



---

## Security Newsletter

6 Dec 2021

[Subscribe to this newsletter](#)

# Hacked Cryptocurrency Platform Begs Hacker to Please Return \$119 Million



Last week, an unknown hacker or hackers stole around 2,100 BTC (\$118,500,000) and 151 ETH (\$679,000) worth of cryptocurrency tokens from a blockchain company called BadgerDAO.

Now, the blockchain "bridge" protocol BadgerDAO is pleading with the hacker to return the stolen funds. "You have taken funds that do not belong to you, but we are willing to work with you and compensate you for identifying this vulnerability in the systems," BadgerDAO wrote in a public announcement. "We are providing you with a direct line of communication to discuss a peaceful resolution without involving any outside parties. Contact us to discuss further and do the right thing on behalf of the community."

The hack on BadgerDAO took advantage of an old-school web-based attack: The hacker was able to steal an API key that gave them control of BadgerDAO's account on Cloudflare, the project's content delivery network for its site. This gave the hacker the ability to inject a malicious script on the site that prompted users to give up wallet permissions, which then allowed the hackers to steal customers' cryptocurrency.

[Read More on Vice](#)

# Facebook Will Force More At-Risk Accounts to Use Two-Factor



For years, Facebook has given its users the option of protecting their accounts with two-factor authentication. Soon, the platform's highest-risk users will no longer have a choice: The social network will require them to lock up their profiles with more than just a password. Good.

Facebook's parent company, Meta, has required since last year that advertising accounts and administrators of popular pages turn on two-factor. It's not the only platform taking this step; in May, Google announced a move toward making two-factor authentication the default for all of its users.

And while Meta says that its current initiative applies only to the politicians, activists, journalists, and others enrolled in its Facebook Protect program, this seems like a sort of test for figuring out how to make two-factor authentication as easy as possible for everyone to turn on. Meta is also working to make sure it can help troubleshoot any related issues that may arise for users around the world.

[Read More on Wired](#)

## More #News

- [Researcher Found Way to Brute Force Verizon Customer PINs Online](#)
- [NSO Group Spyware Hits at Least 9 US State Department Phones](#)
- [Thieves Using AirTags to "Follow" Cars](#)
- [Intel Is Maintaining Legacy Technology for Security Research](#)
- [Who Is the Network Access Broker 'Babam'?](#)
- [Ubiquiti Developer Charged With Extortion, Causing 2020 "Breach"](#)

- [US State Dept employees' phones hacked using NSO spyware](#)
- [Researchers discover 14 new data-stealing web browser attacks](#)
- [Bulletproof hosting founder imprisoned for helping cybercrime gangs](#)
- [Europol: 18k money mules caught laundering money from online fraud](#)
- [Smartwatches for children are a privacy and security nightmare](#)

## #Breach Log

- [Hackers Steal \\$150M From Crypto Exchange Billed as 'Most Trusted'](#)
- [A Planned Parenthood LA Hack Affects 400,000 Patients](#)
- [Nordic Choice Hotels hit by Conti ransomware](#)
- [Hundreds of SPAR stores shut down, switch to cash after cyberattack](#)
- [Malicious Android app steals Malaysian bank credentials, MFA codes](#)
- [DNA testing firm discloses data breach affecting 2.1 million people](#)

## #Patch Time!

- [Zoho: Patch new ManageEngine bug exploited](#)
- [Mozilla fixes critical bug in cross-platform cryptography library](#)
- [8-year-old HP printer vulnerability affects 150 printer models](#)

## #Tech and #Tools

- [Azure Privilege Escalation via Azure API Permissions Abuse](#)
- [Smishing Botnets Going Viral in Iran](#)
- [Discovering Full Read SSRF in Jamf](#)
- [uBlock, I exfiltrate: exploiting ad blockers with CSS](#)
- [GSOH No! Hunting for Vulnerabilities in VirtualBox Network Offloads](#)
- [Encryption Does Not Equal Invisibility – Detecting Anomalous TLS Certificates with the Half-Space-Trees Algorithm](#)
- [XMPP: An Under-appreciated Attack Surface](#)
- [Eyeballer 2.0 Web Interface and Other New Features](#)
- [What does APT Activity Look Like on macOS?](#)
- [Jumping the air gap: 15 years of nation-state effort](#)
- [This shouldn't have happened: A vulnerability postmortem](#)



This content was created by [Kindred Group Security](#). Please share if you enjoyed!

## Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on [www.kindredgroup.com](http://www.kindredgroup.com).

You can access the previous newsletters at <https://news.infosecgur.us>