-lazarus-netherlands-belgium/> Jun 2021APT actor Lazarus attacks defense industry, develops supply chain attack capabilities
<https://usa.kaspersky.com/about/press-releases/2021_apt-actor-lazarus-attacks-defense-industry-develops-supply-chain-attack-capabilities> Nov 2021Lazarus hackers target researchers with trojanized IDA Pro
<https://www.bleepingcomputer.com/news/security/lazarus-hackers-target-researchers-with-trojanized-ida-pro/> Dec 2021Lazarus Trojanized DeFi app for delivering malware

<https://securelist.com/lazarus-trojanized-defi-app/106195/> 2022Analysis Report on Lazarus Threat Group's Volgmer and Scout Malware
<https://asec.ahnlab.com/en/57685/> Jan 2022North Korea's Lazarus APT leverages Windows Update client, GitHub in latest campaign
<https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/> Jan 2022Lazarus Targets Chemical Sector
<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical> Feb 2022Operation "LolZarus"
Qualys Threat Research has identified a new Lazarus campaign using employment phishing lures targeting the defence sector.
<https://blog.qualys.com/vulnerabilities-threat-research/2022/02/08/lolzarus-lazarus-group-incorporating-lolbins-into-campaigns> Feb 2022On February 10, Threat Analysis Group discovered two distinct North Korean government-backed attacker groups exploiting a remote code execution vulnerability in Chrome, CVE-2022-0609.
<https://blog.google/threat-analysis-group/countering-threats-north-korea/> Early 2022Tracing State-Aligned Activity Targeting Journalists, Media
<https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists> Feb 2022Lazarus and the tale of three RATs
<https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html> Feb 2022MagicRAT: Lazarus' latest gateway into victim networks
<https://blog.talosintelligence.com/2022/09/lazarus-magicrat.html> Mar 2022A hacker stole $625 million from the blockchain behind NFT game Axie Infinity
<https://www.theverge.com/2022/3/29/23001620/sky-mavis-axie-infinity-ronin-blockchain-validation-defi-hack-nft>
<https://www.cisa.gov/uscert/ncas/alerts/aa22-108a> Apr 2022Lazarus Group Exploiting Log4Shell Vulnerability (NukeSped)
<https://asec.ahnlab.com/en/34461/> May 2022Lazarus Group Exploits Zero-Day Vulnerability to Hack South Korean Financial Entity
<https://thehackernews.com/2023/03/lazarus-group-exploits-zero-day.html> Jun 2022North Korea accused of orchestrating $100 million Harmony crypto hack
<https://therecord.media/north-korea-accused-of-orchestrating-100-million-harmony-crypto-hack/> Jun 2022Stealing the LIGHTSHOW
<https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970>
<https://www.mandiant.com/resources/blog/lightshift-and-lightshow> Jun 2022ZINC weaponizing open-source software
<https://www.microsoft.com/en-us/security/blog/2022/09/29/zinc-weaponizing-open-source-software/> Jun 2022฿uyer ฿eware: Fake Cryptocurrency Applications Serving as Front for AppleJeus Malware
<https://www.volexity.com/blog/2022/12/01/buyer-beware-fake-cryptocurrency-applications-serving-as-front-for-applejeus-malware/>
<https://www.microsoft.com/en-us/security/blog/2022/12/06/dev-0139-launches-targeted-attacks-against-the-cryptocurrency-industry/> Jul 2022Lazarus and the tale of three RATs
<https://blog.talosintelligence.com/lazarus-three-rats/> Aug 2022deBridge Finance crypto platform targeted by Lazarus hackers
<https://www.bleepingcomputer.com/news/security/debridge-finance-crypto-platform-targeted-by-lazarus-hackers/> Aug 2022Lazarus 'Operation In(ter)ception' Targets macOS Users Dreaming of Jobs in Crypto
<https://www.sentinelone.com/blog/lazarus-operation-interception-targets-macos-users-dreaming-of-jobs-in-crypto/> Aug 2022Operation "No Pineapple!"
North Korean hackers stole research data in two-month-long breach
<https://www.bleepingcomputer.com/news/security/north-korean-hackers-stole-research-data-in-two-month-long-breach/>

Sep 2022SlowMist: Investigation of North Korean APT's Large-Scale Phishing Attack on NFT Users <https://slowmist.medium.com/slowmist-our-in-depth-investigation-of-north-korean-apts-large-scale-phishing-attack-on-nft-users-362117600519> Sep 2022Lazarus and the FudModule Rootkit: Beyond BYOVD with an Admin-to-Kernel Zero-Day <https://decoded.avast.io/janvojtesek/lazarus-and-the-fudmodule-rootkit-beyond-byovd-with-an-admin-to-kernel-zero-day/> Late 2022DPRK Using Unpatched Zimbra Devices to Spy on Researchers <https://www.darkreading.com/remote-workforce/dprk-using-unpatched-zimbra-devices-to-spy-on-researchers-> Late 20223CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible <https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain> Late 2022North Korean hackers linked to defense sector supply-chain attack <https://www.bleepingcomputer.com/news/security/north-korean-hackers-linked-to-defense-sector-supply-chain-attack/> Nov 2022DPRK hacking groups breach South Korean defense contractors <https://www.bleepingcomputer.com/news/security/dprk-hacking-groups-breach-south-korean-defense-contractors/> Early 2023Lazarus Group's infrastructure reuse leads to discovery of new malware <https://blog.talosintelligence.com/lazarus-collectionrat/> Early 2023Lazarus Group exploits ManageEngine vulnerability to deploy QuiteRAT <https://blog.talosintelligence.com/lazarus-quiterat/> Mar 2023More evidence links 3CX supply-chain attack to North Korean hacking group <https://therecord.media/3cx-attack-north-korea-lazarus-group> <https://securelist.com/gopuram-backdoor-deployed-through-3cx-supply-chain-attack/109344/> <https://www.3cx.com/blog/news/mandiant-initial-results/> Mar 2023Linux malware strengthens links between Lazarus and the 3CX supply-chain attack <https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/> Mar 2023Lazarus luring employees with trojanized coding challenges: The case of a Spanish aerospace company <https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/> May 2023Lazarus Group Targeting Windows IIS Web Servers <https://asec.ahnlab.com/en/53132/> Jun 2023North Korea's Lazarus Group Likely Responsible For $35 Million Atomic Crypto Theft <https://hub.elliptic.co/analysis/north-korea-s-lazarus-group-likely-responsible-for-35-million-atomic-crypto-theft/> Jun 2023Lazarus Threat Group Exploiting Vulnerability of Korean Finance Security Solution <https://asec.ahnlab.com/en/54195/> Jul 2023North Korea Leverages SaaS Provider in a Targeted Supply Chain Attack <https://www.mandiant.com/resources/blog/north-korea-supply-chain> Jul 2023Security alert: social engineering campaign targets technology industry employees <https://github.blog/2023-07-18-security-alert-social-engineering-campaign-targets-technology-industry-employees/> Jul 2023Lazarus Threat Group Attacking Windows Servers to Use as Malware Distribution Points <https://asec.ahnlab.com/en/55369/> Jul 2023CoinsPaid blames Lazarus hackers for theft of $37,300,000 in crypto <https://www.bleepingcomputer.com/news/security/coinspaid-blames-lazarus-hackers-for-theft-of-37-300-000-in-crypto/> Jul 2023Lazarus hackers linked to $60 million Alphapo cryptocurrency heist <https://www.bleepingcomputer.com/news/security/lazarus-hackers-linked-to-60-million-alphapo-cryptocurrency-heist/> Jul 2023A cascade of compromise: unveiling Lazarus' new campaign <https://securelist.com/unveiling-lazarus-new-campaign/110888/> Aug 2023VMConnect: Malicious PyPI packages imitate popular open source modules <https://www.reversinglabs.com/blog/vmconnect-malicious-pypi-packages-imitate-popular-open-source-modules> <https://www.reversinglabs.com/blog/vmconnect-supply-chain-campaign-continues> Sep 2023FBI Identifies Lazarus Group

Cyber Actors as Responsible for Theft of $41 Million from Stake.com
<https://www.fbi.gov/news/press-releases/fbi-identifies-lazarus-group-cyber-actors-as-responsible-for-theft-of-41-million-from-stakecom> Sep 2023CoinEx confirms hack after $31 million in cryptocurrency allegedly stolen from exchange
<https://therecord.media/coinex-confirms-hack-after-31-million-allegedly-stolen>
<https://therecord.media/coinex-cryptocurrency-heist-north-korea> Oct 2023Multiple 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/> Oct 2023Operation “Dream Magic”
<https://asec.ahnlab.com/en/57736/> Oct 2023Elastic catches DPRK passing out KANDYKORN
<https://www.elastic.co/security-labs/elastic-catches-dprk-passing-out-kandykorn>
<https://www.sentinelone.com/blog/dprk-crypto-theft-macos-rustbucket-droppers-pivot-to-deliver-kandykorn-payloads/> Oct 2023Diamond Sleet supply chain compromise distributes a modified CyberLink installer
<https://www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/> Jan 2024Lazarus Group Uses the DLL Side-Loading Technique
<https://asec.ahnlab.com/en/60792/> Feb 2024New Malicious PyPI Packages used by Lazarus
<https://blogs.jpcert.or.jp/en/2024/02/lazarus_pypi.html> Feb 2024Slow Pisces Targets Developers With Coding Challenges and Introduces New Customized Python Malware
<https://unit42.paloaltonetworks.com/slow-pisces-new-custom-malware/> May 2024The Crypto Game of Lazarus APT: Investors vs. Zero-days
<https://securelist.com/lazarus-apt-steals-crypto-with-a-tank-game/114282/> May 2024FBI links North Korean hackers to $308 million crypto heist
<https://www.bleepingcomputer.com/news/security/fbi-links-north-korean-hackers-to-308-million-crypto-heist/> Jun 2024Fake recruiter coding tests target devs with malicious Python packages
<https://www.reversinglabs.com/blog/fake-recruiter-coding-tests-target-devs-with-malicious-python-packages> Jun 2024An Offer You Can Refuse: UNC2970 Backdoor Deployment Using Trojanized PDF Reader
<https://cloud.google.com/blog/topics/threat-intelligence/unc2970-backdoor-trojanized-pdf-reader> Aug 2024North Korean threat actor Citrine Sleet exploiting Chromium zero-day
<https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/> Sep 2024Gleaming Pisces Poisoned Python Packages Campaign Delivers PondRAT Linux and MacOS Backdoors
<https://unit42.paloaltonetworks.com/gleaming-pisces-applejeus-poolrat-and-pondrat/> Oct 2024Radiant links $50 million crypto heist to North Korean hackers
<https://www.bleepingcomputer.com/news/security/radiant-links-50-million-crypto-heist-to-north-korean-hackers/> Nov 2024Operation “SyncHole”
Operation SyncHole: Lazarus APT goes back to the well
<https://securelist.com/operation-synchole-watering-hole-attacks-by-lazarus/116326/> Jan 2025Operation “99”
North Korean State Sponsored Supply Chain Attack on Tech Innovation
<https://securityscorecard.com/wp-content/uploads/2025/01/Report_011325_Strike_Operation99.pdf> Jan 2025Operation “Phantom Circuit”
Operation Phantom Circuit: North Korea’s Global Data Exfiltration Campaign
<https://securityscorecard.com/wp-content/uploads/2025/01/Operation-Phantom-Circuit-Report_012725_03.pdf> Jan 2025Operation “Marstech Mayhem”
Lazarus Group’s Open-Source Trap: North Korea’s New Malware Tactic Targeting Developers and Crypto Wallets
<https://securityscorecard.com/wp-content/uploads/2025/02/Operation-Marstech-Mayhem-Report_021025_03.pdf> Feb 2025North Korean hackers linked to $1.5 billion ByBit crypto heist
<https://www.bleepingcomputer.com/news/security/north-korean-hackers-linked-to-15-billion-bybit-crypto-heist/>

<https://therecord.media/north-koreans-initial-laundering-bybit-hack> Apr 2025Beyond the Pond Phish: Unraveling Lazarus Group’s Evolving Tactics
<https://blog.bitmex.com/bitmex-busts-lazarus-group/> May 2025BitoPro exchange links Lazarus hackers to $11 million crypto heist
<https://www.bleepingcomputer.com/news/security/bitopro-exchange-links-lazarus-hackers-to-11-million-crypto-heist/> Counter operationsDec 2017Microsoft and Facebook disrupt ZINC malware attack to protect customers and the internet from ongoing cyberthreats
<https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/> Sep 2018North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions
<https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and> Sep 2019Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups
<https://home.treasury.gov/index.php/news/press-releases/sm774> Mar 2020Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group
<https://home.treasury.gov/news/press-releases/sm924> Jul 2020EU imposes the first ever sanctions against cyber-attacks
<https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/> Feb 2021Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe
<https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and> Apr 2022The Treasury Department's Office of Foreign Assets Control (OFAC) has sanctioned the address that received the cryptocurrency stolen in the largest cryptocurrency hack ever, the hack of Axie Infinity's Ronin network bridge.
<https://www.bleepingcomputer.com/news/security/fbi-links-largest-crypto-hack-ever-to-north-korean-hackers/> Aug 2022US sanctions crypto mixer Tornado Cash used by North Korean hackers
<https://www.bleepingcomputer.com/news/security/us-sanctions-crypto-mixer-tornado-cash-used-by-north-korean-hackers/> Feb 2023South Korea Sanctions Pyongyang Hackers
<https://www.bankinfosecurity.com/south-korea-sanctions-pyongyang-hackers-a-21193> Aug 2023FBI Identifies Cryptocurrency Funds Stolen by DPRK
<https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk> Oct 2023Justice Department Announces Court-Authorized Action to Disrupt Illicit Revenue Generation Efforts of Democratic People’s Republic of Korea Information Technology Workers
<https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-action-disrupt-illicit-revenue-generation> Nov 2023US seizes Sinbad crypto mixer used by North Korean Lazarus hackers
<https://www.bleepingcomputer.com/news/security/us-seizes-sinbad-crypto-mixer-used-by-north-korean-lazarus-hackers/> Feb 2025EU sanctions North Korean tied to Lazarus group over involvement in Ukraine war
<https://therecord.media/eu-sanctions-north-korea-ukraine-war-lazarus-group> Information<https://blog.malwarebytes.com/threat-analysis/2019/03/the-advanced-persistent-threat-files-lazarus-group/>
<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations>
<https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies>
<https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c>
<https://content.fireeye.com/apt/rpt-apt38>
<https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity>
<https://www.us-cert.gov/ncas/alerts/aa20-106a>
<https://www.us-cert.gov/ncas/current-activity/2020/05/12/north-korean-malicious-cyber-activity>
<https://global.ahnlab.com/global/upload/download/techreport/%5BAhnLab%5DAndariel_a_Subgroup_of_Lazarus%20(3).pdf>

<https://exchange.xforce.ibmcloud.com/threat-group/0c0c39d309b5c7f00a0a7edd54bb025e>
<https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/>
<http://www.documentcloud.org/documents/7038686-US-Army-report-on-North-Korean-military.html>
<https://public.intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals/>
<https://www.hvs-consulting.de/media/downloads/ThreatReport-Lazarus.pdf>
<https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army>
<https://blogs.jpcert.or.jp/en/2021/01/Lazarus_tools.html>
<https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazarus-recruitment/>
<https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-hermit-kingdoms-ransomware-play.html>
<https://asec.ahnlab.com/en/48223/>
<https://securelist.com/the-lazarus-group-deathnote-campaign/109490/>
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a>
<https://www.trmlabs.com/post/inside-north-koreas-crypto-heists>
<https://www.elliptic.co/blog/how-the-lazarus-group-is-stepping-up-crypto-hacks-and-changing-its-tactics>
<https://thehackernews.com/2023/10/north-koreas-lazarus-group-launders-900.html>
<https://www.hhs.gov/sites/default/files/manage-engine-vulnerability-sector-alert-tlpclear.pdf>
<https://eng.nis.go.kr/common/download.do?type=&seq=8E464392CD0485169FA97278AEE8B607>
<https://go.recordedfuture.com/hubfs/reports/cta-2023-1130.pdf>
<https://www.trmlabs.com/post/north-korean-hackers-stole-600-million-in-crypto-in-2023>
<https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_6_dongwook-kim_seulgi-lee_en.pdf>
<https://www.elliptic.co/blog/north-korean-hackers-return-to-tornado-cash-despite-sanctions>
<https://www.bleepingcomputer.com/news/cryptocurrency/coinstats-says-north-korean-hackers-breached-1-590-crypto-wallets/>
<https://www.group-ib.com/blog/apt-lazarus-python-scripts/>
<https://www.group-ib.com/blog/stealthy-attributes-of-apt-lazarus/>
<https://securelist.com/lazarus-new-malware/115059/>
<https://www.sonatype.com/hubfs/White_Papers/How-North-Korea-Backed-Lazarus-Group-is-Weaponizing-Open-Source-Whitepaper.pdf> MITRE ATT&CK<https://attack.mitre.org/groups/G0032/>
