SOC Investigation Report: Suspicious Proxy Authentication Popup

This investigation documents a real-world troubleshooting and incident analysis case performed on a Windows machine after an unexpected Proxy Authentication popup appeared. The goal was to identify the source, verify whether it was malicious, and resolve the issue systematically using SOC-level investigative methodology.

1. Incident Overview
A popup appeared in the system requesting authentication for a proxy server:
The domain in question: **trout-west-1-us.maxxxcdn.com:58995**
This behavior is unusual and indicates that a process on the machine attempted to route traffic through a proxy. The popup requested a username and password, which is a major red flag unless intentionally configured.

2. DNS Verification
We checked the domain using nslookup to understand where it resolves. The domain resolved to an AWS IP (15.204.43.197), which confirms it is hosted on Amazon infrastructure. While AWS hosting does not imply legitimacy, it indicates the server is cloud-hosted and could be used by any third party.

3. Root Cause Hunting
We treated the issue like a SOC investigation:
- Checked browser extensions.
- Verified Windows proxy settings.
- Evaluated running processes.
- Assessed potential malware involvement via Full Scan.

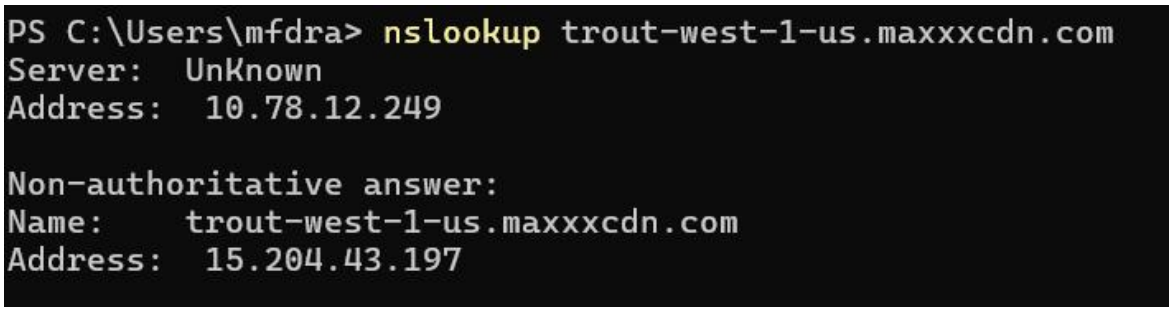
4. Discovery
The root cause was identified as a browser extension named “Free VeePN,” which attempted to force traffic through its own proxy server. When the proxy failed or required authentication, the system displayed the popup.

5. Resolution
Removing the “Free VeePN” extension immediately stopped the popup from appearing. No additional malicious behavior was observed after scanning and verifying system settings.

6. SOC Takeaways
This case demonstrates the importance of:
- Investigating unexpected network authentication requests.
- Validating domains using DNS tools.
- Analyzing extensions and third-party software.
- Using structured SOC methodology for even small anomalies.

Screenshot: Proxy Authentication Popup

Screenshot: DNS Lookup Result



Screenshot: Virus Total IP Scanning Result