Blog

Clipboard Security: Don't be the Next Victim

Published April 26, 2022

Your clipboard is one of the most vulnerable places on your computer. Every time you copy and paste something, it's stored in your clipboard history. And if you're not careful, that information can be accessed by anyone with access to your computer.

Clipboard data has become a new target for cybercriminals. In the past year, there have been several high-profile cases of clipboard hijacking, where malicious actors were able to access sensitive information like passwords and credit card numbers.

So how can you protect your company from clipboard hijacking? The first step is understanding what it is and how it works.

What is clipboard data?

Clipboard data is the information that you copy and paste on your device. It's stored in a temporary location on your hard drive, and it can be accessed by any program or application on your computer or mobile device.

When you copy something on your computer, it's stored in the clipboard as plain text. This means that if someone were to access your clipboard data, they would be able to see the exact same thing that you copied.

What is clipboard hijacking?

Clipboard hijacking is an illicit practice of taking data from the victims' clipboards and using it for malicious purposes. In most cases, attackers leverage malware that either steals data

or replaces general clipboard data with malicious links. As soon as the target victim pastes the link in their browser, it leads them to a malicious site. Adware and some flash banner ads can also help attackers hijack clipboards and attack a system.

How can clipboard hijacking affect users?

There are a lot of ways clipboard hijacking malware can pose severe threats. Anytime a user copies any sensitive data or credential, such as online bank details, passwords, secret PIN, etc., while shopping online or paying bills through online banking, users can become victims of clipboard hijacking. Users often copy-paste their credentials to expedite the process. However, if a user's system gets infected with clipboard hijacking malware, it could steal all the copied information.

The threat does not only affect the operating system. It can modify the operating system's clipboard data for the benefit of itself or its operators. Consider a scenario where a user attempts to pay an online bill and copies the receiver's bank account number. The clipboard malware can change the actual bank account number to the attacker's account number. If this is done, the payment will go to the attacker's bank account instead.

This is why it's important to be careful about what you copy and paste. Any sensitive information like passwords or credit card numbers should be avoided at all costs.

Watch out for apps that snoop on your clipboard

data

Clipboard hijacking is not only done through malicious software. There are also apps that have been caught snooping on users' clipboard data.

For example, a recent report found that the popular iOS app AccuWeather was caught accessing users' clipboard data without their permission. The app was caught copying the content of users' clipboards and sending it to an analytics company. The report found that the app had been doing this since August 2018.

While the app's developers claimed that they were only collecting data to "provide users with the most personalized experiences possible," the report found that the app was accessing users' clipboard data without their knowledge or consent.

This is a major privacy concern, as it means that the app was able to access sensitive information like passwords and credit card numbers without the users' knowledge or consent.

Many other popular apps have been found guilty of this as well. Some of the most popular ones are TikTok, Russia Today, 8 Ball Pool, PubG Mobile, and Accuweather.

The takeaway: clear your clipboards!

Copying something else can overwrite what's currently in your clipboard. So if you've copied something sensitive, be sure to clear your clipboard data afterwards.

Here are some additional steps to ensure that everything from your clipboard is completely

erased from your system.

Clear clipboard data for Mac

Clipboard data remains stored in RAM. Users can restart their system to clear the RAM and release the used part.

Or,

Navigate to Finder -> Applications -> Terminal and type the command "pbcopy < /dev/null" (without quotes) within the Terminal, and hit Enter.

Clear clipboard data for Windows

Users can restart their Windows system to clear all RAM data.

Or,

Go to Start -> Type "Settings" -> System -> From the side panel, click "Clipboard" -> Press the "Clear" button to clear all data.

Clear clipboard data for Linux

Users can restart their Linux system to clear all RAM data.

Or,

Right-click and go to Linux Terminal and type the following commands:

- $ touch blank
- $ xclip -selection clipboard blank

How can enterprise systems avoid clipboard-based malware attacks?

There are several ways that enterprises can avoid clipboard-based malware attacks:

1. Educate employees about the dangers of clipboard hijacking and make sure they know not to copy and paste any sensitive information.

2. Use a secure enterprise file-sharing solution that encrypts all data in transit and at rest.

3. Implement two-factor authentication for all sensitive systems and data.

4. Use a malware detection and removal solution to scan for and remove any clipboard-based malware.

5. Keep all systems and software up to date with the latest security patches.

Conclusion

If you're not already clearing your clipboard, it's time to start. It takes just a few seconds and can help protect your business from clipboard hijackers. Contact the packetlabs team for more information on how we can help keep your data safe.

Toronto | HQ

401 Bay Street, Suite 1600

Toronto, Ontario, Canada

M5H 2Y4

San Francisco | HQ

580 California Street, 12th floor

San Francisco, CA, USA

94104

Contact Us

Learn

Services

Packetlabs Portal

Partner Program

Careers

About

FAQ

LinkedIn

Twitter

Facebook

Privacy Policy Terms of Service