EINPRESSWIRE

The Lazarus Hack of CoinsPaid: How Attackers Stole and Laundered $37M USD

CoinsPaid was attacked by Lazarus Group, resulting in the theft of 37.3M USD. The conducted investigation was able to trace the money trail of perpetrators.

TALLINN, ESTONIA, August 9, 2023 /EINPresswire.com/ -- On July 22nd, 2023, CoinsPaid ecosystem was attacked by allegedly Lazarus Hacking Group, resulting in the theft of 37.3M USD. In collaboration with Match Systems, CoinsPaid conducted its own investigation and was able to trace the attack by minute, as well as track the money trail of perpetrators. The full story is available in CoinsPaid blog article.

Hackers Tracked CoinsPaid for 6 Months:
- March 2023: CoinsPaid registers constant unsuccessful attacks on the company of various kinds, including social engineering, DDos and BruteForce.
- April-May 2023: Hackers conducted 4 major attacks on our systems to gain access to accounts of CoinsPaid employees and customers.
- June-July 2023: Perpetrators aggressively tried to bribe and fake-hire critical company personnel.
- July 7, 2023, a massive, carefully planned and prepared attack was executed targeting CoinsPaid infrastructure and applications. From 20:48 to 21:42, we registered unusually high network activity: over 150,000 different IP addresses were involved.

The hackers' plan involved tricking a critical employee into installing software to gain remote control of a computer for the purpose of infiltrating and accessing CoinsPaid's internal systems.

A fake job offer that resulted in a theft of 37M USD:

Disguising themselves as recruiters from top crypto companies, perpetrators contacted our employees via LinkedIn and various Messengers, offering lucrative salaries: 16,000-24,000 USD a month. One of CoinsPaid's employees responded to a fake job offer from Crypto.com. In the course of the interview, they installed an application with malicious code disguised as a technical task. After opening the test task, hackers were able to steal profiles and keys from the computer and establish a connection with the company's infrastructure. Then the attackers exploited the vulnerability in the cluster to open a backdoor. Hackers were able to reproduce legitimate withdrawal requests to steal the funds from CoinsPaid operational storage vault.

The company's internal security measures set off the alarm system, enabling us to promptly halt the harmful actions and remove the hackers from our premises.

Blockchain Scoring Proves Ineffective Against Money Laundering:

Following the usual steps after a hacking incident, CoinsPaid informed major exchanges and cybersecurity companies and shared information about the hackers' addresses. They were then included in a markup to prevent the further movement and laundering of the funds associated with these addresses.
However, it takes about an hour for the markup to update. In comparison, CoinsPaid hackers managed to withdraw the funds in a matter of minutes. This problem makes blockchain scoring largely ineffective against money laundering in 2023.

The Money Trail: Tracing the Stolen Funds:
Right after the attack happened, we took immediate action in collaboration with Match System specialists to track down and possibly block the stolen money.

- Step 1: We marked the hackers' addresses as suspicious on major blockchain analyzers.
- Step 2: We quickly alerted top cryptocurrency exchanges and AML officers and shared the hackers' addresses with the stolen money.
- Step 3: We added the hackers' addresses to the watchlist of Match Systems.

Hackers Withdrew Majority of Funds to SwftSwap :

Most of the funds were transferred to the SwftSwap service in the form of USDT tokens on the Avalanche-C blockchain. Afterwards, a part of the money was moved to the Ethereum blockchain and then transferred again to the Avalanche and Bitcoin networks. A considerable amount of money from SwftSwap was sent to the attacker's addresses, which showed a high volume of transactions. These same addresses were also used to move the stolen funds from the Atomic Wallet. Moreover, approximately 15% of the stolen funds were lost on the "operational costs" of the hackers, including exchange fees and rate slippages.

Lazarus Hacking Group as The Main Suspect:

Based on our investigation, we have grounds to believe the advanced hacker group known as Lazarus might be responsible for the attack on CoinsPaid. The attackers used methods and money-laundering techniques similar to those recently seen in the Atomic Wallet heist attributed to Lazarus.
Labelled as one of the "leading global cyber threat groups," Lazarus Group has gained notoriety for orchestrating hacking operations across the globe. While specific details about their members and identities remain uncertain, this cybercriminal organization is believed to have ties to the government of North Korea.

Match System specialists discovered similar patterns that Lazarus previously used in their recent 100M USD Atomic Wallet hack.
Hackers utilised swap services, such as SunSwap, SwftSwap, and SimpleSwap, as well as Sinbad cryptocurrency mixer, to launder illegally obtained funds without any KYC and AML procedures.
In both CoinsPaid and Atomic wallet hacks, most of the stolen funds were sent in the form of USDT to the SwftSwap cryptocurrency service on the Avalanche-C blockchain.

What’s next?
CoinsPaid is actively preparing to host a dedicated round-table aimed at addressing the urgent challenges faced by blockchain-related businesses in mitigating the impact of hacking incidents. This initiative holds great significance in our journey toward establishing a more robust and impervious blockchain ecosystem.

Let's work together to develop innovative approaches and ensure our industry remains safe and secure. If you are interested in participating or learning more about the discussion, please reach out to CoinsPaid CMO: Eugen Kuzin on Linkedin.

Yuliya Mironchyk
Dream Finance OU
+48 505 750 937
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/649035247