PXA Stealer targets sensitive data in users' browsers: Here's how to stay safe!

Enabling autofill in your browser isn't just convenient for you. It's also a goldmine for hackers, especially with malware like PXA Stealer targeting all the sensitive data stored in your favorite browser.

Enabling autofill in your browser isn't just convenient for you. It's also a goldmine for hackers, especially with malware like PXA Stealer targeting all the sensitive data stored in your favorite browser. There are several ways to protect yourself.

PXA Stealer disguises itself as harmless applications and documents.

This is not uncommon for malware. By hiding itself, it easily tricks users into downloading and installing it. At the time of writing, the Vietnamese hacking group had stolen over 200,000 passwords worldwide and gained access to over 4,000 IP addresses.

Their primary target is the browser's autofill data. For many users, this is filled with passwords, addresses, credit card numbers, etc.

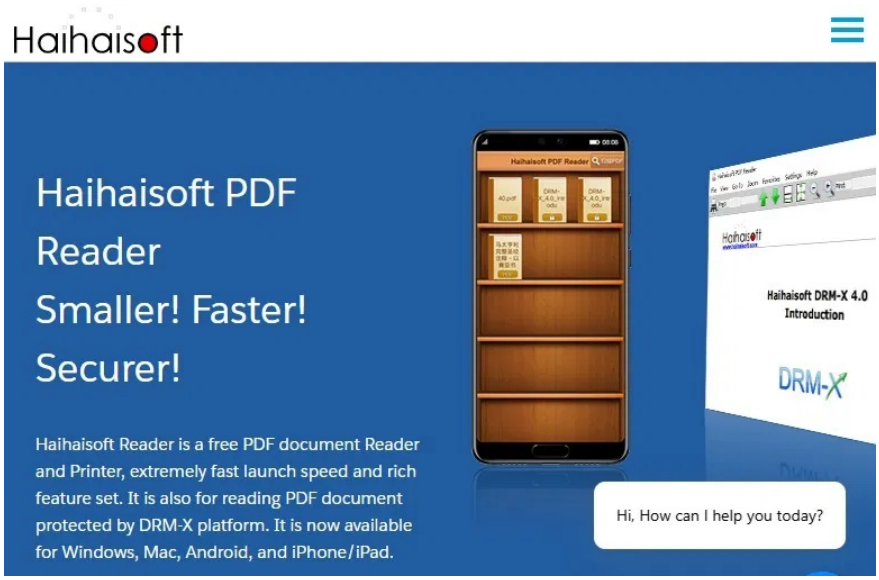
Of course, you won't get infected with PXA Stealer just by browsing online. Instead, you have to install or download something. In this case, cybercriminals mainly focus on a free PDF tool and Microsoft Word 2013 files in email attachments.

After installing a PDF tool or opening a Word file, you may encounter more problems than expected. Malware will be installed, and it may even collect additional malware stored remotely on Dropbox accounts.

Stay away from Haihaisoft PDF Reader!

Free PDF readers are great, but be careful about what and where you download them. Especially when you already have Adobe Acrobat Reader for free and most major browsers can open PDF files , along with many other popular PDF readers. Although PXA Stealer is currently targeting Windows, macOS users also have plenty of PDF readers to choose from without having to worry about malware infections.

Hackers use phishing websites to trick you into downloading the free Haihaisoft PDF Reader software. It might even be a digitally signed download, which is generally considered safe. But, once you download and try to install it, you'll get infected with malware.



Technically, this PDF reader software is real and legitimate, but it has been the target of malicious activity for years. If you choose to download it, make sure you access Haihaisoft directly. Do not access any other website. And, check the download link via VirusTotal first.

The advice is to always thoroughly research any application/software/tool ??before installing it. Avoid clicking on links to websites from random emails or pop-up windows. Most importantly, always download from the official website instead of a third-party website.

Ignore Microsoft Word attachments

It's tempting to click on that little attachment link to see the contents inside that completely unexpected Microsoft Word attachment . Don't do it. The results won't be good.

Phishing emails are becoming increasingly sophisticated and often appear to come from trusted companies, colleagues, friends, and family. The problem is, once you open that attachment, you don't get a second chance to verify whether it's real or malicious. The damage has already been done, and you have to try to remove the malware and change all your passwords.

Since PXA Stealer's preferred method of infection is through Word file attachments within .ZIP files, be extra cautious if you encounter such a file.

When you try to extract the file, you'll receive an error message. It seems quite harmless, but it's just a way to mask that malware is being installed in the background.

Always think carefully before downloading any attachments. This week it might be a Word document. Next week, it could be a PDF, a spreadsheet, or even plain text. If you're not entirely sure, delete it.

Avoid storing sensitive information in your browser.

Enabling autofill in your browser increases your risk of having your data stolen by hackers. The reason is simple. A phishing website might look legitimate and only ask you to fill in a few details for a newsletter, such as your name and email address. What you don't see is that hidden fields are collecting everything else your browser has already stored.

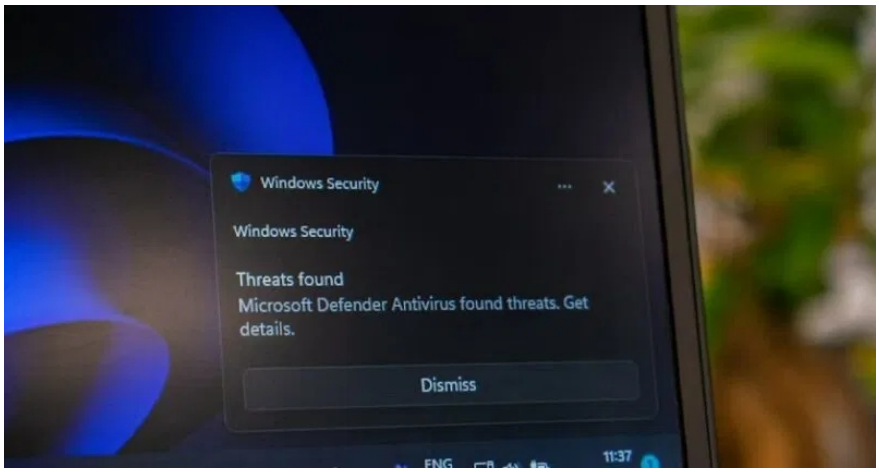
With PXA Stealer, the malware will collect any autofill data you use, including passwords, cryptocurrency wallet details, credit card information, etc. It can collect all your browser cookies by using a DLL that bypasses your browser's encryption protections.

Browsers aren't the best security when it comes to storing personal information. It's best to rely on your own memory or use a third-party password manager. With a password manager, you have to unlock the data first.

Of course, if you are a victim of malware, it can still collect any autofill data from your password manager.

Tips to avoid PXA Stealer

Accidents can happen. You click on a link without thinking, or download an attachment that looks legitimate. Even that great-looking app (a PDF reader in this case) might seem perfect for your needs.



The best ways to avoid PXA Stealer are:

1. Verify the links in your email before clicking on them (hover over them to see where they lead).
2. Access the official websites directly to download the software, or simply click on links on trusted websites.
3. Check download links and websites through VirusTotal
4. Never download attachments that you don't expect.
5. Scan all downloaded files and attachments using your antivirus and/or anti-malware application.

Remember, it's not just Windows users who are at risk. Every operating system is vulnerable. For example, Android users were targeted by the Godfather malware. And WhatsApp users should always be vigilant to avoid scams and malware.