North Korean cryptocurrency hackers expand target list

By Tonya Riley

Published: 2023-01-25 · Archived: 2026-04-02 11:22:32 UTC

North Korean hackers known for cryptocurrency heists are expanding their targets to include education, government and healthcare, according to researchers tracking the group. The activity could be a sign that the group, which is suspected in two high-profile cryptocurrency hacks in 2022, may have even bigger plans for 2023.

Researchers at the cybersecurity firm Proofpoint observed in early December a massive wave of phishing emails from a cluster of North Korea-related hacking activity linked to TA444, the firm's name for the group. The latest campaign, which blasted more emails than researchers attributed to that group in all of 2022, tried to entice users to click a URL that redirected to a credential harvesting page.

Proofpoint could not disclose the specifics about targets for confidentiality reasons, but most related to finance in some way. Documents attached in the emails included titles like "Profit and Loss," "Invoice and statement receipts" and "Salary adjustments." The malicious emails also included lures mentioning "analyses of cryptocurrency blockchains, job opportunities at prestigious firms, or salary adjustments" according to the report. To help avoid phishing detection tools, TA444 uses email marketing tools to engage with targets.

Researchers say that the campaign is unusual for a few reasons. Technically, it deviates from the group's previous activity in that the hackers focused on trying to steal the target's login and passwords rather than a direct deployment of malware.

The bigger question is why a group known to be financially motivated would target government and education sectors alongside the far more lucrative financial sector. TA444, like other clusters of activity associated with the North Korean government, is almost exclusively financially motivated. In more recent years, North Korean hackers have honed in especially on the cryptocurrency industry.

TA444 has overlapped with Lazarus, a group of North Korean hackers to which the FBI attributed a record $600 million dollar cryptocurrency attack on Ronin Bridge, the infrastructure that connected the Axie Infinity video game with the Ethereum blockchain. The FBI on Monday attributed a separate $100 million hack of the Harmony Bridge to the group after the hackers recently tried to launder $60 million worth of currency stolen in the heist.

The December campaign comes on the heels of a noticeable shift in delivery tactics researchers began to notice in the fall, demonstrating that the group might be taking on more of a "start-up" mentality, Proofpoint researchers wrote.

"We can't always derive the motive behind shifts in strategy. But we may have the answer later, when we see more of these attacks," said Alexis Dorais-Joncas, senior manager of threat research at Proofpoint. "It might be a one-off. It might be a test to see how much success they could have hacking other types of organizations. But right now, it's not really clear to us why they are actually doing that."

Researchers at Kaspersky in December also noted North Korean hackers pivoting malware delivery methods. They found that hackers had created numerous fake domains, most of them imitating Japanese venture capital firms. Domains flagged by Proofpoint also included attempts to spoof Japanese financial institutions.

Proofpoint could not rule out that another actor had compromised TA444's server or that the group was potentially moonlighting for other purposes, which could signal more differentiation in targets going forward.
