This fake password manager reminds you to be careful where you download from

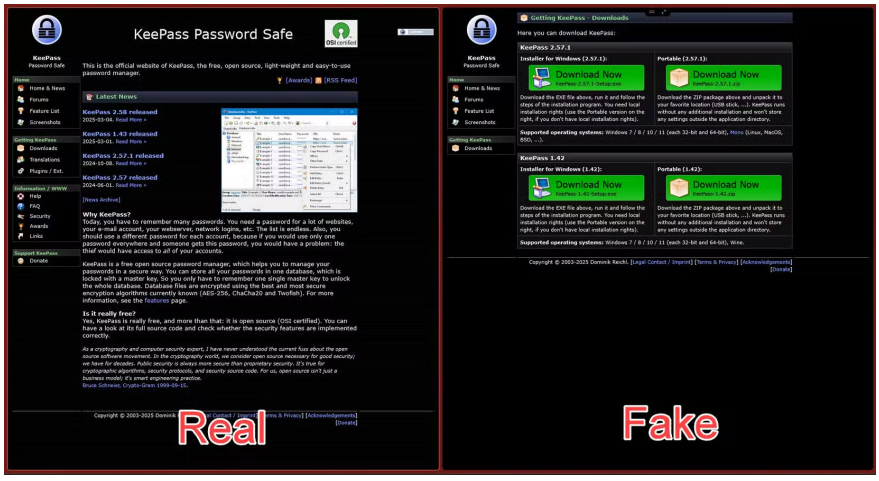
If you use third-party sources or torrents, this fake password manager is a useful reminder of why official sources are so important.

Downloading the program is a fairly easy task, but only if you use official websites or app stores. If you use third-party sources or torrents , this fake password manager is a useful reminder of why official sources are so important.

This password manager steals your passwords

Security researchers at WithSecure have discovered a malware campaign in which hackers have been distributing trojanized versions of the KeePass password manager since at least October 2024. These versions install malware called Cobalt Strike alongside the password manager, which can steal saved passwords and other credentials from your PC and deploy ransomware on your network.

Since KeePass is open source, it was easy for hackers to access the source code and create a convincing copy. This malicious version, called KeeLoader, contained all the functionality of KeePass, except it saved all your passwords as a text file and sent them to hackers using Cobalt Strike beacons.



Distribution is handled by fake websites using hijacked domains such as:

1. keeppaswrd.com
2. keegass.com
3. KeePass.me
4. keespass.biz
5. keebass.com
6. KeePassx.com

Some of these domains are still active and distributing fake versions of KeePass. For more information, the legitimate KeePass website is **keepass.info.** The fake sites are available through Microsoft's Bing search engine. WithSecure claims that the fake domains are being served through DuckDuckGo ads. However, since Microsoft and DuckDuckGo have formed a partnership on Microsoft-powered advertising, it is likely that they are also being advertised with Bing.

The entire campaign was uncovered during WithSecure's investigation into a ransomware incident at a European IT service provider. It turns out that the fake password manager was not only stealing credentials, but also installing ransomware on the company's VMware ESXi servers. WithSecure notes that this is the first time an open-source password manager has been used simultaneously as a credential stealer and a malware loader.

Be careful when downloading programs!

You can use a browser-based password manager with precautions, but using a dedicated program is a much safer alternative. Hackers target password managers for exactly this reason – it puts the risk where you least expect it, meaning they can catch you off guard.

You should always download all programs, especially sensitive ones like password managers, from their official website or your platform's app store. Downloading software and games from third-party websites or torrents always carries the risk of your program being bundled with malware.

As an added precaution, you should also avoid clicking on ads and sponsored links that encourage you to download a program. Even if the ad displays the program's legitimate URL , hackers have repeatedly proven that they can bypass advertising policies and display the legitimate URL while still redirecting you to fake websites.