Cyber Security Internship

Task 7: Identify and Remove Suspicious Browser Extensions

Suchismita Maity

November 24, 2025

Internship Details

Organization: Elevate Labs
Program: Cyber Security Internship
Deliverable: List of suspicious extensions found, removed, and research findings.

Objective

The objective of this task was to learn how to spot and remove potentially harmful browser extensions to secure the browsing environment. Malicious extensions can serve as an entry point for data theft, adware, and browser hijacking.

Methodology

To complete this task, a manual security audit was performed on the primary web browser (Google Chrome). The following steps were taken in accordance with the task guide:

1. **Access Manager:** Opened the browser's extension manager via `chrome://extensions`.
2. **Review:** Reviewed the list of all installed extensions.
3. **Verification:** Checked the permissions requested by each extension (e.g., "Read and change all your data on websites you visit").
4. **Source Check:** Verified that extensions were published by reputable developers on the official Web Store.
5. **Clean-up:** Identified unused or unnecessary extensions for removal.

Audit Findings & Actions Taken

During the audit of the browser environment, the following observations were recorded:

1. Installed Extensions Overview

A total of **4** extensions were found installed on the browser.

- **AdBlock Plus:** Verified. Source is trusted. Status: *Kept*.
- **Google Docs Offline:** Verified. Official Google extension. Status: *Kept*.
- **Grammarly:** Verified. Necessary for workflow. Status: *Kept*.

- **Honey Coupon Finder:** Identified as “Unused/Legacy”. While not malicious, it had not been used in 6 months and required extensive read permissions.

2. Action Taken

Removal: The “Honey Coupon Finder” extension was removed to reduce the attack surface.
Suspicious Activity: No actively malicious extensions (e.g., unrecognized search bars, crypto-miners) were detected during this scan.

Research: Risks of Malicious Extensions

As part of the task requirements, research was conducted on how malicious extensions harm users. Key findings include:

1. **Data Theft & Spyware:** Malicious extensions often request permission to “read and change all data on websites you visit.” This allows them to capture sensitive information like passwords, credit card numbers, and browsing history.
2. **Adware Injection:** Some extensions exist solely to inject unwanted advertisements into legitimate websites, degrading performance and leading users to phishing sites.
3. **Browser Hijacking:** These extensions forcibly change the default search engine and homepage (e.g., to a fake search site) to intercept search queries and track user behavior.
4. **Botnet Participation:** Advanced malicious extensions can use the victim’s browser as a proxy node, routing illegal traffic through the user’s IP address without their knowledge.

Conclusion

The browser environment has been secured by auditing installed add-ons and removing unused software. The remaining extensions have been verified as necessary and safe. This task highlighted the importance of the “Least Privilege” principle—only installing extensions that are absolutely necessary and granting them minimum permissions.