

EBOOK

Understanding Browser Extension Risks



Table of Contents

What is a Browser Extension?	03
Browser Extensions Key Risks	03
The Most Dangerous Use Cases	04
Case Study	05
Examples of the Most Dangerous Permissions	06
Common Browser Extension Permissions	07
Risks Associated with Permissions	09
Examples of Well Known Risky Browser Extensions	10
Industry Use Cases: Healthcare	11
Industry Use Cases: Automotive Manufacturing	12
Industry Use Cases: Software	14
Best Practices for Ongoing Risk Management	16
The Source of the Problem: Lack of Visibility	17
Solution: SpinOne by Spin.AI	18

What is a Browser Extension?

A Browser Extension is a small piece of software that adds functionality or features to a web browser to enhance browser experience. Extensions can be used in browsers like Google Chrome, Firefox, Edge, or Safari. **They are powerful tools that can be used for good or for bad.**

Browser Extensions Key Risks

Browser Extensions can:

1. Spy on you
2. Steal your data
3. Perform account hijacking
4. Collect & sell your data
5. Delete, encrypt, or damage your data
6. Lead to non-compliance



Example: [Let's build Chrome Extension that steals everything](#)

The Most Dangerous Use Cases



Data Exfiltration

Browser extensions require multiple permissions to your hard drive, to your cookies, to other SaaS apps like Google Workspace, M365, Salesforce, etc. You have to be very careful when you grant permissions to new browser extensions. Here's an example of what kind of permissions can be potentially dangerous for your organization. [Learn More >](#)



Ransomware

Once you provide full access to a suspicious browser extension, it may start encrypting your SaaS data immediately. Watch how ransomware spreads to the cloud. [Learn More >](#)



Non-Compliance

Many browser extensions are developed by unknown companies or developers using @gmail.com email addresses. This can lead to significant compliance and regulatory issues.



Search Hijacking

Search hijacking is a tactic used by some malicious browser extensions to manipulate and redirect users' search queries. [Learn More >](#)



Ads Injection / Spam

Fake Ad-blockers can distribute unsolicited ads (spam). [Learn More >](#)

Case Study: RedDirection Malicious Extension Attack Campaign

Summary

In January 2025, a sophisticated malware campaign compromised [36 browser extensions](#) across Chrome and Edge stores, affecting [16.5 million users](#) through fake productivity tools that performed browser surveillance and hijacking.

Timeline: What Happened

- Campaign Launch: Attackers created legitimate-appearing browser extensions (emoji keyboards, weather tools, VPN proxies) that achieved verified badge status and high user ratings.
- Malicious Updates Deployed: Previously legitimate extensions received malicious code through routine updates, bypassing security reviews since updates install automatically.
- Discovery: Initial researcher analysis of "Color Picker, Eyedropper – Geco colorpick" extension revealed the RedDirection campaign affecting 2.3 million users.
- Spin.AI Researchers Expanded Investigation Cross-referencing threat intelligence uncovered 18 additional malicious Chrome extensions, revealing 14 million more affected users (7x the initial discovery).
- Patches Deployed Malicious extensions were patched or removed after an average of 98 days from initial compromise.

Risks to End Users

Users faced comprehensive browser surveillance, credential theft through fake banking pages, malware distribution via fake updates, and man-in-the-middle attacks that intercepted logins for personal and business systems over a 3+ month exposure window.

What Could Have Helped

Continuous extension monitoring with comprehensive threat intelligence from SpinCRX or SpinSPM would have identified malicious patterns and correlations across the campaign much earlier.

How it would have helped:

- Real-time detection of suspicious extension behaviors and update patterns
- Cross-referencing IOCs against comprehensive extension databases to reveal connected threats
- Automated response when extensions matched known malicious indicators
- Automated remediation to revoke extensions' access
- Forensic capabilities to identify which extension versions were compromised and when

Examples of the Most Dangerous Permissions

FullAccess

Can read, write, edit, delete, encrypt your data.

History

Gets full access to your browser history.

LocalDrive

Gets access to your local files on your hard drive.

PageCapture

Gets access to your desktop and can take a screenshot of your desktop every second and send it out without your permission.

Cookies

Gets access to your cookies. Can steal your login and password to your accounts or get, unauthorized access, or session hijacking.

WebRequest

It can sniff the request going to every website and see what it's sending. Can send all your credit cards information.

WebNavigation

Collects any website you navigate to.

CertificateProvider

Allows an extension to act as a certificate provider, generating or providing digital certificates for authentication, encryption, or digital signatures. This permission can affect security protocols by manipulating certificates, which can lead to potential man-in-the-middle attacks if misused. It requires careful handling and should only be granted to trusted extensions.

KeyLogger

Can steal your password managers data. Gets access to the input fields.

Identity

Allows the extension to access the Chrome Identity API for OAuth2 authentication, enabling user sign-in and access to profile information. While essential for integrating with user accounts, this permission can potentially expose personal information and should be granted to extensions that handle authentication securely.

PlatformKeys

Provides access to the platform's cryptographic keys for signing, verifying data, and generating new keys and certificates.

This permission can impact data integrity and security. Misuse can lead to unauthorized signing or verification of data, compromising security.

Common Browser Extension Permissions

Browser extensions can request a variety of permissions to access different parts of a user's browser or system. Below is a list of common permissions that browser extensions might request, along with a brief explanation of each:

tabs

Allows the extension to access information about the browser's tabs, including which ones are open, their URLs, and their titles.

activeTab

Grants temporary access to the currently active tab, allowing the extension to perform actions like modifying the page or accessing its content.

bookmarks

Permits the extension to access and modify the user's bookmarks.

history

Allows the extension to access the user's browsing history.

cookies

Lets the extension read and write cookies on the websites that the user visits.

webRequest

Enables the extension to observe and modify network requests made by the browser, which can be used to block certain requests or modify headers.

webNavigation

Allows the extension to monitor and react to browser navigation events, such as page loads and redirects.

downloads

Permits the extension to manage and manipulate browser downloads.

geolocation

Enables the extension to access the user's location data.

notifications

Allows the extension to display desktop notifications.

storage

Grants access to the browser's local storage, where the extension can store and retrieve data.

clipboard

Read / clipboardWriteAllows the extension to read from or write to the user's clipboard.

contentScripts

Enables the extension to inject scripts into web pages that the user visits, allowing it to modify the content of those pages.

management

Lets the extension manage other installed extensions, including enabling, disabling, or uninstalling them.

proxy

Allows the extension to control the browser's proxy settings.

native

Messaging Enables the extension to communicate with native applications installed on the user's computer.

alarms

Lets the extension schedule tasks to run at specific times or intervals.

idle

Allows the extension to detect when the user's device is idle.

identity

Grants access to the user's identity, often used to integrate with the user's Google account or other online services.

background

Allows the extension to run in the background, performing tasks even when no browser windows are open.

hosts (e.g., "http://*/", "https://*/")

Grants access to specific websites or all websites (<all_urls>), allowing the extension to interact with the content on those pages.

privacy

Allows the extension to control certain privacy-related settings of the browser.

sessions

Permits the extension to manage and restore browsing sessions.

devtools

Enables the extension to integrate with the browser's developer tools.

unlimitedStorage

Allows the extension to store an unlimited amount of data using the browser's storage APIs.

fileSystem

Grants the extension access to the user's file system, allowing it to read and write files.

sync

Allows the extension to synchronize data across different devices using the browser's sync feature.

webview

Enables the extension to embed web content inside an application or another webpage, similar to an iframe.

experimental

Grants access to experimental APIs that are not yet part of the stable browser version.

hostPermissions

Specifies which domains the extension is allowed to access, generally used in conjunction with other permissions like webRequest or cookies.

Risks Associated with Permissions

Each of these permissions can pose different levels of risk. For example:

`webRequest` and `proxy`

These can be used to intercept and modify network traffic, potentially for malicious purposes.

`tabs` and `activeTab`

These can allow an extension to spy on a user's browsing activity.

`nativeMessaging`

This can be used to communicate with other software on the user's machine, potentially leading to broader system compromise.

`clipboardRead/Write`

These can allow an extension to read or inject data into the user's clipboard, potentially capturing sensitive information or inserting malicious content.

Understanding the permissions an extension requests and the potential risks involved is crucial for maintaining security.

Examples of Well Known Risky Browser Extensions

Search Hijacking and Ads Injection

Adblocker for YouTube — Youtube Adblocker:

(2,000,000+ users on the Chrome Web Store).

The extension loads a seemingly harmless script with 'analytics' from fly-analytics.com. After some time, it updates the script that check the search results from Bing or Google and loads an image from a rouge lh3.googleusercontent.com mimicking original Google's domain that contains ads encoded into the image using steganography technique to bypass security checks. Finally, these ads are injected into the page with the search results.

Cookie Stuffing

uBlocker — #1 Adblock Tool for Chrome:

(1,000,000+ users on the Chrome Web Store).

The extension performs ad fraud with the help of the technique called Cookie Stuffing. Cookie stuffing is a deceptive tactic in affiliate marketing. In affiliate marketing, individuals (affiliates) are compensated for enticing consumers to buy products through specially crafted URLs that set cookies on users' browsers to track which affiliate referred the user to the site. The extension can receive a command from the attacker's server that leads to setting special affiliate cookies. For example, when a user visits Booking.com, they set their affiliate cookie so when the user makes a purchase, the extensions owner will be paid a commission by Booking.com.

Spam

Adblocker for YouTube™: (5,000,000+ users,

86 reviews on the Chrome Web Store). The extension loads 'Google Tag Manager' code, which means that Google Tag Manager account owner can change the 'tag' at any point and upload completely new code to this extension. The new code was used to send SPAM.

Stealers

Chat GPT For Google: (9,000+ users on the

Chrome Web Store). Fake ChatGPT application that mimics genuine open-source extension "ChatGPT For Google" compromises Facebook accounts under a cover of a ChatGPT integration for your Browser using the techniques called Cookie-Hijacking. As result, the malicious extension sent to the attacker all current Facebook session cookies active on the browser as AES-encrypted data attached to the 'X-Cached-Key' HTTP header value.

Cyber Espionage

AF: A malicious extension distributed by Kimsuky

(North Korea) cybercriminal group through phishing emails that contain a link to download the extension that is used to read Gmail communication on Google Chrome, Microsoft Edge, as well as the South Korean browser Naver Whale. When the victim opens Gmail in the compromised browser, it automatically starts sending the victim's correspondence to the hackers' C2 server.

Industry Use Cases: Healthcare

Doctors use laptops in consultation rooms during patient appointments to capture PII (Personally Identifiable Information) data or in surgery rooms for video scanning and other tasks. This PII data could be accessed and stolen by malicious extensions, leading to risks such as non-compliance, data breaches, reputational damage, or, even worse, negatively impacting the patient during surgery, which could potentially result in death. **The use of browser extensions in healthcare organizations improves productivity but can present several negative impacts at the same time, including:**

Data Privacy and Security Risks

Sensitive Data Exposure: Healthcare organizations handle sensitive patient information, including personal health records (PHRs), which are protected under regulations like HIPAA. Browser extensions can inadvertently or intentionally collect, store, or transmit this sensitive data, leading to potential breaches.

Malware and Phishing Attacks: Malicious extensions can introduce malware or be used for phishing attacks. Once installed, these extensions can intercept or manipulate web traffic, potentially leading to unauthorized access to patient data or other critical systems.

Regulatory Compliance Issues

Violation of HIPAA and Other Regulations: Extensions that are not compliant with healthcare regulations can result in violations of HIPAA or other relevant laws. This can lead to significant fines, legal consequences, and damage to the organization's reputation.

Auditing and Monitoring Challenges: Browser extensions can make it difficult for IT departments to monitor and audit web activity for compliance.

Unauthorized extensions might introduce vulnerabilities that go unnoticed until a security breach occurs.

Performance & Reliability Concerns

System Slowdowns: Some browser extensions can negatively impact system performance by consuming excessive resources. This can be particularly problematic in healthcare settings, where slowdowns can affect the timely delivery of care.

Compatibility Issues: Extensions may conflict with existing healthcare applications or electronic health records (EHR) systems, leading to functionality issues or downtime, which can disrupt patient care.

Potential for Data Leakage

Third-Party Data Sharing: Some extensions collect data to share with third-party advertisers or other entities. In a healthcare context, this could lead to unauthorized sharing of sensitive patient information, even if the intent is not malicious.

Industry Use Cases: Automotive & Manufacturing

Dealers use extensions for business collaboration across their networks and need visibility into the vast number of extensions used and control of unsanctioned apps and extensions through allowlists and blocklists. Automotive companies work with a lot of contractors with BYOD policy that allows external employees install any type of browser extensions without initial risk assessment. As a result, there is no visibility on that and there is no risk assessment process in place. The use of browser extensions in the automotive industry and car manufacturing companies can lead to several negative impacts, including:

Data Security Risks

Intellectual Property Theft: Automotive companies handle sensitive data related to vehicle designs, manufacturing processes, and proprietary technology. Malicious browser extensions can steal or leak this intellectual property, leading to significant competitive disadvantages and financial losses.

Cybersecurity Vulnerabilities: Browser extensions can serve as entry points for cyberattacks, such as malware or phishing attempts. If a compromised extension is used on systems connected to the manufacturing process, it could disrupt operations or lead to unauthorized access to critical systems.

Compliance & Legal Issues

Violation of Industry Regulations: Automotive companies must comply with various industry regulations and standards, such as ISO/TS 16949. Unvetted browser extensions can introduce vulnerabilities that might lead to non-compliance, resulting in legal consequences, fines, and loss of certifications.

Data Privacy Concerns: Browser extensions can collect and share data with third parties, leading to potential breaches of customer and employee privacy. This can result in legal actions and significant damage to the company's reputation.

Operational & Performance Challenges

System Interference: Browser extensions can interfere with software applications used in the automotive industry, such as CAD (Computer-Aided Design) software, PLM (Product Lifecycle Management) systems, or ERP (Enterprise Resource Planning) tools. This interference can cause slowdowns, crashes, or other operational disruptions.

Inconsistent User Experience: Allowing the use of various browser extensions across a large organization can lead to inconsistencies in the user experience. This can affect productivity, especially if extensions cause unexpected behavior in web-based applications critical to automotive design and manufacturing.

Supply Chain Risks

Third-Party Risk Exposure: Automotive companies often collaborate with a network of suppliers and partners. Malicious browser extensions can be a vector for supply chain attacks, where a breach in one organization leads to vulnerabilities across the entire supply chain.

Data Leakage: Extensions that collect data for third-party services can lead to inadvertent data leakage, exposing sensitive supply chain information or details about upcoming products to unauthorized entities.

Product Development & Innovation Risks

Disruption to R&D Processes: Browser extensions can potentially disrupt research and development (R&D) activities by interfering with tools and applications used by engineers and designers. This can slow down innovation and delay the launch of new products.

Intellectual Property Compromise: In the competitive automotive industry, maintaining the confidentiality of new designs and technologies is crucial. Browser extensions that access and transmit data could compromise this confidentiality, resulting in leaked information and reduced competitive advantage.

To mitigate these risks, automotive companies should enforce strict controls over the installation and use of browser extensions, regularly audit their systems for unauthorized software, and educate employees about the potential dangers associated with browser extensions.

Industry Use Cases: Software

Software companies use extensions for efficiency and collaboration but need to assess the risks to their development environments and source which could impact continuity in software delivery. The use of browser extensions in the software industry can have several negative impacts, including:

Security Vulnerabilities

Data Breaches: Browser extensions can be a vector for data breaches, exposing sensitive company information, such as source code, project files, client data, and internal communications. Malicious extensions can access and exfiltrate this data, leading to significant security incidents.

Supply Chain Attacks: Software companies often rely on a complex network of third-party tools and services. A compromised browser extension could introduce vulnerabilities that propagate through the supply chain, affecting clients and partners as well.

Intellectual Property Risks

Source Code Theft: Extensions that have access to web developer tools or internal systems can potentially steal or leak source code, which is often the most valuable asset of a software company. This can lead to intellectual property theft, loss of competitive advantage, and legal battles.

Compromise of Proprietary Tools: If an extension has access to proprietary development environments, it could compromise them, leading to unauthorized use or distribution of the company's intellectual property.

Compliance & Legal Issues

Violation of Data Protection Regulations: Software companies are often required to comply with data protection regulations like GDPR, CCPA, or HIPAA (if working with healthcare data). Browser extensions that mishandle data can lead to non-compliance, resulting in fines and legal repercussions.

Audit and Monitoring Challenges: The use of unauthorized or unvetted browser extensions can make it difficult to maintain audit trails and monitor compliance with industry standards and regulations, potentially leading to legal issues.

Operational Disruptions

Interference with Development Tools: Browser extensions can interfere with critical development tools, such as Integrated Development Environments (IDEs), code editors, or Continuous Integration/Continuous Deployment (CI/CD) pipelines. This can lead to delays, bugs, and reduced productivity.

Incompatibility Issues: Extensions may cause compatibility issues with web-based applications or development environments, leading to unexpected behavior or crashes that disrupt the software development process.

Quality & Integrity of Software

Code Quality Concerns: Extensions that alter how web pages are displayed or interact with code repositories can introduce bugs or inconsistencies. This can compromise the quality of the software being developed or lead to issues that are difficult to trace.

Integrity of Testing Environments: Extensions might affect how web applications behave in testing environments, leading to false positives or negatives in testing results. This can undermine the integrity of software testing and result in flawed products reaching the market.

Productivity & Performance Issues

System Slowdowns: Some browser extensions can consume significant system resources, leading to slowdowns or crashes. For developers, this can be particularly disruptive, reducing efficiency and increasing frustration.

Distraction and Fragmentation: Browser extensions that are not work-related can serve as distractions, reducing focus and productivity. Additionally, the use of multiple extensions by different team members can lead to fragmentation and inconsistencies in development workflows.

Reputational Damage

Public Relations Fallout: A security incident or operational failure caused by a browser extension can lead to negative publicity, harming the company's image and potentially affecting sales, partnerships, and market position.

Innovation & Competitive Risks

Leakage of R&D Data: Browser extensions could be used to access and leak information about ongoing research and development projects, which could lead to the premature exposure of new products or features. This could undermine the company's competitive strategy and innovation efforts.

Loss of Trade Secrets: Extensions that have access to internal communication platforms or project management tools could lead to the exposure of trade secrets, giving competitors an unfair advantage.

To mitigate these risks, software companies should implement strict policies regarding the use of browser extensions, perform regular security risk assessment, and educate employees about the potential dangers.

Best Practices for Ongoing Risk Management



Visibility

Maintain an up-to-date catalog of all browser extensions across the organization. This inventory serves as a critical foundation for systematically assessing and prioritizing the organization's threats and vulnerabilities.



Risk Assessment & Reassessment

Perform a comprehensive risk assessment of every browser extension, including an evaluation of its business operations, security, privacy, and compliance risks. This assessment must be continuously performed to account for any changes in the browser extension.



Automation & Incident Response

Leverage automation to immediately respond to incidents. By automating this process, organizations can effectively contain the risks, minimize the potential impact, and maintain continuous protection.

The Source of the Problem: Lack of Visibility



Solutions: SpinOne & SpinCRX from Spin.AI

SpinOne Features

- Visibility for 400,000+ apps & browser extensions assessed by our AI-algorithms
- Automated Continuous Risk Assessment
- Fast Incident Response
- Risk Score History
- Granular Security Policies
- Approval Process
- Integration with 3rd-party solutions: Splunk, ServiceNow, Jira, Slack, CrowdStrike
- Misconfigurations detection
- API-based, Agentless

[BOOK A DEMO](#)

SpinCRX Features

- Visibility for 300,000+ browser extensions assessed by our AI-algorithms
- Automated Continuous Risk Assessment
- Fast Incident Response
- Risk Score History
- Granular Security Policies
- Streamlined Approval Process
- Flexible Deployment Models
 - Agent-based for comprehensive browser coverage
 - Browser-based for corporate extension management only

Request a demo of SpinOne today.

Recognized by

Gartner

FORRESTER

GIGAOM

Integrated with

Google

FORTINET

About Spin.AI Spin.AI is an innovative provider of SaaS security solutions for mission-critical SaaS apps (Microsoft 365, Google Workspace, Salesforce, Slack, and dozens more). Our all-in-one SpinOne platform helps organizations mitigate risk, save time, reduce downtime, and improve compliance.