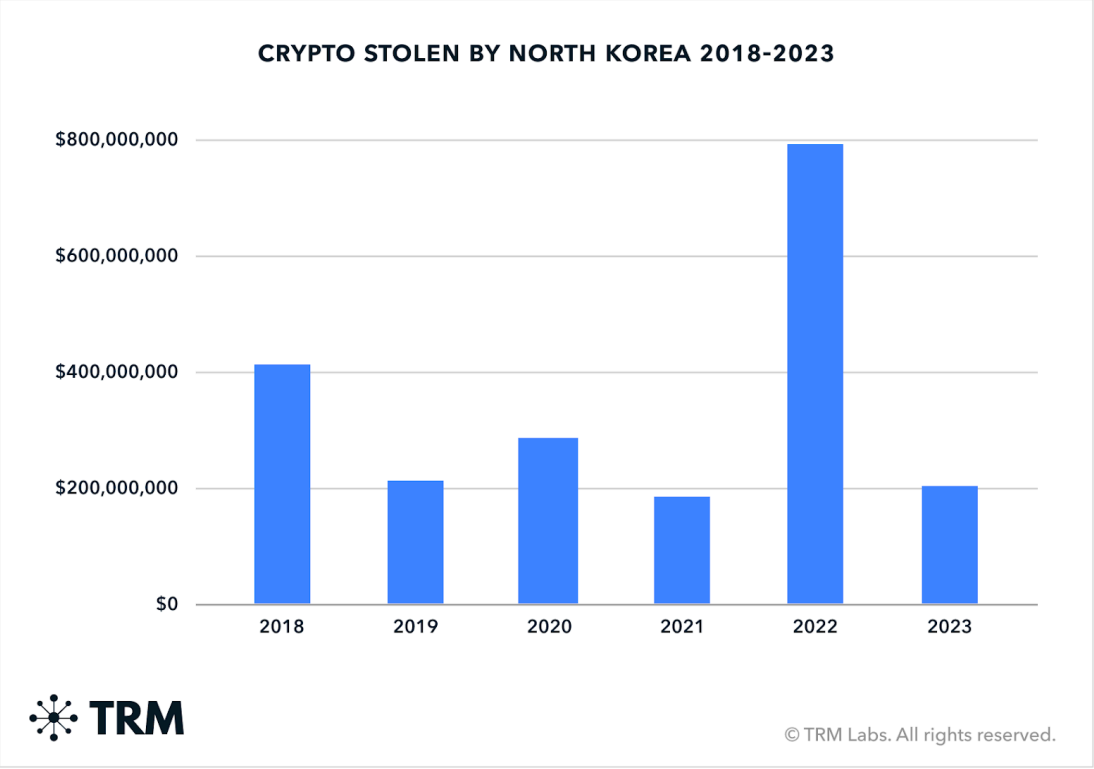
Inside North Korea's Crypto Heists: $200M in Crypto Stolen in 2023; Over $2B in the Last Five Years | TRM Blog

Archived: 2026-04-05 13:42:16 UTC

Over the past five years, North Korean hackers have stolen over USD 2 billion in cryptocurrencies in over 30 attacks, according to TRM Labs. While reports have indicated the amount of crypto stolen by North Korea since 2018 to be as high as $3 billion, our research indicates that this figure likely includes multiple large hacks misattributed to North Korea.

In 2023, although the total amount stolen in cryptocurrency attacks is down from a record-setting 2022, North Korea has maintained its focus on the crypto ecosystem. Year-to-date, North Korea has stolen USD 200 million in cryptocurrency, accounting for over 20% of all stolen crypto this year.

North Korean cyberattacks have been successful. In fact, their hacks in 2023 are 10 times larger than attacks by other actors.



North Korean Hackers Continue To Evolve Their Targets, Techniques, and Money Laundering Patterns in a Multi-Chain Crypto Landscape

North Korean hacks appear to be opportunistic – reflected by an array of target and exploit types that have resulted in unprecedented gains.

In recent years, North Korea has almost exclusively targeted the DeFi ecosystem. Cross-chain bridges, which hold increasing volume, are a continued target. In 2022, North Korea stole over USD 800 million in three attacks against cross-chain bridges.

North Korea exploits vulnerabilities in the crypto ecosystem in a variety of ways including through phishing and supply chain attacks, and through infrastructure hacks which involve private key or seed phrase compromises. These types of attacks are often enabled by conventional cyber operations and allow the attackers to seize and transfer the cryptocurrency to wallets they control. According to the FBI, North Korea conducted the largest cryptocurrency hack on record, stealing USD 625 million from Ronin Bridge in March 2022 using stolen private keys.

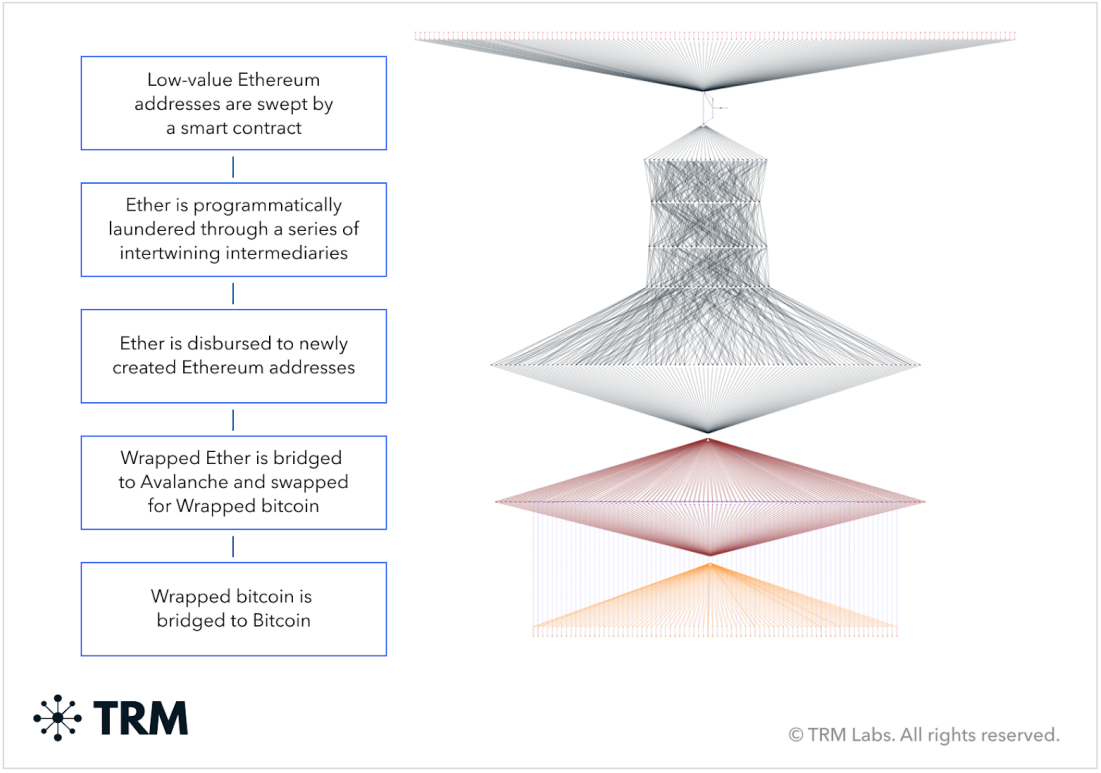
While North Korea's targets and techniques have evolved over time, so has their on-chain laundering methodologies. North Korea's early exploits – which tend to involve the direct use of cryptocurrency exchanges – now feature highly complex, multi-stage money laundering processes in response to more aggressive OFAC sanctions, law enforcement focus, and improved tracing capabilities. A 2023 hack by North Koreans on Atomic Wallet exemplifies this evolution.

A Profile of North Korea's 2023 Atomic Wallet Hack

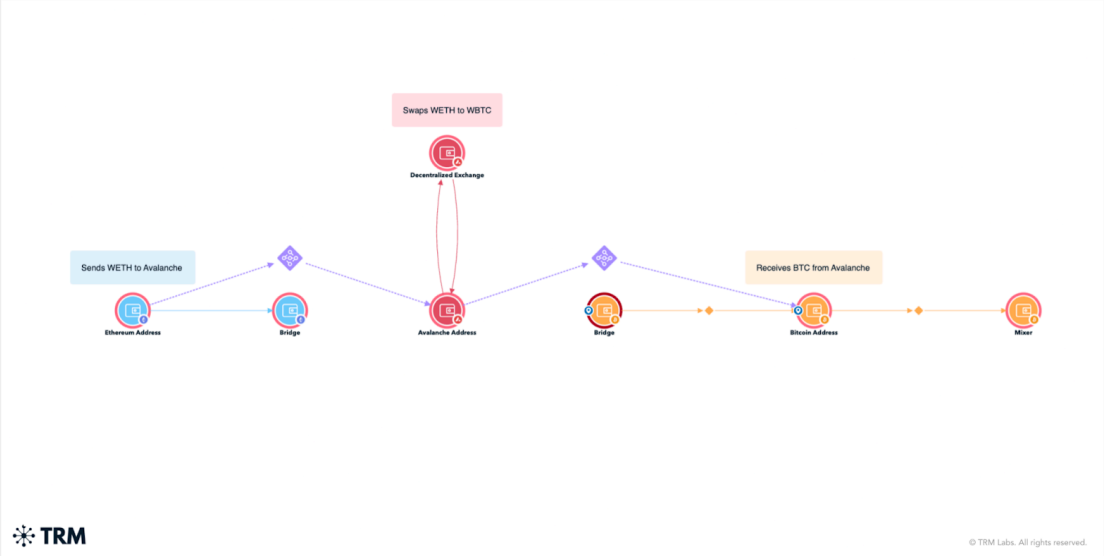
On June 3, 2023, North Korean hackers targeted users of Atomic Wallet, a non-custodial wallet provider, resulting in the theft of approximately USD 100 million worth of cryptocurrency, from over 4,100 individual addresses. The nature of the attack on Atomic Wallet indicates that the exploit was most likely carried out through a phishing or supply chain attack.

The hackers drained victims' wallets on the Ethereum, Tron, Bitcoin, XRP, DOGE, Stellar, and Litecoin blockchains, and sent funds to freshly created addresses under their control. ERC-20 and TRC-20 tokens were swapped to native assets (Ether and Tron) through decentralized exchanges, and then laundered through a range of complex techniques including the use of automated software programs, mixers and cross-chain swaps.

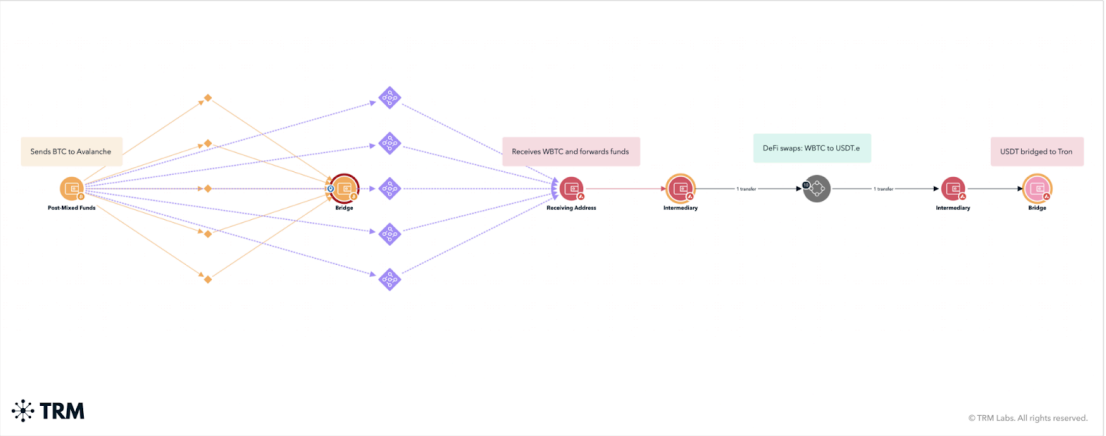
The hackers – who operate brazenly without fear of being caught as they operate almost exclusively inside North Korea – then drain high value wallets rapidly and send the funds directly to centralized exchanges in a race to off-ramp the funds. Once the hack is discovered, hackers then move the funds through a series of more complex laundering techniques, stages of which have been visualized in TRM Forensics software below.



Stages of Atomic Wallet hack visualized in TRM Forensics: ETH is programmatically laundered through several layers of intermediaries with intertwining paths, before exiting to ninety two (92) first-time Ethereum addresses. WETH is then bridged to Avalanche blockchain, swapped to WBTC and then bridged to the Bitcoin blockchain.



Stages of Atomic Wallet hack visualized in TRM Forensics: WETH from Ethereum is bridged to Avalanche, swapped for WBTC, bridged to Bitcoin, and then sent to a mixing service.



Stages of Atomic Wallet hack visualized in TRM Forensics: Post-mixed bitcoin is bridged to Avalanche, where the receiving address forwards funds to an intermediary address. A decentralized exchange is used to swap WBTC for USDT.e with the USDT.e being forwarded to a new address - rather than returned to the initiator. This provides an additional layer of obfuscation to the flow of funds. USDT.e is then bridged to the Tron blockchain.

The Role of Blockchain Intelligence in Following North Korean Stolen Funds

North Korea's recent Atomic Wallet hack is one example of its evolved obfuscation techniques in a multi and cross-chain ecosystem. Blockchain intelligence – blockchain data enriched with open-source and proprietary threat intelligence – as represented by TRM Forensics in the Atomic Wallet hack profile, enables investigators to follow the money in cryptocurrency to ultimately identify threat actors and seize illicit funds including funds stolen and laundered by North Korea.

In 2019, in response to the growing number of blockchains and the growing use of different chains by cybercriminals, TRM Labs introduced cross-chain analytics in TRM Forensics, our flagship tracing tool. This enables investigators to trace funds from multiple blockchains and multiple assets in a single visualization.

In 2022, TRM identified the growing use of chain-hopping as an obfuscation technique, and introduced TRM Phoenix, the industry's first solution for automatically tracing the flow of funds across blockchains through bridges and other services.

As North Korea continues to attack the growing crypto ecosystem, the ability to follow stolen funds is more critical than ever, and, as North Korea's laundering methodologies evolve so must the tools investigators rely on.

Source: https://www.trmlabs.com/post/inside-north-koreas-crypto-heists