North Korea's Top APT Swindled $1B From Crypto Investors in 2022

By Nate Nelson

Published: 2023-01-25 · Archived: 2026-04-05 13:49:25 UTC

Source: Cavan Images via Alamy Stock Photo

The blockchain industry hemorrhaged money last year, with the global market for cryptocurrencies plummeting 63%. But investors didn't only lose money to half-baked coins and overhyped NFTs.

In a report published today, researchers from Proofpoint detailed how North Korean state-backed hackers managed to siphon more than $1 billion dollars in cryptocurrencies and other blockchain assets in the 2022 calendar year (all the more impressive considering how depressed those assets had become).

Proofpoint attributed the success of the TA444 group and related clusters — variously referred to as APT38, Bluenoroff, BlackAlicanto, Stardust Chollima, and Copernicium — to their startup-like approach.

Hallmarks, the researchers said, include "rapid iteration, testing products on the fly, and failing forward." The group regularly experiments with new methods of intrusion, and has cycled through different and better malware in recent years.

"While we do not know if the group has ping-pong tables or kegs of some overrated IPA in its workspace," the authors wrote, "TA444 does mirror the startup culture in its devotion to the dollar and to the grind."

TA444's Evolving Threat

There's an element of "move fast and break things" to TA444.

In recent years, the group has iterated on their social engineering tactics many times over. Sometimes it sent private messages from hijacked LinkedIn accounts of representatives from legitimate companies, other times it abused email marketing tools in order to circumvent spam filters. It has engaged with victims in English, but also Japanese, Polish, and Spanish.

In one oddball case, it email-blasted organizations across the US healthcare, education, finance, and government sectors, using barebones, typo-laden phishing lures. At best, their lures made reference to specific brand names in the industry, sometimes promising salary increases or job opportunities, but the efforts here were mainly rudimentary.

Where other cybercrime groups may focus on perfecting social lures and delivery mechanisms, researchers explained that malware creation is where TA444 really distinguishes itself.

Their collection of post-exploitation backdoors has included the msoRAT credential stealer, the SWIFT money laundering framework DYEPACK, and various passive backdoors and virtual "listeners" for receiving and processing data from target machines.

"This suggests that there is an embedded, or at least a devoted, malware development element alongside TA444 operators," according to the report.

North Korea: The OG Crypto Bro

To supplement its maladroit command economy, the government of North Korea has long used hackers for fundraising, targeting wherever a financial opportunity happens to lie. That includes everything from retailers in the United States to the SWIFT banking system, and, in one notorious case, the entire world.

Because cryptocurrency companies offer few safeguards against theft, transactions are generally irreversible, and parties to those transactions are difficult to identify, the industry is rife with financially motivated cybercrime. North Korea has been dipping into this well for years, with campaigns against startups, botnets that mine coins, and ransomware campaigns soliciting crypto payments.

Last year, though, the scale of the theft reached a new level. Blockchain research firm Chainalysis assessed that the country stole nearly $400 million dollars in cryptocurrency and blockchain assets in 2021. In 2022, they surpassed that figure with a single attack — against a blockchain gaming company called SkyMavis — estimated to be worth over $600 million at the time. Add in other attacks throughout the calendar year, and their total haul reaches 10 figures.

"While we may poke fun at its broad campaigns and ease of clustering," the researchers warned, "TA444 is an astute and capable adversary."

Proofpoint's report noted that monitoring for MSHTA, VBS, Powershell, and other scripting-language execution from new processes or files can help detect TA444 activity. It also recommended using best practices for a defense-in-depth approach to combat TA444 intrusions: Using network security monitoring tools, using robust logging practices, a good endpoint solution, and an email monitoring appliance, in addition to training the workforce to be aware of heist activity that stems from contact on WhatsApp or LinkedIn.

"Additionally, given the credential phishing campaign activity we observed, enabling MFA authentication on all externally accessible service would help limit the impact of credentials eventually getting stolen," the researchers said via email.

About the Author

Contributing Writer

Nate Nelson is a journalist and scriptwriter. He writes for "Darknet Diaries" — the most popular podcast in cybersecurity — and co-created the former Top 20 tech podcast "Malicious Life." Before joining Dark Reading, he was a reporter at Threatpost.
