

ELEVATE LABS

Cyber Security Internship

Intern Name – Imam Shraf

Task 7: Identify and Remove Suspicious Browser Extensions

Objective

This task aims to identify suspicious browser extensions, understand their potential security risks, and remove them if necessary.

Extension Details

Extension Name: Free VPN for Chrome - VPN Proxy VeePN

Version: 3.6.2

Size: 3.3 MB

Status: Installed and active

Permissions Requested:

- Read and change all your data on all websites.
- Display notifications.
- Manage your apps, extensions, and themes.
- Change your privacy-related settings.

1. Unknown Installation

The extension appeared in the browser without the user's conscious installation. This could result from bundled software, deceptive pop-ups, phishing sites, or malware. Such behavior violates user consent and raises suspicion.

2. Excessive Permissions

The permissions granted are overly broad and invasive, giving the extension complete access to sensitive browsing data and settings. This makes it a high-risk extension.

3. VPN Extensions and Trust Issues

Many free VPNs have been reported to sell user data, log activity, or redirect traffic. An unknown VPN extension with full access raises serious concerns.

4. Unverified Developer Credibility

The extension lacks a credible developer profile or detailed privacy policies. This absence of transparency increases the risk of misuse.

5. Potential for Malware Distribution

With the permissions granted, the extension could log keystrokes, hijack sessions, perform clickjacking, and update itself with malicious scripts.

6. Behavioral Red Flags

Suspicious behaviors such as redirects, ads on trusted sites, sluggish performance, and unauthorized changes to settings indicate possible malicious intent.

7. Lack of Transparent Privacy Policy

No clear privacy policy was provided, indicating potential misuse of user data without accountability.

8. Broader Industry Pattern

Free VPNs have a history of covert data collection and privacy violations. This extension fits that pattern.

9. No User Consent for Incognito Mode

While not enabled in incognito mode, extensions with these permissions can still attempt to track private activity.

Conclusion

The extension was classified as suspicious due to unknown installation, broad permissions, questionable origin, and alignment with known risky VPN behaviors. Removal was necessary to protect browser security.

Action Taken

- Disabled the extension immediately.
- Uninstalled the extension completely.
- Cleared browser cache and cookies.
- Restarted the browser.
- Reviewed all installed browser extensions.
- Reset browser privacy and security settings.
- Conducted a full system malware and antivirus scan.
- Verified no suspicious network activity remained.
- Documented all steps for traceability.
- Shared learnings with peers for cybersecurity awareness.

Key Learnings

- Extensions with VPN capabilities can pose high risks if not from trusted sources.
- Always verify the origin, developer credibility, and reviews before installing browser extensions.
- Regular auditing of browser extensions is essential to maintain browser and system security.