CYBER
THREAT
ANALYSIS
NORTH KOREA

Recorded Future®

By Insikt Group®

November 30, 2023

Crypto Country: North Korea's Targeting of Cryptocurrency

Executive Summary

Since 2017, North Korea has greatly expanded its targeting of the cryptocurrency industry, stealing over an estimated $3 billion worth of cryptocurrency. Prior to this, the regime saw previous success in stealing from financial institutions by hijacking the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network. However, this activity brought heavy attention from international authorities, and financial institutions responded by investing in improving their cyber defenses. During the cryptocurrency bubble of 2017, when the technology reached the mainstream, North Korean cyber operators shifted their targeting from traditional finance to this new digital financial technology by first targeting the South Korean cryptocurrency market before significantly expanding their reach globally. North Korean threat actors were accused of stealing an estimated $1.7 billion worth of cryptocurrency in 2022 alone, a sum equivalent to approximately 5% of North Korea's economy or 45% of its military budget. This amount is also almost 10 times more than the value of North Korea's exports in 2021, which sat at $182 million, according to the Observatory of Economic Complexity (OEC).

North Korean threat actors' operations targeting the cryptocurrency industry and how they launder the stolen cryptocurrency often mirror traditional cybercriminal groups that use cryptocurrency mixers, cross-chain swaps, and fiat conversions. However, state support allows North Korean threat actors to expand the scale and scope of their operations to a level not possible by traditional cybercriminal groups, with approximately 44% of stolen cryptocurrency in 2022 traced to North Korean threat actors. Targeting is not limited to cryptocurrency exchanges, with individual users, venture capital firms, and alternative technologies and protocols all having been targeted by North Korean threat actors. All of this activity puts anyone operating in the industry at risk of becoming a potential target of North Korean threat actors and allows the regime to continue operating and funding itself while under international sanctions.

Anyone operating in the cryptocurrency industry — individual users, exchange operators, and financiers with a portfolio of startups — should be aware of the potential to be targeted by North Korean threat actors. Entities operating in the traditional finance space should also be on the lookout for North Korean threat group activities. Once cryptocurrency is stolen and converted into fiat currency, North Korean threat actors funnel the funds between different accounts to obscure the source. Oftentimes stolen identities, along with altered photos, are used to bypass anti-money-laundering and know-your-customer (AML/KYC) verification. Anyone who is a victim of an intrusion linked to a North Korean threat group may have their personally identifiable information (PII) used to set up accounts to facilitate the laundering of stolen cryptocurrency. As a result, companies operating beyond the cryptocurrency and traditional finance industries should also be on the lookout for North Korean threat group activity and for their data or infrastructure being used as a launch pad for further intrusions. Since most intrusions by North Korean threat groups start with social engineering and a phishing campaign, organizations should train employees to monitor for this activity and implement strong multi-factor authentication such as FIDO2-compliant passwordless authentication.

The regime has clearly identified the continued theft of cryptocurrency as a major source of revenue, especially for funding its military and weapons programs. While it is unclear exactly how much of the stolen cryptocurrency ends up directly financing ballistic missile launches, it is clear that both the amount of cryptocurrency being stolen and the amount of missile launches have dramatically increased in recent years. Absent stronger regulations, cybersecurity requirements, and investments in cybersecurity for cryptocurrency firms, North Korea will almost certainly continue to target the cryptocurrency industry as a source of additional revenue to support the regime.

Key Findings

- There has been a steady increase in the number of cyberattacks against the cryptocurrency industry attributed to North Korean threat actors since at least 2017.
- Even though movement in and out of and within the country is heavily restricted, and its general population is isolated from the rest of the world, the regime's ruling elite and its highly trained cadre of computer science professionals have privileged access to new technologies and information.
- The privileged access to resources, technologies, information, and sometimes international travel for a small set of selected individuals with promise in mathematics and computer science equips them with the necessary skills for conducting cyberattacks against the cryptocurrency industry.
- In 2017, North Korean threat actors were highly active in targeting the South Korean cryptocurrency industry during the cryptocurrency bubble before greatly expanding their targeting to the international cryptocurrency market.
- North Korea has developed an extensive money-laundering network to facilitate the movement of billions of dollars worth of stolen cryptocurrency from when it's stolen to when it's converted to fiat currency or used to purchase goods and services for the regime.
- North Korean threat actors' cybercrime operations and money laundering mirror those of other traditional cybercriminal groups; however, state backing allows North Korean threat actors to scale their operations beyond what is possible for traditional cybercriminals.
- North Korea has stolen over an estimated $3 billion worth of cryptocurrency, with $1.7 billion stolen in 2022 alone, possibly funding up to 50% of its ballistic missile program.

Background

North Korea has been called the "Hermit Kingdom" for its isolation from the rest of the world. The regime's strict control of society, including the movement of goods, people, and, most importantly, information, means that very little information gets in or out. But even though the general population is heavily isolated from the outside world, leadership in Pyongyang is acutely aware of new technologies and actively exploits new technologies to fund its regime. In recent years, Pyongyang has found great success in stealing from both traditional fiat currency-based banks and digital assets such as cryptocurrency. This begs the question: despite being such a closed society, how has the regime been so successful in its cyber operations as well as its intrusions?

On July 12, 2023, American enterprise software company JumpCloud announced that a North Korean state-sponsored threat actor had gained access to its network. Researchers at Mandiant later published a report stating the group responsible was UNC4899, which "likely corresponds to TraderTraitor", a North Korean cryptocurrency-focused threat actor. As recently as August 22, 2023, the United States (US) Federal Bureau of Investigation (FBI) issued a notice that North Korean actors were behind the heists affecting Atomic Wallet, Alphapo, and CoinsPaid, totaling $197 million in stolen cryptocurrency. The theft of cryptocurrency has allowed the regime to continue operating under strict international sanctions, funding up to 50% of its ballistic missile program. By 2018, some estimates assessed that North Korea was responsible for half the total amount of stolen cryptocurrency. While in recent years, most of the attention has been on the large cryptocurrency heists the regime has continuously pulled off, North Korea has a long history of using illicit activities to fund itself.

In our previous 2017 report, we highlighted the regime's previous forays into criminality that go back decades. North Korea has been involved in smuggling since at least the 1970s and a recent report by the Financial Times showed that through the help of organized crime groups in East Asia, the regime continues to engage in smuggling activities today. As recently as 2019, Chinese authorities have caught North Korean officials smuggling methamphetamine across the border. The regime has also been identified participating in the manufacture and distribution of illicit drugs, as well as counterfeiting American $100 bills. It was estimated in 2016 that illicit economic activities generate $550 million to $1 billion annually for the country.

North Korea also recognized the asymmetric advantages of cyber when the internet was still in its nascent stage. While the regime initially deployed its cyber operators to conduct disruptive cyberattacks against its traditional adversary, South Korea, the country's leadership quickly learned that cyber could also be used as a means to generate more illicit revenue. Initially, North Korean cyber operators focused on stealing personal information from websites and creating tools to steal cash from online games and then selling them to other criminal actors in the underground economy. The estimated amount of illicit revenue earned per North Korean operator in 2013 was approximately $500 per month. More recently, in October 2023, the FBI said that overseas North Korean IT workers had sent millions of dollars in wages back to North Korea for years.

It was not long afterward that the regime realized that it could generate more illicit revenue from targeting financial institutions instead of keeping its cyber operators on the fringes of internet cybercrime. From 2015 onward, North Korea likely targeted financial institutions in at least 38 countries. The most well-known heist, the cyberattack on Bangladesh Bank, resulted in $101 million in fraudulent transfers via the SWIFT protocol, $35 million of which was recovered. North Korean cyber operators also participate in ATM cash-out schemes, compromising payment switch application servers to approve fraudulent transactions at banks in Asia and Africa. While the full extent of the regime's activities is unknown, some estimates put the amount of stolen funds in the tens of millions from banks in over 30 countries.

In order for North Korea to steal and launder millions of dollars, it requires a large number of well-trained cyber operators committed to the regime's objectives. On September 6, 2018, the US Department of Justice (DOJ) unsealed a criminal complaint against one such individual, Park Jin Hyok (박진혁). Park graduated from a prestigious North Korean university, Kim Chaek University of Technology (김책공업종합대학), and reportedly is proficient in multiple programming languages. Based on evidence in the complaint, it is estimated that Park was dispatched to Dalian, China, in late 2010 to work for Chosun Expo, a front company for the North Korean government, and returned to North Korea sometime in late 2013 or early 2014.

In addition to Park, the US DOJ also sentenced a US researcher to 5 years in prison for conspiring to help North Korea evade US sanctions and indicted 2 other North Korean cyber operators, Jon Chang Hyok (전창혁) and Kim Il (김일), in 2021. Kim previously lived in Singapore; North Korea has a diplomatic mission in the city-state, and Kim contacted individuals there when he took part in a cryptocurrency scheme to sell shares in Marine Chain, a blockchain-enabled platform for vessel transactions. While many North Korean cyber operators work from inside North Korea, the regime also sends some abroad to work, both in semi-legitimate IT consulting work and in conducting cybercrime from other countries. The 2 indictments also show that while these North Korean individuals were heavily involved in numerous schemes to earn money for the regime, from SWIFT hijacking to ATM cash-out schemes from 2015 to 2019, North Korean operators have increasingly focused on earning money through the extensive cryptocurrency system that has grown in recent years.

As mentioned above, the regime's cyber operators attempted to steal money from financial institutions around the world, with a high amount of activity between 2015 and 2019. Despite their success, these efforts brought a lot of attention to North Korea's activities and the scrutiny of government agencies and international organizations that were determined to stop them. Moreover, the financial institutions that the North Korean cyber operators were trying to steal from are some of the most well-defended private organizations in the world — for example, Bank of America announced its cybersecurity budget would increase to $1 billion a year in 2021. All of this took place as the lightly regulated cryptocurrency industry continued to grow in size, increasing from an estimated $1.09 billion in worldwide revenue in 2017 to a projected $37.87 billion in revenue in 2023. Many cryptocurrency companies are venture-backed startups with small staffs, and while it is unknown how many cybersecurity professionals are working in these small businesses, a recent survey reported that only 8% of small businesses with fewer than 50 employees had a cybersecurity budget. The North Korean regime seems to have found a rapidly growing financial technology industry that has little oversight and is unprepared for a relentless cyber assault.

Threat Analysis

A History of Cryptocurrency Targeting

While North Korean threat actors targeted cryptocurrency users and exchanges prior to 2017, we see the first uptick in reported activity (1, 2) against exchanges in South Korea in that year. North Korean cyber operators compromised the South Korean exchanges Bithumb, Youbit, and Yapizon in 2017, stealing cryptocurrency that was worth approximately $82.7 million at the time. There were also reports of cryptocurrency users being targeted after a breach of customer PII of Bithumb users in July 2017.

In addition to stealing cryptocurrency, North Korean threat actors learned how to mine it as well. In April 2017, researchers at Kaspersky Labs identified Monero cryptocurrency mining software that was installed in an APT38 intrusion, and in January 2018, researchers at the South Korea Financial Security Institute announced that the North Korean group Andariel compromised the server of an unnamed company in the summer of 2017 and used it to mine approximately 70 Monero coins worth about $25,000 at the time.

The cryptocurrency-related intrusions continued at an increasing pace. In 2017, North Korean threat actors conducted spearphishing attacks against the cryptocurrency industry (1, 2, 3), targeting executives and other employees at cryptocurrency exchanges by spoofing other businesses in the industry and pretending to be job applicants. Throughout 2018 and 2019, North Korean threat actors continued to target cryptocurrency companies and users with spearphishing emails containing cryptocurrency themes and trojanized cryptocurrency trading applications, duping users into downloading the apps before stealing their cryptocurrency. This type of attack, which is called a "permit phishing attack", is when an attacker sends over a malicious script or smart contract for the victim to receive tokens or approve a transaction. Once the permit is authorized or agreed to, the attacker can drain the victim's assets. With the increased use of MacOS operating systems, especially among tech start-ups, North Korean threat actors included MacOS malware in these campaigns to target even more cryptocurrency users.

In 2020, security researchers continued to report on new cyberattacks attributed to North Korean threat actors targeting the cryptocurrency industry. The North Korean threat group APT38 targeted cryptocurrency exchanges in the US, Europe, Japan, Russia, and Israel, using Linkedin as a method to initially contact targets (1, 2). The group also sent innocuous emails to potential targets, possibly to prescreen which individuals were more likely to open emails, before sending spearphishing emails with malicious payloads. Of note, in at least one instance, the malware performed a check for antivirus products, and in the case of Qihoo360 Total Security, an antivirus company based in China, it deleted itself and took no further action, indicating that the author of the malware did not want to infect a system with Qihoo360. While the reason for this is unclear, it is possible that, at the time, North Korea did not want to target cryptocurrency firms that were more inclined to use an antivirus software produced by a company in China.

2021 was also a prolific year for North Korea's targeting of the cryptocurrency industry, with North Korean threat actors breaching at least 7 cryptocurrency organizations and stealing $400 million worth of cryptocurrency. Additionally, North Korean threat actors started targeting alternative coins (altcoins), including Ethereum Request for Comment (ERC-20)-based tokens, as well as non-fungible tokens (NFTs). ERC-20 is a standard set of basic guidelines that govern the Ethereum (ETH) blockchain, including coins, smart contracts, and NFTs. ETH, Polygon (MATIC), Shiba Inu (SHIB), ApeCoin (APE), and Wrapped Bitcoin (WBTC) are just some examples of ERC-20-based tokens. APT38 continued its assault on the industry, abusing the brands of fintech, venture capital firms, and other cryptocurrency companies in spearphishing campaigns. The group targeted individuals and companies in the cryptocurrency industry in Russia, Poland, Slovenia, Ukraine, the Czech Republic, China, India, the US, Hong Kong, Singapore, the United Arab Emirates (UAE), and Vietnam. However, despite their large amount of success in stealing cryptocurrency, North Korean threat actors were not in a rush to cash out. In January 2022, researchers at Chainalysis identified $170 million in cryptocurrency that still needed to be cashed out from breaches dating back to 2017.

The pace of reports on North Korean threat activity targeting the cryptocurrency vertical continued to increase in 2022, with threat actors using phishing emails containing links to fake cryptocurrency job descriptions as lure documents. Notable attacks in 2022 attributed to APT38 include the Ronin Network cross-chain bridge ($600 million in losses), the Harmony blockchain bridge ($100 million in losses), the Qubit Finance bridge ($80 million in losses), and the Nomad bridge ($190 million in losses). These 4 attacks specifically targeted the cross-chain bridges of these platforms. Cross-chain bridges connect 2 blockchains, which allows users to send 1 type of cryptocurrency from 1 blockchain to another blockchain that contains a different cryptocurrency. Most bridges work by using validators similar to miners, where transactions on the blockchain are entered into a smart contract and then validated. Private keys are needed to use a validator to sign a transaction. Once they are validated, the funds are then sent and transferred to the end target cryptocurrency. During these attacks, North Korean threat actors targeted the validator keys of these organizations.

The geographic breakdown of North Korean threat groups' targeting in the cryptocurrency industry is similar to our previous reporting, where Kimsuky has been seen targeting the cryptocurrency industry in South Korea, and Lazarus Group has a more global presence in their cryptocurrency targeting operations. In 2022, Lazarus used strategic web compromise as an initial access vector when targeting individuals in the cryptocurrency vertical, something not as commonly seen in North Korean cyberattacks against targets in the industry. North Korean threat actors also experimented with trojanized DeFi applications that will manage a user's wallet but will also install a backdoor on their host machine.

In October 2022, the Japanese National Police Agency announced that Lazarus Group had targeted companies operating in the cryptocurrency industry in Japan. While specific details were not given, the announcement stated that some companies were successfully compromised and had cryptocurrency stolen. In the same month, North Korean threat actors created a fake cryptocurrency application for Android phones that was designed to steal money, and toward the end of 2022, security researchers at

SlowMist reported on a new phishing campaign targeting NFT users attributed to North Korean threat actors using fake NFT websites, including a fake DeFi platform run by the North Korean threat actors.

While theft amounts are down from August 2022, 2023 has so far been a profitable year for North Korean threat actor groups. Between January and August 2023, APT38 allegedly stole $200 million from Atomic Wallet ($100 million in losses), AlphaPo ($60 million in losses across 2 attacks), and CoinsPaid ($37 million in losses). Also in January, the US FBI confirmed that APT38 was behind the $100 million theft of virtual currency from Harmony's Horizon bridge. In the July 2023 CoinsPaid attack, APT38 operators likely posed as recruiters and specifically targeted employees of CoinsPaid, sending recruiting emails and LinkedIn messages to notable CoinsPaid engineers. CoinsPaid said it believed that APT38 spent 6 months attempting to gain access to its network.

On July 20, 2023, CrowdStrike assessed that the Lazarus Group accessed systems of the US-based enterprise software company JumpCloud in order to target the company's cryptocurrency clients and steal cryptocurrency funds. JumpCloud is a directory-as-a-service company that aims to provide a replacement for Active Directory (AD) and offers features such as password and device management. On the same day, SentinelOne also reported that JumpCloud was targeted by a North Korean state-sponsored APT. The incident was initially discovered on June 27, 2023, and although initially no evidence was found to suggest customers were affected, on July 5, 2023, unusual activity was detected in the commands framework for a small group of customers during a follow-up investigation. JumpCloud disclosed that the attack was highly targeted and affected specific customers. Details regarding the number of affected customers have not been released; however, many were reportedly in the cryptocurrency vertical.

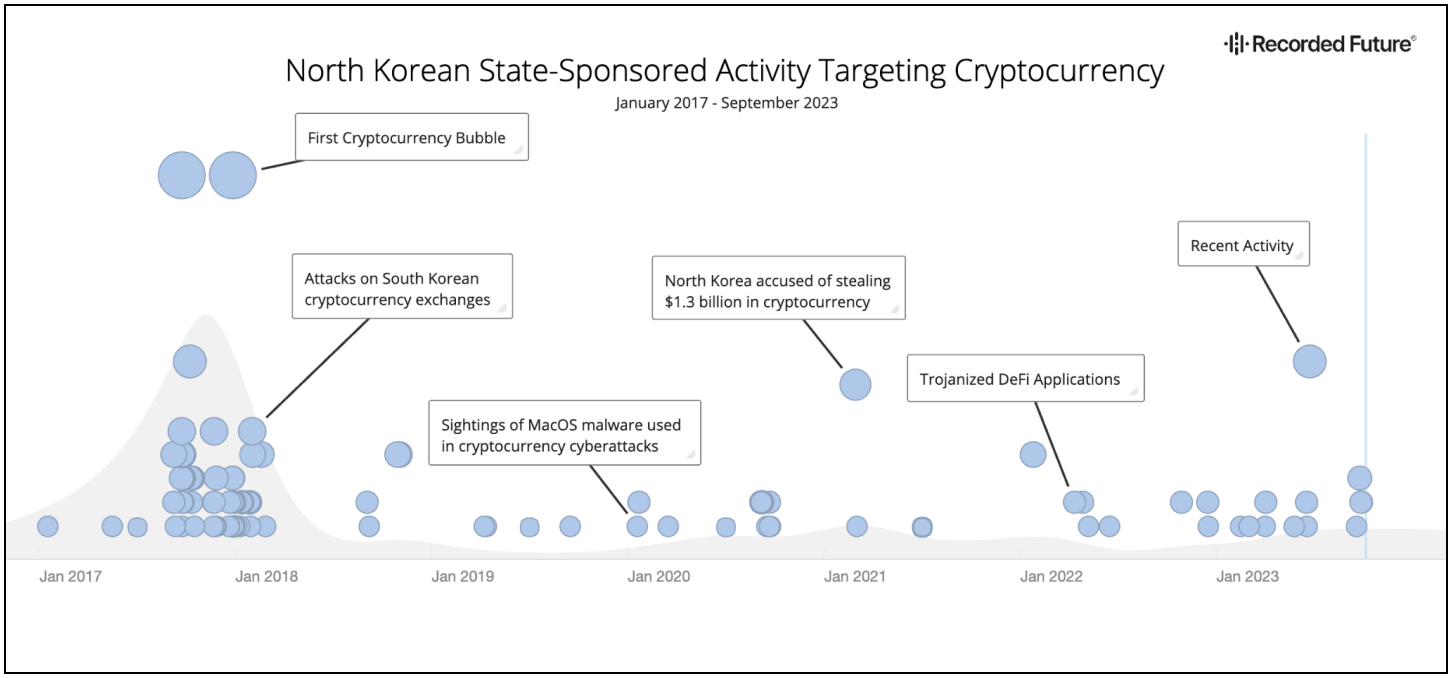

Figure 1: *North Korean state-sponsored activity targeting the cryptocurrency industry (Source: Recorded Future Intelligence Cloud)*

Moving the Stolen Assets

As previously mentioned, North Korea has an extensive history of conducting illicit smuggling and other criminal activities that naturally caused the country to build up asset-laundering networks and methods. In 2020, leaked documents from the US Financial Crimes Enforcement Network show individuals openly laundering tens of millions of dollars through the US financial system, routing money through China, Singapore, Cambodia, and elsewhere to support the North Korean regime. Often these individuals work for North Korea's primary intelligence organization, the Reconnaissance General Bureau (RGB), as in the case of a North Korean intelligence officer who was extradited and sentenced in the US for setting up front companies and laundering money for the regime.

While there are few details regarding most of these money-laundering operations and the effort to track them is complex and time-consuming for authorities, there is 1 instance where many of the details were made public. In the 2016 Bangladesh Bank theft, the North Korean cyber operators sent the stolen money to 4 bank accounts in the Philippines and then converted $61 million USD into Philippine pesos for use at the Solaire Resort, a casino in the Philippines. In 2017, the US State Department identified the Philippines as a major money-laundering location. The stolen money was used to gamble at the casino, and any winnings would have been untraceable. The two individuals responsible for most of the gambling, only known as Ding and Gao, boarded charter flights to Macau after the operation was complete. Macau has a history of North Korean operations, including being the location where the North Korean spy responsible for the 1987 Korean Air flight bombing trained, a hub for laundering counterfeit $100 notes in the early 2000s, and where Kim Jong Un's older half-brother lived in exile before he was assassinated in Malaysia in 2017.

North Korea must also launder, clean, and anonymize stolen cryptocurrency. In 2022, 2 popular cryptocurrency mixers — Blender[.]io (1) and Tornado[.]cash (1) — were identified as being used by North Korean threat actors to launder stolen cryptocurrency. It is suspected that North Korean threat actors used Blender[.]io to launder over $25 million worth of stolen funds from the Ronin Network as well as using Tornado[.]cash to launder just over $553 million stolen during the Ronin Network, Harmony Bridge, and Nomad attacks. In August 2023, the founders of Tornado Cash were charged with over $1 billion worth of cryptocurrency laundering for North Korea. In March 2020, the US DOJ charged 2 Chinese nationals with laundering over $100 million in cryptocurrency that was stolen by North Korean threat actors in 2018. The North Koreans first attempted to obscure the flow of the stolen cryptocurrency by mixing it before using some of it to purchase online infrastructure used in further cyberattacks against the financial industry. They employed 2 Chinese nationals who would convert the cryptocurrency into fiat currency for a fee at two unnamed cryptocurrency exchanges. Afterward, the money was deposited into a bank account at China Guangfa Bank. One of the individuals would also sell cryptocurrency in exchange for iTunes gift cards, a commonly known form of money laundering.

North Korean threat actors also use the accounts and personal information of phishing victims to register verified accounts at trusted cryptocurrency exchanges where they can send the stolen cryptocurrency and cash out, as was the case where approximately $40 million in BTC was stolen from

an unnamed exchange and transferred to an account at an exchange in South Korea registered with stolen personal information. Obtaining these verified accounts, which often provide valid information for KYC and AML requirements, is often a crucial step during this process as funds coming from these verified exchanges, banks, and finance applications are viewed as less suspicious and raise fewer red flags to law enforcement and fraud teams. To circumvent KYC regulations, North Korean threat actors use stolen personal IDs with altered photos of individuals, which are submitted to the exchanges when registering. After the accounts are registered, the threat actors use a peel chain, where a small amount of cryptocurrency is deposited at a time into the cashout account from hundreds or thousands of addresses, which is less likely to draw scrutiny than a one-time large transaction. The peel chains are conducted in an automated fashion, where a computer script is used to rapidly send the cryptocurrency to the desired address.

On May 28, 2020, the US DOJ unsealed an indictment charging 28 North Koreans and 5 Chinese citizens with laundering more than $2.5 billion in assets to help fund North Korea's nuclear weapons program. Many of the individuals in the indictment were employees of the Foreign Trade Bank (FTB) of North Korea, which operated covert branches in Beijing, Shenyang, and Zhuhai, China, including multiple front companies used to purchase goods and launder money. Additional covert branches of the bank were identified in Austria, Libya, Kuwait, Thailand, and Russia. In addition to laundering money on behalf of the North Korean regime, these individuals were sent abroad to "study fast developing financial technologies and experiences of other countries". As seen in Recorded Future's previous research, North Korea has a long history of sending promising, loyal individuals abroad to gain exposure and skills not easily accessible from within the country. In total, over 250 front companies were created by the individuals listed in the indictment, often creating new front companies after their old ones were discovered to have links to the North Korean regime.

North Korean individuals also conspire with cryptocurrency traders to conceal the laundering of stolen cryptocurrency. In April 2023, the US DOJ unsealed 2 indictments charging a North Korean FTB representative for conspiring with a Chinese national and a Hong Kong British National to launder stolen cryptocurrency and to purchase goods through front companies based in Hong Kong. Some of this stolen cryptocurrency was traced back to APT38 cyberattacks, and the FTB representative used the stolen currency to purchase goods for the regime through the Hong Kong front companies. The FTB representative also conspired to launder funds earned through North Korean IT workers who illegally worked in the tech and cryptocurrency industries, often obscuring their true identities through fake personas and asking to be paid in cryptocurrency for their work.

Comparison to Traditional Cybercrime

North Korea, like any state, conducts cyber-espionage operations to gain information from adversary governments to support national security objectives or further national interests. The country also conducts economic cyber espionage to help develop its own domestic industry, something most countries partake in as they develop their economies (1, 2). North Korea differs from almost any other country, however, because it is a state that devotes much of its education and intelligence resources to running criminal operations with the goal of earning money for the regime. The level of activity and how

the state launders its stolen proceeds is discussed above, but how does this activity compare to more traditional financially motivated cybercriminal groups that are not employed by a state?

North Korean state-sponsored cyber operators, like other cybercriminals, are often engaged in the same kinds of activities when stealing cryptocurrency. This includes phishing, credential harvesting, airdrop scams, and rug pulls. Phishing remains one of the most prevalent tactics used by scammers and cybercriminals to steal funds and sensitive information from victims. Cryptocurrency users have become heavily targeted by phishing campaigns, which have used various known and novel techniques to achieve their objectives. Known techniques include typosquatting and impersonating major cryptocurrency platforms and projects; more novel techniques include targeting users of Discord, a popular chatting platform used by the gaming and tech communities, including cryptocurrency users. North Korean threat actors also employ phishing campaigns that attempt to steal credentials for cryptocurrency accounts and wallets. While there is little evidence of how active North Korean cyber operators are on more novel communities such as Discord, we see them active in chat platforms in South Korea, such as KakaoTalk.

Traditional cybercriminals also conduct giveaway scams (also known as airdrops within the cryptocurrency ecosystem) impersonating reputable organizations or individuals to persuade victims to either provide personally identifiable information, click on phishing links, or directly give or be awarded a cryptocurrency token or other asset. Airdrops are distributions of cryptocurrency or NFTs sent to users for free. Giveaway scams are often combined with known social engineering techniques observed in cybercriminal campaigns, such as typosquatting domains imitating cryptocurrency exchanges. Numbers suggest that giveaway scams are skyrocketing, with cybersecurity company Group-IB witnessing an aggressive 335% increase in domain registrations tied to giveaway scams in the first half of 2022 compared to the entirety of giveaway scam domains observed in 2021. North Korean threat actors also engage in such scams, as seen in 2022 Kimsuky activity in South Korea spoofing an NFT compensation for victims of a previous cryptocurrency scam. The group set up a credential-harvesting website to steal victim accounts.

Another popular scam in the cryptocurrency industry is rug pulls, in which scammers advertise a promising-sounding cryptocurrency project to raise funds before either selling all tokens (similar to pump-and-dump schemes in traditional finance), blocking sell orders, or stealing funds from users using flawed blockchain contracts. All three actions typically lead to a crash in the asset's price while scammers take in a significant profit and disappear from the public eye. These events typically lead to heavy financial losses for investors, who either lose their tokens completely or see the value of existing tokens drop to near zero. According to Privacy Affairs, scammers and crypto developers conducted more than 188,000 rug pulls in 2022. In 2021, rug pulls accounted for 35.9% of cryptocurrency losses in scams ($2.8 billion out of $7.8 billion), according to blockchain analysis firm Chainalysis. Previous Recorded Future research identified a North Korea-linked cryptocurrency platform, Marine Chain, which was supposedly an asset-backed cryptocurrency that enabled the tokenization of maritime vessels for multiple users and owners. It is unclear how many individuals were duped into investing funds in the scam.

Money Laundering

After cryptocurrency is stolen — whether by North Korean threat actors supporting the regime's nuclear program or low-tier cybercriminals looking to make a small profit — it needs to be laundered. Both groups need to obscure the source of their stolen currency through a series of steps we've previously identified in Insikt Group's report on The Business of Fraud. First, the illegally acquired currency enters the financial system and is disguised in a process called "placement". Next, the funds are "layered" using methods like converting cash or wiring money between accounts to make the activity harder to trace for law enforcement. Finally, in the "integration" phase, the funds are reintroduced as legitimate currency through methods that make them appear as normal activity.

North Korean threat actors, just like non-state-backed cybercriminals, use cryptocurrency mixers to obscure the flow of their illegally acquired cryptocurrency from law enforcement. Threat actors in the cybercriminal underground have also relied on exchanging stolen funds via legitimate crypto trading platforms to swap them for "clean" cryptocurrency, which clients of an illicit service would then use to withdraw the funds from any exchange. Insikt Group observed entry-level "cleaning" tutorials on English forums such as Nulled Forum in 2021. Money mules are also used by both cybercriminals and North Korean threat actors, with mules likely to continue to be used, knowingly or unknowingly, to launder money for various criminal operations.

While both North Korean threat actors and cybercriminals conduct the same types of cybercrime and use similar methods to clean and cash out their funds, the difference between the two groups appears to be the scale of operations. According to a Chainalysis report, in 2022, $3.8 billion worth of cryptocurrency was stolen, with North Korean threat actors stealing an estimated $1.7 billion of it. Traditional cybercriminal organizations don't have the resources to support and scale their operations that North Korean state-sponsored threat actors do, and North Korea can use diplomatic cover to conduct cybercrime, smuggling, and other illicit activities. Additionally, as seen in the background section and our previous report on North Korea's cyber strategy, the regime has a long history of illicit activity, building up its networks over decades, and it steers its whole society to support these operations, grooming promising youth for future careers conducting cybercriminal operations. Its status as a state allows the regime to scale cybercriminal and other Illicit operations to a level other cybercriminal groups can only dream of.

Mitigations

As many North Korean cyberattacks targeting cryptocurrency users and firms start with phishing, Insikt Group suggests the following:

- Enable MFA for software wallets and transactions with a hardware device such as YubiKey.
- Enable any available MFA settings for cryptocurrency exchanges to best protect accounts from unauthorized logins or thefts.
- Validate verified social media accounts and check username handles for special characters or number substitutions for letters.
- Ensure requested transactions are legitimate and validate any airdrops or other free cryptocurrency or NFT promotions.
- Double-check the official source when someone sends an airdrop or anything else pretending to be Uniswap or any other big cryptocurrency platform.
- Always check URLs and watch redirects after clicking on a link to make sure that the websites are official websites rather than phishing sites.

Below are general tips for defending against other cryptocurrency social engineering scams:

- Exercise the utmost caution when conducting cryptocurrency transactions. Cryptocurrency assets are not protected by any of the institutional safeguards that mitigate “traditional” fraud.
- Use hardware wallets. Hardware wallets can be much more secure than “hot wallets” like MetaMask, which are always connected to the internet. For hard wallets that are connected to MetaMask, all transactions must be approved via the hard wallet, which provides an additional security layer.
- Only use trustworthy dApps (Decentralized Applications) and verify smart contract addresses to confirm their authenticity and integrity. True NFT-minting interactions rely on smart contracts that may be part of a larger dApp. Contract addresses can be verified using MetaMask, block explorers like Etherscan, or sometimes directly within the dApp.
- Double-check the web addresses of official websites to avoid imitations. Some cryptocurrency drainer phishing pages may rely on typosquatting to victimize unsuspecting users.
- Question offers that are too good to be true. Cryptocurrency-drainer phishing pages attract victims with advantageous cryptocurrency exchange rates or cheap gas fees for NFT-minting interactions.
- Resist pressure tactics. Scams often induce a sense of urgency to pressure victims into impulse actions, and cryptocurrency-drainer phishing scams are no exception.

Additional mitigations to prevent cryptocurrency losses from thefts, scams, and other malicious activities include:

- Transfer existing cryptocurrency investments into stablecoins that are backed by governments or pegged to a fiat currency to insulate them from market fluctuations.

- If cashing out cryptocurrency or other digital assets, only utilize well-known exchanges that implement verification and KYC policies. Conduct research on cryptocurrency exchanges or withdrawal services.
- Do not use OTC exchanges or unvetted mixers/tumbling services.
- Consider moving coins, NFTs, and other assets to hardware wallets, as exploits and scams targeting software wallets will likely increase as users begin to sell off these assets.
- Monitor both software and hardware wallet balances to ensure the balance remains intact.
- Remember seed phrases and ensure they are written down on a physical medium. If they are held on a digital medium, ensure that it is encrypted and stored in a secure manner.
- Be alert and aware of a possible increase in phishing scams and attempts during this downturn as users and investors attempt to withdraw coins and assets.
- Enable 2FA on software wallets on cryptocurrency wallets and change seed phrases every few weeks if possible to help mitigate the impact of a seed phrase cracker.
- Attempt to verify any links posted within the official Discord or other P2P communication platforms used by NFT creators and sponsors.
- If investing in a new coin or NFT, conduct research and invest small amounts over time to mitigate the impact of a rug pull.
- Refrain from downloading apps from untrusted sources, review app permission requests before approving root access, and regularly keep Android and iOS devices' operating systems, applications, and firmware updated. Furthermore, Europol recommends users perform a factory reset to wipe all data in the partitions that can host malware.
- Use anti-cryptomining extensions, such as the Google extensions minerBlock, NoMiner, and Anti-Miner, to block cryptominers across the web and use Ad-Blockers that can detect and block malicious cryptomining code. Furthermore, organizations should reduce the exposure of control devices to ensure they remain inaccessible from the internet.
- The Recorded Future® Intelligence Cloud can assist with the detection of compromised credential information linked to valid accounts to assist in providing context surrounding suspicious user behavior that may include keylogging activity. Recorded Future Intelligence Cloud users can continue to monitor underground sources to identify the spyware and keylogging tools that are likely to have the greatest impact on their immediate infrastructure or supply chain.

Outlook

North Korea has seen major success in its cybercriminal operations targeting the cryptocurrency industry, but how much of an impact has this had on the country? As previously stated, some estimate up to 50% of the country's ballistic missile program is funded through stolen cryptocurrency. North Korea's gross domestic product (GDP) in 2019 was estimated to be roughly $33.5 billion, and in 2023, according to the Bank of Korea, South Korea's national bank, North Korea's economy had shrunk for 3 straight years in a row. Using the 2019 estimate, the amount of cryptocurrency stolen by North Korean threat actors in 2022 equals approximately 5% of North Korea's economy. This does not include any other form of illicit activity or illegal employment of North Korean workers in the IT sector or otherwise. To put this in perspective, roughly 4.2% of US GDP is in the arts, entertainment, recreation, accommodation, and food services sectors. Looking at the amount of cryptocurrency stolen in 2022 as a percentage of North Korea's estimated military budget of $4 billion in 2021, the country could finance 45% of it with cryptocurrency.

While it is unclear exactly how much of the stolen cryptocurrency ends up directly financing ballistic missile development and tests, it is clear that both the amount of cryptocurrency being stolen and the amount of missile launches have dramatically increased in recent years. According to the Nuclear Threat Initiative, a US-based think tank that tracks the number of North Korean missile launches, the number of launches since 2015 has greatly increased, with a noticeable dip during the COVID-19 pandemic. However, 2022 saw the most North Korean missile launches in a year since the regime began, with almost 70 launches during the year. As there doesn't appear to be a slowdown in the number of cryptocurrency heists attributed to the North Korean regime, it is very likely that some of these funds will end up in the regime's nuclear and ballistic missile programs. Additionally, as seen above, given the amount of cryptocurrency being stolen in relation to the size of North Korea's military budget, the regime has identified a lucrative way to avoid international sanctions and to keep developing its nuclear and missile technology. Absent stronger regulations, cybersecurity requirements, and investments in cybersecurity for cryptocurrency firms, we assess that in the near term, North Korea will almost certainly continue to target the cryptocurrency industry due to its past success in mining it as a source of additional revenue to support the regime.

Regimes such as North Korea are likely to continue to target and attack entities, organizations, and elements of the cryptocurrency ecosystem. The Ronin Network attack, one of the single largest cryptocurrency thefts in 2022 ($600 million in losses), was allegedly conducted by a state-sponsored APT group. With the success of these attacks, in the future, these groups are likely to continue to improve their tradecraft for stealing, laundering, and monetizing cryptocurrency in both the short and long term. It is even possible other heavily sanctioned entities, such as Russia, will attempt to duplicate this success or try to recruit insiders who are working at cryptocurrency firms and exchanges, following in North Korea's footsteps.

Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com