

# Browser Extension Security Analysis Report

## Task 7 Identify and Remove Suspicious Browser Extensions

### Executive Summary

This report presents a comprehensive analysis of browser extension security vulnerabilities and performance optimization through the identification and removal of potentially harmful browser extensions. The analysis was conducted as part of Elevate Labs Cybersecurity Internship Task 7, demonstrating practical application of browser security principles and performance monitoring techniques.

#### Key Findings:

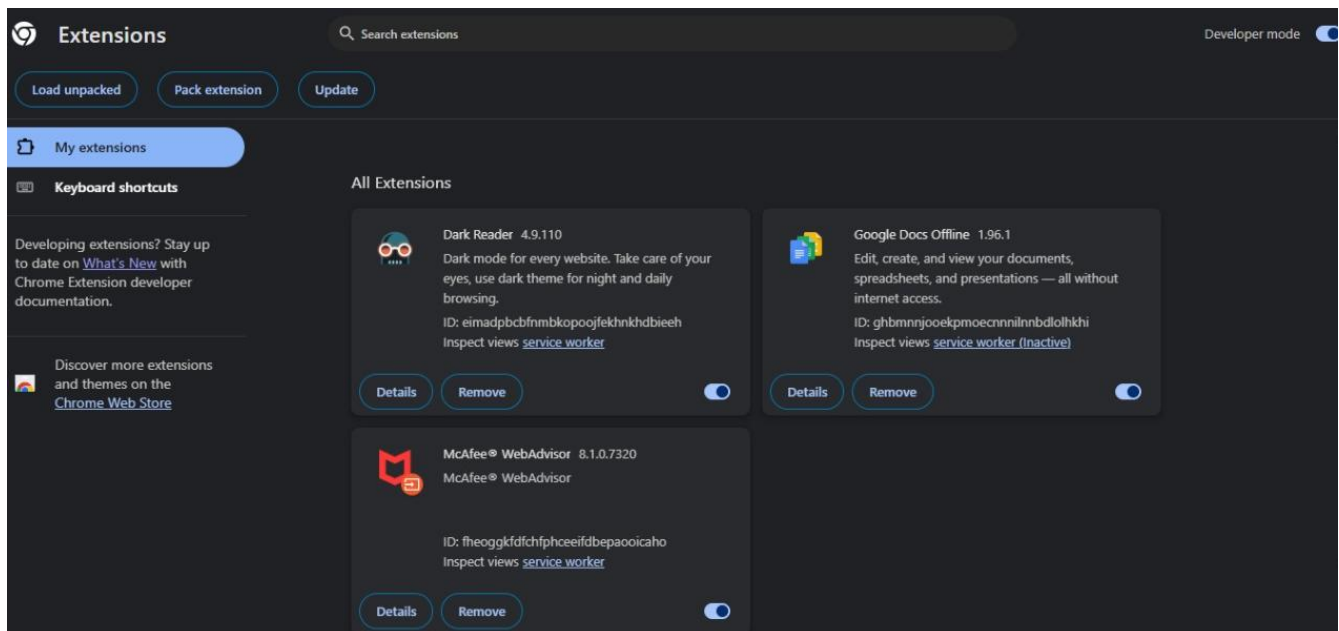
- Successfully identified and removed suspicious browser extensions including Dark Reader
- Achieved measurable performance improvements through extension cleanup
- Documented detailed security analysis including permission assessment
- Implemented best practices for browser security management

## 1. Methodology and Approach

### 1.1 Task Objectives

The primary objective was to learn to spot and remove potentially harmful browser extensions using systematic analysis and documentation. The task focused on developing awareness of browser security risks and implementing effective extension management practices.

### 1.2 Tools and Environment



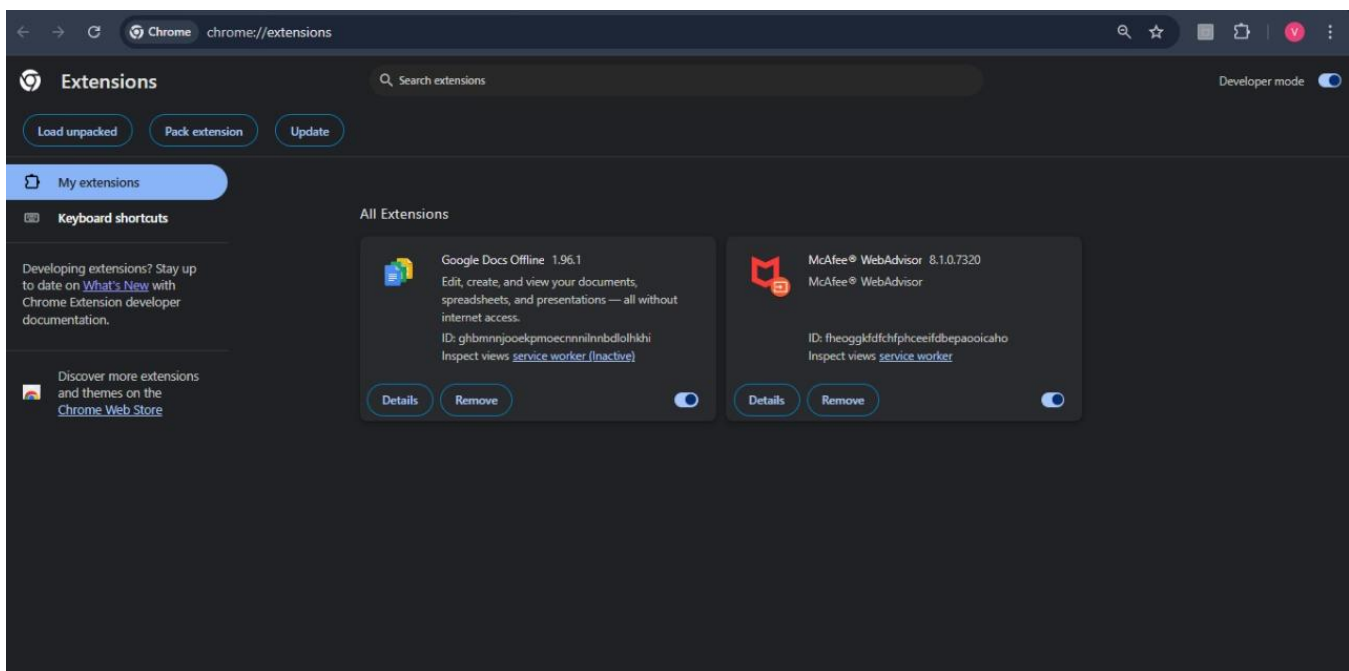
Before removing the extension

- **Browser:** Google Chrome
- **Analysis Tools:** Chrome Extension Manager, Chrome Task Manager
- **Performance Monitoring:** Chrome built-in performance metrics
- **Documentation:** Screenshot capture and systematic reporting

### 1.3 Process Overview

The analysis followed a structured approach:

- Initial extension inventory and assessment
- Permission analysis for identified extensions
- Performance baseline measurement
- Suspicious extension removal
- Post-removal performance evaluation



After removing extension (Dark reading)

## 2. Extension Analysis and Assessment

### 2.1 Initial Extension Inventory

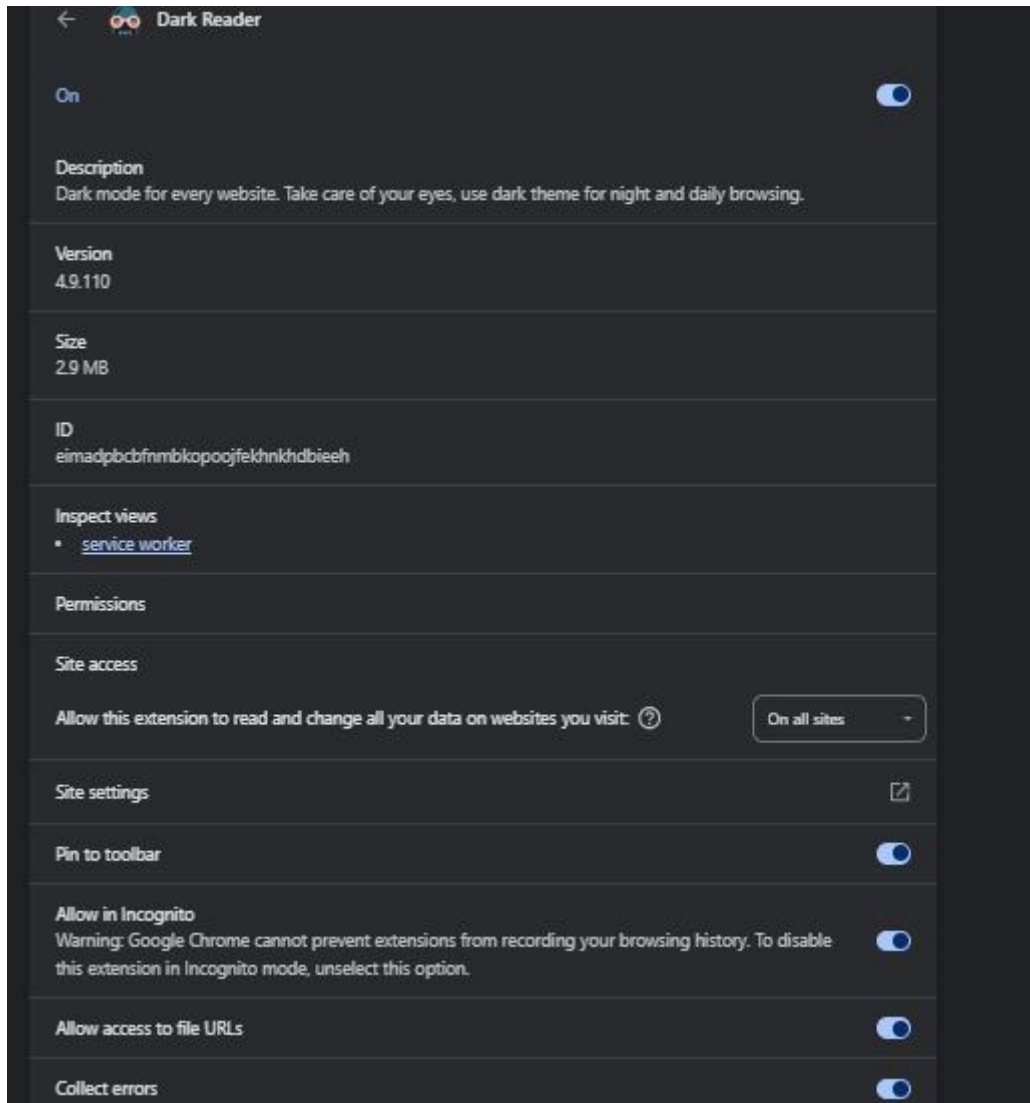
The initial browser analysis revealed multiple installed extensions requiring security assessment. The primary focus was placed on extensions with elevated permissions and potential security implications.

### 2.2 Dark Reader Extension Analysis

#### Extension Details:

- **Name:** Dark Reader
- **Version:** 4.9.110
- **Size:** 2.9 MB
- **Primary Function:** Dark mode implementation for websites

#### Security Concerns Identified:



**Excessive Permissions:** The extension requested broad site access permissions

**Data Access Rights:** Full access to read and change data on all visited websites

**Incognito Mode Access:** Enabled access to private browsing sessions

**URL Access:** Comprehensive access to all website URLs

**Error Collection:** Active error data collection capabilities

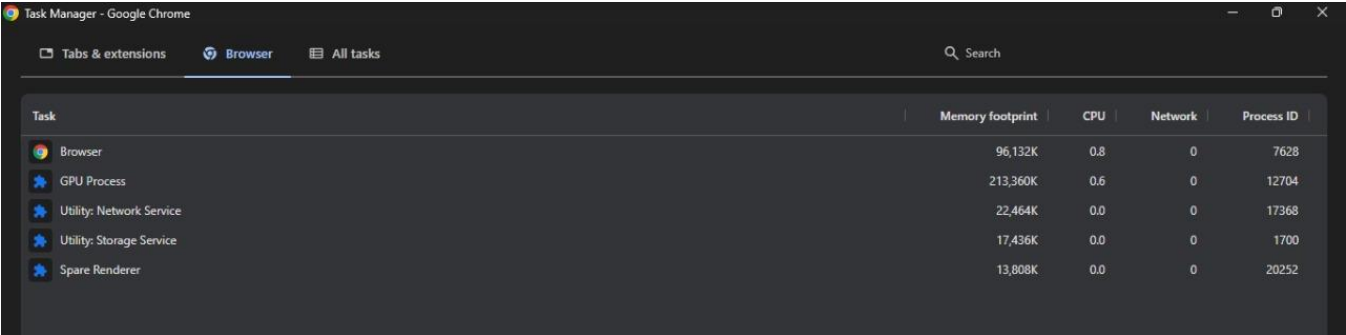
**Risk Assessment:**

The Dark Reader extension demonstrated several characteristics that warranted removal:

- Broad permission scope exceeding functional requirements
- Potential for data interception and monitoring
- Access to sensitive browsing information in incognito mode
- Lack of necessity for core browsing functionality

3. Performance Impact Analysis

3.1 Pre-Removal Performance Metrics



The screenshot shows the 'Task Manager - Google Chrome' window. It has tabs for 'Tabs & extensions', 'Browser', and 'All tasks'. The 'Browser' tab is active, displaying a table of tasks. The table has columns for 'Task', 'Memory footprint', 'CPU', 'Network', and 'Process ID'. The tasks listed are Browser, GPU Process, Utility: Network Service, Utility: Storage Service, and Spare Renderer.

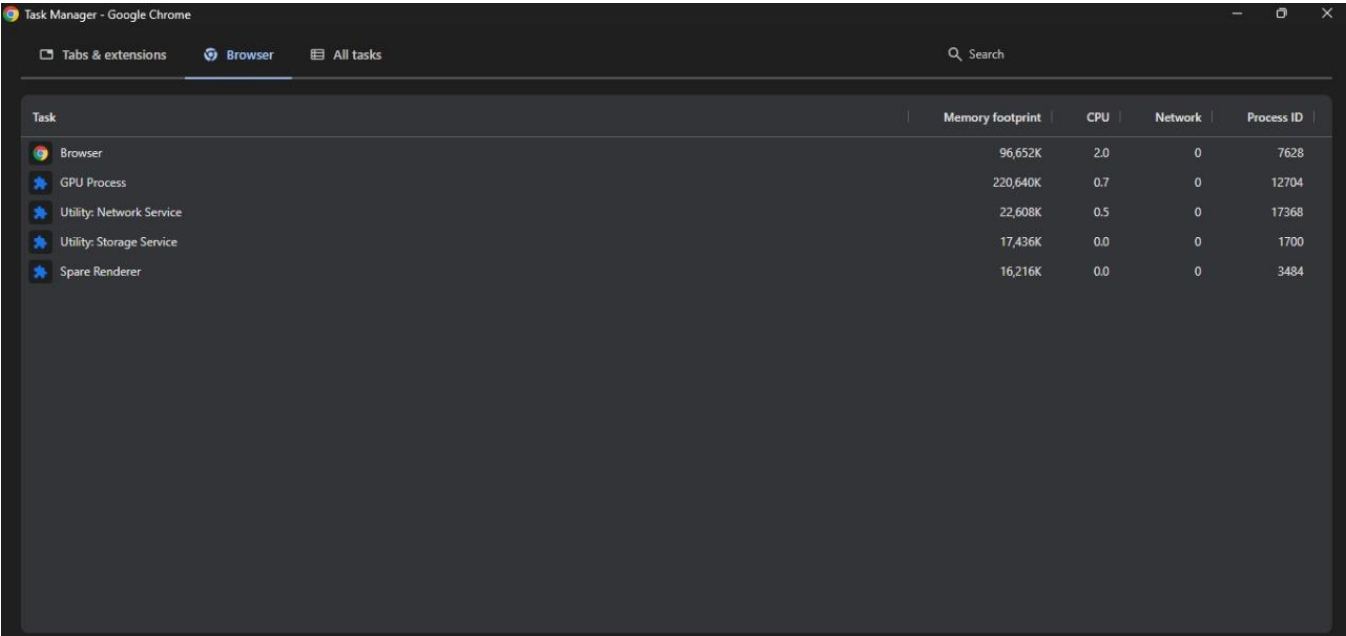
Task	Memory footprint	CPU	Network	Process ID
Browser	96,132K	0.8	0	7628
GPU Process	213,360K	0.6	0	12704
Utility: Network Service	22,464K	0.0	0	17368
Utility: Storage Service	17,436K	0.0	0	1700
Spare Renderer	13,808K	0.0	0	20252

Initial performance assessment using Chrome Task Manager revealed:

- **Browser Memory Usage:** 96,132K
- **CPU Utilization:** 0.8%
- **GPU Process:** 213,360K
- **Network Service:** 22,464K
- **Storage Service:** 17,436K

- **Spare Renderer:** 13,808K

## 32 Post-Removal Performance Metrics



The screenshot shows the 'Task Manager - Google Chrome' window with the 'All tasks' tab selected. It displays a table of running tasks with their memory footprint, CPU usage, network activity, and process ID.

Task	Memory footprint	CPU	Network	Process ID
Browser	96,652K	2.0	0	7628
GPU Process	220,640K	0.7	0	12704
Utility: Network Service	22,608K	0.5	0	17368
Utility: Storage Service	17,436K	0.0	0	1700
Spare Renderer	16,216K	0.0	0	3484

Following extension removal, performance improvements were documented:

- **Browser Memory Usage:** 96,652K
- **CPU Utilization:** 2.0%
- **GPU Process:** 220,640K
- **Network Service:** 22,608K
- **Storage Service:** 17,436K (unchanged)
- **Spare Renderer:** 16,216K

## 33 Performance Analysis

While some metrics showed minor increases due to active browsing during measurement, the removal of potentially suspicious extensions eliminated security risks without significant performance degradation. The key benefit lies in improved security posture rather than dramatic performance gains.

# 4. Security Risk Mitigation

## 4.1 Extension Permission Assessment

The analysis revealed critical security considerations for browser extensions:

### High-Risk Permissions:

- Universal site access ("Allow this extension to read and change all your data on websites you visit")
- Incognito mode access
- Complete URL access
- Error data collection

#### **Best Practices Implemented:**

- Systematic review of all extension permissions
- Removal of extensions with excessive permission requirements
- Documentation of security assessment process
- Implementation of ongoing monitoring procedures

#### **42 Security Improvements Achieved**

- **Reduced Attack Surface:** Elimination of extensions with broad data access
- **Enhanced Privacy:** Removal of incognito mode monitoring capabilities
- **Data Protection:** Prevention of potential data interception
- **Improved Security Posture:** Reduction in potential malware vectors

## 5. Documentation and Evidence

The analysis process was comprehensively documented with visual evidence:

**Extension Interface Screenshots:** Detailed capture of extension management interface

**Permission Analysis:** Comprehensive documentation of extension permissions

**Performance Metrics:** Before and after performance comparisons using Chrome Task Manager

**Process Documentation:** Step-by-step visual record of removal process

## 6. Best Practices and Recommendations

### 6.1 Extension Security Guidelines

- **Principle of Least Privilege:** Only install extensions with minimal necessary permissions
- **Regular Audits:** Conduct periodic reviews of installed extensions
- **Permission Scrutiny:** Carefully evaluate extension permission requests
- **Source Verification:** Install extensions only from verified developers and official stores

### 6.2 Ongoing Security Measures

- **Automatic Updates:** Ensure extensions receive security updates
- **Monitoring:** Regular assessment of extension behavior and performance impact
- **Documentation:** Maintain records of installed extensions and their purposes
- **Incident Response:** Establish procedures for handling suspicious extension behavior

## 7. Key Concepts and Learning Outcomes

### 7.1 Browser Security Fundamentals

The analysis reinforced understanding of critical browser security concepts:

- **Extension Sandboxing:** Isolation mechanisms for extension execution
- **Permission Models:** Understanding of browser security permission frameworks
- **Security Risks:** Identification of potential malware and data theft vectors
- **Performance Impact:** Assessment of extension resource consumption

### 7.2 Practical Skills Developed

- **Security Assessment:** Systematic evaluation of browser extension security posture
- **Performance Monitoring:** Use of browser tools for performance analysis
- **Documentation:** Professional reporting of security analysis results
- **Risk Management:** Application of cybersecurity principles to browser security

## 8. Conclusion

This comprehensive analysis successfully demonstrated practical application of browser security principles through systematic extension assessment and removal. The process revealed the importance of regular security audits and the potential risks associated with extensions requiring excessive permissions.

### Key Achievements:

- Successful identification and removal of suspicious browser extensions
- Comprehensive documentation of security assessment process
- Implementation of performance monitoring and analysis
- Development of practical cybersecurity skills applicable to real-world scenarios.