How malware steals autofill data from browsers

By Sergey Golubev

Published: 2019-08-07 · Archived: 2026-04-06 03:12:12 UTC

Most browsers kindly offer to save your data: account credentials, bank card details for online stores, billing address, name, and passport number for travel sites, and so on. It's convenient and saves having to fill out the same forms all over again or worry about forgotten passwords. However, there is a catch: All of this autofill data can be scooped up by cybercriminals if your computer gets infected by a stealer — a piece of malware that steals information, including from browsers.

Such programs are becoming increasingly popular with online scammers: In the first half of this year alone, Kaspersky's security products detected more than 940,000 stealer attacks. That is a one-third increase from the same period of 2018.

Strictly speaking, stealers are interested in more than just browsers' autofill data — they are also looking for cryptocurrency wallets and gaming data, and they steal files from the desktop as well (we hope you don't store valuable information there, such as password lists).

However, browsers have become a hub of work and play, including shopping, banking and more, and are often a source of far more confidential information than other programs. Let's take a look at how stealers get their thieving hands on browser data.

How browsers store your autofill data

Browser developers seek to protect the information entrusted to them. To do so, they encrypt it, and decryption is possible only on the same device and from the same account that saved it. So if someone simply steals a file with autofill data, they won't be able to use it — everything in it is securely encrypted.

But, there's a but. By default, browser developers assume that your device and account are well protected, meaning that any program running from your account on your computer is acting on your behalf and therefore should be able to extract and decrypt saved data. Unfortunately, this also applies to malware that has penetrated the device and is running under your account.

The only browser that offers extra protection for stored data against third parties is Firefox, which allows you to create a master password that you have to enter when you need the data to be decrypted and used for autofill. However, this option is disabled by default.

How malware steals data from Chrome

Google Chrome and other browsers based on the Chromium engine (such as Opera and Yandex.Browser) always store user data in the same place, so stealers have no problem finding it. In theory at least, this data is stored in

encrypted form. However, if the malware has already penetrated the system, then its actions are done in your name.

Therefore, the malware simply puts in a polite request to the browser's data encryption tool to decrypt information stored on your computer. With requests seemingly from the user considered safe by default, in response the stealer gets all your passwords and credit card details.

How malware steals data from Firefox

Firefox operates a bit differently. To hide password databases and more from strangers, the browser creates a profile with a random name, so the malware cannot know in advance where to look for it. However, the name of the file with the saved data does not change, so there is nothing to prevent the stealer from sifting through all profiles (the folders containing them are stored in one place) and identify the desired file.

After that, the malware again asks the relevant browser module to decrypt the files, and it succeeds, because it is supposedly acting on your behalf.

How malware steals data from Internet Explorer and Edge

Native Windows browsers use special storage for your data. The precise method and type of storage depend on the version of the application, but regardless, the reliability leaves much to be desired. Here, too, the malware can easily retrieve your passwords and credit card details by requesting it from storage, seemingly on your behalf.

The problem is that the malware's request for the decryption of browser data appears to come from the user, so the browser has no reason to say no.

What happens to data stolen by the stealer?

Once the malware has the autofill data in plain text, it sends them back to cybercriminals. From there, either of two scenarios may unfold. The malware's handlers can use it themselves or, more likely, sell it to other malefactors on the black market, where such products are always highly prized.

Either way, if usernames and passwords were among the stored information, the crooks will likely steal a couple of your accounts and try to finagle money out of your friends. If you saved bank card data in the browser, the losses could be more direct; your money will either be spent or transferred elsewhere.

Stolen accounts can be used for many other purposes too, from spamming and promotion of websites or apps, to sending viruses and laundering money stolen from others (and if the police get involved, they may come knocking on your door).

How to protect data from stealers

As you can see, if malware penetrates your computer, data stored in the browser is at risk, and with it your finances and reputation. To avoid such a situation:

- Do not entrust important information such as bank card details to your browser for safekeeping. Instead, enter them manually each time — it takes longer but is safer. You can also store passwords in a password manager.
- If you use Firefox, you can protect browser-stored data with a master password. To do so, click on the three bars in the upper right corner of the browser and select *Options*, go to the *Privacy & Security* tab, scroll down to *Logins and Passwords*, and select the *Use a master password* box. The browser will ask you to create this password — the longer and more complex, the harder it will be for attackers to crack.
- Most important: The best way to safeguard data is to prevent malware from getting onto your computer in the first place. To do so, install a reliable security solution that will keep infections at bay. No malware, no problem!
