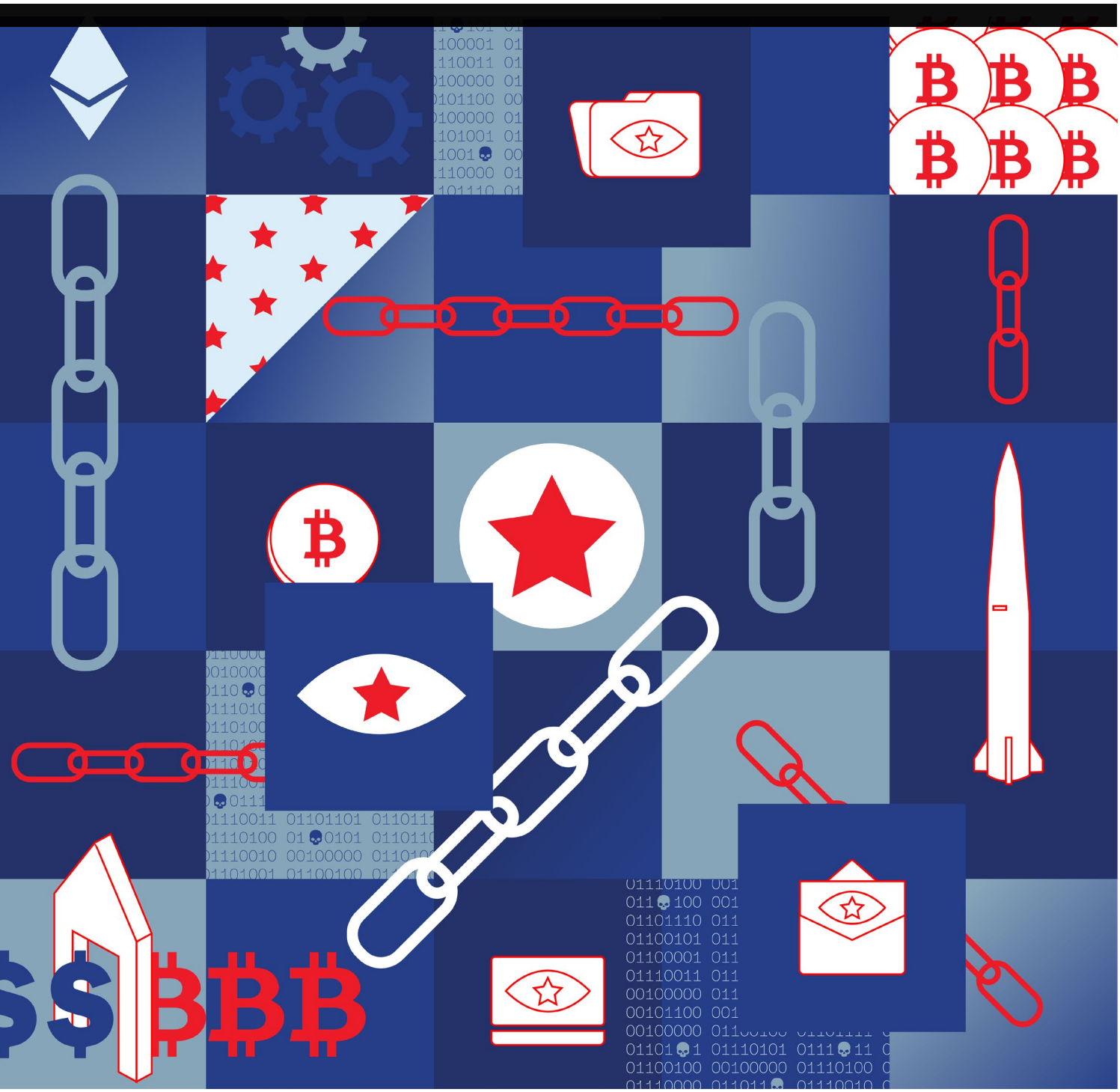
FEBRUARY 2022

Following the Crypto

Using Blockchain Analysis to Assess the Strengths and Vulnerabilities of North Korean Hackers

Jason Bartlett



CNAS

About the Author

Jason Bartlett is a Research Assistant for the Energy, Economics, and Security Program at the Center for a New American Security (CNAS). He analyzes developments and trends in U.S. sanctions policy and tactics to evade sanctions, counterproliferation finance, and cyber-enabled financial crime, with regional focus on North Korea, Venezuela, and Iran. He also leads research and writing for the program's Sanctions by the Numbers series and is a contributing author for The Diplomat. Previously Bartlett worked at several think tanks in Washington, D.C., and Seoul, South Korea, and he provided years of linguistic and administrative assistance to human rights groups resettling North Korean defectors in South Korea and the United States. Fluent in Korean and Spanish, Bartlett graduated from the Korean Language Institute (KLI) at Yonsei University in Seoul, and also holds an MA in Asian Studies from the School of Foreign Service and a graduate certificate in Refugee and Humanitarian Emergencies from Georgetown University, as well as a BS in Spanish and a BA in International Studies from SUNY Oneonta.

About the Energy, Economics, and Security Program

The Energy, Economics, and Security Program explores the changing global marketplace and implications for U.S. national security and foreign policy. In a highly interconnected global financial and trade system, leaders must increasingly leverage economic and financial assets to defend and promote U.S. national interests. The Energy, Economics, and Security Program develops practical strategies to help decisionmakers understand, anticipate, and respond to these developments.

Acknowledgments

The author would like to thank Yaya Fanusie, Nick Carlsen, and TRM Labs for their feedback, guidance, and invaluable blockchain analysis support. He is grateful as well to Emily Kilcrease, Aaron Arnold, Alex Zerden, and Laura Brent for their thoughtful reviews of this report; and he acknowledges the editorial and production efforts of the entire Publications and Communications Team at CNAS, in particular Maura McCarthy, Melody Cook, Emma Swislow, Rin Rothback, and Anna Pederson. Lastly, the author thanks Euihyun Bae for his citation support. This report was made possible with the generous support of the John D. and Catherine T. MacArthur Foundation.

TABLE OF CONTENTS

Executive Summary

Under heavy and sustained pressure from decades of economic sanctions, North Korea has rapidly expanded its illicit activity within the cyber domain. In particular, Pyongyang has demonstrated an increasing interest in using evolving financial platforms, such as cryptocurrency and blockchain technology, to compensate for the fiscal losses related to economic sanctions on more traditional forms of commercial activity. Since 2014, the Pyongyang-led cybercrime organization known as the Lazarus Group has transformed from a rogue team of hackers to a masterful army of cybercriminals and foreign affiliates, capable of compromising major national financial networks and stealing hundreds of millions of dollars' worth of virtual assets.

The international community and national governments often incorrectly correlate North Korea's lack of access to modern computer hardware within its borders to its ability to successfully execute software-reliant cyberattacks. While Beijing and Moscow captivate the attention of most democratic governments concerned about pending cyber intrusions, Pyongyang continues to defy miscalculated expectations by successfully employing myriad sophisticated cyberattacks that target new and developing financial technology. North Korea will likely continue to adapt its cybercrime tactics targeting cryptocurrency to circumvent obstacles presented by economic sanctions on more traditional forms of financial activity and commerce.

This report provides in-depth analysis of North Korea's demonstrated ability to exploit financial technologies, in particular cryptocurrencies and blockchain technology, to procure funds for its illicit nuclear and ballistic weapons development programs. This research was supported through blockchain analysis conducted in partnership with TRM Labs, a leading blockchain intelligence firm that seeks to monitor, investigate, and mitigate crypto fraud and financial crime.

Through analyzing three case studies of major North Korean hacks, this report outlines key strengths and vulnerabilities in the Lazarus Group's campaigns to infiltrate cryptocurrency exchanges and steal, launder, and liquidate funds. The report also provides a snapshot of key policy oversights within the regulatory environment in the crypto space of central stakeholders and countries, such as China, the United States, and South Korea. Lastly, this study offers a prospective look into the future of North Korea–led crypto hacks and provides a series of policy recommendations to strengthen cyber resilience against these efforts.

Summary of Recommendations

The following recommendations are proposed for U.S. domestic and foreign policymakers, as well as those in the private sector:

U.S. Domestic Policymakers

- Financial regulators and lawmakers should work to remove any loopholes that allow decentralized finance (DeFi) platforms and other emerging financial technology to circumvent U.S. regulations on anti–money laundering (AML) and combating the financing of terrorism (CFT).
- Congress should adopt legislation that requires all cryptocurrency exchanges to report cyber incidents to the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the FBI that could involve the financial and/or personal information of U.S. citizens and/or entities.
- Within the new National Cryptocurrency Enforcement Team, the executive branch should designate specific research on state-sponsored cybercrime groups.

U.S. Foreign Policymakers

- The U.S. Department of the Treasury should expand sanctions designations to any individual or entity supporting and/or facilitating North Korean cybercrime, including foreign over-the-counter (OTC) brokers and telecommunications companies that provide to North Korea technical services, know-how, and equipment that its hackers use to conduct malicious cyber operations.
- The U.S. government should incorporate specific joint research and investigative initiatives on cryptocurrency-related illicit activity within the ongoing U.S.-ROK cyber working group established during the 2021 Biden-Moon Summit.
- The U.S. government should enhance overall cyber-related intelligence sharing and communication channels with Southeast Asian allies and partners to foster greater understanding of cybersecurity risks.
- The Financial Crime Enforcement Network (FinCEN) should engage with relevant foreign legislative and enforcement bodies to require that virtual asset service providers (VASPs) operating or seeking to operate within their jurisdictions fully implement all Financial Action Task Force (FATF) guidance on virtual assets.

Private Sector Actors

- All cryptocurrency exchanges should adopt company-wide best practices for increased cyber hygiene, such as incorporating relevant CISA guidelines on cybersecurity and executing quarterly mock email phishing campaigns for all employees.

Case Studies

Throughout this report, all North Korean operatives involved in the three case studies presented here are referred to as the Lazarus Group, the umbrella term for Pyongyang-designated cyber operatives targeting institutions across the globe under the direction of the country's main intelligence agency, the Reconnaissance General Bureau (RGB). After a review of the background for each operation, the level of sophistication, and mistakes that point to the Lazarus Group, key takeaways are offered. Specific cyberattacks targeting cryptocurrency exchanges in 2018, 2019, and 2020 are analyzed here because of the wealth of blockchain transaction data available for these hacks, their high probability of connection to the Lazarus Group, and their temporal correlation to new innovations within the crypto space. These hacks also demonstrate North Korea's capabilities and obstacles in using complex financial technologies and obfuscation tactics when stealing and laundering cryptocurrency assets.

The United Nations Panel of Experts on the Democratic People's Republic of Korea (DPRK) assesses that these hacks, along with other illicit financial activity affiliated with North Korean operatives, both directly and indirectly supported the country's illegal nuclear and ballistic weapons development programs.[1] As economic sanctions have curtailed Pyongyang's more traditional sources of exports and commodities trade, the revenues generated by cyber-enabled financial crime almost certainly represent a share of the hard currency Pyongyang uses to support its illicit weapons development program.[2]

Methodology

On-chain information refers to cryptocurrency transactions that are recorded and verified on a public blockchain. Based on this publicly available information, the laundering techniques used in these hacks were analyzed in partnership with blockchain intelligence firm TRM Labs. Open-source information in English and Korean was used to examine the hacking methods employed in each case.

Gate.io Hack

In April 2018, North Korean hackers compromised an unnamed cryptocurrency exchange through an email phishing campaign. An employee of the exchange was targeted with an infected file, which the employee downloaded. This led to the theft of enormous quantities of Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Dogecoin, and several other altcoins. The hack totaled nearly $230 million dollars' worth of crypto assets at then-prevailing prices. However, the exchange never publicly confirmed the hack, which likely delayed involvement from law enforcement, and might have hampered efforts to seize and return all stolen funds to the victims.

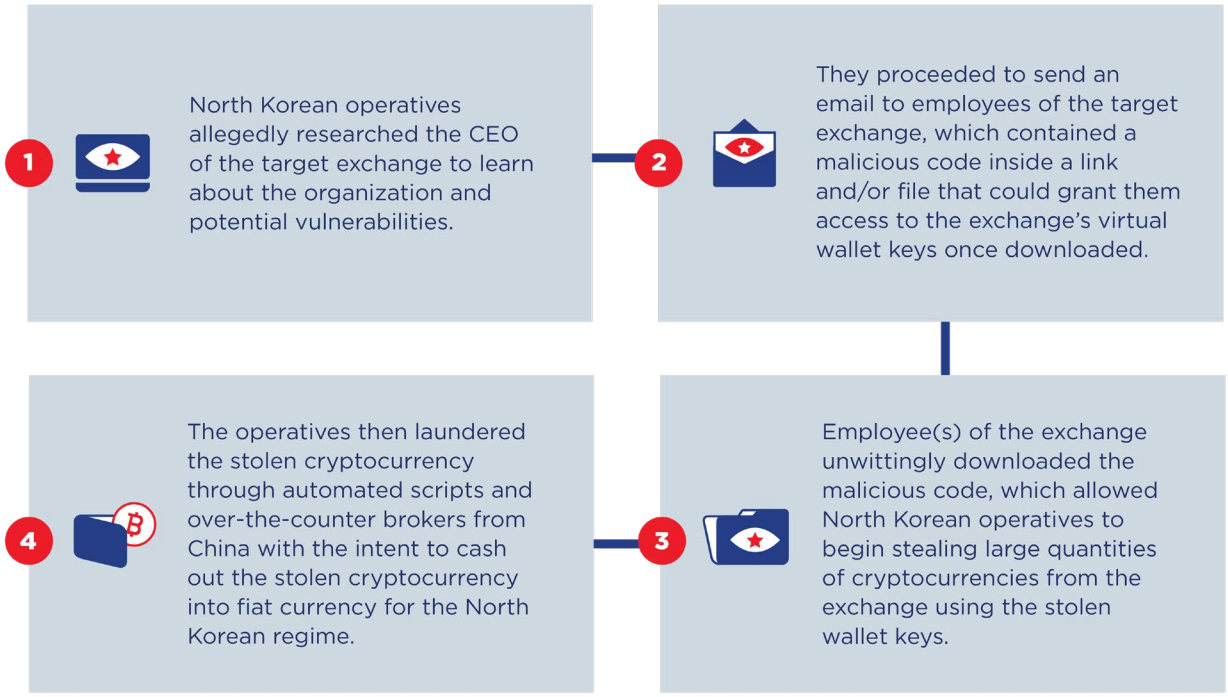
North Korean hackers applied a mixture of basic and advanced laundering techniques during this hack, but in comparison with the other two case studies, this operation was less sophisticated because rapidly exchanging virtual currency for real fiat currency was preferred over obfuscation. Blockchain evidence clearly connected this theft to a victimized Gate.io and the crypto addresses the exchange has been using for years, including during its earlier days as the Bter exchange before rebranding as Gate.io in 2017.[3]

The international response to this cyberattack was minimal because the targeted exchange did not publicly disclose that it was hacked. Roughly two years later, the U.S. Department of Justice, filed a civil forfeiture action against two Chinese nationals charged with laundering more than $100 million in cryptocurrency on behalf of Pyongyang.[4] The civil forfeiture also mentioned that the Lazarus Group and its affiliates, including the two Chinese nationals, used 113 cryptocurrency addresses to launder the stolen funds. However, the indictment did not identify the hacked exchange by name, and instead anonymized the exchange as Virtual Currency Exchange 1 (VCE1). Further blockchain analysis of data provided by TRM Labs revealed with high probability that VCE1 was Gate.io, a formerly China-based exchange now incorporated in the Cayman Islands.[5]

LEVEL OF SOPHISTICATION

Through this hack, North Korea demonstrated its software and coding capability by programming automated scripts to rapidly launder and reconsolidate stolen funds into exchanges before transferring them into Lazarus-affiliated wallets. The hackers employed common obfuscation techniques such as peel chains—sending numerous amounts of crypto to wallets they controlled at various exchanges—in an attempt to minimize suspicion from the exchanges' AML compliance personnel. Automation was apparent due to the large number of transactions made simultaneously and then split into complex patterns. However, the North Korean hackers appear to have needed external support in this operation to bridge the gap between crypto and fiat currencies, because they enlisted the aid of two Chinese nationals to help cash out the stolen cryptocurrency into fiat currency.[6]

GATE.IO HACK AND LAUNDERING OPERATION



To cash out cryptocurrency funds into fiat currency, many crypto users often rely on OTC brokers—individuals who specialize in facilitating cryptocurrency transactions and transfers. OTC brokers often use accounts on exchanges to hold and move crypto on behalf of the brokers' clients. While they can operate within completely legitimate guidelines, OTC brokers can also provide professional money laundering services to facilitate illicit activity, as in the Gate.io hack. It is unknown whether the two Chinese nationals were fully aware that their client was the Lazarus Group, but given the criminal nature of these OTC brokers involved in the money laundering business, it is highly unlikely that the connection to North Korea would have discouraged them from participating in laundering the hack proceeds.

MISTAKES

While the hackers succeeded in stealing cryptocurrency, the fact that they were seemingly unable to launder each type of stolen crypto asset at the same speed and level of complexity suggests North Korean operatives who were relatively more advanced in hacking speed than in overall laundering and obfuscation techniques. The Lazarus Group rapidly laundered stolen Bitcoin, Ethereum, and Dogecoin shortly after the hack, but operatives delayed laundering the Litecoin for roughly two years. A possible explanation is that a North Korean hacker could have tried to store a portion of the funds in a secret wallet for his or her personal use. Regardless of the reason, which remains unknown, this demonstrates a potential vulnerability in the Lazarus Group's laundering capabilities that significantly impacted its net gain from the intrusion. Further analysis shows that from its initial theft to its eventual cash-out, the value of the LTC dropped by nearly two-thirds, from approximately $1.5 to $0.5 million.

KEY TAKEAWAYS: GATE.IO HACK

- Wallet keys were compromised through spear phishing campaigns targeting an employee of the victim cryptocurrency exchange.
- North Korean hackers utilized automated scripts to launder many of the stolen assets.
- The final conversion of cryptocurrency to fiat for Bitcoin occurred with the assistance of two Chinese over-the-counter brokers.
- Speed rather than obfuscation was a clear focus of this operation, as most assets were converted to fiat as rapidly as possible.

DragonEx Hack

On March 24, 2019, the Singaporean exchange DragonEx was hacked, losing roughly $7 million in several cryptocurrencies. Through an elaborate phishing campaign, North Korean hackers used a trojanized version of a legitimate crypto trading application, QtBitcoinTrader, which they called Worldbit-bot.[7] To enhance their credibility, the hackers registered websites for their fake companies and created several fictitious social media profiles for employees of the fabricated firms.

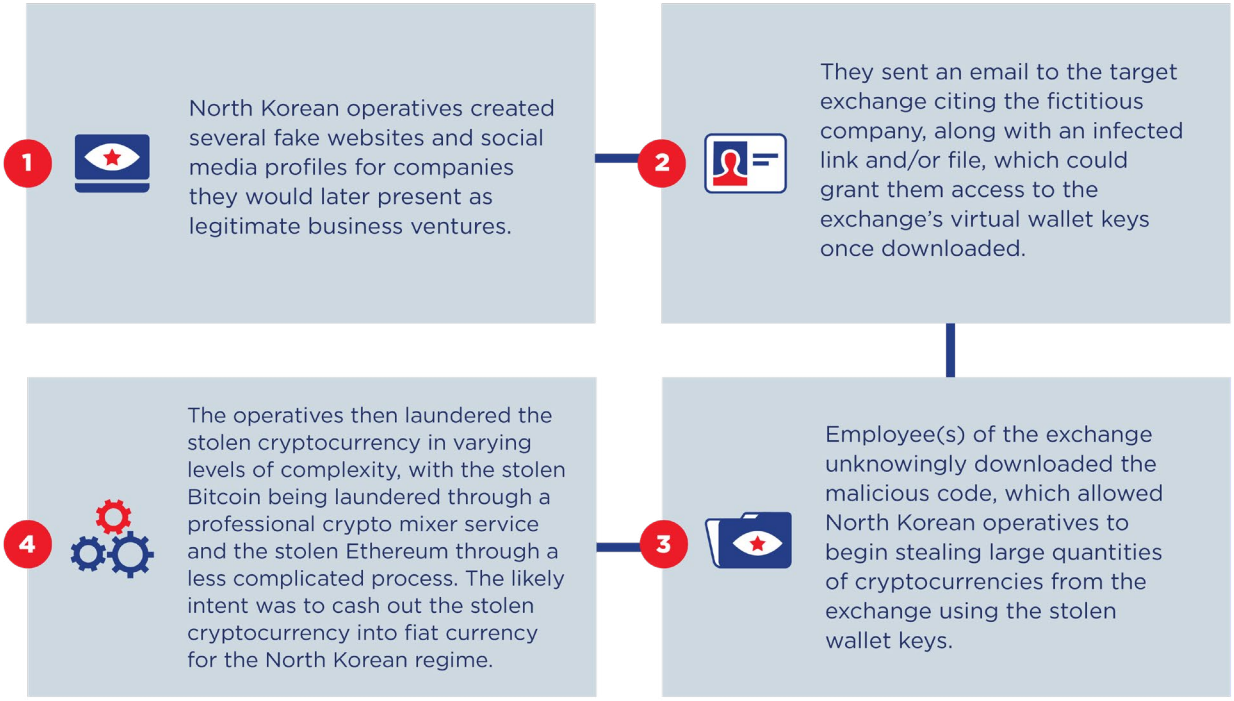
While much smaller in fiscal scale than the Gate.io attack, the DragonEx hack demonstrated substantial improvement in North Korean hackers' laundering techniques. However, these advances were not consistent across all cryptocurrency blockchains. This campaign formed the template for many of Lazarus's subsequent hacks, which continue to use trojanized software as bait to lure unsuspecting crypto exchange employees into infecting company systems.[8] While most cyberattacks attributed to North Korea are often categorized under the wide umbrella of the Lazarus Group, the United Nations Security Council publicly attributed this hack to a specific unit within the Lazarus Group known as APT38, as well as to a particular North Korean operative named Jon Chang Hyok.[9] Additionally, DragonEx confirmed it was hacked within a day of the March 2019 attack,[10] which likely assisted law enforcement investigations.

LEVEL OF SOPHISTICATION

The North Korean hackers used remarkably sophisticated techniques both to hack the exchange and to launder the stolen cryptocurrency. Operatives funneled stolen crypto assets through mixing services, which suggests increased knowledge of the cryptocurrency environment and its tools. In contrast to the Gate.io hack, operatives involved in the DragonEx intrusion seemingly favored obfuscation over pure speed. They held their captured Bitcoin dormant within a single unhosted wallet for approximately two months and then patiently deposited the assets into a trusted mixing service over a period of several months. This followed a buy-and-hold strategy, often referred to as HODL, to maximize potential gains from cashing out the stolen cryptocurrency into fiat currency during a high exchange rate period.

The hackers used incredibly complicated intermediate transactions to divide, then recombine, a large proportion of the stolen Bitcoin, mostly likely

DRAGONEX HACK AND LAUNDERING OPERATION



to obfuscate the origin of the funds. While there were several Bitcoin mixing services available at the time of the hack, only one was chosen: Wasabi Wallet, likely due to its reputation as highly safe and reliable compared to other mixing services, which are often fraudulent sites that steal users' funds.[11]

MISTAKES

Despite the increase in sophistication demonstrated in this hack, the DragonEx laundering efforts indicate remaining vulnerabilities in the Lazarus Group's capabilities, and these allowed law enforcement to attribute the hack to North Korea. For example, the same mixing service was used after reconsolidating the stolen funds, and this minimized effectiveness because it risked detection due to repeated use. Although the hackers used different Bitcoin addresses to move the stolen funds, they still combined them into a handful of clusters, making it easier to link their ownership to a single origin.

Further blockchain analysis of other cryptocurrencies stolen in this hack provides more evidence indicating a possible inability, or lack of desire, to launder all stolen forms of cryptocurrency with equal caution in order to avoid future attribution of the hack. Unlike with Bitcoin, Lazarus employed no mixing service to obscure the movement of the stolen Ethereum and used even simpler methods to liquidate the funds stolen from another cryptocurrency known as Tron. There are three possible reasons for this: first, to ensure high potential cash-out into fiat currency, the hackers may have focused on using only enough obfuscation techniques to avoid the seizure of their stolen assets; second, they may have been concerned about detection and hastened laundering efforts; third, they assumed that only a few investigators were competently following the blockchain analytics of Tron and Ethereum compared with Bitcoin at the time of the hack. Additional obfuscation during the laundering process requires more time and resources, often including the need to pay for additional blockchain services to hide the origin and owners of crypto transactions.

KEY TAKEAWAYS: DRAGONEX HACK

- The hackers employed an elaborate email phishing campaign to compromise DragonEx. They used trojanized software and created multiple, seemingly legitimate social media profiles to increase the perceived legitimacy of the original email.
- The hackers laundered all stolen Bitcoin through the Wasabi Wallet mixer, but other coins stolen were laundered with markedly less sophisticated—though ultimately successful—processes.
- Employing the HODL technique, these hackers waited to sell a large proportion of stolen ETH at then-high prices in August 2020, almost a year and a half after the hack.

KuCoin Hack

On September 26, 2020, a Singapore-based cryptocurrency exchange called KuCoin suffered a massive breach in its cybersecurity, with hackers stealing more than $280 million worth of various cryptocurrencies from the exchange's hot wallets.[12] No details have been made public about how access was gained to KuCoin's systems, but the exchange publicly announced on the day of the hack that it had experienced a "security incident."[13] The majority of these stolen funds were various ERC20 tokens, though substantial quantities of Bitcoin and several other altcoins were also stolen.[14] This major intrusion included a range of sophisticated hacking and laundering techniques, including a professional mixing service and the use of new DeFi platforms in an attempt to obfuscate the activity. The KuCoin hack demonstrates radical improvements in the Lazarus Group's ability to obfuscate the origin of the stolen cryptocurrency. However, these hackers ultimately compromised their anonymity near the end of the operation, which allowed investigators to link pre- and post-mixed assets directly to the original hack.

LEVEL OF SOPHISTICATION

The breadth and intricacy of laundering techniques applied in this hack indicate a dramatic increase in the Lazarus Group's sophistication and adaptability with crypto. The laundering of KuCoin's stolen assets diverged sharply from prior Lazarus operations. Instead of partially haphazard obfuscation efforts during past intrusions, this time North Korean hackers showed more rigor through employing several advanced techniques to try to comprehensively obscure their activity. For this hack, the Lazarus Group used a total of three professional mixers: two to wash the stolen BTC through Wasabi Wallet and ChipMixer, and one—Tornado Cash, which is significantly more complicated to use—to wash the stolen ETH.[15] The Lazarus Group also used an increasingly popular set of blockchain services known as decentralized finance, DeFi. As the international community began to introduce stronger regulatory measures on the cryptocurrency industry in 2018–19, focusing mainly on the mining and trading of cryptocurrencies, the Lazarus Group showed remarkable adaptation to evolving regulations within the virtual asset space through using new platforms such as DeFi.

The use of Tornado Cash, in particular, demonstrated a notable advancement in Lazarus' laundering efforts. Understanding how this professional mixer functions is important to identifying the strengths and weaknesses of the North Korean operatives involved in this hack. A user seeking to anonymize the movement of Ethereum can deposit the cryptocurrency into Tornado in varying increments, most commonly 0.1, 1, 10, and 100 ETH. All crypto users deposit funds of equal value, and these deposits are held in a single address, making it virtually impossible to positively link any one withdrawal with any one deposit. Therefore, the longer a depositor waits to withdraw ETH, the greater the anonymity achieved, effectively providing more cover for North Korean operatives attempting to launder the stolen ETH. Users of Tornado Cash are not required to pay any "gas"—a fee to conduct a transaction on the Ethereum blockchain—to withdraw funds from Tornado after completing the mixing process. Instead, a series of intermediary addresses called relayers supply the necessary gas for a withdrawal, significantly adding to the withdrawer's anonymity and increasing the total level of obfuscation.

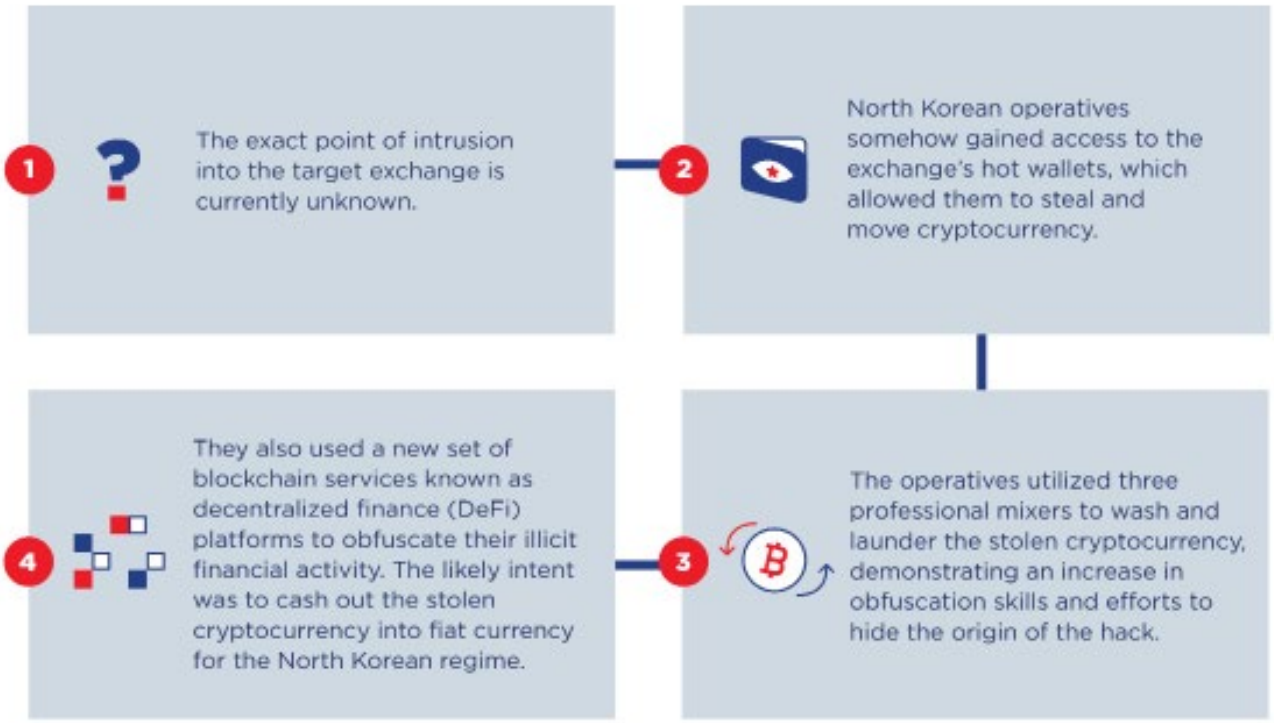
MISTAKES

Even during this elaborate and fiscally lucrative cyber heist, the Lazarus Group seemingly chose speed over total obfuscation. The North Korean hackers elected not to use the more anonymity-preserving features of Tornado Cash, which would have required a transaction fee, likely because they sought to maintain the highest amount of stolen Ethereum for eventual liquidation. As a result, investigators were able to link the post-Tornado withdrawals together and, given the size of the KuCoin theft, ultimately connect them to the original hack.[16] North Korean hackers are well trained and focused, but this misstep in the laundering process clearly signaled their involvement in the theft. This suggests that the Lazarus Group favored higher potential cash-out in a short period of time over complete, long-term obfuscation for the operation, strengthening the claim that overall speed over total obfuscation remains a main priority for Lazarus.

KEY TAKEAWAYS

- The hackers relied heavily on decentralized exchanges to convert less-liquid and easily frozen tokens into secure, fungible assets such as ETH.
- The use of DeFi platforms was a major advance from previous attacks, demonstrating the hackers' high level of adaptation to the evolving crypto space and new decentralized tools.

KUCOIN HACK AND LAUNDERING OPERATION



Research Insights on the Lazarus Group's Modus Operandi

As cryptocurrency technology innovation continues to outpace regulation of the crypto space, comprehensive analysis of these cyber operations shows that the Lazarus Group has rapidly improved both its hacking and blockchain-enabled money laundering capabilities. However, unlike more traditional hackers who spend valuable bandwidth on securing long-term anonymity by hiding their identities through meticulous obfuscation practices, North Korean hackers have demonstrated only moderate concern over eventual attribution. This lack of fear over getting caught is likely linked to the lack of legal retribution for their illicit cyber activities. To date, only one North Korean national has been extradited to the United States for money laundering charges, and this was a remarkably uncommon development in U.S. law enforcement against North Korean targets.[17] In addition to their lack of fear of retribution from foreign law authorities, North Korean hackers have demonstrated a need for only a few days or weeks of anonymity to successfully transfer some portions of stolen funds from a hack. For the Lazarus Group, creating a sufficient level of obfuscation to successfully steal, launder, and transfer funds is enough to complete their official duties.

Equally notable, most North Korea–led cyberattacks begin with some variation of a phishing campaign. This provides ample opportunity for responsible nations and financial institutions to increase their cyber resiliency against North Korean hackers by strengthening cyber hygiene practices through training employees on email phishing schemes. This report's appendix highlights the various techniques and developments demonstrated in each of the three hacks, providing a visualization of the growth of the Lazarus Group's cyber capabilities and money laundering skills.

> **North Korean hackers have demonstrated only moderate concern over eventual attribution. This lack of fear over getting caught is likely linked to the lack of legal retribution for their illicit cyber activities.**

Gaps and Developments in Current Crypto Regulations

In recent years, both intergovernmental bodies and federal governments have increased efforts to better bring the crypto space under their regulatory perimeters by introducing new guidelines and policies. Despite notable advancements, several key vulnerabilities remain and allow ample opportunity for continued exploitation by the Lazarus Group and its affiliates.

The Financial Action Task Force

First created in 1989, FATF has evolved into an intergovernmental anti–money laundering policymaking body that provides guidance to national governments related to combating global money laundering and terrorist financing. Although countries to which this report is relevant are members of FATF, such as China, the United States, and South Korea, FAFT guidance is not legally binding on member nations. While FATF recently updated its guidance for governments and virtual asset service providers on how to apply to the cryptocurrency industry measures for anti–money laundering and combating the financing of terrorism, many vulnerabilities remain within the crypto regulation space, and North Korean operatives will likely continue to exploit these.[18]

For example, VASPs have yet to develop policies to restrict or discourage transactions on blockchains with unhosted wallets, despite the potentially heightened risk this presents to the security of financial platforms for customers transacting cryptocurrency.[19] One of the greatest exploits for North Korean operatives are unhosted wallets, as they often provide opportunities for increased obfuscation when crypto assets are stolen and laundered. As a result, transactions involving unhosted wallets are typically more difficult to trace and seize, as exemplified by the Lazarus Group using an unhosted wallet to hold stolen Bitcoin in the DragonEx hack before transferring funds into a mixing service for laundering purposes. This kind of obfuscation technique has caught the attention of U.S. policymakers who seek to increase scrutiny and regulatory oversight on unhosted wallets and the platforms that support them.[20] Implementation of FATF's standards varies widely among countries, allowing illicit actors to exploit jurisdictions with weak regulation and enforcement. Until VASPs undertake major reform in their approach to unhosted wallets, or until national governments urge VASPs to do so, North Korea will likely find ample jurisdictions and VASPs where it can move funds between unhosted wallets without much scrutiny.

China

Laundering illicit crypto is likely to become more difficult in China. Beijing has steadily increased government crackdowns on cryptocurrency exchanges, and this has impacted the ability of Chinese OTC brokers to operate freely. In March 2020, the U.S. Department of Justice indicted two Chinese nationals charged with laundering more than $100 million worth of stolen cryptocurrency on behalf of North Korea in an operation linked to the first hack studied in this report.[21] However, the last Chinese government crackdown in May 2021 reportedly sent dozens of cryptocurrency exchanges abroad, and Chinese authorities recently outlawed nearly all crypto trading and mining.[22] While the exile of these companies began as early as 2017, as seen in Gate.io moving offshore from mainland China to the Cayman Islands, this blanket ban on trading crypto could affect the future level of assistance that Chinese cybercriminals can offer the Lazarus Group from within mainland China.[23] However, these regulations apply only to Chinese crypto users operating within the legal jurisdiction of China. This means that professional Chinese money launderers and other cybercriminals operating outside of China can still offer their services to North Korean hackers.

United States

Compared with China's efforts, the U.S. regulation of cryptocurrency and associated financial technology has been more targeted, focusing on anti–money laundering and combating the financing of terrorism. Since 2013, Financial Crimes Enforcement Network (FinCEN) of the Treasury has provided regulatory guidance related to the crypto space, allowing for a relatively more permissive environment as long as cryptocurrency exchanges follow the AML/CFT rules established for money service businesses. Currently the U.S. government considers cryptocurrency a commodity and the U.S. Internal Revenue Service treats cryptocurrency as a taxable asset, requiring any transfer worth $10,000 or more to be reported to the IRS.[24] Recently, FinCEN issued a notice of proposed rulemaking to suggest establishing requirements for transactions involving legal tender digital assets and cryptocurrency.[25] This will allow banks and other financial institutions to verify the identities of customers, submit reports, and keep records of transactions exceeding $3,000 using digital wallets that are either not hosted by a financial institution or hosted by an institution within a "high-risk jurisdiction."

These broad efforts are likely connected to U.S. government initiatives to increase transparency and reporting within the crypto space. However, the proposed rulemaking, which was made near the end of the Trump administration, has not been formally addressed under the Biden administration. Instead, the current administration has used its first year to assess the stability and financial crime risks around digital currency technology, especially stablecoins.[26] Given the difficulty of enforcing a ban on unhosted wallets and DeFi platforms due to their wide availability as downloadable open-source software, the U.S. government has not offered any targeted regulation pertaining to unhosted wallets and DeFi platforms. Instead, in keeping with FATF's recent update to its virtual asset guidance, the Treasury has encouraged VASPs to enact case-specific, risk-based approaches to mitigate the illicit financial risks of cryptocurrency technology.

Compared with China's efforts, the U.S. regulation of cryptocurrency and associated financial technology has been more targeted, focusing on anti–money laundering and combating the financing of terrorism.

Beyond indictments from the U.S. Department of Justice against North Korean operatives and their accomplices for illicit financial activity, the U.S. government has taken broader actions that may mitigate North Korea's hacking ability by targeting possible networks offering advanced technologies and new intrusion software.[27] The U.S. Department of Commerce's new rule barring the export and resale to China and Russia of cyber "intrusion software" and equipment without a license will likely make it difficult for the Lazarus Group to obtain new cyber intrusion technology from Chinese and Russian cybercrime groups.[28] Beijing and Moscow continue to help Pyongyang evade sanctions, including illegally hosting North Korean cybercriminals and information technology workers inside their jurisdictions—against U.N. Resolution 2397. Therefore, U.S. companies that provide intrusion software and equipment to Chinese and Russian companies and individuals are at risk for inadvertently providing North Korea with the same technology.[29]

Additionally, the Treasury's Office of Foreign Assets Control issued new cyber sanctions on several Russian individuals, as well as on a Latvia- and Russia-based virtual currency exchange affiliated with ransomware attacks and related payment.[30] The Biden administration linked these actions to its broader strategy to counter the spread and use of ransomware, signaling executive interest in strengthening national cybersecurity with a wide range of U.S. economic tools.[31]

South Korea

Despite any positive developments in inter-Korea relations, Pyongyang will likely continue to target South Korean financial institutions and other entities as it has in the past, including a South Korean cryptocurrency exchange in 2017 and even a government-run think tank researching nuclear power in 2021.[32] According to South Korean media outlets, Seoul's National Intelligence Service believes that roughly 90 percent of all cyberattacks targeting South Korea are led by North Korean hackers, signaling the country's urgent need to strengthen its cyber resilience against the Lazarus Group and its affiliates.[33]

While not referencing North Korea–led cyberattacks, Seoul has adopted new regulations and guidelines for all VASPs and exchanges; this could potentially raise the difficulty threshold for the Lazarus Group to steal crypto assets from the South Korean virtual market.[34] The first rule requires all VASPs and exchanges, including foreign VASPs, to receive Information Security Management System certifications from the Korea Internet and Security Agency in order to operate within the Korean market.[35] Additionally, VASPs must partner with South Korean banks to create "real-name" verified bank accounts for customers, instead of using anonymous crypto wallets, and are required to register with the Korea Financial Intelligence Unit (KoFIU) for license approval.[36] These guidelines from Seoul demonstrate strong government interest in requiring all contributors to the global financial market to incorporate stricter company-wide cybersecurity and regulatory practices.

The South Korean Ministry of Science and Information and Communications Technology has also demonstrated interest in raising national resilience against cyber-enabled financial crime. The ministry organized a two-week-long cybersecurity exercise involving 230 South Korean companies, which detected 114 security vulnerabilities that could have resulted in successful cyber intrusions through email phishing campaigns and ransomware attacks.[37] Although not specifically North Korea–focused, such government-led initiatives and enhanced coordination with the private sector are essential to creating a comprehensive strategy against the evolving North Korean cyberthreat.

Future Outlook on North Korean Hackers

As the crypto space and its users continue to grow, Pyongyang will likely invest more resources in exploiting financial technology to compensate for the economic losses inflicted through international sanctions targeting more traditional forms of commerce.

Continuing to Exploit Cryptocurrency Exchanges

The Lazarus Group is highly effective at infiltrating cryptocurrency exchanges through email phishing campaigns, trojan software, and other malicious codes. Weak cybersecurity protocols exacerbate vulnerabilities to blockchain-enabled money laundering because they grant the hacker direct access to private keys connected to crypto wallets, which hold virtual assets within the exchange. The first two hacks described in this report involved email phishing campaigns that resulted in the loss of hundreds of millions of U.S. dollars in crypto assets, and North Korea continues to demonstrate interest in using this tactic in future cyberattacks on cryptocurrency.[38] Despite efforts from some cryptocurrency exchanges, such as Binance, to assuage concerns over money laundering and other illicit cyber-enabled financial activity, major vulnerabilities remain that are inherent to decentralized finance platforms—which currently are not subject to any major forms of regulation.[39]

Additionally, cryptocurrency exchanges are not subjected to any form of security audit from an investigatory agency that could reveal an exchange's network crucial exploits that hackers could use for infiltration. This likely restricts the spread of institutional knowledge on proper cyber hygiene and international guidelines throughout the exchange, as well as channels by which the exchange can properly communicate with relevant law authorities both during and after a hack.

Exploiting New and Evolving Financial Platforms

DeFi platforms allow individual crypto users to swap one type of cryptocurrency for another, such as Ethereum to Bitcoin, without a centralized platform ever taking custody of the users' funds to facilitate the swap. The lack of centralized custody in DeFi platforms often results in poor or nonexistent collection of user-specific information from the customer, a practice referred to as know-your-customer (KYC) protocol, which makes it easier for cybercriminals to transfer stolen funds with greater anonymity.[40] In a recent example of present-day concerns, some websites publicly advertise ways to trade cryptocurrency in North Korea through popular DeFi platforms, such as Uniswap.[41]

Beyond DeFi, North Korean hackers may also target other evolving financial platforms such as new play-to-earn crypto computer and mobile games.[42] Through these new technologies, cryptocurrency enthusiasts and amateur gamers can earn cryptocurrency as rewards for completing tasks and activities while playing with virtually no in-game financial regulations or cybersecurity equivalent to basic FATF guidelines. In the past, Pyongyang has successfully exploited the online gaming community to its fiscal benefit, which suggests a high likelihood of further exploitation given the growing global interest in and adaption of cryptocurrency.

For example in 2011, the Seoul Metropolitan Police Agency highlighted an estimated two-year-long cybercrime operation that involved North Korean hackers collaborating with South Korean criminals to earn foreign currency from exploiting the South Korean online gaming community.[43] Through alleged rendezvous points in China, Pyongyang transferred North Korean–manufactured gaming software purposefully infected with malicious codes to South Korean accomplices who later sold and distributed the software inside South Korea, compromising the personal data of roughly 660,000 South Korean citizens. While the total amount of funds North Korea acquired remains unknown, the police report claims that the operation generated at least 6.4 billion won (about $5.3 million). As North Korean cybercrime innovation continues to outpace regulation of the crypto space, Pyongyang will likely continue to leverage new and evolving financial technologies within its illicit cyber campaigns.

Utilizing Foreign OTC Brokers

North Korean operatives will likely continue to rely on foreign OTC brokers for access to the traditional financial system, including banks and the U.S. dollar. Pyongyang's reliance on foreign OTC brokers to launder stolen funds highlights the need for North Korea to obtain reliable access to U.S.-dollar-denominated bank accounts to cash out cryptocurrency. However, Beijing's sustained crackdowns on crypto mining and domestic OTC brokers may reduce Pyongyang's overall reliance on Chinese cybercriminals, who will have to operate outside of mainland China. Future operations may show greater demographic diversity in foreign OTC brokers assisting the Lazarus Group. For example, more Russian-speaking OTC brokers may participate in North Korean cyber heists due to reportedly preexisting ties with Eastern European cybercrime groups.[44]

The Lazarus Group likely depends on OTCs to bridge the gap between crypto and fiat currencies because unlike North Korea, which is heavily sanctioned under both U.S. and U.N. regimes, these foreign launderers still have access to the U.S. financial system and traditional financial institutions.[45] A foreign national willing to endanger his or her own personal and legal security is essential for North Koreans to convert stolen crypto assets into fiat currencies, most likely U.S. dollars. Additionally, Pyongyang could allow its hackers to obtain dual citizenship in a foreign country, or to forge passports, to circumvent sanctions preventing North Korean nationals from accessing traditional financial institutions to cash out stolen cryptocurrency. Although North Korea does not officially recognize dual citizenship, Pyongyang has historically issued fraudulent IDs and passports to North Korean operatives known as "illegals": intelligence officers who use false foreign identities to infiltrate targets.[46]

Receiving Help from Abroad

In efforts ranging from finding foreign nationals to provide technological know-how to offering money laundering services, North Korea will likely continue to pursue engagement with external resources to support its illicit cyber activity. In 2019, the U.S. government reported that U.S. citizen Virgil Griffith, a former senior researcher and developer for the Ethereum Foundation, provided Pyongyang with technical advice on using blockchain technology to evade sanctions, as well as conspiring to recruit other U.S. citizens, liaising deals with cryptocurrency and blockchain service providers on behalf of Pyongyang, and facilitating cryptocurrency exchanges between North and South Korea.[47] Given North Korea's demonstrated success in using blockchain technology to evade sanctions before 2019, it is possible that Griffith did not provide any new information to North Korea.[48] But whatever the case may be in this instance, security concerns surrounding the direct or indirect involvement of foreign nations in illicit cyber activity benefiting Pyongyang must be addressed.

Additionally, several intelligence reports from security firms indicate that the Lazarus Group has likely expanded its networks into Eastern Europe through Russian-speaking cybercriminals. In particular, the intelligence company Intel 471 has identified TrickBot as a Russian-speaking cybercriminal group operating out of Eastern Europe with potential ties to North Korea and other outlets. Intel 471 has cited evidence of communication channels between TrickBot and the Lazarus Group before North Korean cyber operations were carried out.[49] Pyongyang will likely continue this trend of seeking foreign assistance to expand and advance its global cybercrime campaigns.

Fostering the Next Generation of North Korean Hackers

Domestic developments inside North Korea also suggest increased government resources for fostering the next generation of the Lazarus Group. In May 2020, Pyongyang allegedly recruited at least 100 of its highest performing graduates from top North Korean science and technology universities into its military to manage its tactical planning systems.[50] Reports have indicated that North Korea's leading hacking academy, Mirim College or the University of Automation, continues to graduate hundreds of hackers every year, demonstrating sustained government interest in fostering the next generation of hackers.[51] North Korean state media confirmed the establishment of a new science and technology university during a military parade in October 2020, and ties to the country's cyberwarfare and weapons development program are possible.[52] When viewed comprehensively, this suggests that Pyongyang will continue to pursue cybercrime as a lucrative method to obtain funds for the regime. The international community focuses mostly on North Korea furthering the development of its nuclear weapons, but increased attention should be directed at its development of well-trained cybercriminals tasked with infiltrating the global financial systems to procure funds for the development of these lethal weapons.

Continuing to Target Vulnerable Jurisdictions

North Korea has orchestrated a series of sophisticated cyberattacks from foreign jurisdictions with virtually no major punitive repercussions.[53] In particular, Pyongyang has historically used areas of China and Southeast Asia as preferred regions to cultivate myriad cyber-enabled financial crime campaigns.[54] These illicit activities include, but are not limited to, the largest known cyber bank heist, totaling an estimated $81 million worth of funds stolen from the central bank of Bangladesh. These funds were then transferred to a five-year-long money laundering scheme launched in Malaysia.[55] Previous reports have outlined key contributing factors to North Korea's continued pressure in Southeast Asia, including that region's proximity to North Korean proliferation networks, its sophisticated trade and finance infrastructure, major gaps in local regulatory and compliance frameworks, and a nascent but expanding

cryptocurrency industry.[56] Although the U.S. government was successful in the extradition of a North Korean operative stationed in Malaysia who laundered money for the regime through shell companies, this was a remarkably rare achievement that will not likely discourage Pyongyang from continuing illicit activity abroad, including within the global cyber space.[57]

> **While Washington tasks its intelligence and defense agencies with a wide-range of security issues, Pyongyang has a much narrow focus: support the Kim regime at all costs through information, economic, and military espionage.**

Because potential gains from cyberattacks targeting new financial technology still significantly outweigh potential punitive risks for North Korean hackers, Pyongyang will likely increase its presence in jurisdictions and institutions that fail to adopt stricter cyber-related, and crypto-specific, regulatory guidelines and security protocols. While Washington tasks the U.S. intelligence and defense community with a broad set of international security issues, Pyongyang tasks its overseas-facing intelligence agencies with a much narrower set of duties: support the Kim regime at all costs through information, economic, and military espionage targeting mainly the United States and South Korea.[58] This is perhaps the cornerstone of why North Korean hackers continue to outmaneuver U.S. and other nations' cybersecurity strategies. Along with like-minded nations and institutions, U.S. policymakers should invest more resources into analyzing weaknesses in the Lazarus Group's cybercrime modus operandi and create policies to strengthen resilience against increased cyberattacks and blockchain-enabled laundering of virtual assets.

Policy Recommendations

The following recommendations seek to inform U.S. policymakers and relevant stakeholders, such as the private sector, about potential tools and strategies to strengthen overall cyber resilience against the Lazarus Group and its affiliates, which seek to exploit cryptocurrency and blockchain technology.

U.S. Domestic Policymakers

- **Financial regulators and lawmakers should work to remove any loopholes that allow DeFi platforms and other emerging financial technology to circumvent U.S. AML/CFT regulations.** As DeFi platforms and other emerging financial technology host an enormous amount of illicit pseudonymous activity, Pyongyang will likely increase its presence within these unregulated spaces, which often provide greater levels of autonomy and anonymity in transactions compared with other financial platforms. Although DeFi platforms may receive more scrutiny and oversight when users on regulated financial platforms send or receive funds from them, they still pose significant risk for continued exploitation. A website outlining ways to buy Uniswap in North Korea as recently as December 2021 is a clear indication of a greater need for U.S. government-wide understanding of blockchain and collaboration with DeFi platforms to ensure stronger cybersecurity protocols.[59] U.S. financial regulators and lawmakers should follow FATF guidance to identify entities that are responsible for DeFi platforms to ensure they comply with basic AML and CFT requirements. In particular, unhosted wallets present significant risks, as they are present only on DeFi platforms. However, unhosted wallets are not inherently bad because fully licit reasons exist for their use, such as a desire for increased user privacy and security for financial transactions. While unhosted wallets should not be banned, VASPs under U.S. jurisdiction should make sure to study and account for risk patterns that are likely to emanate from financial technology tools lacking KYC information. Regulating DeFi and unhosted wallet activity will constrain the space where cybercriminals can operate and launder stolen funds.
- **Congress should adopt legislation that requires all cryptocurrency exchanges to report cyber incidents to CISA and the FBI that could involve the financial and/or personal information of U.S. citizens and/or entities.** Many private companies, including cryptocurrency exchanges, refrain from publicly reporting or disclosing cyber incidents because of concerns about negatively impacting their reputations. However, withholding information regarding cyber incidents that could negatively impact existing and new users poses a significant threat to their financial and personal security. The United States can lead a global effort in cyber incident reporting

through adopting legislation that requires all cryptocurrency exchanges to report cyber incidents that affect U.S. citizens and/or companies to CISA and the FBI within 72 hours of confirmation, or another reasonable time frame to be defined. Congress should then decide whether failure to report a confirmed cyber incident involving a U.S. person and/or entity is legally punishable through fines or other punitive measures. This measure may also encourage cryptocurrency exchanges to adopt better know-your-customer protocols to determine the presence of U.S. citizens within their user base. Following the report of cyber incidents, early cooperation with the U.S. government has proven to increase a company's odds of returning stolen crypto assets and/or information to the affected users.[60]

- **Within the new National Cryptocurrency Enforcement Team, the executive branch should designate specific research on state-sponsored cybercrime groups.** Because Lazarus is perhaps the most advanced group of state-sponsored cybercriminals targeting financial institutions and cryptocurrency exchanges, the U.S. government should adapt existing cybersecurity frameworks to reflect this grave threat. Bearing in mind the successful forfeiture of millions of dollars in cryptocurrency stolen and laundered during past cybercrime campaigns by North Korean and non–North Korean actors, the Biden administration should add a North Korea–specific portfolio to the National Cryptocurrency Enforcement Team.[61] Recent examples of the threat include the 2014 Sony Pictures Entertainment embezzlement scheme and the 2017 WannaCry ransomware attack. Established in October 2021, the National Cryptocurrency Enforcement Team is tasked to "tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors"—all of which are points of exploitation targeted by Pyongyang for years.

  Alongside the National Cryptocurrency Enforcement Team, an interagency taskforce consisting of the U.S. Department of Justice, the Federal Bureau of Investigation, and the U.S. Cyber Command can support U.S. citizens and entities targeted by North Korean cyberattacks. While some cryptocurrency exchanges offer an insurance policy on stolen cryptocurrency if the exchange itself is hacked, most do not provide the same policy to individuals who have been hacked themselves.[62] This means that if a user's cryptocurrency wallet or private keys are compromised through a hack, the victim is fully responsible for the loss of virtual assets from a personal cyber breach. If a U.S. citizen or entity is a victim of a supposed North Korean hack, this interagency taskforce should assist the affected parties in recovering stolen virtual assets. Previously, the U.S. Cyber Command has successfully launched countermeasures against North Korean hackers, thereby setting a precedent for continued action.[63]

U.S. Foreign Policymakers

- **The Treasury should expand sanctions designations to any individual or entity supporting and/or facilitating North Korean cybercrime, including foreign OTC brokers and telecommunications companies providing to North Korea technical services, know-how, and equipment that its hackers use to conduct malicious cyber operations.** The Treasury has issued sanctions against Russian and Chinese institutions for providing financial, material, and technological support to North Korea related to its nuclear weapons program, but no foreign entities have been designated for their assistance in expanding North Korean cybercrime capabilities.[64] Major Russian and Chinese telecommunications companies have indirectly supported North Korean cyber-enabled financial crime campaigns by providing increased internet bandwidth and connectivity to North Korean operatives, allowing them to enhance their hacking capabilities and use virtual private networks to hide their true location.[65] Sanctioning telecommunication companies that facilitate cybercrime can reduce Pyongyang's hacking capabilities and discourage other telecommunications companies from engaging with North Korean cybercriminals. North Korean hackers have likely used these internet lines to conduct a wide range of cyberattacks. The internet connections are not extended to the general public, since only certain government officials and members of the elite class are legally allowed to access the internet. In terms of impacts on the general population, ordinary North Koreans can only access the country's intranet, known as the *Kwangmyong* (광명망), meaning that the sanctioning of telecommunications companies that offer connections to the internet for hackers will not impact the daily lives of the average population.[66]

The Treasury has several sanctions programs through which designations can be imposed against individuals and entities for direct and/or indirect involvement in North Korea–led cyber operations: DPRK3, CYBER2, and the Countering America's Adversaries through Sanctions Act (CAATSA). Created under Executive Order 13722 and 13757, respectively, DPRK3 and CYBER2 permit designations related to conducting and/or facilitating illicit cyber activity. The Treasury used both programs to target the two Chinese nationals mentioned earlier in this report who offered OTC services to the Lazarus Group.[67] Under provisions 311(b)(I) of CAATSA, the Treasury can levy sanctions against any individual or entity that "directly or indirectly, engaged in, facilitated, or was responsible for the online commercial activities of the Government of North Korea."[68] All three programs provide the legal framework to impose sanctions against telecommunications companies that assist North Korean hackers through offering improved internet bandwidth and connectivity, but the Treasury will need to conduct significant investigation and intelligence analysis prior to issuing sanctions.

- **The U.S. government should incorporate specific joint research and investigative initiatives on cryptocurrency-related illicit activity within the ongoing U.S.-ROK cyber working group established during the 2021 Biden-Moon Summit.** Although Washington and Seoul pledged in May 2021 to create a bilateral cyber working group for enhanced cyber and law enforcement cooperation, their agreement failed to mention cryptocurrency or financial technology.[69] Key U.S. agencies such as the FBI, CISA, the Treasury, and the Department of Justice should seek support and enhanced partnership with their most well-equipped South Korean counterparts, mainly the ROK National Intelligence Service, the National Policy Agency, and the KoFIU. These South Korean agencies have demonstrated their capability and vested interest in combating cyber-enabled financial crime through successful shutdowns of cybercriminal groups.[70] Enhanced partnership could expand the overall bandwidth of U.S. investigations and analysis potential. As Pyongyang shifts more resources and capital into its hackers targeting cryptocurrency exchanges and DeFi platforms, Washington and Seoul must also update their joint cybersecurity initiatives with greater integration of cryptocurrency expertise and investigatory capabilities.
- **The U.S. government should enhance overall cyber-related intelligence sharing and communication channels with Southeast Asian countries to foster greater understanding of cybersecurity risks.** Beyond increasing collaborative efforts with traditional allies such as South Korea, the United States should also pursue engagement with key countries that are often the victims of North Korea–sponsored cyberattacks, as well as those, whether unwittingly or not, that host North Korean hackers within their jurisdictions. Washington has several options to increase cyber intelligence sharing with Southeast Asian allies and partners regarding best practices to enhance cyber hygiene and mitigate potential risks. As in the Washington-Seoul bilateral agreement, the United States can pursue joint cybersecurity initiatives with Southeast Asian countries with the inclusion of crypto-specific language.
- **FinCEN should engage with relevant foreign legislative and enforcement bodies to require that VASPs operating or seeking to operate within their jurisdictions fully implement all FATF guidance on virtual assets.** The Lazarus Group will continue to operate in jurisdictions with weak cybersecurity and regulatory protocols that allow hackers to launder stolen funds, use unhosted wallets with little scrutiny, exploit DeFi platforms, and launch a series of cyberattacks. Although full implementation of FATF guidance in non-crypto finance remains a difficult task for national governments and jurisdictions, implementing FATF guidance across countries is the best current strategy to address this cyber-related issue. For example, South Korea's KoFIU has begun to regulate VASPs according to guidelines seemingly inspired by FATF reports.

  Another option is for FinCEN to lead a multinational summit in partnership with a Southeast Asian counterpart agency on cybersecurity with emphasis on blockchain-enabled financial crime, cryptocurrency, and DeFi platforms. Given its history with North Korea–led cybercrime, Singapore would be an ideal partnership country to host an international forum. It was one of the 30 countries to participate in the U.S.-led virtual counter-ransomware initiative meeting in October 2021, suggesting that the U.S. and Singaporean governments would be interested in collaborating on joint cybersecurity measures.[71] FinCEN can also draw on the 2018 Europol conference on law enforcement related to cryptocurrency, to discuss multinational cooperation on blockchain-enabled financial crime.[72] Beyond national governments, major cryptocurrency exchanges should also be invited, as they could potentially provide insightful feedback and lessons learned from previous cyber incidents.

Private Sector Actors

- **All cryptocurrency exchanges should adopt company-wide best practices for increased cyber hygiene, such as incorporating relevant CISA guidelines on cybersecurity and executing quarterly mock email phishing campaigns for all employees.** Protection may be enhanced by establishing default two-factor authentication requirements for crypto users seeking to access the financial services of a cryptocurrency exchange, but this fails to protect the exchange itself from North Korean hacks and cyber intrusions. The majority of North Korea–led cyberattacks start with some form of an email phishing scheme that does not target individual crypto users, but the employees and network system of a cryptocurrency exchange. This highlights the importance and increasing need for responsible organizations to encourage employees to adopt stricter cyber hygiene protocols.

Cryptocurrency exchanges should require all employees to undergo quarterly cyber hygiene training, including how to identify and report phishing scams. Routine exercises should include quarterly company-wide cyber hygiene testing, involving mock email phishing campaigns sent to unsuspecting employees. If a targeted employee accesses or downloads an infected link or file, that employee should be required to complete additional training, which can be found on numerous websites designed to teach how to spot and avoid cyber scams. CISA regularly publishes guidelines and phishing tip cards to inform the U.S. public about common red flag indicators of fraudulent emails seeking to infiltrate system networks through hidden malicious codes.[73]

Conclusion

Over the years, North Korea has demonstrated high adaptability and advancement within the illicit cyber and crypto space using new technology to exploit vulnerabilities in the global financial system. Foreign assistance from key allies such as Beijing and Moscow has allowed Pyongyang to expand its cyber intrusion capabilities in ways ranging from hosting North Korean hackers within their jurisdictions to providing improved data connections to expand the country's international bandwidth and connectivity.[74] While North Korea does not fully operate on a public internet system, it has revolutionized its restricted but ample connections to global cyberspace as a tool for proliferation finance.[75] In the past, unidentified actors have been successful in temporarily cutting North Korea's access to the internet, but the country's cyber infrastructure remains a more elusive target for retaliation and direct countermeasures compared with other cyber aggressors such as Russia and China. The latter share much deeper connections to the public online domain.[76] In contrast to cybersecurity threats originating in China and Russia, North Korean hackers present a unique risk to U.S. national security by specifically targeting the global financial system. This calls for expanding current U.S. cybersecurity strategy to include specific guidelines for improving resilience against cyber-enabled financial crime, especially attacks targeting cryptocurrency, new financial technology, and the applicable service providers.[77]

Appendix

TECHNIQUES USED	HACK 1 | GATE.IO (2018)	HACK 2 | DRAGONEX (2019)	HACK 3 | KUCOIN (2020)
Email Phishing Scheme	YES	YES	UNKNOWN
Automated Scripts	YES	NO	NO
Peel Chains	YES	NO	YES
Professional Mixer	NO	YES	YES
OTC Broker	YES	UNKNOWN	UNKNOWN
Unhosted Wallet(s)	NO	YES	YES
DeFi Platform(s)	NO	NO	YES

Glossary

The following are the author's brief definitions for key terminology used in this report.

An **altcoin** refers to any type of cryptocurrency other than Bitcoin.

BTC is the abbreviation used for the Bitcoin cryptocurrency.

Blockchain is a digital and immutable public ledger that is duplicated and distributed across an entire network of computer systems to facilitate and record the process of virtual asset transactions, often cryptocurrency.

Cryptocurrency is typically decentralized digital money designed to be used over the internet through blockchain technology. Cryptocurrency is not controlled by any government or other central authority, such as a bank, and is managed through peer-to-peer networks of computers running open-source software.

A **cyber intrusion** is the act of compromising a computer system by breaking into the system or network security, causing it to enter an insecure state. While some companies may legally employ third-party contractors to purposely infiltrate into their network system to test for security vulnerabilities, most cyber intrusions are unauthorized and illegal. A **cyberattack**, however, involves purposefully disrupting, disabling, destroying, and/or controlling a system.

A **cryptocurrency wallet** is a hardware device or downloadable software program that stores the public and private keys for facilitating cryptocurrency transactions. Public keys allow other users to send transactions to the digital address associated with that wallet, whereas private keys enable the spending of cryptocurrency associated with the digital address of the wallet.

DeFi is short for "decentralized finance," a broad term for a variety of software applications based on blockchain technology where financial services such as lending, trading, and swaps of cryptocurrencies are offered without a regulated financial intermediary.

An **ERC20** token is a cryptocurrency standard used for creating and issuing smart contracts on the Ethereum blockchain. Smart contracts are computer programs stored on a blockchain that follow a specific transaction protocol for digital contracts when predetermined conditions are met, such as "if/when . . . then" scenarios. They can be used to create new cryptocurrency tokens, release designated funds to the appropriate parties, and more.

ETH is the abbreviation used for the Ethereum cryptocurrency.

An **exploit** is a code that takes advantage of a software vulnerability or security flaw. It is typically written by either security researchers as a proof-of-concept threat or by malicious actors to use in their cyber operations.

Fiat money is government-issued currency that is not backed by a commodity such as gold. Most modern paper currencies, such as the U.S. dollar, are fiat currencies.

The **Financial Action Task Force (FATF)** is an intergovernmental anti–money laundering policymaking body that provides national governments with non–legally binding guidance related to combating global money laundering and terrorist financing.

HODL is a term used by cryptocurrency users to describe a buy-and-hold strategy where users wait a lengthy period before selling acquired cryptocurrency in anticipation of rising crypto-to-fiat currency exchange rates. The term is believed to have originated from a typo in a Bitcoin forum for "hold," but now it means "hold on for dear life" in the crypto space.

A **hot wallet** is a virtual currency wallet that is accessible online and facilitates cryptocurrency transactions between the owner and end-users, while a cold wallet is stored on an offline platform and is only accessible after connecting to the internet. Since hot wallets are connected to the internet, they are vulnerable to cyber hacks and unauthorized access, while cold wallets are not.

A **mixer** or **tumbler** is a cryptocurrency service that mixes different streams of identifiable cryptocurrency to improve the anonymity of digital transactions and their users.

A **stablecoin** is any cryptocurrency designed to have a relatively stable, as opposed to fluctuating, price. This is typically achieved through pegging the stablecoin to a commodity, a specific currency, or through having its digital supply regulated by a certain algorithm.

A **trojan** is a type of malicious code or software that appears to be legitimate and benign but, once downloaded, will damage, disrupt, or steal targeted data and/or an entire network. It can also take control of the targeted device.

An **unhosted**, or **non-custodial wallet**, is a digital wallet in which crypto users can store their own cryptocurrency without any gatekeeping or oversight from an intermediary financial institution or cryptocurrency exchange in a way that resembles holding cash in a physical wallet as opposed to in a bank account. Unhosted wallets are found only on decentralized finance platforms. While there are many licit reasons to own an unhosted wallet, such as user privacy and security, the unregulated nature of unhosted wallets presents opportunities for illicit cyber actors to exploit them.

A **virtual asset service provider (VASP)** is an individual or business that facilitates the exchange, transfer, custody, offer, or sale of a virtual asset such as cryptocurrency.

Wash is a term used to describe the act of laundering funds by increasing anonymity through a mixing service or other obfuscation services or practices.

1. Panel of Experts final report for distribution, pursuant to resolution 1874 (2009), report no. S/2021/211, (United Nations Security Council, March 4, 2021), https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_211.pdf.

2. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, unclassified report, ATA-2021,(April 9, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

3. Gate.io Support, "如何一键转入比特儿账户资产？" (How to Instantaneously Transfer Assets to My Gate.io Account?), Gate.io, updated April 2021, https://support.gate.io/hc/zh-cn/articles/115002650193-如何一键转入比特儿账户资产-.

4. "Two Chinese Nationals Charged with Laundering over $100 Million in Cryptocurrency from Exchange Hack," U.S. Department of Justice, press release, March 2, 2020, https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack.

5. Gate.io Support, " How to Instantaneously Transfer Assets to My Gate.io Account?"; Gate.io Review, Cryptonews, https://cryptonews.com/reviews/gate-io/.; Gate.io User Agreement, Gate.io, https://www.gate.io/docs/agreement.pdf.

6. "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," U.S. Department of Treasury, press release, March 2, 2020, https://home.treasury.gov/news/press-releases/sm924.

7. "APT-C-26 (Lazarus) 组织对数字货币交易所的最新攻击预警" (Apt-C-26 Warning on [Lazarus] Group's Latest Attack Warning on Digital Currency Exchanges), 安全内参 (Security Internal Reference), March 29, 2019, https://www.secrss.com/articles/9511.; Yuriy Kudlovich, "How Cryptocurrency Mixers and Anonymous Wallets Work," DeCenter, January 17, 2018, https://decenter.org/en/how-cryptocurrency-mixers-and-anonymous-wallets-work.

8. United States v. Jon Chang Hyok, Kim Il, Park Jin Hyok, CR 2:20-cr-00614-DMG (District Court for the Central District of California, 2020), https://www.justice.gov/opa/press-release/file/1367701/download.

9. Panel of Experts midterm report, pursuant to resolution 1874 (2009), report no. S/2019/691 (United Nations Security Council, August 30, 2019), https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf.

10. Derek Tonin, "DragonEx Exchange Shuts Down, Confirms It's Been Hacked," Coingeek, March 26, 2019, https://coingeek.com/dragonex-exchange-shuts-down-confirms-its-been-hacked/.

11. Kai Sedgwick, "Review: Wasabi's Privacy-Focused BTC Wallet Aims to Make Bitcoin Fungible Again," Bitcoin.com, January 8, 2019, https://news.bitcoin.com/review-wasabis-privacy-focused-btc-wallet-aims-to-make-bitcoin-fungible-again/.

12. Cryptopedia staff, "Hot Wallets vs. Cold Wallets", Cryptopedia, updated July 4, 2021, https://www.gemini.com/cryptopedia/crypto-wallets-hot-cold.

13. "KuCoin Security Incident Update," KuCoin, September 25, 2020, https://www.kucoin.com/news/en-kucoin-security-incident-update.

14. Nathan Reiff, "What Is ERC-20 and What Does It Mean for Ethereum?" Investopedia, updated August 5, 2021, https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/.

15. Wasabi Wallet, https://wasabiwallet.io/.; ChipMixer, dnstats, https://dnstats.net/site/chipmixer/.; Tornado Cash, https://tornado.cash/; and Michelle Nicols and Raphael Satter, "U.N. Experts Point Finger at North Korea for $281 Million Cyber Theft, KuCoin Likely Victim," Reuters, February 9, 2021, https://www.reuters.com/article/us-northkorea-sanctions-cyber/u-n-experts-point-finger-at-north-korea-for-281-million-cyber-theft-kucoin-likely-victim-idUSKBN2AA00Q.

16. Koh Wei Jie, "Deanonymising the Kucoin Hacker," Medium, October 30, 2020, https://weijiek.medium.com/deanonymising-the-kucoin-hacker-418fa5e9911d.

17. Jason Bartlett, "Mun Chol Myong: The First-Ever North Korean Criminal Facing Extradition to the U.S.," The Diplomat, March 10, 2021, https://thediplomat.com/2021/03/mun-chol-myong-the-first-ever-north-korean-criminal-facing-extradition-to-the-us/.

18. "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (Financial Action Task Force, October, 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

19. Yaya Fanusie, "What FATF's Latest Guidance Means for DeFi, Stablecoins and Self-Hosted Wallets," CoinDesk, updated November 9, 2021, https://www.coindesk.com/policy/2021/11/09/what-fatfs-latest-guidance-means-for-defi-stablecoins-and-self-hosted-wallets/.

20. Agata Ferreira, "Authorities Are Looking to Close the Gap on Unhosted Wallets," Cointelegraph, May 23, 2021, https://cointelegraph.com/news/authorities-are-looking-to-close-the-gap-on-unhosted-wallets; U.S. Department of the Treasury, Financial Crimes Enforcement Network, *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets,* 31 CFR parts 1010, 1020, and 1022, RIN 1506-AB47, *Federal Register* (December 23, 2020), https://public-inspection.federalregister.gov/2020-28437.pdf.

21. "Two Chinese Nationals Charged with Laundering over $100 Million in Cryptocurrency from Exchange Hack," U.S. Department of Justice.

22. "Explainer: What Beijing's New Crackdown Means for Crypto in China," Reuters, May 19, 2021, https://www.reuters.com/world/china/what-beijings-new-crackdown-means-crypto-china-2021-05-19/.; Helene Braun, "Crypto OG Bobby Lee Says China's OTC Desks Are Next to Go," CoinDesk, September 27, 2021, https://www.coindesk.com/business/2021/09/27/crypto-og-bobby-lee-says-chinas-otc-desks-are-next-to-go/.

23. Gate.io Support, "How to Instantaneously Transfer Assets to My Gate.io Account?"; Gate.io Review; Alun John, Samuel Shen, and Tom Wilson, "China's Top Regulators Ban Crypto Trading and Mining, Sending Bitcoin Tumbling," Reuters, September 24, 2021, https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/.

24. "The State of Crypto: Making Sense of U.S. Cryptocurrency Regulations," Thomson Reuters, July 15, 2021, https://legal.thomsonreuters.com/en/insights/articles/how-will-emerging-us-regulations-impact-cryptocurrencies.

25. "The State of Crypto."

26. "President's Working Group on Financial Markets Releases Report and Recommendations on Stablecoins," U.S. Department of Treasury, press release, November 1, 2021, https://home.treasury.gov/news/press-releases/jy0454.

27. "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes across the Globe," U.S. Department of Justice, press release, February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

28. Ellen Nakashima, "Commerce Department Announces New Rule Aimed at Stemming Sale of Hacking Tools to Russia and China," *The Washington Post*, October 20, 2021, https://www.washingtonpost.com/national-security/commerce-department-announces-new-rule-aimed-at-stemming-sale-of-hacking-tools-to-repressive-governments/2021/10/20/ecb56428-311b-11ec-93e2-dba2c2c11851_story.html?outputType=amp.

29. Panel of Experts final report for distribution, pursuant to resolution 1874 (2009), report no. S/2021/211; United Nations Security Council, "S/RES/2397" (UNSC, December 22, 2017), https://undocs.org/S/RES/2397(2017).

30. "Treasury Continues to Counter Ransomware As Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange," U.S. Department of Treasury, press release, November 8, 2021, https://home.treasury.gov/news/press-releases/jy0471; "Treasury Takes Robust Actions to Counter Ransomware," U.S. Department of Treasury, press release, September 21, 2021, https://home.treasury.gov/news/press-releases/jy0364.

31. "Ongoing Public U.S. Efforts to Counter Ransomware," The White House, press release, October 13, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/.

32. "이재철 [Lee Jae-Chul], "가상화폐 노린 북한… 한국 빗썸에도 200억 요구했다" (North Korea Targeted Cryptocurrency . . . Demanded 20 Billion Korean Won from South Korea's Bithumb), Maeil Business, April 1, 2021, https://www.mk.co.kr/news/world/view/2021/04/313610/.; Hyonhee Shin, "North Korea Hackers Target S. Korea Nuclear Think Tank: Lawmaker," Reuters, June 18, 2021, https://www.reuters.com/world/asia-pacific/north-korea-hackers-target-skorea-nuclear-think-tank-lawmaker-2021-06-18/.

33. "N. Korea's Hacking Ability Continues to Evolve," KBS World, July 22, 2021, https://world.kbs.co.kr/service/contents_view.htm?lang=e&menu_cate=northkorea&id=&board_seq=407145.

34. Euihyun Bae, "South Korea Takes First Step to Regulate Virtual Asset Service Providers," The Diplomat, September 24, 2021, https://thediplomat.com/2021/09/south-korea-takes-first-step-to-regulate-virtual-asset-service-providers/.

35. Norbert Gehrke, "Korea Regulations for Virtual Asset Service Providers," Tokyo FinTech, June 3, 2021, https://medium.com/tokyo-fintech/korea-regulations-for-virtual-asset-service-providers-b34c20efa58f.

36. AML/CFT Framework, Korea Financial Intelligence Unit, https://www.kofiu.go.kr/eng/regime/framework.do.

37. "S. Korea Faces Increasing Ransomware Attacks This Year," *The Korea Herald*, July 6, 2021, http://www.koreaherald.com/view.php?ud=20210706000765.

38. Darien Huss and Selena Larson, "Triple Threat: North Korea–Aligned TA406 Steals, Scams and Spies," (Proofpoint, November 2021), 48, https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-threat-insight-paper-triple-threat-N-Korea-aligned-TA406-steals-scams-spies.pdf.

39. Patricia Kowsmann and Caitlin Ostroff, "$76 Billion a Day: How Binance Became the World's Biggest Crypto Exchange," *The Wall Street Journal*, November 11, 2021, https://www.wsj.com/articles/binance-became-the-biggest-cryptocurrency-exchange-without-licenses-or-headquarters-thats-coming-to-an-end-11636640029; Tom Schoenberg, "Binance Faces Probe by U.S. Money-Laundering and Tax Sleuths," Bloomberg, May 13, 2021, https://www.bloomberg.com/news/articles/2021-05-13/binance-probed-by-u-s-as-money-laundering-tax-sleuths-bore-in.

40. Chainalysis team, "Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options," Chainalysis, February 9, 2021, https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack/.

41. "How to Buy Uniswap in North Korea," Glonvest, https://goinvest.io/uniswap/how-to-buy-uniswap-uni-in-north-korea; Uniswap, https://uniswap.org/.

42. Jason Bartlett, "How North Korea Might Exploit New Video Games for Crypto," The Diplomat, January 20, 2022, https://thediplomat.com/2022/01/how-north-korea-might-exploit-new-video-games-for-crypto/.

43. "김계연 [Kim Kye-yeon]"北해커 남한 온라인게임 털어 외화벌이(종합)" (North Korean Hackers Earn Foreign Currency by Knocking Off South Korean Online Games [Roundup]), Yonhap News, August 4, 2011, https://www.yna.co.kr/view/AKR20110804127800004.

44. Mark Arena, "Partners in Crime: North Koreans and Elite Russian-Speaking Cybercriminals," Intel 471, September 16, 2020, https://intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals/; Raphael Satter, "North Korean Hackers Are working with Eastern European Cybercriminals: Report," Reuters, December 11, 2019, https://www.reuters.com/article/us-usa-cyber-north-korea/north-korean-hackers-are-working-with-eastern-european-cybercriminals-report-idUSKBN1YF1KA.

45. Jason Bartlett and Francis Shin, "Sanctions by the Numbers: Spotlight on North Korea" (Center for a New American Security, February 8, 2021), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-north-korea.

46. Korea, North (Democratic People's Republic of Korea), "Citizenship Laws of the World," report no. IS-1 (U.S. Office of Personnel Management Investigations Service, March 2001), multiplecitizenship.com, https://www.multiplecitizenship.com/wscl/ws_NORTH_KOREA.html; "문경근" (Moon Kyung-geun), "北, 최근 20년간 동남아 3개국서 비밀공작" (North Korea, Secret Spying Operations in Three Southeast Asian Countries over Past 20 Years), *The Seoul Shinmun*, February 19, 2017, https://m.seoul.co.kr/news/newsView.php?id=20170220003012&wlog_tag3=daum; "조건희, 김동혁, 김정훈" (Cho Gyeon-hee, Kim Dong-hyuk, Kim Jung-hoon), "스님 행세하며 암약…9년만에 '직파 간첩' 잡았다" (Pretending to Be a Monk . . . Spy Caught after 9 Years), *Dong-A Ilbo*, July 5, 2019, https://www.donga.com/news/View?gid=96683699&date=20190725; Claire Lee, "A Life Stranger Than Fiction," *The Korea Herald*, December 6, 2013, http://www.koreaherald.com/view.php?ud=20131206000769.

47. "United States Citizen Pleads Guilty to Conspiring to Assist North Korea in Evading Sanctions," U.S. Department of Justice, press release, September 27, 2021, https://www.justice.gov/usao-sdny/pr/united-states-citizen-pleads-guilty-conspiring-assist-north-korea-evading-sanctions; Jason Bartlett, "U.S. Citizen Helped North Korea Evade Sanctions through Blockchain," The Diplomat, September 28, 2021, https://thediplomat.com/2021/09/us-citizen-helped-north-korea-evade-sanctions-through-blockchain/.

48. David Carlisle and Kayla Izenman, "Closing the Crypto Gap," Royal United Services Institute, April, 2019, https://static.rusi.org/20190412_closing_the_crypto_gap_web.pdf.

49. Mark Arena, "Partners in Crime: North Koreans and Elite Russian-Speaking Cybercriminals"; Raphael Satter, "North Korean Hackers Are Working with Eastern European Cybercriminals."

50. Jeong Tae Joo, "Around 100 Top Technology University Graduates Join Military," Daily NK, May 18, 2020 (translated by Jason Bartlett), https://www.dailynk.com/english/around-100-top-technology-university-graduates-join-military/.

51. Headquarters, Department of the Army, *North Korean Tactics*, ATP 7-100.2, (July 2020), https://irp.fas.org/doddir/army/atp7-100-2.pdf.

52. "N.K. Establishes University Named after Leader Kim," Yonhap News Agency, October 14, 2020, https://en.yna.co.kr/view/AEN20201014003000325.

53. David E. Sanger and Martin Fackler, "N.S.A Breached North Korean Networks before Sony Attack, Officials Say," *The New York Times*, January 18, 2015, https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html; Jordan Robertson, Dune Lawrence, and Chris Strohm, "Sony's Breach Stretched from Thai Hotel to Hollywood," Bloomberg, December 7, 2014, https://www.bloomberg.com/news/articles/2014-12-07/sony-s-dark-seoul-breach-stretched-from-thai-hotel-to-hollywood.

54. David Carlisle and Kayla Izenman, "Closing the Crypto Gap."

55. "Bangladesh Bank Heist Was 'State-Sponsored': U.S. Official," Reuters, March 29, 2017, https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-heist-was-state-sponsored-u-s-official-idUSKBN1700TI; Jason Bartlett, "Mun Chol Myong: The First-Ever North Korean Criminal Facing Extradition to the U.S."

56. David Carlisle and Kayla Izenman, "Closing the Crypto Gap."

57. "North Korean in Malaysia Loses Final Appeal against U.S. Extradition," Malay Mail, March 9, 2021, https://www.malaymail.com/news/malaysia/2021/03/09/north-korean-in-malaysia-loses-final-appeal-against-us-extradition/1956186.

58. Jason Bartlett, "Why Is North Korea So Good at Cybercrime?" The Diplomat, November 13, 2020, https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime/.

59. "How to Buy Uniswap in North Korea."

60. Sujit Raman, "It's Time for National Cyber-Incident Reporting Legislation," Bloomberg Law, July 12, 2021, https://news.bloomberglaw.com/privacy-and-data-security/its-time-for-national-cyber-incident-reporting-legislation.

61. Alexander Mallin and Luke Barr, "DOJ Seizes Millions in Ransom Paid by Colonial Pipeline," ABC News, June 7, 2021, https://abcnews.go.com/Politics/doj-seizes-millions-ransom-paid-colonial-pipeline/story?id=78135821; "United States Files Civil Action to Return $150 Million in Embezzled Funds to Sony; FBI Tracks Money to Bitcoin," U.S. Department of Justice, press release, December 20, 2021, https://www.justice.gov/usao-sdca/pr/united-states-files-civil-action-return-150-million-embezzled-funds-sony-fbi-tracks.

62. How Is Coinbase Insured? Coinbase Help Center, Coinbase, https://help.coinbase.com/en/coinbase/other-topics/legal-policies/how-is-coinbase-insured.

63. Karen DeYoung, Ellen Nakashima, and Emily Rauhala, "Trump Signed Presidential Directive Ordering Actions to Pressure North Korea," *The Washington Post*, September 30, 2017, https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html.

64. "Treasury Sanctions Perpetrators of Serious Human Rights Abuse on International Human Rights Day," U.S. Department of Treasury, press release, December 10, 2021, https://home.treasury.gov/news/press-releases/jy0526.

65. Martyn Williams, "Russia Provides New Internet Connection to North Korea," 38 North, October 1, 2017, https://www.38north.org/2017/10/mwilliams100117/.

66. 김일억 [Kim Il-uk], "北 자체 인프라 활용한 전자상거래 꾸준히 발전 중" (North Korea Using Its Own Infrastructure to Steadily Develop E-Commerce)", Seoul Pyongyang News, April 26, 2021, http://www.spnews.co.kr/news/articleView.html?idxno=38626.

67. Exec. Order No. 13722, *Blocking Property of the Government of North Korea and Workers' Party of Korea, and Prohibiting Certain Transactions with Respect to North Korea, Code of Federal Regulations*, title 3, *Federal Register*, 81 no. 53 (March 18, 2016), 14943–46, https://home.treasury.gov/system/files/126/nk_eo_20160316.pdf; "Cyber-Related Designations; North Korea Designations; North Korea Designations Removals," U.S. Department of Treasury, March 2, 2020, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200302; "Two Chinese Nationals Charged with Laundering over $100 Million in Cryptocurrency from Exchange Hack," U.S. Department of Justice; Jason Bartlett and Megan Ophel, "Sanctions by the Numbers: Spotlight on Cyber Sanctions" (Center for a New American Security, May 4, 2021), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber.

68. Public Law 115, *Countering America's Adversaries through Sanctions Act*, 2017, 866-955, U.S. Statues at Large 44.

69. "United States–Republic of Korea Partnership," The White House, press release, May 21, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/21/fact-sheet-united-states-republic-of-korea-partnership/.

70. "State Spy Agency Says It Has Foiled 14 Hacking Attempts from Abroad This Year," Yonhap News Agency, November 8, 2021, https://en.yna.co.kr/view/AEN20211108005600325; "Korea to Fund Interpol Projects Combating Cyber-Enabled Crime," Interpol, February 11, 2020, https://www.interpol.int/en/News-and-Events/News/2020/Korea-to-fund-INTERPOL-projects-combating-cyber-enabled-crime; Catalin Cimpanu, "Ukrainian Police Arrest Clop Ransomware Members, Seize Server Infrastructure," The Record, June 16, 2021, https://therecord.media/ukrainian-police-arrest-clop-ransomware-members-seize-server-infrastructure/.

71. "Background Press Call on the Virtual Counter-Ransomware Initiative Meeting," The White House, press release, October 13, 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/10/13/background-press-call-on-the-virtual-counter-ransomware-initiative-meeting/.

72. "Cryptocurrency Meets Law Enforcement at Europol's 5th Virtual Currencies Conference," Europol, July 1, 2018, https://www.europol.europa.eu/media-press/newsroom/news/cryptocurrency-meets-law-enforcement-europol%E2%80%99s-5th-virtual-currencies-conference.

73. Phishing Tip Card, U.S. Department of Homeland Security, https://www.cisa.gov/sites/default/files/publications/Phishing%20508%20compliant%20508%20compliant.pdf.

74. Williams, "Russia Provides New Internet Connection to North Korea."

75. "How North Korea Revolutionized the Internet As a Tool for Rogue Regimes," Recorded Future, February 9, 2020, https://www.recordedfuture.com/north-korea-internet-tool/.

76. Sebastian Anthony, "North Korea Kicked Off the Internet by Giant DDos: Was It the USA, or Someone Else?" Extreme Tech, December 23, 2014, https://www.extremetech.com/extreme/196375-north-korea-kicked-off-the-internet-by-giant-ddos-was-it-the-usa-or-someone-else.

77. "Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity," The White House, press release, August 25, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, DC, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan.


Center for a
New American
Security