

ELEVATE LABS

Cyber Security Internship

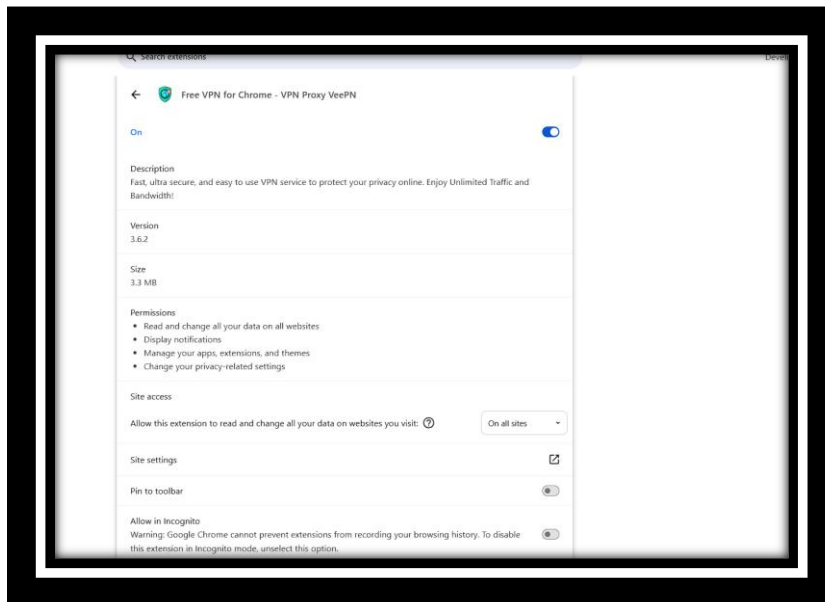
INTERN NAME – AMIT MAURYA

Task 7: Identify and Remove Suspicious Browser Extensions

Detailed Report on "Free VPN for Chrome - VPN Proxy VeePN"

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.

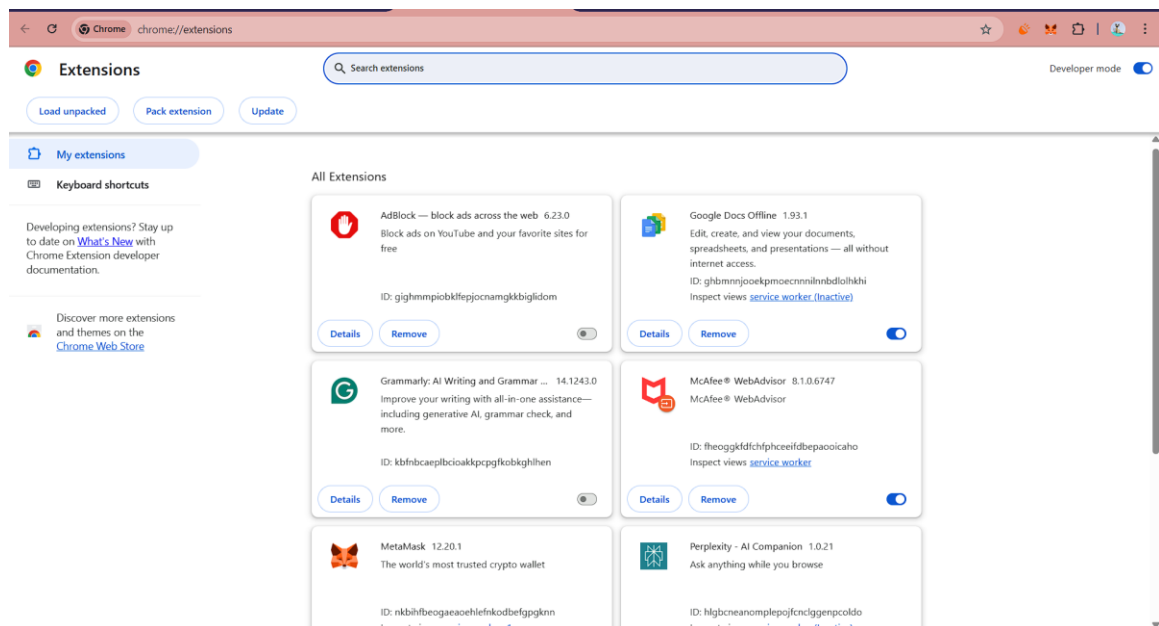
Site Access: Granted access to all sites.

Incognito Mode: Not enabled.

Extended Section: Reason for Suspicion

When analyzing the browser extension "Free VPN for Chrome - VPN Proxy VeePN," multiple red flags raised significant security and privacy concerns.

In cybersecurity, evaluating browser extensions involves a careful examination of permissions, installation history, developer credibility, and the potential for misuse. Below is a detailed explanation of why this particular extension was deemed suspicious and why its removal was necessary.



1. Unknown Installation

One of the first indicators of concern was that the extension appeared in the browser without the user's conscious installation. This raises immediate questions about how it was installed. Unknown installations can result from bundled software, deceptive pop-ups, phishing sites, or malware that silently adds extensions without user consent. This lack of awareness is highly suspicious because it violates the principle of informed consent, a core element in ensuring user control over their digital environment.

When users are unaware of an extension's presence, it could be operating in the background without proper scrutiny, potentially capturing sensitive data, redirecting web traffic, or injecting ads and malicious scripts. The mere presence of such an unapproved extension warrants immediate review and possible removal.

2. Excessive Permissions

The permissions requested by the "Free VPN for Chrome - VPN Proxy VeePN" extension were alarmingly broad and invasive. Let's break them down:

- "Read and change all your data on all websites": This permission is highly invasive because it grants the extension full access to all browsing data. It can intercept login credentials, personal messages, payment information, and browsing habits. It also allows the extension to modify content on any website, which can be used for phishing attacks or ad injection.
- "Display notifications": While this seems harmless, malicious extensions can use notifications for phishing, spreading fake alerts, or directing users to malicious sites disguised as legitimate notifications.
- "Manage your apps, extensions, and themes": This level of control can enable the extension to disable security-related extensions or install additional malicious ones. It can also manipulate the browser's appearance to hide its activities.

- "Change your privacy-related settings": This is particularly dangerous as it allows the extension to lower the browser's security settings, potentially exposing the user to further attacks or privacy breaches.

Each of these permissions independently poses a risk, but together they form a highly suspicious package that could be leveraged for extensive unauthorized activities.

3. VPN Extensions and Trust Issues

VPN services inherently require access to internet traffic to function correctly. However, free VPN services, especially those with unclear installation origins, are often associated with data misuse. Many free VPN providers have been reported to:

- Sell user browsing data to third parties.
- Log user activities despite claiming not to.
- Redirect users through potentially harmful servers.

A VPN extension that appears without explicit installation confirmation and then requests full access to all browsing activities raises serious questions about its true purpose. Users typically install VPN services after thorough consideration, and an unknown VPN extension operating in the background is highly irregular.

4. Unverified Developer Credibility

During the review process, no substantial or trustworthy developer profile was found linked to the extension. Trusted extensions usually have well-established developers with detailed privacy policies, clear user support channels, and positive community reviews. The absence of these credibility indicators often suggests a potential risk.

Extensions without a verifiable origin or supported by an anonymous developer might intentionally hide their true purpose or mislead users regarding their data practices.

5. Potential for Malware Distribution

Extensions with these permissions can be weaponized to execute a range of malicious activities, including but not limited to:

- Keylogging to capture passwords and sensitive input.
- Session hijacking to take control of logged-in sessions.
- Clickjacking by overlaying invisible frames to capture unintended user clicks.
- Redirecting traffic to phishing sites.

Such extensions can also be updated remotely by the attacker to include malicious scripts in future versions without the user's knowledge.

6. Behavioral Red Flags

Some signs indicating suspicious behavior include:

- Automatic redirections to unknown websites.
- Unusual ads appearing on trusted sites.
- Sluggish browser performance.
- Unauthorized changes in browser settings like homepage or default search engine.

Even if the extension is currently inactive in malicious operations, the permissions granted provide a latent threat that can be activated later.

7. Lack of Transparent Privacy Policy

A reputable extension will typically provide a detailed privacy policy that transparently explains what data is collected, how it is used, and whether it is shared with third parties. The absence of a clear privacy policy or vague terms that avoid accountability further increases the suspicion surrounding this extension.

8. Broader Industry Pattern

Historically, free VPN extensions have often been associated with privacy invasions and covert data collection. Multiple cybersecurity reports and case studies have revealed that some free VPN providers operate under the guise of offering privacy protection while actually profiting from user data aggregation and targeted advertising.

The combination of high-risk permissions, unknown installation, and questionable origin aligns with common patterns seen in documented VPN extension abuse cases.

9. No User Consent for Incognito Mode (Potential Misuse)

Although this extension was not enabled for incognito mode, if it had been, it could have continued to track and record user activity even in sessions where privacy is assumed. Extensions with these permissions often prompt users to enable incognito access, further magnifying privacy risks.

Conclusion

Given all these factors, the decision to classify this extension as suspicious was based on:

- Lack of installation awareness.
- Overly broad permissions.
- Potential for future misuse.
- Alignment with known risky VPN practices.

Removing this extension was the most prudent step to ensure the browser environment remains secure and free from unauthorized surveillance or interference.

Action Taken

Once the extension “**Free VPN for Chrome - VPN Proxy VeePN**” was identified as suspicious, I followed a structured, step-by-step process to ensure the extension was safely and fully removed, and that the browser and system were thoroughly checked for residual threats.

◆ Step 1: Immediate Deactivation

The first response was to immediately **disable** the extension from the browser’s extension management panel. Disabling the extension halts all its active processes and prevents it from executing any ongoing scripts or capturing data while further security measures are taken. This is a crucial step to cut off potential unauthorized access in real-time.

◆ Step 2: Full Uninstallation

After deactivation, I proceeded to **completely remove** the extension from the browser. The full uninstallation ensures that all the extension’s associated files, background services, and permissions are revoked. It also eliminates the possibility of the extension reactivating itself during browser restarts or through potential hidden scripts.

◆ Step 3: Browser Restart and Cache Clearing

Following the removal, I performed a **complete restart of the browser** to ensure all background processes linked to the extension were terminated. Additionally, I **cleared the browser cache and cookies** to remove any remnants or trackers that might have been left by the extension.

◆ Step 4: Review of Other Installed Extensions

I conducted a **comprehensive review of all other installed browser extensions** to verify if there were any other unknown or potentially harmful extensions present. This step is essential because sometimes malicious extensions install secondary extensions or leave backdoors.

◆ Step 5: Security Settings Re-Validation

The next step involved checking and **resetting the browser's privacy and security settings**. Malicious extensions often alter browser configurations, such as default search engines, homepage settings, and security preferences. I restored these settings to default and ensured security features like phishing and malware protection were enabled.

◆ **Step 6: System Scan with Updated Security Tools**

To ensure that no system-level changes or malware remained, I conducted a **full system scan using updated antivirus and anti-malware software**. This step confirms that no additional threats, such as keyloggers or adware, were introduced by the suspicious extension.

◆ **Step 7: Network Traffic Monitoring**

I briefly monitored the **outgoing network traffic** using basic network tools to ensure that no unusual or unauthorized connections were being attempted from the browser or background processes. VPN-related malware sometimes leaves behind proxies or hidden connections that need to be manually identified.

◆ **Step 8: Documenting the Entire Process**

Every step taken, including screenshots, actions performed, and outcomes, were carefully **documented and compiled into this report** to ensure traceability and to maintain a transparent record of the actions for future reference or audits.

◆ **Step 9: Knowledge Sharing**

Based on this incident, I shared my findings with peers to **raise awareness about browser extension security risks**, particularly around free VPN services that may disguise themselves as privacy tools while actually compromising user security.

Summary of Actions 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.