**Investigators Believe Unauthorized API Key Allowed Malicious Snippet to Set User Web3 Permission to Attacker Wallet**

**Summary of Findings**

On Dec 2 2021, a [**series of unauthorized transactions**](https://badger.com/exploit/updates) occurred, resulting in the loss of funds from Badger users. Following the exploit, Badger engineers worked with cybersecurity firm [**Mandiant**](https://www.mandiant.com/) to investigate the incident and have prepared the following initial report.

At this time, Badger believes that, as publicly reported, the phishing incident that occurred on 2 Dec, 2021 was the result of a maliciously injected snippet provided by [**Cloudflare Workers.**](https://developers.cloudflare.com/workers/runtime-apis/html-rewriter)  Cloudflare Workers is an interface to run scripts that operate on and alter web traffic as it flows through Cloudflare proxies. The attacker deployed the worker script via a compromised API key that was created without the knowledge or authorization of Badger engineers.  The attacker(s) used this API access to periodically inject malicious code into the Badger application such that it only affected a subset of the user base.

**Sequence of Events**

Badger appreciates our Community’s patience while we figure out how to balance our commitment to transparency with the fact that this is still an ongoing investigation with rapidly changing information. We are sharing the following sequence of events at this time to help protect our Community and to help others who might be similarly targeted.

* In late September, users on a Cloudflare community support forum reported that unauthorized users were able to create accounts and were also able to create and view (Global) API keys (which cannot be deleted or deactivated) before email verification was completed (see [**Cloudflare Forum Post**](https://web.archive.org/web/20211202160431/https:/community.cloudflare.com/t/someone-else-can-create-an-account-and-api-token-on-your-email-address/309492/5)). It was noted that an attacker could then wait for the email to be verified, and for the account creation to be completed, and they would then have API access.
* Upon reviewing Cloudflare logs after the exploit, Badger identified unauthorized account creation and API key generation for three Badger accounts; two in late August, one in early September.
* In mid-September, Badger unknowingly completed the account creation for one of these three compromised accounts, which were used for legitimate Cloudflare management activities. The UI did not make it obvious that the account had already been created and an API key was accordingly generated.
* On November 10, the attacker began using their API access to inject malicious scripts via Cloudflare Workers into the html of [**app.badger.com**](http://app.badger.com/). The script intercepted web3 transactions and prompted users to allow a foreign address approval to operate on ERC-20 tokens in their wallet.  On November 20, the first on-chain malicious [**approval**](https://etherscan.io/tx/0x9a900fbe6136a44bbfd43de9c18947977990acee5fb41e7d9a76562aed960a51) was made for the exploiter wallet.
* The attacker used several anti-detection techniques in their attack. They applied and removed the script periodically over the month of November, often for very short periods of time. The attacker also only targeted wallets over a certain balance, and explicitly avoided targeting listed signers of the Dev Multisig. Finally, the attacker accessed the API from multiple proxy and VPN IP addresses and changed the script on each deployment so they each had a unique hash, rendering static indicators of limited value.
* The Badger community raised an alert via Discord about a large, suspicious [**transaction**](https://etherscan.io/tx/0x951babdddbfbbba81bbbb7991a959d9815e80cc5d9418d10e692f41541029869) on December 2
* Badger immediately paused most vault activity within 30 minutes of the alert. A handful of older contracts with a single, inaccessible guardian were paused approximately 15 hours later.
* After this incident, Cloudflare API keys have been rotated, passwords changed, and the MFA was transferred following discovery of the incident.

As this exploit involved Web 2 vectors which are unusual to DeFi attacks, we will provide a short post-mortem of the Web 2 events that occurred, and a full Web 3 post mortem that follows standards of reporting in DeFi.

**Web2 Event Log**

Badger is providing the following details in order to help other people identify a similar Web2 compromise.

Here’s what our Cloudflare audit logs look like for one of the exploited accounts:

The earliest evidence we currently have of the attacker trying to take over an account is August 20, 2021.

Per the responses on the Cloudflare forum, the vulnerability appears to have been mitigated around September 29.  
  
Here’s what Badger’s app looked like with the injected code:

[**Archived version of the Badger App with code injected**](https://web.archive.org/web/20211129101319/https:/app.badger.com/)

Badger is redacting the malicious scripts from the summary below at this time while the investigation is ongoing.

On November 10, 2021 here’s the first example of malicious activity:

The following table shows the times when malicious scripts were running on the site:

**Web3: On-chain events**

**Mitigation Steps**

At around 2:05 AM UTC, on 2 Dec, 2021, Badger was alerted of suspicious activity on the platform. The attack was noticed by a Community member when approximately [**900 BTC were removed**](https://etherscan.io/tx/0x951babdddbfbbba81bbbb7991a959d9815e80cc5d9418d10e692f41541029869) from the Yearn wBTC vault.

After a quick investigation, the issue was marked a high priority and urgent. At 3:14 AM UTC, Badger began pausing all vault and strategy contracts.

Per [**BIP-33**](https://forum.badger.finance/t/bip-33-phase-1-of-decentralizing-badger-dao/2607), addresses approved on the [**guardian contract**](https://etherscan.io/address/0x6615e67b8B6b6375D38A0A3f937cd8c1a1e96386#writeProxyContract) have the ability to pause contracts. The pausing functionality of these contracts operates in a manner that blocks any deposit, withdrawal, transfer for ERC20 vaults, withdrawals from strategies, and any minting/redeeming of ibBTC until the unpause function is called on them. Unpausing is restricted to the Dev Multisig, which requires governance approval. Eight older strategies and one vault also require a timelock to unpause.

Most contracts were paused by 3:30 AM UTC. Some older vaults, (namely bcrvRenBTC, bcrvSBTC, bcrvTBTC, bBADGER, bharvestcrvRenBTC and buniWbtcBadger) do not have pause functionality on the vault contract. Their strategies were nevertheless paused to prevent withdrawals. At the time Badger engineers were unable to access the guardian account of the bBADGER, bharvestcrvRenBTC and buniWbtcBadger strategies. Further investigation revealed the strategist who helped come up with this smart contract idea also had pausing capabilities, and pausers were eventually able to pause the strategies with the strategist account.

A list of all of the pausing txs can be found [**here**](https://docs.google.com/spreadsheets/d/1jEyKhad85RFUXr0PshnlGyQu_IJHjhLrAoNWbzD3WWQ/edit#gid=0). As soon as the vaults were paused, the [**exploiter’s**](https://etherscan.io/txs?a=0x1fcdb04d0c5364fbd92c73ca8af9baa72c269107&p=1) transferFrom calls began to fail.

The graphs below show the movement of Badger Sett tokens stopping after pausing. (Note: The y axis shows the raw number of Badger Sett tokens)

All Setts except bBADGER, bharvestcrvRenBTC, and buniWbtcBadger:

Below is the graph demonstrating the movement of all Badger Sett tokens, including those that were late to pause

It is worth mentioning that the [**last malicious withdrawal**](https://etherscan.io/tx/0xbf83cd37a8bb82a2c6b4ffb60048a27dda454e0bac83fd4bde73fe8e846f864c) from the unpaused vaults occurred at 4:57 AM UTC. All withdrawals that took place after this and until the pausing of the last strategy were conducted by regular users.

It is also worth mentioning that the attacker was able to compromise non-Sett tokens, such as BADGER, wBTC, CVX and cvxCRV, and was able to liquidate them after Badger had enacted the pauses.

**Attack Execution**

Through the Web2 intrusion, the attacker was able to phish for ERC20 token approvals from Badger users through the user interface. The hacker tricked users into signing token approve or increaseAllowance calls allowing the main exploiter EOA account (0x1fcdb04d0c5364fbd92c73ca8af9baa72c269107) to spend funds.

After phishing a number of approvals, a [**funding account**](https://etherscan.io/address/0xa0d34572fb3be1bca9f36b5d41e86c135e580553) sent 8 ETH to the exploiter’s account to fuel a series of transferFrom calls on the users’ approved tokens. This allowed the attacker to move funds on behalf of the users to other accounts, which then liquidated the funds and exited via the Badger Bridge to BTC.

**Involved Parties**

Badger is actively tracking all funds associated with the incident and relevant information is available below:

Destination Addresses:



**Protocol Impact (Stolen Funds)**

Impact by underlying assets:

**Note: Estimated USD prices are based on fixed pricing taken from the time when the collection script was run (2 Dec, 2021).  They should be taken as an indication and not absolute. A detailed token breakdown can be found**[**here**](https://docs.google.com/spreadsheets/d/1IPwk-_ZtZ3aIxaJgYm8wZ7W6biB65Ou46lkYnniAHzQ/edit?usp=sharing)**.**

**Post Incident Plan**

The Badger Cloudflare account has had the password updated, MFA changed and all API keys either deleted or refreshed where possible.

Badger has verified that the exploit has been patched on the Cloudflare side.  New accounts are no longer allowed to view API keys until the email address has been verified.

As [**previously advised**](https://badger.com/exploit/updates), some funds were transferred by the exploiter but not yet withdrawn from the Badger vaults.  We are working on a plan to recover these funds.  
  
Badger is working with Chainalaysis, Mandiant, and the crypto exchanges as well as authorities in the US and Canada to recover any funds possible  
  
Badger is continuing to work with Cloudflare to collect more relevant data, fully scope this incident and assist in their own post-mortem.

**The Path Forward**

Badger is currently assessing and working on a plan towards implementing the following potential improvement ideas:

* To review the emergency functionality on all smart contracts, in order to ensure that it is universal, and automates a “pause everything” feature with the goal of bringing Badger’s emergency break time from 15 minutes down to 2 - 3 minutes.
* Before re-launching the protocol, completing 3rd party audits of all web2 and web3 infrastructure
* Badger could potentially fund a hack-a-thon that is focused on building detection technology in order to watch all smart contracts for unexpected approvals or to automatically issue an alert when there are heuristic changes to how calls are made
* Add a trust minimized, IPFS deployed version of the Badger App
* Create public repositories for people to build from source
* Badger could educate the Community about the importance of vigilance and set up new channels to make sure that changes in usage behaviors by Community members are quickly heard, and analyzed
* Badger could build monitoring tools in order to compare the site served by all routes on [**https://app.badger.com**](https://app.badger.com/) and match them with a locally built SPA to ensure there is no code injection in the future

**Note to DeFi Devs and Infosec Researchers:**

Although the report is preliminary and does not include all information from its investigation, Badger would be more than happy to discuss some additional findings and share more information with the DeFi and Infosec community, to the extent possible given the ongoing investigation.

**Contact**[**help@badger.finance**](mailto:help@badger.finance).