TRM

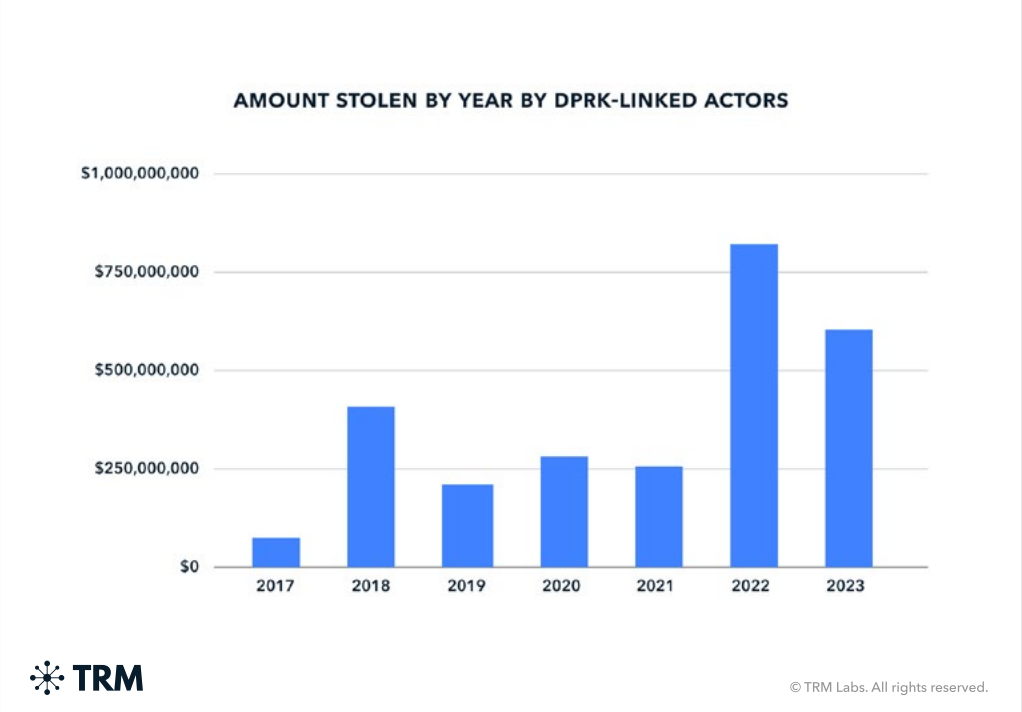
TRM on the North Korea Threat

An Update on Cyber Activity and Cryptocurrency Theft

trmlabs.com

Nearly USD 3 billion worth of cryptocurrency has been lost to Pyongyang-linked threat actors since 2017. In 2023, hackers tied to North Korea stole approximately USD 700 million in cryptocurrency, according to research by TRM Labs.

That was over a third of all funds stolen in crypto attacks last year, despite an approximately 20% reduction from the USD 850 million haul in 2022. On average, hacks perpetrated by North Korea in 2023 resulted in ten times more losses than those perpetrated by other actors.



With nearly USD 1.5 billion stolen in the past two years alone, North Korea's hacking prowess demands continuous vigilance and innovation from business and governments as well as a deep understanding of the ways in which its cyber actors move and launder stolen funds.

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

TRM has observed North Korean actors conduct phishing and supply chain attacks, as well as infrastructure hacks that 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 cryptocurrency to wallets they control.

In 2023, North Korean operatives typically followed a phased process to launder cryptocurrency assets. According to TRM's on-chain analysis, funds were usually immediately swapped from USDT or USDC into native assets like Ethereum. This is likely because, as centrally issued tokens, USDT and USDC can be frozen, unlike decentralized native currencies such as Ethereum. These funds are then often held in stasis for weeks or even months. This delay is possibly the result of a backlog of assets needing to be laundered given the large sums stolen last year by North Korean hacker groups.

Once North Korean hackers begin the laundering process in earnest, the parked assets are quickly moved through swap services and then pushed through cross-chain bridges. The first destination of these funds is almost always Bitcoin. Until late-2022, the preferred bridge for these kinds of cross-chain movements was the Ren Bridge. However, Ren was wholly owned by FTX and was shut down following its collapse...

Throughout the first half of 2023, North Korean hackers heavily favored the Avalanche Bridge to transfer funds to Bitcoin, as described in TRM's recent report on North Korean crypto thefts.

In the second half of 2023, North Korean hackers began to diversify the bridges they use. They also began reducing the value of individual bridging transactions while increasing the velocity of transactions in an apparent effort to evade interdictions.

North Korean Hackers Leveraged an Evolving Roster of Mixers and Over-the-Counter Brokers

Having been bridged to Bitcoin, the hacked funds are funneled into a handful of Bitcoin mixing services. Throughout much of 2023, North Korea's mixing service of choice was Sinbad. However, just as North Korea's hackers diversified bridging services, they also began using other mixers as the year unfolded. These services included YoMix, Wasabi Wallet and CryptoMixer.

For account-based blockchains, North Korean hackers used several mixing services in 2023, most notably Railgun, in an attempt to launder the proceeds of the Harmony Bridge hack in January. North Korean hackers also consistently used ZKWrapper, a USDT-anonymization service on the Tron blockchain. Towards the end of 2023, TRM also observed North Korean hackers returning to Tornado Cash, a service they had largely abandoned following its designation by OFAC.

Following the bridging and mixing processes described above, North Korean hackers have typically ended their laundering process by converting funds to USDT and transferring them to the Tron blockchain. Given its popularity with Chinese users – who are nominally forbidden from using cryptocurrencies – the Tron blockchain is populated by many high-volume brokers servicing Chinese customers through informal financial channels.

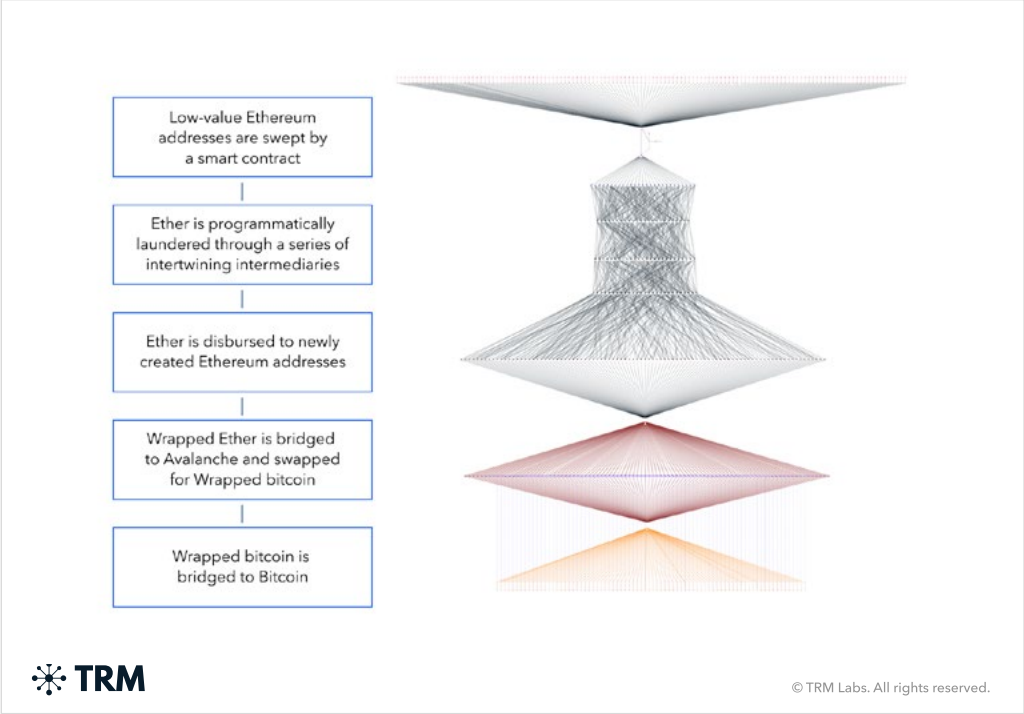
A Profile of North Korea's 2023 Atomic Wallet Hack

The 2023 hack by North Korea on Atomic Wallet exemplifies the evolution and sophistication of North Korea's crypto laundering.

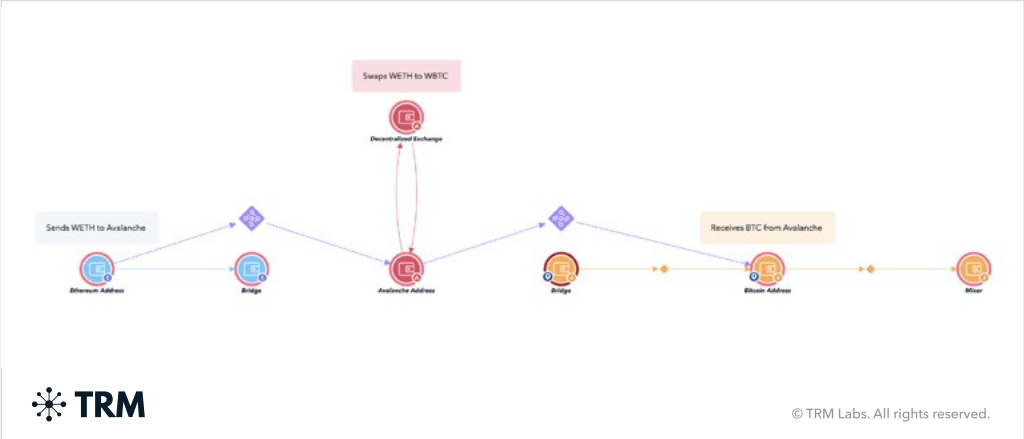
On June 3, 2023 North Korean hackers targeted users of Atomic Wallet, a non-custodial wallet provider. The hack resulted in the theft of approximately USD 100 million worth of cryptocurrency from over 4,100 individual addresses. The exploit was most likely carried out through a phishing or supply chain 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 key stages of the Atomic Wallet hack are visualized in the TRM Forensics graph below:



It shows ETH programmatically laundered through several layers of intermediaries with intertwining paths, before exiting to 92 first-time Ethereum addresses. WETH is then bridged to the 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.

As shown in TRM's analysis below, ETH and BSC assets were swapped into unfreezable native assets and then parked. The Polygon/MATIC funds were swapped and bridged via Squid Router. After further swaps, generally from MATIC to USDT or USDC, they were moved to Avalanche. On Avalanche, they were swapped into wrapped BTC, then bridged to Bitcoin, where they sat until they were liquidated as USDT on Tron. This type of activity is a hallmark of recent Lazarus Group exploits.

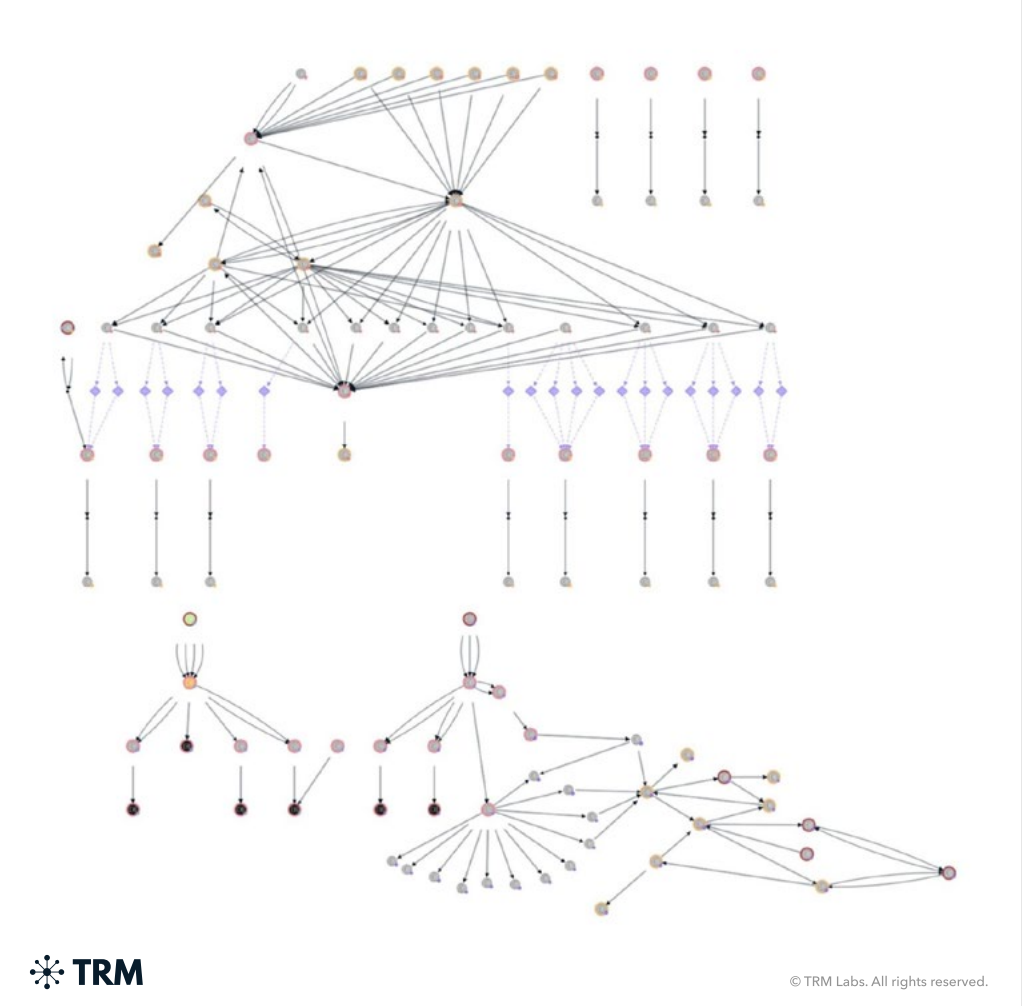


Figure 1 shows that the hackers quickly moved the stolen funds across multiple currencies and multiple chains

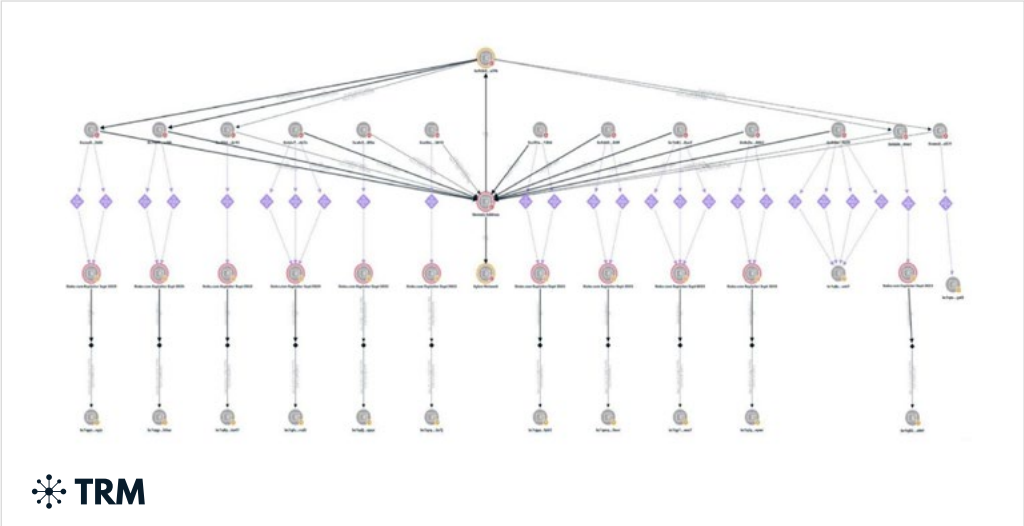


Figure 2 shows a closer look at some of the specific cross-chain swaps from AVAX to Bitcoin

North Korea Will Continue To Prioritize Speed and Tools Continue To Improve

TRM assesses that North Korean hackers will continue to prioritize speed and automation over anonymity as transaction monitoring tools constantly reduce latency. These hackers operate under unique circumstances: because they are based almost exclusively inside North Korea or friendly third countries, they face little risk of arrest or extradition. As such, they have little motivation to achieve the kind of anonymity other hackers require.

The reasons for the relatively low level of activity from North Korean hackers in the first half of 2023 are not totally clear. However, depressed crypto prices and a large backlog of funds from the Ronin and Harmony Bridge hacks are likely to have played a role. Remaining backlogs from the Poloniex and HTX Bridge hacks, as well as the Orbit Bridge hack – which we suspect was perpetrated by North Korea hackers – may slow down hacking activity in the first half of 2024. However, hacking efforts may accelerate in the second half of the year as they did in 2023.

The techniques used by North Korea hackers evolve in response to advances in law enforcement. Continued action from the Member States - such as potential additional sanctions against mixing services, regulations targeting bridges and swap services, or potential criminal investigations against these services or the brokers who liquidate mixed funds - will likely prompt additional adaptation.

The Role of Blockchain Intelligence in Following North Korea Stolen Funds

As North Korea's laundering methodologies evolve, so must the tools on which investigators rely.

Blockchain intelligence – blockchain data enriched with open-source and proprietary threat intelligence – 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.

TRM is a provider of Blockchain Intelligence solutions. In response to the growing number of blockchains, and their use by illicit actors, TRM introduced the idea of cross-chain analytics in order to enable investigators to trace funds across multiple blockchains and assets in a single visualization. TRM has also developed the capability to automatically trace the flow of funds across blockchains through bridges and other services.