Malicious 'Safepal Wallet' Firefox add-on stole cryptocurrency

By **Ax Sharma (https://www.bleepingcomputer.com/author/ax-sharma/)**

September 27, 2021 07:21 AM **0**

A malicious Firefox add-on named "Safepal Wallet" scammed users by emptying out their wallets and lived on the Mozilla add-ons site for seven months.

Safepal is a cryptocurrency wallet application capable of securely holding more than 10,000 types of assets, including Bitcoin, Ethereum, and Litecoin.

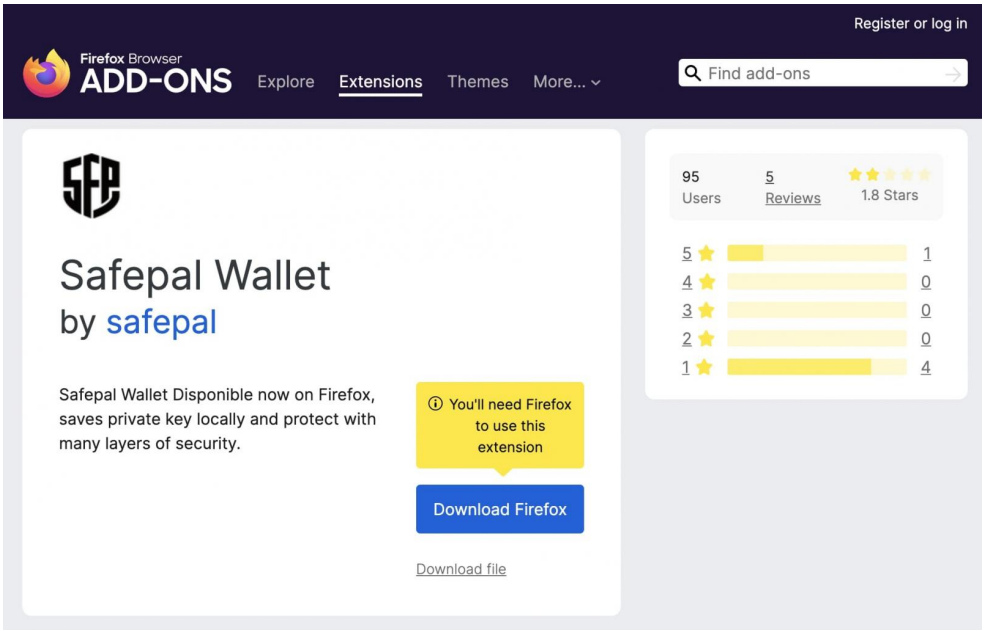
Although the malicious browser add-on has been taken down, BleepingComputer has seen the phishing website set up by the threat actors is still up.

$4,000 lost to malicious Firefox add-on

"Today I browsed [through] the add-on list of Mozilla Firefox, I was searching for Safepal wallet extension to use my cryptocurrency wallet also in the web browser," explains a Mozilla add-ons user who goes by the name, Cali.

Little did Cali know what was coming for them. A few hours after installing and logging in to the add-on with their real Safepal credentials, the user saw their wallet balance drop to $0.

"I was deep in shock... I saw my last transactions and saw that [$4,000 of my funds] were transferred to another wallet. I could not believe it [was an] add-on that is deployed in the add-on list of Mozilla Firefox," continues (http://discourse.mozilla.org/t/got-hacked-by-the-add-on-called-safepal-wallet/85797) the user in Mozilla's support forum.



Fake 'Safepal Wallet' add-on on the Mozilla Firefox store (BleepingComputer)

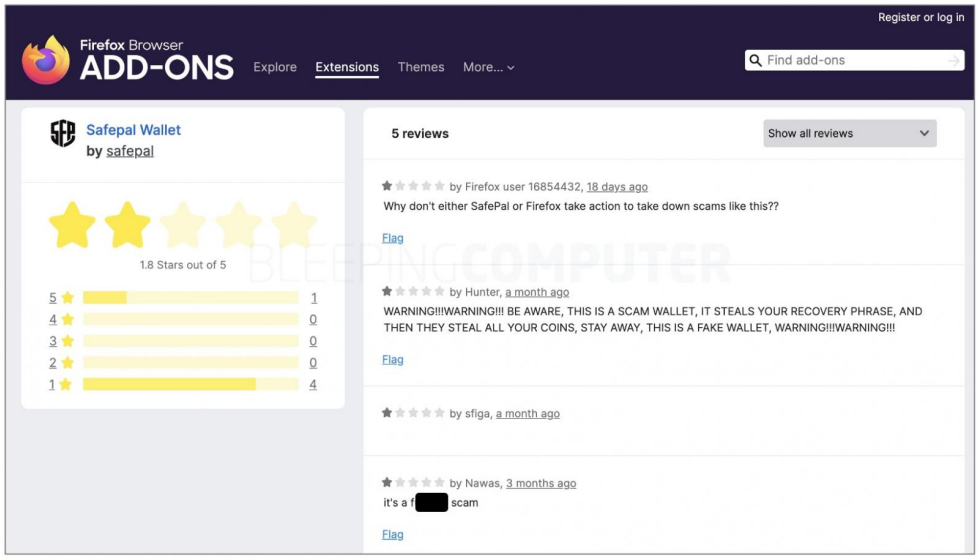
The add-on page for 'Safepal Wallet', seen by BleepingComputer, stated the add-on was up since at least February 16th, 2021.

On the same page, the 235 KB add-on touts itself to be a Safepal application for "saving private keys locally" securely, next to convincing product images and marketing materials.

Within five days of Cali's public report of the incident this month, a Mozilla spokesperson responded (https://discourse.mozilla.org/t/got-hacked-by-the-add-on-called-safepal-wallet/85797/2) that they were investigating. The page has since been removed by Mozilla.

Although Safepal has official smartphone apps available on both Apple AppStore (https://apps.apple.com/app/safepal-wallet/id1548297139) and Google Play (https://play.google.com/store/apps/details?id=io.safepal.wallet&hl=en_GB&gl=US), we are not aware of there being authentic 'Safepal' browser extensions.

Thankfully, on Mozilla add-ons site, some users had posted one-star reviews warning others not to download 'Safepal Wallet':



Safepal fake add-on reviews by users (BleepingComputer)

But, for Cali, it seems a little too late in the game, and the chances of them getting their funds back are bleak.

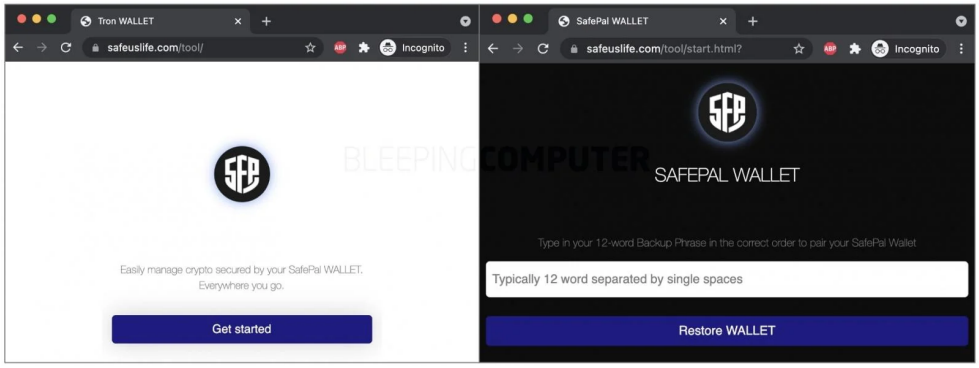
"I already talked with the police they can do nothing for me. They told me that there is no way they can trace the hacker. The only solution is left for me is maybe some of you can help me out by figuring out who the hacker was and how I can get my funds back," states (https://discourse.mozilla.org/t/got-hacked-by-the-add-on-called-safepal-wallet/85797/6) the user.

'Safepal' phishing domain still up, collecting recovery phrases

While investigating the malicious Firefox add-on, BleepingComputer came across the phishing domain used by the add-on. This webpage, shown below, was also listed as the "support site" link on the fake add-on's home page:

https://safeuslife.com/tool/

WHOIS records indicate the phishing site was registered (https://www.namecheap.com/domains/whois/result?domain=safeuslife.com) in January this year via Namecheap. At the time of writing, the webpage is still live and instructs the victim to key in their "12-word Backup Phrase in the correct order to pair your SafePal Wallet."



Phishing page entices Safepal wallet user to enter their recovery phrase (BleepingComputer)

But once the recovery phrase is entered and the form is submitted, the page simply refreshes without any noticeable response. The recovery phrase is silently sent to the attacker.

Cryptocurrency wallets, like many online services, use a backup phrase consisting of twelve randomly generated words that can be used for recovering the user's private key and wallet, should they forget their password. But, the recovery phrase is a crucial secret meant to be used under exceptional circumstances and only on the trusted app or website of the service provider.

A stolen recovery phrase can grant attackers control over your wallet along with the ability to access and transfer funds.

In recent times, cryptocurrency scams are growing, with threat actors are finding innovative and hard-to-detect ways to trick users. Just last week, someone hacked the official Bitcoin.org website (https://www.bleepingcomputer.com/news/security/bitcoinorg-hackers-steal-17-000-in-double-your-cash-scam/) and successfully scammed visitors for $17,000.

In previously seen attacks, open-source repositories, including npm (https://www.bleepingcomputer.com/news/security/backdoor-in-popular-javascript-library-set-to-steal-cryptocurrency/), PyPI (https://www.bleepingcomputer.com/news/security/malicious-pypi-packages-hijack-dev-devices-to-mine-cryptocurrency/), and GitHub

(https://www.bleepingcomputer.com/news/security/github-actions-being-actively-abused-to-mine-cryptocurrency-on-github-servers/) have been abused for spreading both cryptostealing and cryptomining malware.

With the increasing presence of threat actors on online platforms, users should be careful when providing their security phrases or transferring cryptocurrency online.

BleepingComputer has reached out to both Mozilla and Safepal for further comment and we are awaiting their responses. We have also reported the phishing domain in question to Namecheap.

Related Articles:

Bitcoin.org hackers steal $17,000 in 'double your cash' scam (https://www.bleepingcomputer.com/news/security/bitcoinorg-hackers-steal-17-000-in-double-your-cash-scam/)

New "Elon Musk Club" crypto giveaway scam promoted via email (https://www.bleepingcomputer.com/news/security/new-elon-musk-club-crypto-giveaway-scam-promoted-via-email/)

Mozilla tests Microsoft Bing as the default Firefox search engine (https://www.bleepingcomputer.com/news/software/mozilla-tests-microsoft-bing-as-the-default-firefox-search-engine/)

Firefox now bypasses Windows 11's messy default browser settings (https://www.bleepingcomputer.com/news/microsoft/firefox-now-bypasses-windows-11s-messy-default-browser-settings/)

Walmart press release hoax causes Litecoin to spike 34% (https://www.bleepingcomputer.com/news/cryptocurrency/walmart-press-release-hoax-causes-litecoin-to-spike-34-percent/)