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.

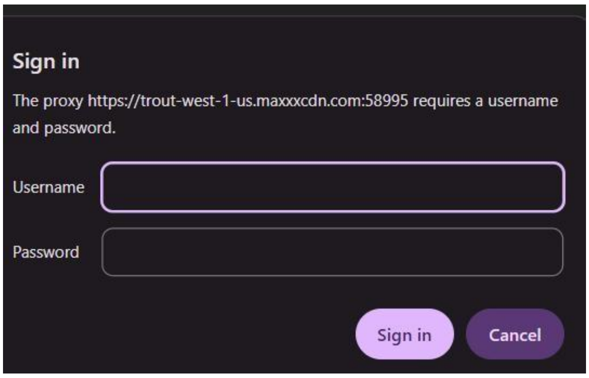
5. Resolution

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.

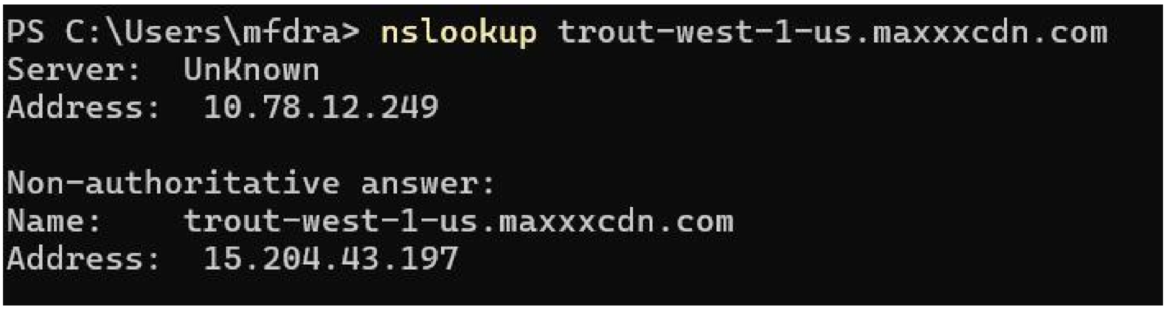
Screenshot: Proxy Authentication Popup



Sign in

The proxy https://trout-west-1-us.maxxxcdn.com:58995 requires a username and password.

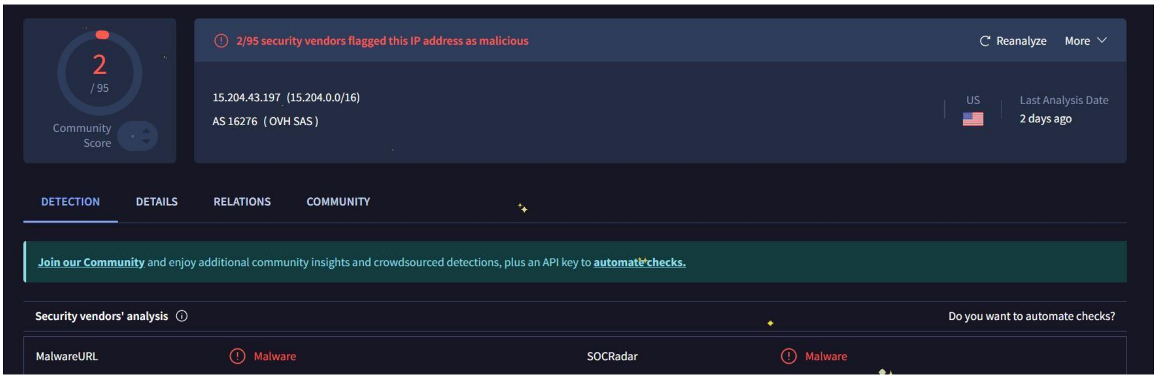
Screenshot: DNS Lookup Result



```
PS C:\Users\mfdra> nslookup trout-west-1-us.maxxxcdn.com
Server:  UnKnown
Address:  10.78.12.249

Non-authoritative answer:
Name:    trout-west-1-us.maxxxcdn.com
Address:  15.204.43.197
```

Screenshot: Virus Total IP Scanning Result



2/95 security vendors flagged this IP address as malicious

15.204.43.197 (15.204.0.0/16)
AS 16276 (OVH SAS)

US

Last Analysis Date
2 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

MalwareURL Malware SOCRadar Malware

5. Security Engineering and Automated Response (SOAR Component)

This section demonstrates how the findings from this manual investigation can be translated into a scalable, automated solution for the enterprise, effectively addressing the root cause and reducing SOC Analyst Toil.

5.1. Detection Rule Enhancement

The core finding was that a browser extension was forcing traffic to an external, unapproved proxy endpoint. We can use this finding to create a strong detection rule rather than relying on user reports:

Indicators: The suspicious domain (trout-west-1-us.maxxxcdn.com), the AWS-hosted IP (15.204.43.197), and the use of a high, non-standard port (58995).

Proposed SIEM Rule Logic: A **High-Priority Alert** should be generated in the SIEM (e.g., Sentinel/Chronicle) when:

A known user application (like a browser executable) initiates a network connection to an IP address categorized as **Public Cloud (AWS)**,

AND the destination port is **high and non-standard** (e.g., above 50000).

5.2. SOAR Playbook Design

To ensure an immediate and company-wide response, the following automated actions are executed by the SOAR platform upon the alert trigger:

Step	***Action (Automation)***	***Engineering Value Added***
1. Verification	Context Enrichment: Automatically submit the suspected IP and Domain to the Threat Intelligence platform (VirusTotal API) to confirm its reputation.	Reduces manual lookup time and increases confidence for the analyst.
2. Network Containment	Global Firewall Enforcement: Immediately send an command to the corporate Firewall and Proxy Gateway to blacklist (block) the malicious domain and the specific IP address.	Rapid Containment: Prevents all other users in the network from connecting to the C2/Proxy endpoint.
3. Endpoint Remediation	Forceful Uninstallation: Send a command to the EDR/MDM system (Endpoint Management) to mass-uninstall the "Free VeePN" extension from all corporate machines.	Systemic Fix: Eradicates the root cause across the organization instantly.

4. Case Management	**Auto-Closure:** Update the incident ticket in the ITSM system with the label **"Closed - Automated Remediation"** and document all actions taken.	***Metric Improvement:*** *Significantly reduces the* ***Mean Time To Resolution (MTTR)*** *and streamlines SOC operations.*