Ritesh Jha | SY-IT(B3) | 16010423076

WazirX Crypto Theft

WazirX, one of India's largest cryptocurrency exchanges founded in 2017, reported a significant security incident in July 2024. With reserves worth $500 million, the exchange faced a massive breach, resulting in the loss of cryptocurrency valued at approximately ₹2000 crore (or $234 million). Around 43% of its users were affected, losing their funds. Hackers used Tornado Cash, an Ethereum-based crypto mixer, to launder the stolen assets, converting them into 59,000 ETH. The Indian Financial Intelligence Unit (FIU) and CERT-In immediately launched investigations into the breach.

In November 2024, the Delhi Police made a breakthrough by arresting Masud Alam from West Bengal. Investigations revealed that Alam exploited a Telegram route to deceive and gain unauthorized access to WazirX's systems. Liminal Custody, a Singapore-based firm responsible for the security of WazirX wallets, refused to cooperate with authorities, hindering the investigation. Despite the significant loss, investigators found no direct security vulnerabilities but concluded that access was obtained through deceptive means.

The incident highlighted vulnerabilities in the operational security of cryptocurrency platforms. WazirX laptops were seized to aid the investigation, but this case underscored the need for stricter regulations and enhanced security measures in the crypto industry to prevent such breaches.

References :

1. https://www.ndtv.com/india-news/wazirx-government-officials-meet-amid-probe-into-rs-2-000-crore-crypto-hack-report-6734854#:~:text=Cryptocurrency%20exchange%20WazirX%2C%20which%20suffered,government%20agencies%20in%20the%20country.
2. https://m.economictimes.com/tech/technology/hacker-behind-234-million-india-crypto-theft-starts-washing-funds/articleshow/113022170.cms

Official Statement By WazirX : https://wazirx.com/blog/managing-your-funds-after-the-cyber-attack/

Thomas Cook India Cyber Attack

Thomas Cook, a global travel agency with its India operations headquartered in Mumbai, experienced a cyber attack on December 31. As a precaution, the company shut down its affected systems to contain the breach. The homepage of their website displayed an error 503, indicating that the service had been deliberately stopped by the administrator.

The company is collaborating with cybersecurity experts to investigate the incident and identify the root cause. In its filing with the Bombay Stock Exchange, Thomas Cook formally disclosed the breach, ensuring transparency with stakeholders. The company is also considering reporting the attack to CERT-In for further assistance and compliance.

This incident highlights the growing risk of cyber attacks in the travel sector, emphasizing the need for robust security measures to safeguard critical systems and sensitive customer data. Thomas Cook India's swift action reflects the importance of proactive responses to mitigate potential damage.

Not much information is available, as the incident is just 5 days old.

https://www.livemint.com/companies/news/thomas-cook-shuts-systems-after-cyber-attack-takes-down-it-infrastructure-11735640407064.html

https://timesofindia.indiatimes.com/technology/tech-news/thomas-cook-india-website-goes-down-after-cyberattack-read-the-companys-statement/articleshow/116851819.cms