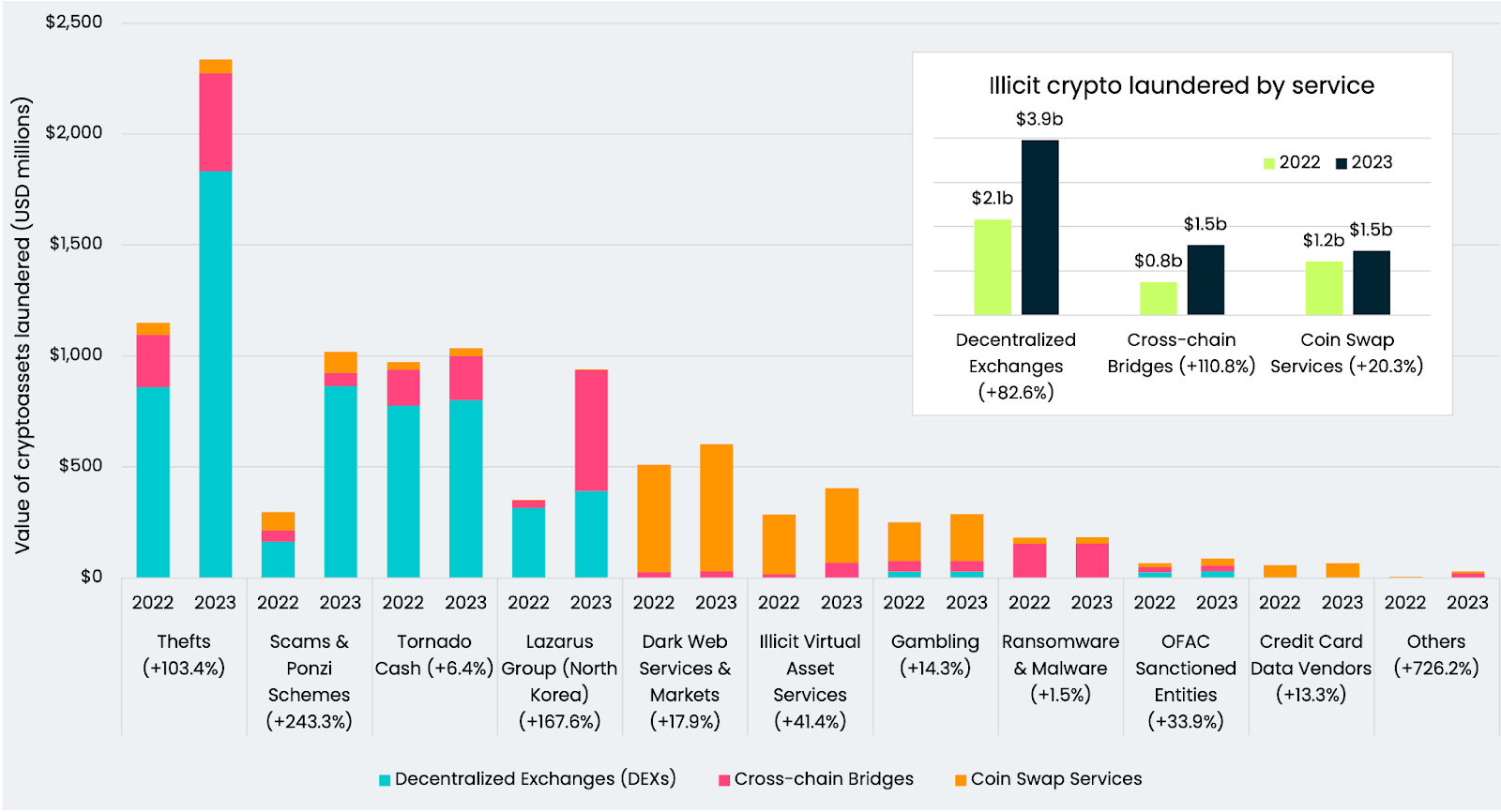
**North Korea-linked APT group Lazarus has laundered $900 million worth of cryptocurrency, Elliptic researchers reported.**



Researchers from blockchain analytics firm Elliptic reported that threat actors have already laundered a record $7 billion through cross-chain crime.

The term “Cross-chain crime” is used to refer to the swapping of crypto assets between different tokens or blockchains to launder illegally gained funds.

North Korea-linked Lazarus Group laundered $900 Million in cryptocurrency between July 2022 and July 2023.

“The biggest rise of cross-chain crime is apparent in the field of crypto thefts, scams and Ponzi schemes and illicit laundering perpetrated by North Korea’s Lazarus Group. This elite cybercrime organization alone is now responsible for approximately 1/7th of all cross-chain crime we are tracking, having laundered over $900 million through these methods.” reads the report published by Elliptic.

Law enforcement operations recently targeted multiple mixers for this reason threat actors, both nation-state actors and cybercrime groups, switched to chain- or asset-hopping typologies to launder the stolen assets. Furthermore, threat actors are exploiting the absence of efficient capabilities in mainstream blockchain analytics solutions to identify and oversee cross-chain activities

North Korea money laundering

Timeframes denote cumulative calculations as of July of each year. They are not annual figures

According to another report recently published by Elliptic, in the past 104 days, the North Korea-linked APT group Lazarus has stolen most of $240 million in crypto assets from multiple businesses, including Atomic Wallet ($100m), CoinsPaid ($37.3M), Alphapo ($60M), and Stake.com ($41M).

The group is also suspected to have recently stolen $31 million from the professional global cryptocurrency exchange CoinEx.

“For virtual asset services and law enforcement investigators, this has major implications for detecting, tracing and mitigating this new era of crypto crime. This in particular affects cross-chain services, including DEXs and bridges. For developers of such services to continue innovating and playing their crucial part in enhancing the wider decentralized finance ecosystem, these risks need to be addressed and managed.” concludes the report