Radiant links $50 million crypto heist to North Korean hackers

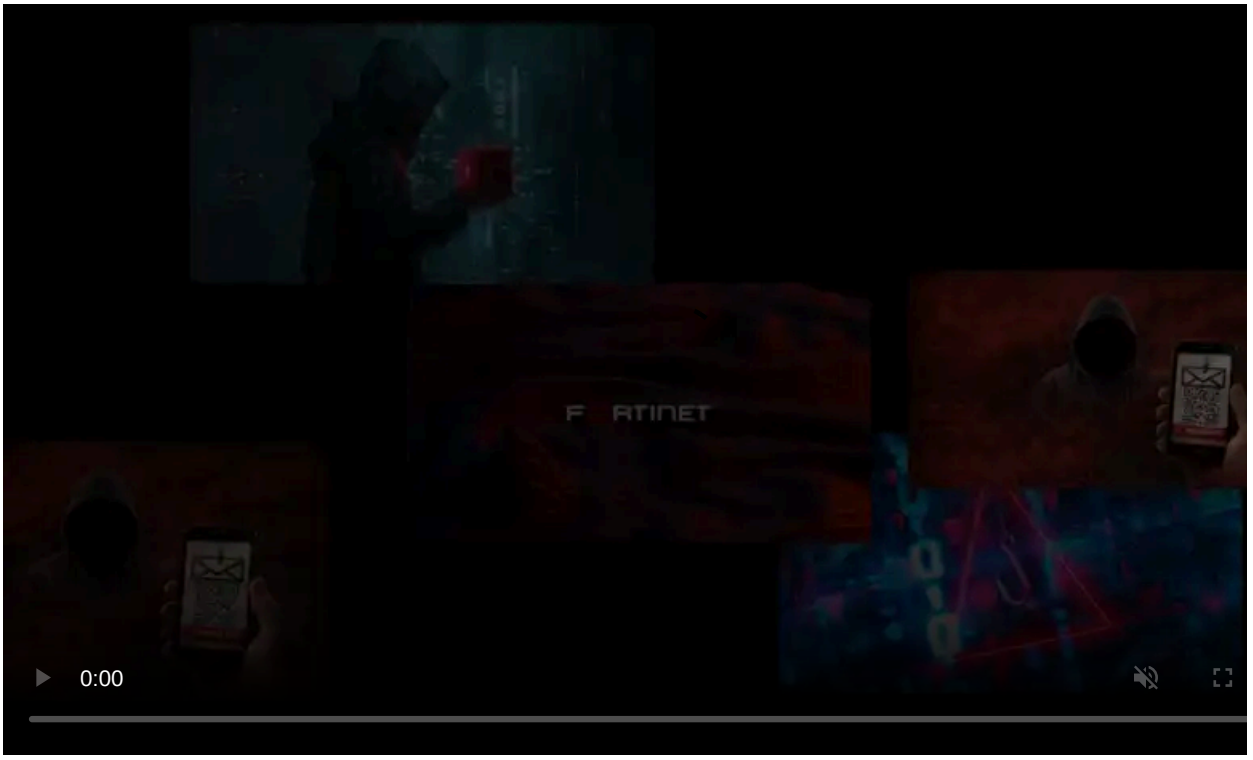
By Bill Toulas

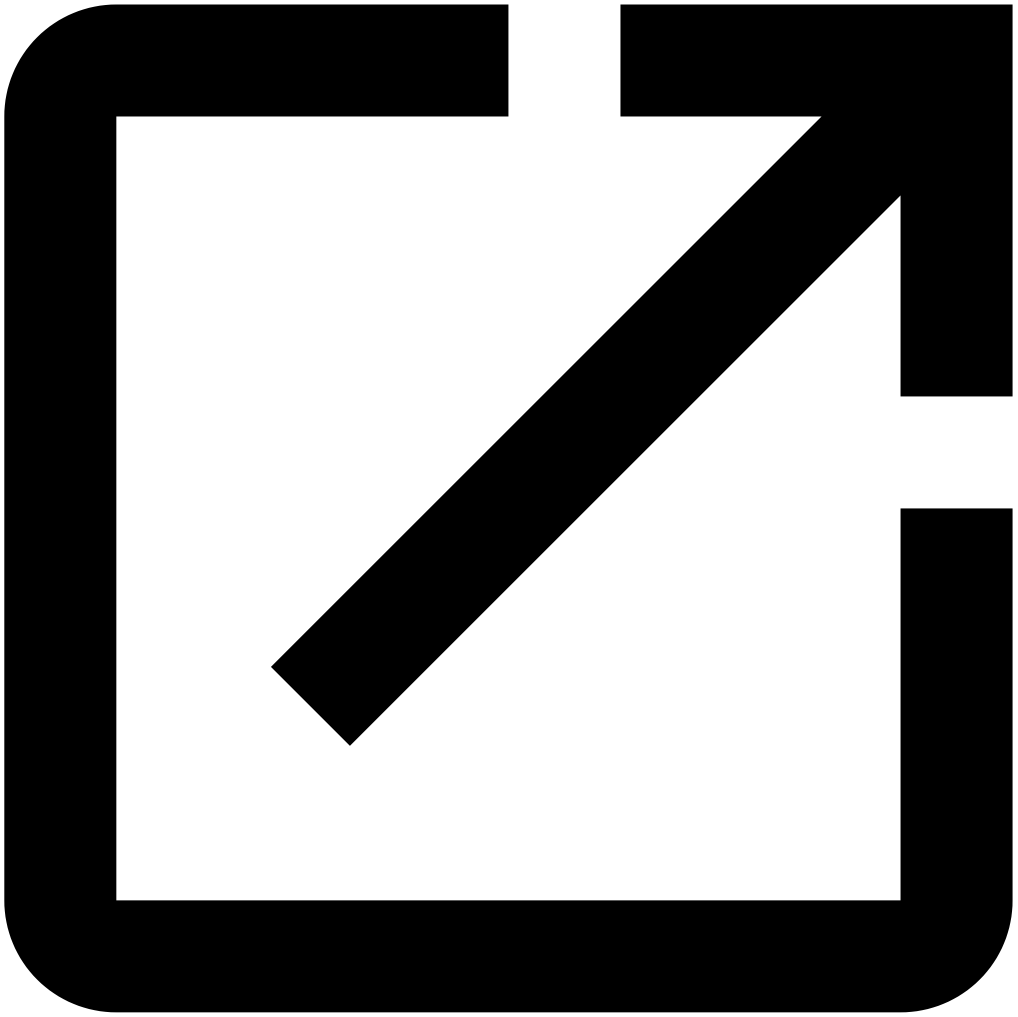
Published: 2024-12-09 · Archived: 2026-04-06 00:36:07 UTC

Radiant Capital now says that North Korean threat actors are behind the $50 million cryptocurrency heist that occurred after hackers breached its systems in an October 16 cyberattack.

The attribution comes after investigating the incident, assisted by cybersecurity experts at Mandiant, who say the attack was conducted by North Korean state-affiliated hackers known as Citrine Sleet, aka "UNC4736 and "AppleJeus."

The US previously warned that North Korean threat actors targeting cryptocurrency firms, exchanges, and gaming companies to generate and launder funds to support the country's operations.


F RTINET
0:00



October incident

Radiant is a decentralized finance (DeFi) platform that allows users to deposit, borrow, and manage cryptocurrency across multiple blockchain networks.

The platform utilizes Ethereum blockchain security through the Arbitrum Layer 2 scaling system and operates under a community-driven system enabling users to participate in governance through RDNT lockers, submit proposals, and vote on active initiatives.

On October 16, 2024, Radiant announced it suffered a $50M breach caused by 'sophisticated malware' targeting three trusted developers whose devices were compromised to execute the unauthorized transactions.

The hackers appeared to have exploited the routine multi-signature process, collecting valid signatures under the guise of transaction errors and stealing funds from Arbitrum and Binance Smart Chain (BSC) markets.

The attack bypassed hardware wallet security and multiple verification layers, and transactions appeared normal during manual and simulation checks, indicative of high sophistication.

Finger pointed at North Korea

Following an internal investigation of the attack, aided by Mandiant, Radiant could now share more information about the malware used and the perpetrators behind it.

The attack started on September 11, 2024, when a Radiant developer received a Telegram message spoofing a former contractor, tricking them into downloading a malicious ZIP file.

The archive contained a PDF file to be used as a decoy and a macOS malware payload named 'InletDrift,' which established a backdoor on the infected device.

Decoy PDF file used in the attack

Source: Radiant

Radiant says the attack was so well-designed and flawlessly executed that it bypassed all security measures in place.

"This deception was carried out so seamlessly that even with Radiant's standard best practices, such as simulating transactions in Tenderly, verifying payload data, and following industry-standard SOPs at every step, the attackers were able to compromise multiple developer devices," explained Radiant.

"The front-end interfaces displayed benign transaction data while malicious transactions were signed in the background. Traditional checks and simulations showed no obvious discrepancies, making the threat virtually invisible during normal review stages."

Mandiant assessed with high confidence that the attack was conducted by UNC4736, the same threat group that was exposed for exploiting a zero-day vulnerability on Google Chrome earlier this year.

Given the successful bypass of its security measures, Radiant underlines the need for more robust, device-level solutions to enhance transaction security.

As for the stolen funds, the platform says it is collaborating with U.S. law enforcement and zeroShadow to recover any amounts possible.
