

## Introduction

In order to automate this task (ID.IM-01) we came up with a solution “Anti-PasteJacker”. So first let’s get the idea about paste jacking. Paste jacking, also known as clipboard jacking, is a type of input validation vulnerability. A malicious script is copied to the victim's clipboard, causing him/her to paste it directly in a vulnerable position(like terminal, powershell). This can lead to system compromise, hence clipboard monitoring plays a crucial role while surfing over the web.

The “Anti-PasteJacker” Chrome extension is a security tool designed to protect users from potential clipboard hijacking attacks. It monitors the clipboard for copied content and alerts the user with a popup if something malicious is detected.

## Features:

**Clipboard Monitoring:** Constantly monitors the clipboard for changes in copied content.

**Malicious Content Detection:** Utilizes a predefined list of known malicious content to identify potential threats.

**Popup Alert:** Displays a popup alert to the user if malicious content is detected, prompting them to take action.

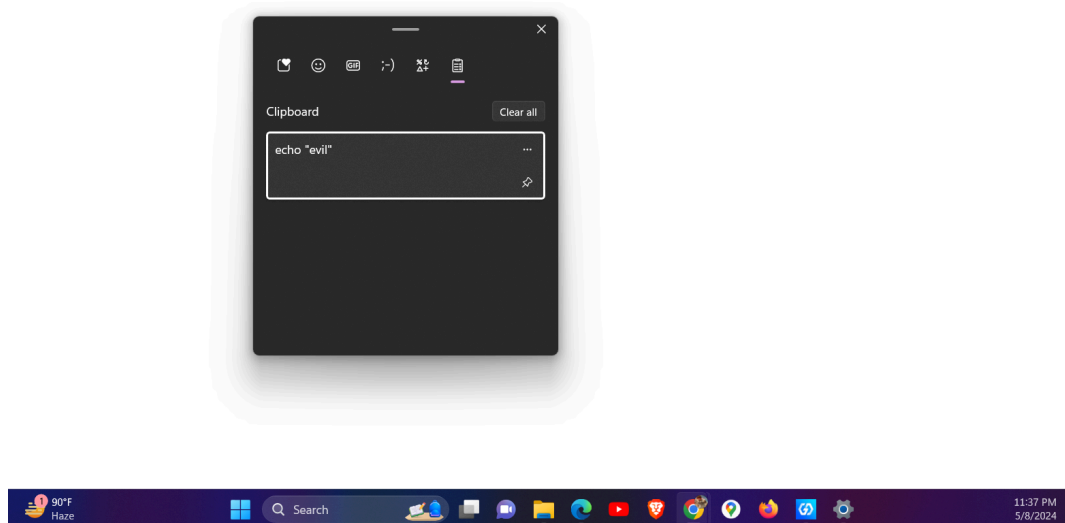
## Usage:

Once installed, the Anti-PasteJacker extension works silently in the background, monitoring the clipboard for any copied content. If malicious content is detected, a popup alert will appear, warning the user about the potential threat.

## Demo of Pastejacking

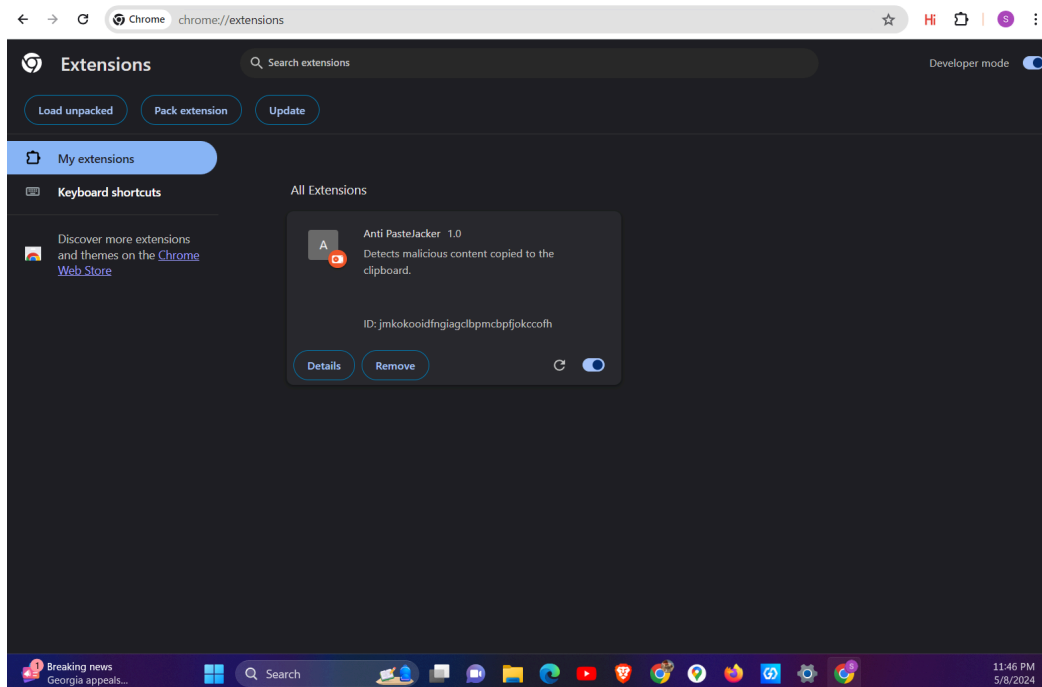
Copy the text below and run it in your terminal for totally not evil things to happen.

```
echo "not evil"
```



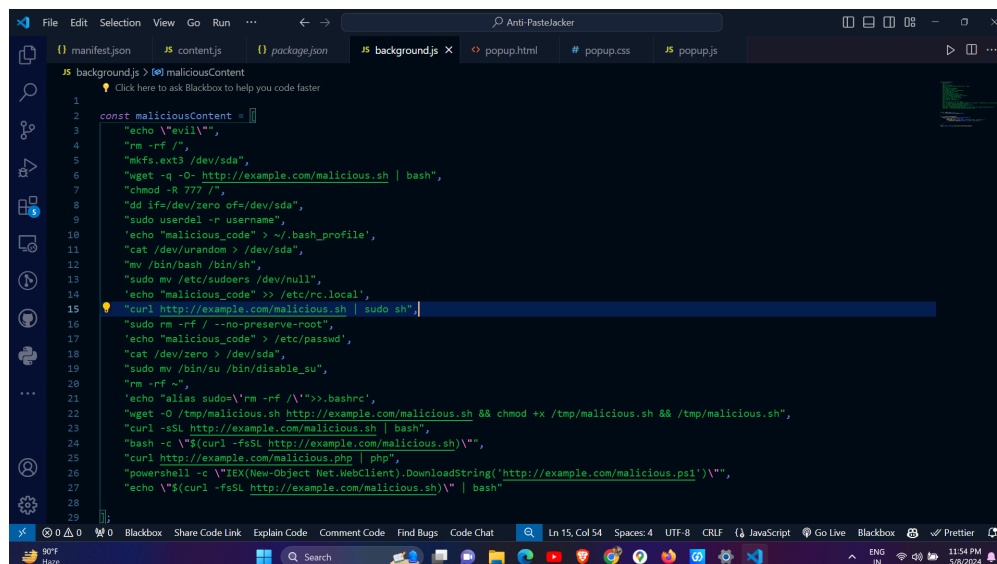
**Fig 1 Pastejacking Demo**

Turn on the developer mode in Chrome extension's page. Load the unpacked folder (the project repository) and after refreshing, pin the extension.

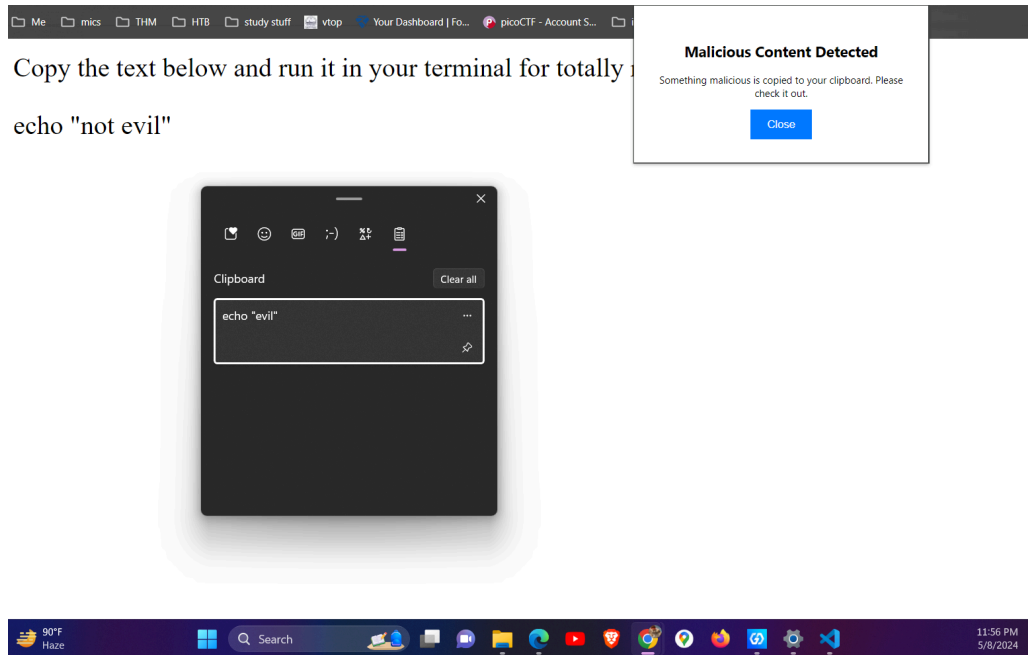


**Fig 2 Loading and pin the extension**

So we come up with the basic logic, that the extension will monitor the clipboard change and if the content of the clipboard matches with the string inside array in the background.js file, it will flag the user with the popup saying “Something malicious is copied to clipboard. Please check it out!”.



**Fig 3 The background.js' array**



**Fig 4 The popup**

In conclusion, our anti-paste jacker can help counteract the possible threats when the clipboard is being tampered with by either snoopers or malware. This way, people using this extension can be protected from data leakage as well as access confidential information by unauthorized persons. Meanwhile, we want to further develop it by frequently modernizing in order to include more sophisticated detection methods into the system. The coming versions should pay attention to users' opinions as well as new danger environments so that it remains useful for safeguarding people against potential threats.