

Forum:[Hack Forums](#)

Thread: [{Hacks, Scams, and Exploits} - #2 - The Lazarus Group. State Sponsored Hackers](#)

Pr0m3th3us - June 26, 2026, 9:28 am

Preface

I've always been extremely fascinated with North Korea. I have many books written by defectors, others by geopolitical analysts, and one in particular by Geoff White, called [The Lazarus Heist](#). I've watched countless docs, and always click on an article if it involves North Korea in any way. When most people think of state-sponsored hacking, they picture espionage, stealing secrets, disrupting infrastructure, and maybe leaking emails before an election (lol Hilary). What they don't picture is a government running a full-time criminal operation to rob banks and crypto exchanges to fund a fucking nuclear weapons program, among other things. But that's exactly what North Korea built, and the story of how they got there is equal parts terrifying and absurd. This isn't about some shadowy genius hacker working alone in a dark room. This is a government department, with a budget, a hierarchy, and a mandate, robbing the global financial system one wallet at a time.

The Hacks

In order to grasp the scope of Lazarus Group, you have to understand the corner North Korea has backed itself into. The regime's nuclear weapons program is the one card it holds at the international table, and with damn good reason in my opinion. It's the reason a country of 25 million impoverished people can demand a meeting with any world leader it wants. But nukes cost money, and international sanctions have choked off almost every legitimate revenue stream. The answer they landed on - hack it. The Lazarus Group is a state-sponsored hacker group alleged to be run by the government of North Korea, operating under the Reconnaissance General Bureau (RGB), a military intelligence agency. Known internally as the 414 Liaison Office according to North Korean defector Kim Kuk-song, it is also tracked by Western security firms under names including Hidden Cobra, ZINC, Diamond Sleet, and APT38. The group didn't start with crypto, they cut their teeth on bank SWIFT attacks and corporate sabotage, but once they smelled the money in cryptocurrency, their entire trajectory shifted...

Their entry point into the crypto world came partly by accident. In May 2017, Lazarus launched WannaCry, the ransomware worm that tore through hundreds of thousands of machines globally and demanded Bitcoin ransom payments. The haul was relatively modest, barely a million dollars, but what it gave them was a crash course in moving and laundering cryptocurrency through the blockchain. Seven months later, in December 2017, they put that education to use. NiceHash, a cryptocurrency cloud mining marketplace based in Slovenia, lost over 4,500 Bitcoin in December 2017, with subsequent investigations linking the attack to the Lazarus Group. The method?...classic phishing. Targeted emails to NiceHash employees, one click, a malware infection, lateral movement through the network until they found what they were looking for, the private keys to NiceHash's Bitcoin wallets. Once you have the private keys, the wallet is yours. At the time of the theft, that Bitcoin was worth around \$75 million, making it the largest theft in Slovenian history and larger than any bank robbery ever carried out in the United States.

The three individuals the DOJ ultimately named and indicted were Jon Chang Hyok, age 31; Kim Il, age 27; and Park Jin Hyok, age 36. All members of units of the Reconnaissance General Bureau, charged with participating in a wide ranging criminal conspiracy to conduct destructive cyberattacks

and steal and extort more than \$1.3 billion in money and cryptocurrency from financial institutions and companies worldwide. Park Jin Hyok had already been indicted separately in 2018 for his role in the Sony Pictures hack and WannaCry. The 2021 indictment folded the crypto heists in alongside those earlier charges. A fourth figure was also charged at the same time: Ghaleb Alaumary, 37, of Mississauga, Ontario, Canada, charged for his role as a money launderer for the North Korean conspiracy, among other criminal schemes. Alaumary was the outside contractor who helped convert stolen cryptocurrency into usable cash, the critical last mile that the North Koreans couldn't easily do themselves.

After NiceHash, the operation scaled up aggressively. The indictment covers the theft of \$75 million from a Slovenian cryptocurrency company in December 2017; \$24.9 million from an Indonesian cryptocurrency company in September 2018; and \$11.8 million from a financial services company in New York in August 2020 using a malicious application called CryptoNeuro Trader as a backdoor. That last entry points to another arm of the operation entirely...fake crypto trading apps. Lazarus built and deployed a series of malware-laced applications. Celas Trade Pro, Union Crypto Trader, QPay Wallet, CoinGoTrade, CryptoNeuro Trader, and Ant to Whale. Each one a legitimate-looking tool that, once downloaded and connected to your wallet, handed the attackers full backdoor access. Brilliant and ingenious. The backdoor was internally called "AppleJeus," and CISA discovered at least seven different versions of the malware since 2018, with Lazarus using a mix of phishing, social networking, and social engineering as infection vectors. When one app got burned by the security community, they just rebranded it and relaunched. The heists kept growing, at \$625 million stolen, the Ronin Bridge exploit in March 2022 remains the biggest DeFi exploit ever, attributed to Lazarus by the FBI. The attackers carried out a spearfishing attack enabling them to obtain the private keys necessary to drain the bridge, then routed the stolen funds through Tornado Cash and several centralized exchanges.

Laundering that much damn cryptocurrency is its own problem. North Korea developed a technique called peel-chaining. Its fucking brilliant, although tedious and this is how it works. transfer stolen funds to a fresh wallet, quickly peel off a small amount before the wallet gets flagged, cash that out through an exchange using fake KYC documents, then repeat. In one documented case, the FBI traced \$230 million to a cryptocurrency exchange that had implemented KYC controls. The exchange handed over verification photos, two different account holders, two different IDs...but when investigators compared the images, both men were sitting in identical chairs, wearing identical shirts, with fingers in identical positions around their respective ID documents. The faces had simply been Photoshopped onto the same base photograph. This was so hilarious i had to LOL at it, i mean really it took the FBI to find something that a human likely would have noticed had the exchange actually employed someone to go over those photos. That was the level of the forgery operation running in parallel with the technical hacking. Beyond fake IDs, two Chinese nationals were charged for offering services to launder stolen cryptocurrency, in some cases converting it into real-world money through iTunes gift cards and other methods to move small amounts out without detection

Impact

Buckle up, because the direct financial damage across the confirmed Lazarus crypto operations is staggering. Chainalysis reported that Lazarus stole \$275 million in crypto in 2020, more than half of all funds hacked across the entire crypto space that year, and \$400 million in 2021. The UN had already been watching this escalation: a United Nations report estimated that North Korea generated as much as \$2 billion from at least 35 cyberattacks targeting banks and cryptocurrency exchanges across over a dozen countries, with DPRK-backed hackers hitting Asian cryptocurrency exchanges between January 2017 and September 2018 believed responsible for \$571 million in losses. By 2025, the tally had climbed to roughly \$6 billion in total crypto stolen since 2017, culminating in the February 2025 Bybit hack where around 400,000 Ethereum worth approximately

\$1.5 billion was stolen, the single largest crypto exchange theft ever recorded, carried out by tricking wallet signers into approving a malicious transaction.

The damage isn't only financial. Every dollar North Korea successfully launders potentially funds weapons development. The US government states that the regime uses the proceeds from its hacking operations to fund illicit activities including its nuclear weapons program. The crypto exchanges and companies that were hit...NiceHash, KuCoin, Coincheck, the Ronin Bridge...faced reputational collapse, customer losses, and in some cases permanent closure. Individual users who had funds sitting in hot wallets on these platforms lost everything with zero recourse, because there is no central authority in crypto, no FDIC equivalent, no dispute resolution. The money simply vanished into wallets on the blockchain, moving through a maze of peel chains and mixers. The North Korean IT worker angle adds another dimension, the indictment also covers the development and marketing of the Marine Chain Token in 2017 and 2018. A fraudulent ICO designed to let investors purchase fractional ownership in shipping vessels, which was in reality a North Korean front operation to raise funds while evading international sanctions. Ordinary investors who would have put money into that ICO would have had no idea they were directly funding a sanctioned government.

What Changed

This is where I have to just laugh at what the US gov did. The indictments themselves, while obviously unenforceable since that the hackers are in North Korea and will never be extradited, nor are they stupid enough to leave the country at this point, had very little (if any) real world consequences. Jon Chang Hyok, Kim Il, and Park Jin Hyok are each charged with conspiracy to commit computer fraud and abuse and conspiracy to commit wire fraud and bank fraud, and are currently on the FBI most wanted list for cybercrimes, which I'm sure they just laughed at all the way to the proverbial "bank". While Ghaleb Alaumary, the Canadian money launderer, was charged with conspiracy to commit money laundering carrying a maximum sentence of 20 years. Alaumary, being in Canada, was actually arrested and prosecuted, a rare instance of the money laundering layer of the operation being possibly dismantled. The US Treasury also sanctioned three North Korean hacking groups (again laughable) Lazarus Group, Bluenoroff, and Andariel in 2019, engaged in funneling stolen financial assets to the North Korean government. Sanctioning the groups themselves meant any exchange that knowingly processed funds linked to those wallets could face serious legal liability. However with how well these groups operate I'm sure they are not going to openly tell exchanges who they are, seriously who would?

The industry response was slower but significant. The NiceHash hack specifically highlighted what security researchers had been saying for years, the separation between hot wallets (connected to the internet, accessible, spendable) and cold wallets (offline, air-gapped) was not optional...it was survival. The NiceHash attack highlighted weak operational separation between hot wallets and business systems, once attackers gained access to credentials or private keys on an exposed system, they were able to drain funds quickly. Exchanges that survived and grew after 2018 did so largely because they adopted multi-signature wallet requirements, hardware security modules for key management, and strict compartmentalization between their operational systems and their wallet infrastructure. The Lazarus fake app campaign pushed CISA to publish detailed advisories about AppleJeus variants, and the broader security community began treating North Korea as a persistent and sophisticated APT rather than an outlier nuisance. The Ronin Bridge hack in 2022 forced the entire DeFi sector to reckon with the security model of cross-chain bridges specifically, which had been chronically under-scrutinized. None of it stopped Lazarus, as of early 2025 they were still pulling off billion-dollar heists, but the industry is at least playing defense more seriously than it was in 2017.

Sources

Geoff White - The Lazarus Heist (book):

https://www.amazon.com/Lazarus-Heist-Hollywood-Finance-Inside/dp/B09V8J17MJ?crid=3RX05V7K3FDR8&dib=eyJ2IjojMSJ9.2urCIyoFTIs0EC7ftaTYQXOUo9TicpKIuhspkCTtuoLLn2S0MF542R4zyS8h8DA46Du6rcM3XEtamdTSQBawL4GUK_z2xXmYcqyWPpbA0HfwKJjqPPAMq-N6AvV9d8NGKOUJI20iyotLPfSz5C6qfQwIYAaDA50oVZyvbFVJx3saDmAlivPia_EGy_MKle4c78RFpPfZFPLuY0i4-bf4E8ScaqpQdk2YuFKIhbgJD84.M-FJUb-AhzMIUGWrNG7mtpDxO72uYNbsqO-xfFOFFR4&dib_tag=se&keywords=the+lazarus+heist&qid=1781796280&sprefix=the+lazurus+he%2Caps%2C485&sr=8-1

Darknet Diaries Ep. 119 - Hot Wallets: <https://darknetdiaries.com/episode/119/>

DOJ Press Release - Three North Korean Hackers Indicted (Feb 2021):

<https://www.justice.gov/archives/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-sceme-commit-cyberattacks-and>

The Hacker News - US Charges 3 North Korean Hackers:

<https://thehackernews.com/2021/02/us-charges-3-north-korean-hackers-over.html>

BleepingComputer - US Indicts North Korean Hackers for Stealing \$1.3 Billion:

<https://www.bleepingcomputer.com/news/security/us-indicts-north-korean-hackers-for-stealing-13-billion/>

Hacken - Inside Lazarus Group: <https://hacken.io/discover/lazarus-group/>

Gizmodo - US Charges Members of North Korean Hacker Group:

<https://gizmodo.com/u-s-charges-members-of-north-korean-hacker-group-of-al-1846288099>

Cybernews - The Largest Ever Crypto Hack (Bybit 2025):

<https://cybernews.com/cybercrime/bybit-hack-lazarus-group/>

Full disclosure: I used Claude to help me locate sources to go over, I read the articles, I listened and re-listened to "Darknet Diaries" podcast while doing this write-up, as he was an inspiration, as well as Geoff's book. I used Claude to go over my write-up for grammar errors, punctuation (im really bad about using apostrophes), and cleaning up the overall writing but keeping my writing style instead of changing it so much i couldn't recognize it. I also told it to point out if i made errors in reporting in my write up. It made my title because i am horrible with that. ChatGPT was used for the Images.

DramaKing - June 26, 2026, 10:59 am

Didn't know that WannaCry was a Lazarus Group operation or that one of the most damaging worms in history cost so little. But have you seen this?

[Video: <https://youtu.be/NlcP-yeq2dg?is=R3n-yirAghNDou6m>]

CL1B - June 26, 2026, 11:25 am

Great write on this, thank you!

Pr0m3th3us - June 26, 2026, 12:45 pm

(Jun 26, 2026 10:59 AM)DramaKing Wrote: [\[CITE\]](#) Didn't know that WannaCry was a Lazarus Group operation or that one of the most damaging worms in history cost so little. But have you seen this?

[Video: <https://youtu.be/NlcP-yeq2dg?is=R3n-yirAghNDou6m>]

Yea they didn't make much money off of it but it cost the companies a lot that's for sure. I will check out the vid.

(Jun 26, 2026 11:25 AM)MarlboroMan Wrote: [\[CITE\]](#) Great write on this, thank you!

Thanks. Writing was my best class in school, I always wanted to be an independent journalist,

travel around to war zones and shit like that. I use to write essays for other kids, we had a whole group, one dude did math, another would forge signatures for grade sheets and parent notes lol.

Raijin - June 26, 2026, 2:17 pm

Thanks for sharing this information. Interesting.

CL1B - June 27, 2026, 1:29 am

You should pursue it, full gas.