# DeFi exchange stolen $120 million

Recently, a hacker withdrew funds from multiple crypto wallets connected to the BadgerDAO decentralized finance platform, and various tokens were stolen in the attack worth around $120 million.

While the investigation was still ongoing, members of Badger informed users that the problem came from hackers inserting a malicious script into the user interface of their website. For any user interacting with the website while the script is active, the script intercepts Web3 transactions and inserts a request to transfer the victim's token to the attacker's chosen address.

Meanwhile, PeckShield pointed to a transfer of 896 Bitcoins to the attacker's wallet worth more than $50 million. According to the research team, the malicious code appeared as early as November 10, when attackers ran malicious scripts at random times to avoid detection.

Decentralized finance (DeFi) systems rely on blockchain technology to allow cryptocurrency holders to perform more typical financial operations such as earning interest through lending. BadgerDAO promises users that they can 'have peace of mind knowing you never have to give up your crypto private keys, you can withdraw anytime you want, and our strategists We're working around the clock to get your property up and running'. Its protocol allows Bitcoin holders to "bridge" their cryptocurrency with the Ethereum platform through tokens and take advantage of DeFi opportunities.

After learning of the unauthorized transfers, Badger halted all smart contracts, essentially freezing the platform and advising users to reject all transactions to the attacker's address.

The company said it was 'withholding the data of Chainalysis forensic experts to uncover the full scale of the incident and that authorities in both the US and Canada have been notified. Badger is fully cooperating with

external investigations as well as conducting its own investigations.

One of the directions Badger is investigating is how an attacker appears to have accessed Cloudflare through an API key that should have been protected with two-factor authentication (MFA). While the attack did not reveal specific vulnerabilities in the blockchain technology itself, it attempted to exploit the older 'web 2.0' technology that most users use to make transactions.

Multi-factor authentication protects accounts against multiple phishing schemes or mass credential stuffing attacks. However, experts repeatedly warn of targeted phishing attacks that can bypass it, while toolkits to automate the process have been available for many years.