

# The Attacker's Distributed Supercomputer: Your Browser

Jerry Hoff  
jerry@sqr.x.com



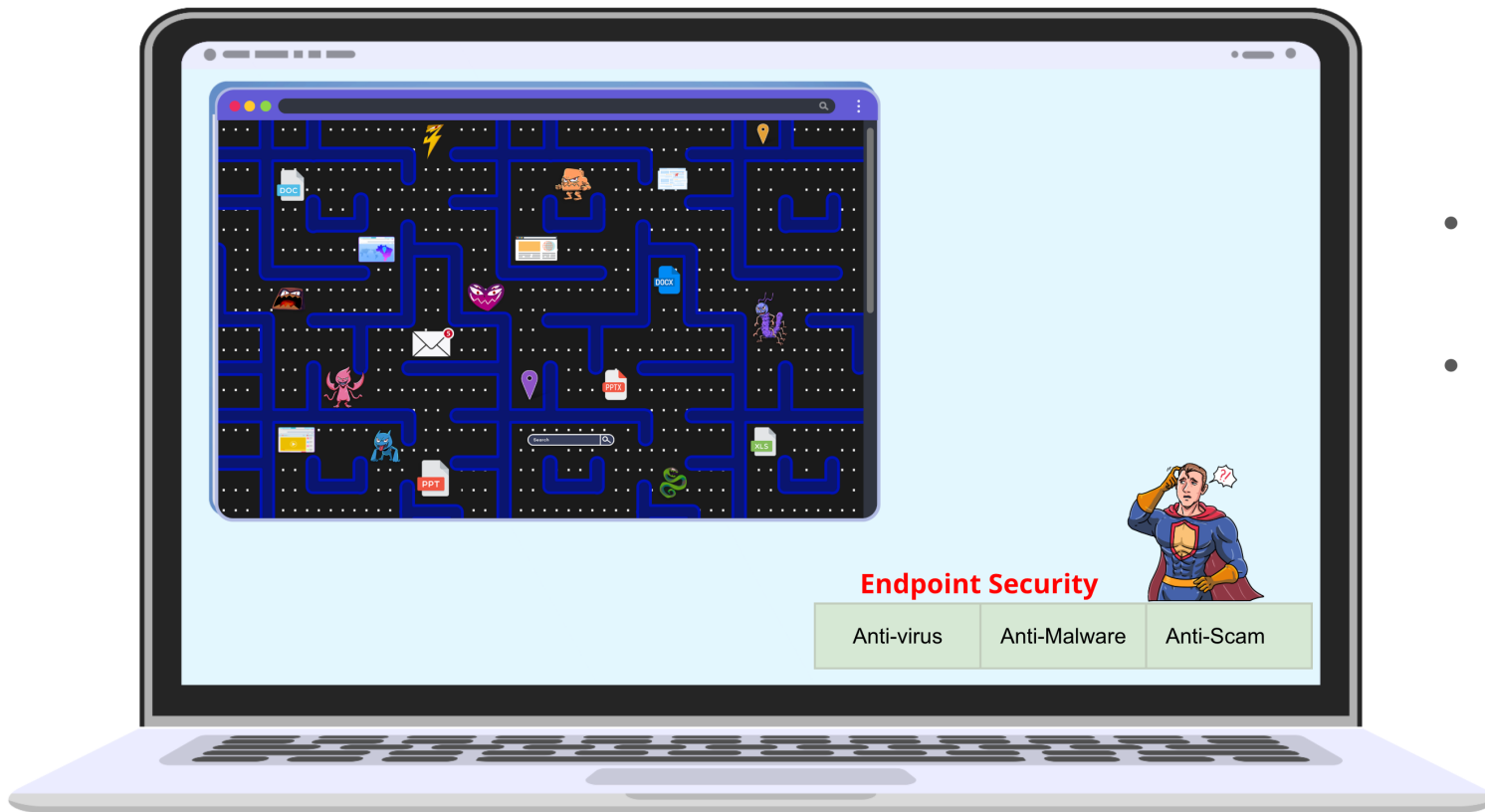
# Browser Security is the next Battleground

- Browsers are the gateway to modern work but lack dedicated monitoring
- Traditional endpoint protection (EDR/XDR) and network security (SWG/SASE) don't fully "see" browser activity
- Most organizations don't inventory or restrict browsers—leaving them exposed
- **The browser is a blind spot in the security stack**

# Power of Modern Browsers

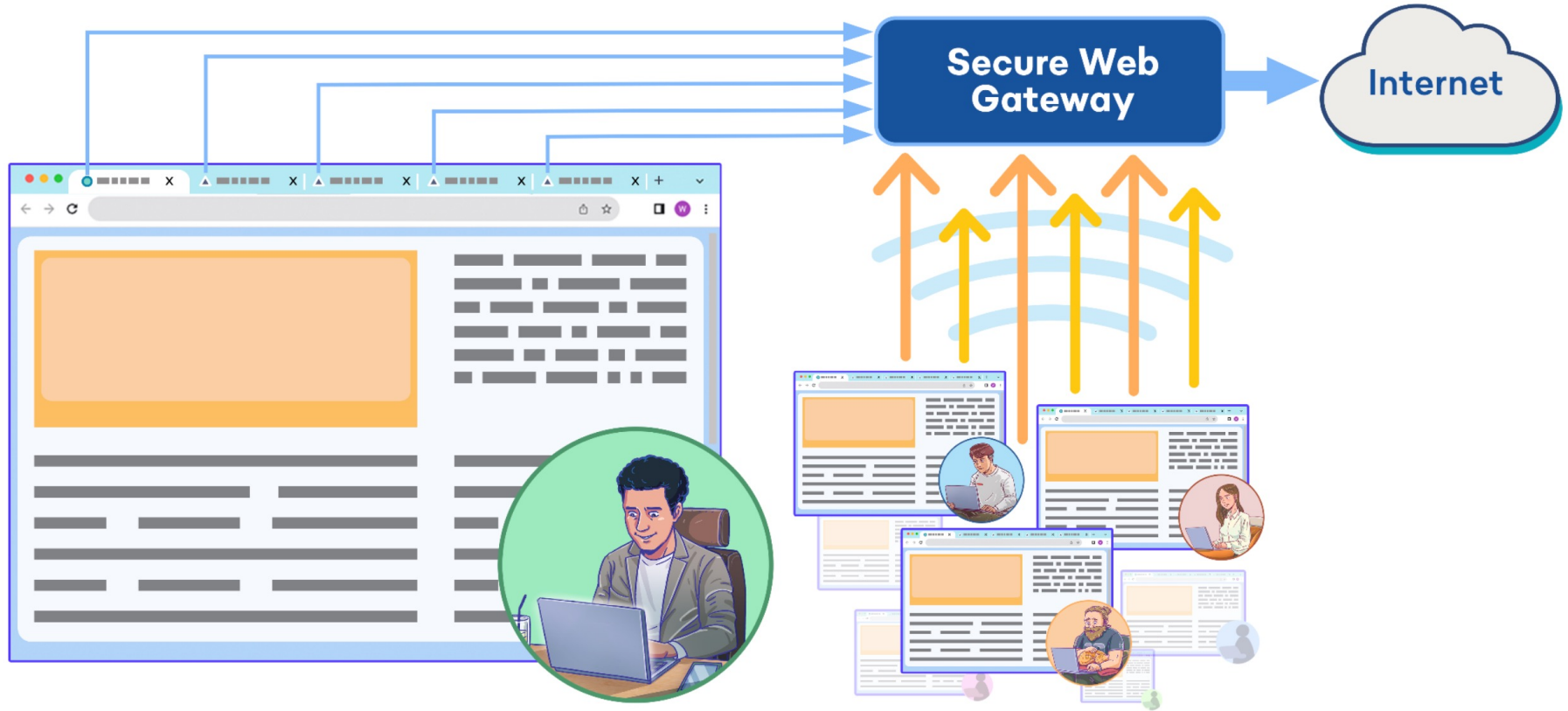
- Browser apps rival native software: Office suites, video editing, gaming, live conferencing
- Evolving features: WebAssembly (WASM), HTML5, WebRTC, file APIs, and more
- Result: Browsers are no longer just “viewers” ... they’re full-fledged platforms
- **More power = larger attack surface**

# Endpoint Security has Zero visibility into the Browser



- Endpoint security primarily monitors only file and process memory
- No visibility into the browser or webapps running in it

# Secure Web Gateways



# The Rise of Browser-Based Attacks

**NEWS** 14 JAN 2025

## Browser-Based Cyber-Threats Surge as Email Malware Declines

Browser-based cyber-threats have surged throughout 2024, marking a significant shift in the tactics employed by malicious actors.

According to new findings from the *2024 Threat Data Trends* report by the eSentire Threat Response Unit (TRU), while malware delivered via email declined last year, browser-sourced threats, including drive-by downloads and malicious advertisements, rose sharply.

These techniques are being increasingly used to deliver malware, such as [Lumma Stealer](#) and NetSupport Manager RAT, with attackers favoring them due to their ability to bypass traditional email filters and security controls.

<https://www.infosecurity-magazine.com/news/browser-cyberthreats-surge-email/>

# The Rise of Browser-Based Attacks

 **paloalto**  
NETWORKS |  **UNIT 42**

## Global Incident Response Report

**2025**

### **The browser is a key conduit for threats.**

Nearly half of the security incidents we investigated (44%) involved malicious activity launched or facilitated through employees' browsers. This included phishing, abuse of URL redirects and malware downloads, each exploiting the browser session without adequate detection or blocking.

The user's interaction with malicious links, domains or files, combined with insufficient security controls led to compromise. Organizations must improve visibility and implement robust controls at the browser level to detect, block and respond to these threats before they spread.

# Browser Supply Chain Attacks

- Dec 25, 2024 Cyberhaven's admin was targeted via phishing
- "Your Chrome extension violated Google's policy"
- Linked to a Google consent screen, requesting permission for an OAuth app called Privacy Policy Extension.
- Admin granted permissions, allowing attackers to upload new versions of the extension
- Malicious version pushed automatically to 400k users, designed to steal passwords, cookies, etc.

## Chrome Web Store

Hi there,

We wanted to let you know that your item is at risk of being removed from the Chrome Web Store. Please see the details below.

**Item name:** Cyberhaven security extension V3

**Item ID:** [pajkinmeojmbapicmbpliphjmcekaac](#).

**Violation(s):**

**Excessive and/or irrelevant keywords in the product description:**

- **Violation:**
  - Unnecessary details in the description
- **Relevant section of the program policy:**
  - *We do not allow extensions with misleading, poorly formatted, non-descriptive, irrelevant, excessive, or inappropriate metadata, including but not limited to the extension description, developer name, title, icon, screenshots, and promotional images.*

The Chrome Web Store requires all developers to comply with both the Developer Program Policies listed below and the Developer Agreement.

Please accept our policies to continue publishing your products.

[Go To Policy](#)

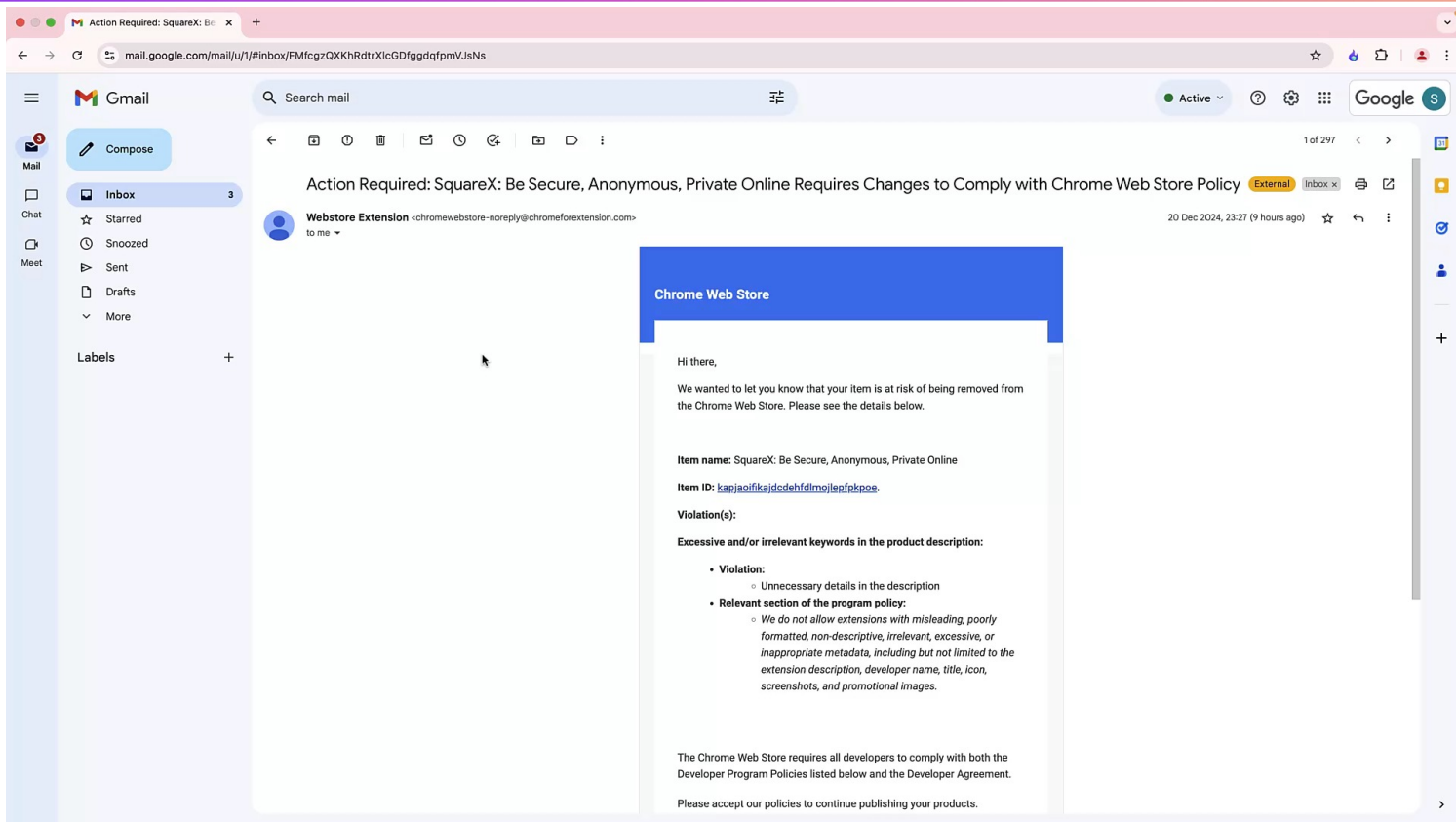
We value developer contributions to the Chrome Web Store, and look forward to helping you bring your item into compliance with our policies.

Thanks,

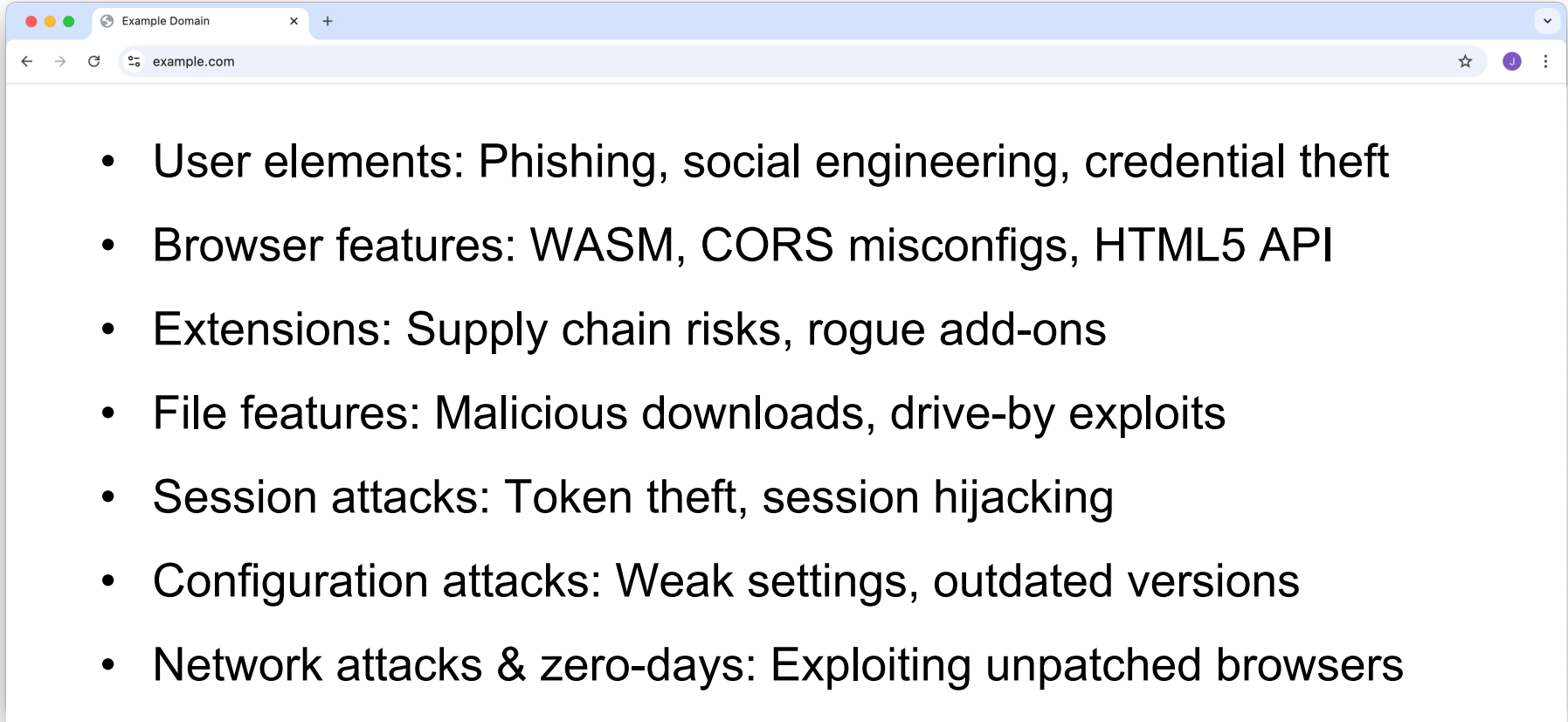
Chrome Web Store Developer Support



# Cyberhaven Attack Video



# Understanding the Brower Attacks Surface



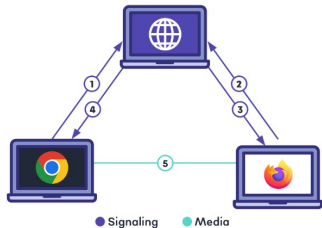
A browser window mockup with a single tab titled 'Example Domain'. The address bar shows 'example.com'. The main content area displays a bulleted list of browser attack surface categories.

- User elements: Phishing, social engineering, credential theft
- Browser features: WASM, CORS misconfigs, HTML5 API
- Extensions: Supply chain risks, rogue add-ons
- File features: Malicious downloads, drive-by exploits
- Session attacks: Token theft, session hijacking
- Configuration attacks: Weak settings, outdated versions
- Network attacks & zero-days: Exploiting unpatched browsers

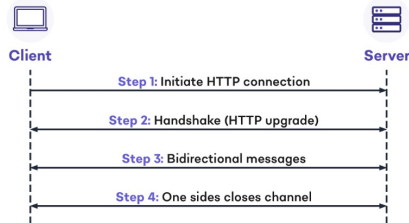
# Network Channel based Attack Vectors: Part I



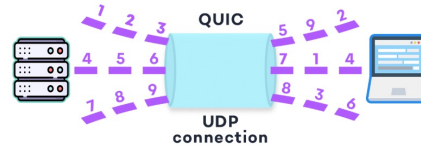
- Created by Google in 2011
- Transmits data with SRTP and SCTP
- Built on top of UDP
- Used for Peer-to-Peer Communication
- Natively Supported by the browser



- Introduced as Part of HTML5
- Built on top of TCP
- Supports Binary and Text data exchange
- Full-Duplex Communication
- Primarily used for Real-Time, Low Latency Communication.



- Supported on Chromium 97, Firefox 114 and later versions. (Rolled out in 2021)
- For Low Latency data exchanges, gaming, etc.
- Supports unreliable/reliable exchange of unordered/ordered data.
- Built on top of HTTP/3 and uses HTTP/2 as fallback



- Created by Google in 2015
- Uses Protocol buffer to encode data
- Built on top of HTTP/2
- Supports bi-directional streaming
- Browser supports gRPC-web and it uses a special proxy to communicate with gRPC services

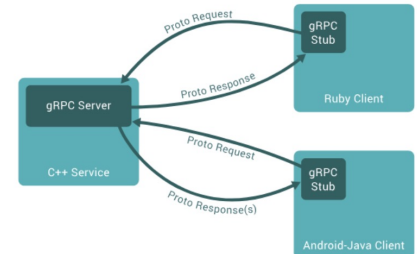


Image Reference: <https://grpc.io/docs/what-is-grpc/introduction/>

# Network Channel based Attack Vectors: Part II



## Server Sent Events

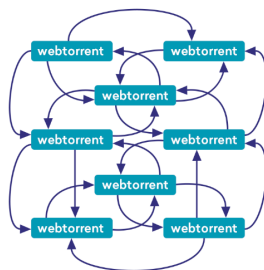
- Introduced by WHATWG and is part of HTML standard
- Built on top of TCP
- Unidirectional stream.
- Used for sending notification and events from the server to client.
- Natively supported by all browsers

### HTTP with Server-Sent Events



## Web Torrent

- Streaming torrent client for web browser
- Uses WebRTC for P2P Communication
- Different than Bittorrent and can only connect to clients that support WebTorrent/WebRTC
- Supported on all popular browser



## Firebase Cloud Messaging

- Formerly known as Google Cloud Messaging (created by Google in 2012)
- Heavily used for delivering notifications on mobile phones and web apps
- Leverages Web Push Protocol
- Natively Supported by the browser

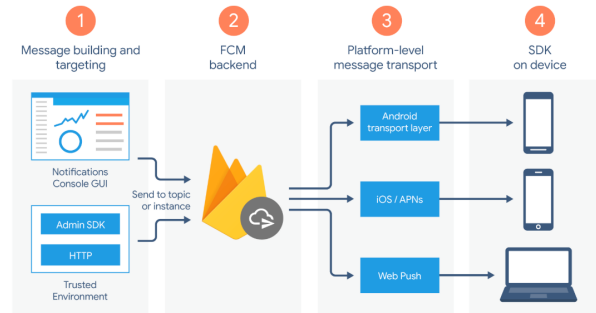
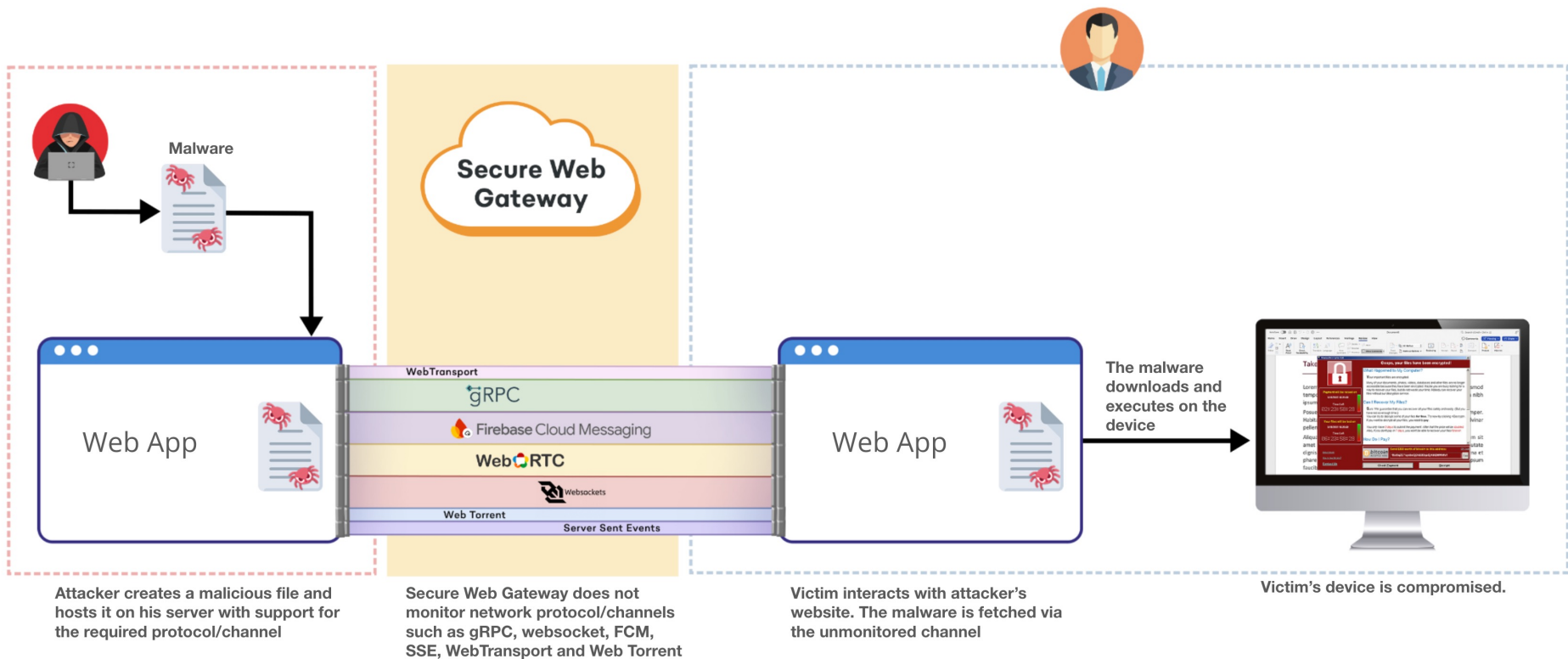


Image Reference: <https://firebase.google.com/docs/cloud-messaging/fcm-architecture>

# Unmonitored Channel Attacks



# Browser Phishing

- SWGs normally check links before allowing connection to user's browser
- Designed to block malicious links based on analysis of webpage
- Attackers are now doing the following:
  - Setting up non-malicious websites that seem legitimate to a SWG
  - Use JavaScript or WASM to maliciously transform the page only in a victim's browser
- Using legitimate sites like google workspace, sharepoint online, etc as a stepping stone to malicious sites

**NEWS** 14 JAN 2025

**Browser-Based Cyber-Threats Surge as Email Malware Declines**

# Clipboard Hijacking (aka "ClickFix")

## Verify You Are Human

Please verify that you are a human to continue.



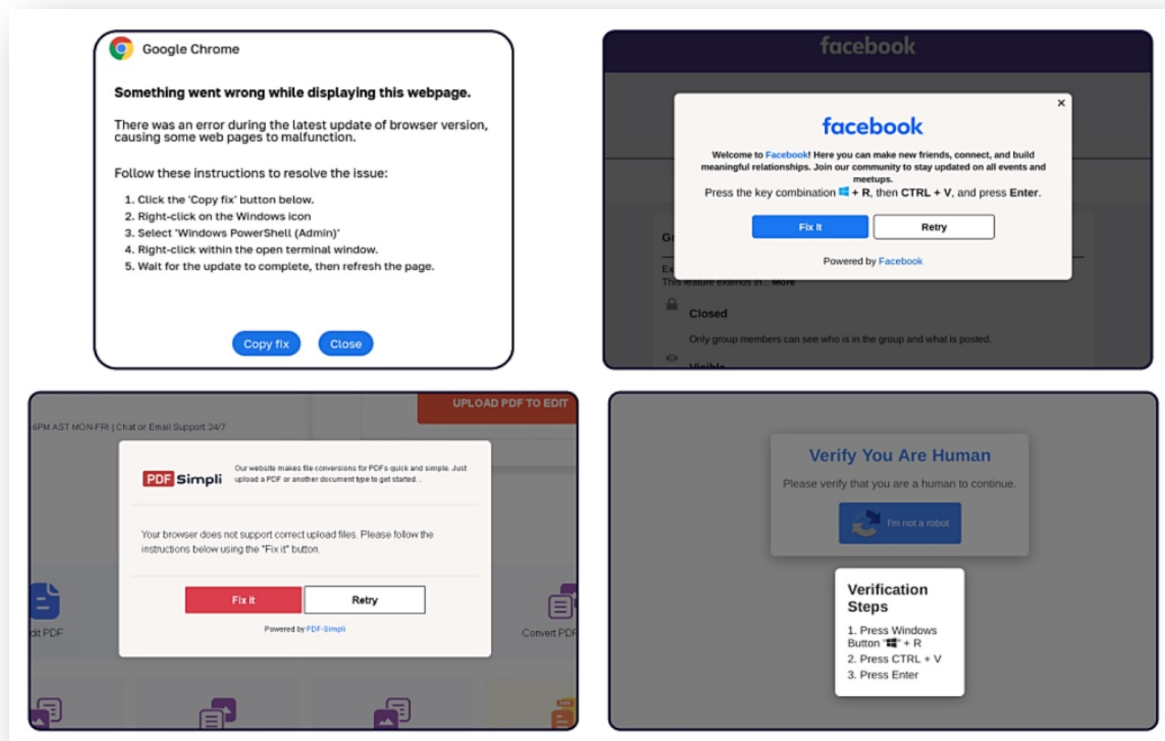
I'm not a robot

## Verification Steps

1. Press Windows Button "  " + R
2. Press CTRL + V
3. Press Enter

<https://krebsonsecurity.com/2025/03/clickfix-how-to-infect-your-pc-in-three-easy-steps/>

# Clipboard Hijacking (aka "ClickFix")





# Extensions

- Extend the capabilities of the browser
- Are often highly over privileged
- Minimal checks via the web app store
- Recent movements from V2 to V3 has improved security, not all browsers enforcing this

# Extension Capabilities

- Read and modify every web page
- Exfiltrate data silently
- Inject malicious code into uploads/downloads
- Modify DOM elements
- Act on behalf of the user session
- Even modify or disable other extensions

# Web Store Badges

You can find badge icons below the name of an extension in the Chrome Web Store.

## **Featured badge**

Featured extensions follow our technical best practices and meet a high standard of user experience and design.

Before it receives a Featured badge, the Chrome Web Store team must review each extension. The team checks for adherence to [CWS best practices](#), an intuitive user experience, and use of the latest platform APIs, among other things.

## **Established Publisher badge**

The Established Publisher badge features publishers who are verified and demonstrates compliance with our [developer program policies](#). This badge is granted to publishers who meet both of these conditions:

- The publisher's identity is verified.
- The publisher has a consistent positive track record with Google services.

**Tip:** Publishers can't pay to receive Chrome Web Store badges.

If you're a publisher, [learn more about Chrome Web Store badges](#).

# Attackers Buy & Poison Popular Extensions

Google has forcibly uninstalled the immensely popular 'The Great Suspender' extension from Google Chrome and classified it as malware.

The Great Suspender is a Chrome extension that will suspend unused tabs and unload its resources to decrease the browser's memory usage. When a user is ready to use the tab again, they simply had to click it on to make it visible.

This extension was immensely popular with over 2,000,000 users and has consistently been a recommended extension due to its ability to reduce Chrome's memory usage.

When Google removed it on Thursday, users were left with a message stating that "This extension contains malware," but not providing any further context on how to recover their suspended tabs or why they removed it.

## The Great Suspender's fall from grace

In June 2020, the developer of The Great Suspender sold the extension to an unknown entity as he did not have the time to properly maintain the project.

At the time, users were suspicious of the sale as why would a company purchase a free open-source extension that did not generate any revenue for the developer.

As free extensions have been purchased in the past and then monetized with malicious changes, such as injecting ads or stealing information, users were concerned the same would happen with The Great Suspender.

Unfortunately, the user's concerns were justified when the new maintainer updated the extension in October 2020 to release version 7.1.8, which included scripts that tracked the user's behavior and executed code retrieved from a remote server.

<https://www.bleepingcomputer.com/news/security/the-great-suspender-chrome-extensions-fall-from-grace/>

# Attackers Buy & Poison Popular Extensions

## Tech Note - Malicious browser extensions impacting at least 3.2 million users

13 February 2025 - GitLab Threat Intelligence

### Key Points

- We identified a cluster of at least 16 malicious Chrome extensions used to inject code into browsers to facilitate advertising and search engine optimization fraud. The extensions span diverse functionality including screen capture, ad blocking and emoji keyboards and impact at least 3.2 million users.
- We assess that the threat actor acquired access to at least some of the extensions from their original developers, rather than through a compromise. The threat actor has been trojanizing extensions since at least July 2024.
- The threat actor uses a complex multistage attack to degrade the security of users' browsers and then inject content, traversing browser security boundaries and hiding malicious code outside of extensions. We have only been able to partly reproduce the threat actor's attack chain.
- The threat actor may also be associated with phishing kit development or distribution. The malicious extensions present a risk of sensitive information leakage or initial access.

<https://gitlab-com.gitlab.io/gl-security/security-tech-notes/threat-intelligence-tech-notes/malicious-browser-extensions-feb-2025>

# Polymorphic Extensions

The screenshot shows the Chrome browser's 'Extensions' page. The address bar displays 'chrome://extensions'. The page title is 'Extensions'. On the left, there are links for 'My extensions' and 'Keyboard shortcuts'. Below these, a message says 'Discover more extensions and themes on the [Chrome Web Store](#)'. The main area, titled 'All extensions', contains a grid of 12 extension cards. Each card displays the extension's icon, name, description, and buttons for 'Details', 'Remove', and a toggle switch. The extensions shown are: 1Password – Password Manager, Adobe Acrobat: PDF edit, convert, sign tools, Chrome Capture - Gif & Screenshot tool, Dark Reader, ExpressVPN: VPN proxy for a better internet, Google Dictionary (by Google), Google Translate, Grammarly: AI Writing and Grammar Check..., RSS Feed Reader, The Washington Post, uBlock, and Wiseone - Your AI Search & Reading Copilot. A 'Developer mode' toggle is visible in the top right. A 'SquareX' watermark with the website 'www.sqrX.com' is in the bottom right corner.

Extensions

Search extensions

Developer mode

My extensions

Keyboard shortcuts

Discover more extensions and themes on the [Chrome Web Store](#)

All extensions

- 1Password – Password Manager**  
The best way to experience 1Password in your browser. Easily sign in to sites, generate passwords, and store secure information.  
Details Remove [Toggle]
- Adobe Acrobat: PDF edit, convert, sign tools**  
Do more in Google Chrome with Adobe Acrobat PDF tools. View, fill, comment, sign, and try convert and compress tools.  
Details Remove [Toggle]
- Chrome Capture - Gif & Screenshot tool**  
Record gif or take screenshot of anything in your browser - quicker & easier than ever before.  
Details Remove [Toggle]
- Dark Reader**  
Dark mode for every website. Take care of your eyes, use dark theme for night and daily browsing.  
Details Remove [Toggle]
- ExpressVPN: VPN proxy for a better internet**  
Go online safely with blazing-fast speed. Spoof your location, access content anywhere, and control the ExpressVPN app from Chrome.  
Details Remove [Toggle]
- Google Dictionary (by Google)**  
View definitions easily as you browse the web.  
Details Remove [Toggle]
- Google Translate**  
View translations easily as you browse the web. By the Google Translate team.  
Details Remove [Toggle]
- Grammarly: AI Writing and Grammar Check...**  
Improve your writing with all-in-one assistance—including generative AI, grammar check, and more.  
Details Remove [Toggle]
- RSS Feed Reader**  
Get a simple overview of your RSS and Atom feeds in the toolbar  
Details Remove [Toggle]
- The Washington Post**  
Stay informed with hand-picked stories from the editors of The Washington Post.  
Details Remove [Toggle]
- uBlock**  
A no-nonsense ad blocker  
Details Remove [Toggle]
- Wiseone - Your AI Search & Reading Copilot**  
Wiseone is your ultimate AI tool to enhance your web searches and boost your reading productivity.  
Details Remove [Toggle]

SquareX  
www.sqrX.com

# Client Side File Creation

```
1  const data = "Hello, world!";  
2  const blob = new Blob([data], { type: 'text/plain' });  
3  const url = URL.createObjectURL(blob);  
4  
5  const link = document.createElement('a');  
6  link.href = url;  
7  link.download = 'hello.txt';  
8  link.click();  
9  
10 URL.revokeObjectURL(url); // clean up
```

# Browser Zero Days

Cyber Security News Google Vulnerability

## Google Chrome Browser Zero-Day Vulnerability Exploited in Wild

By **Balaji N** - January 17, 2024

Google Chrome released the first security update in 2024 with a fix for the zero-day bug actively exploited in Wild.

An update to Google Chrome 120.0.6099.234 for Mac, 120.0.6099.224 for Linux, and 120.0.6099.224/225 for Windows will be released in the next days or weeks.

Hackers exploit zero-day flaws as these vulnerabilities are unknown to software vendors, making them valuable for launching attacks before [security patches](#) are developed.

Even exploiting zero-day flaws can provide a strategic advantage to the threat actors in launching targeted and undetected attacks.

Recently, the following cybersecurity researchers identified multiple vulnerabilities, along with a [zero-day](#) flaw exploited in the wild:

- CVE-2024-0517 Reported by Toan (suto) Pham of Qrious Secure on 2024-01-06
- CVE-2024-0518 Reported by Ganjiang Zhou (@refrain\_areu) of ChaMd5-H1 team on 2023-12-03
- CVE-2024-0519 Reported by Anonymous on 2024-01-11

The zero-day exploit ([CVE-2024-0519](#)) hits the V8 JavaScript engine with out-of-bounds memory access. However, Google didn't provide details regarding the attack scope or telemetry.

<https://cybersecuritynews.com/google-chrome-browser-zero-day-vulnerability/>



# What can we do?

- Educate developers, sec pros, and orgs on browser risks
- Include browser security in the overall OWASP security discussion
- Promote browser-specific detection and response
- OWASP guidance on safely building browser extensions
- OWASP can lead the charge in this emerging domain

Thank you!!!

# Q&A

# Discussion

<http://getstarted.sqrx.com/browser-security-academy>

[jerry@sqrx.com](mailto:jerry@sqrx.com)

X @jerryhoff

 <https://www.linkedin.com/in/jerryhoff/>