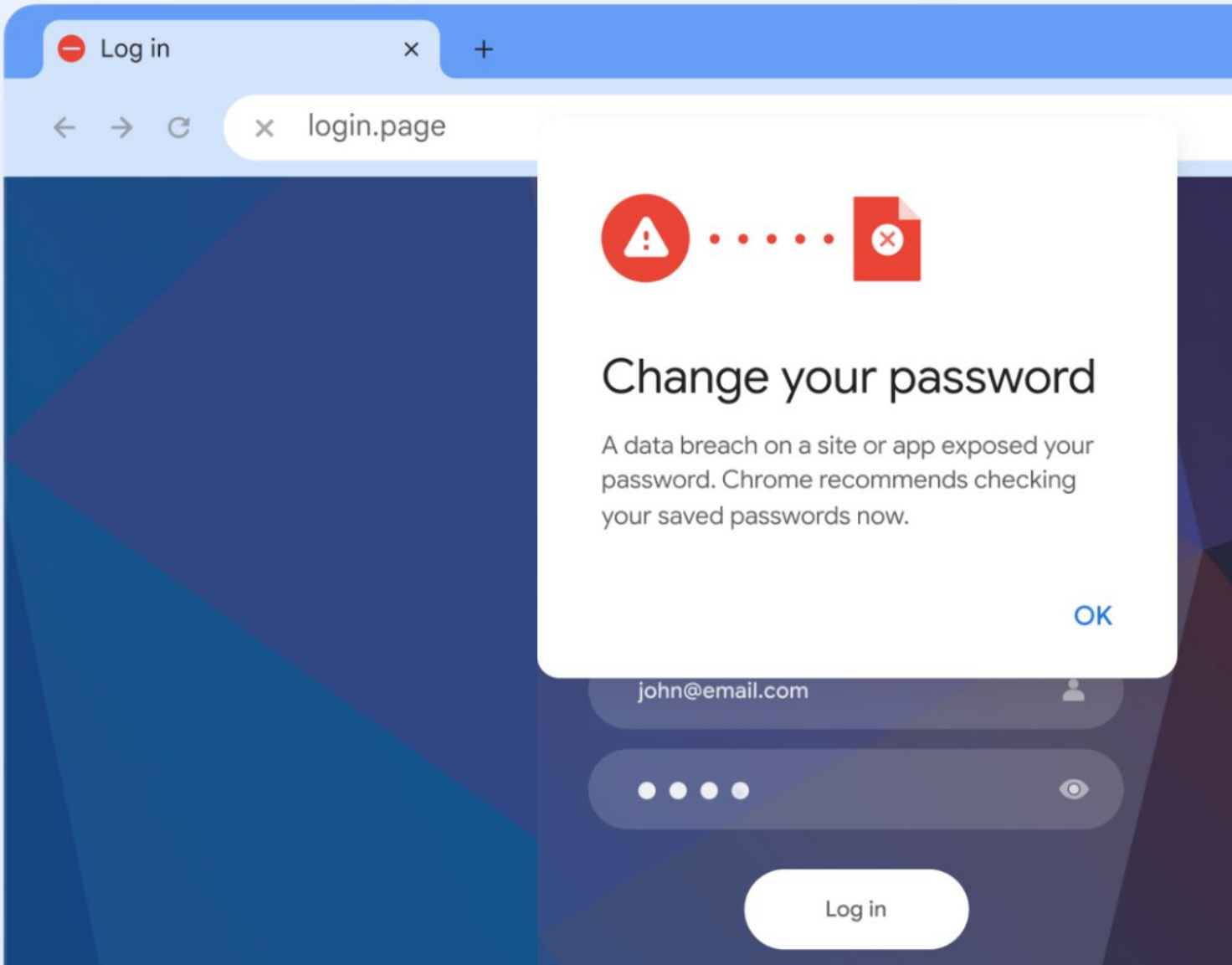
chrome enterprise

Google Cloud
Security

The Security Blindspot: Real Attack Insights from Real Browser Attacks



Introduction

The browser is the home of modern work. It's where we access tools, collaborate, research, engage with peers, transact, and share information. Many critical business applications, from customer relationship management (CRM) systems like Salesforce to collaborative platforms like Google Workspace and Microsoft 365, are accessed entirely through web browsers.

Web applications have become central to productivity, allowing employees to manage projects, communicate, analyze data, and perform countless other tasks without installing software on their local devices. This reliance on SaaS and web apps underscores just how much the browser has become the foundation of modern work, serving as the primary interface for accessing and interacting with the tools and data essential to an organization's daily operations.

For many, browsers are so seamlessly integrated into our daily routines that they've become a fully trusted platform to access the internet. The browser experience is often seamless, and many users have never had a negative experience that would erode that trust. As a result, we click links, open tabs, and download files without a second thought, trusting that the actions we are taking are safe. This complacency can make us vulnerable, especially if we neglect basic security practices like keeping our browser updated, scrutinizing links before clicking, or being wary of downloading files from untrusted sources. We assume that we are protected, but the reality is that the threat landscape is constantly evolving, and browsers and users can be exploited by malicious actors.

Most common initial infection vectors

33%
Exploit

16%
Stolen credentials

14%
Email phishing

9%
Web compromise credentials

Cybersecurity incidents originating from browser-based attacks are a growing threat to individuals and organizations across multiple sectors. These attacks pose a significant and evolving risk, as malicious actors take advantage of users and launch more advanced attacks. The M-Trends 2025 Report notes that the second most common initial infection vector (when identified) was stolen credentials (16%) - a technique that often involves infostealer malware delivered through browsers. The most common vector was exploit (33%), and the third and fourth were email phishing (14%), and web compromise credentials (9%).

Despite the increasing reliance on web browsers for daily operations and the growing threat of browser-based cyberattacks, many organizations allow for a significant gap in their security posture by not fully utilizing the range of security features available in their browser. Traditional cybersecurity strategies often overlook the browser as a critical entry point for attacks, focusing instead on network and endpoint security. This blind spot leaves organizations vulnerable to sophisticated threats like malicious extensions, and data exfiltration through web applications, as threat actors increasingly exploit the inherent trust users place in browsers and utilize legitimate browser features for malicious activities. Often, these are attacks that can be prevented by enabling advanced browser policies and reporting to minimize the opportunity for attacks.

A Blind Spot in the Defense

Cybersecurity is a cat and mouse game where security vendors continually try to thwart threat actors who are always developing new ways to evade detection and achieve their objectives. Enterprises have reinforced their security posture over the past decades by implementing multiple layers of defense, including endpoint detection and response (EDR) solutions, antivirus software, network intrusion detection systems (NIDS), network detection and response (NDR), email protection technologies, zero-trust, and URL reputation checks, to name a few.

The security team's job of detecting malicious activity is becoming increasingly challenging. Threat actors are increasingly using legitimate tools for malicious purposes, a tactic known as "living off the land" (LOTL). LOTL attacks include using built-in networking tools to establish connections to external servers for data exfiltration or configuring scheduled tasks to run malicious code at specific intervals to blend in with legitimate systems. Sadly, the browser has also become another frontier for LOTL attacks.

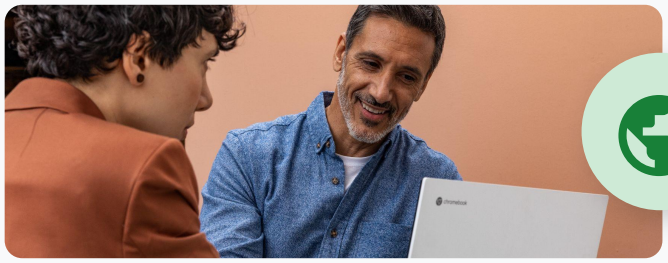
Threat actors are using legitimate browser features, such as HTML5 and JavaScript (like HTML smuggling), to deliver malicious payloads to endpoints escaping several layers of defense.

Browser-based attacks, such as malicious browser extensions, can employ advanced techniques like dynamic configurations to modify their behavior, and utilize modular and obfuscated structures to avoid detection and bypass endpoint protection. EDR telemetry matrices, a project with the objective to evaluate the strengths and weaknesses of EDRs by comparing their telemetry data collection show weakness in telemetry generation related to activities associated with browser usage. When analyzing network traffic telemetry generated by URL or file download activity, we find that some EDR solutions lack a comprehensive overview for browser-based network events. This lack of telemetry hinders security teams' ability to create custom detection rules and increases the risk of missing malicious activity. This increases the blind spot of activities associated with browser usage and advanced browser security needs to be enabled to protect organizations from an ever-evolving threat landscape.

Real Learnings from Real Attacks

The frequency and sophistication of browser-based attacks are escalating at an alarming rate, exploiting vulnerabilities that traditional security measures often fail to address. Many organizations remain unaware of the browser's role as a potential gateway for data breaches, unauthorized access, and malware infections. Organizations are also unaware of the security features and policies available within their browser to strengthen their security posture; often these are policies and features that can be quickly and efficiently deployed across a workforce. By examining real-world scenarios where inadequate security policies within the browser led to security breaches, we aim to underscore the urgent need for organizations to adopt proactive and comprehensive browser security strategies.

As a leader in threat intelligence, incident response and cybersecurity consulting, Mandiant works with many enterprise organizations to boost cyber defenses. By examining previous Mandiant incident response cases, we hope to illuminate the potential consequences of neglecting security at the browser layer and emphasize the importance of integrating advanced browser protection into a holistic security framework.



It started with a click

Phishing and spear-phishing, the more tailored form, remains one of the most prevalent attack vectors today, used from the script-kiddies to the most advanced nation-state backed group and with the rise of the artificial intelligence technologies, it is becoming even harder to spot.

Mandiant Consulting investigated a Business Email Compromise (BEC) case for a client.

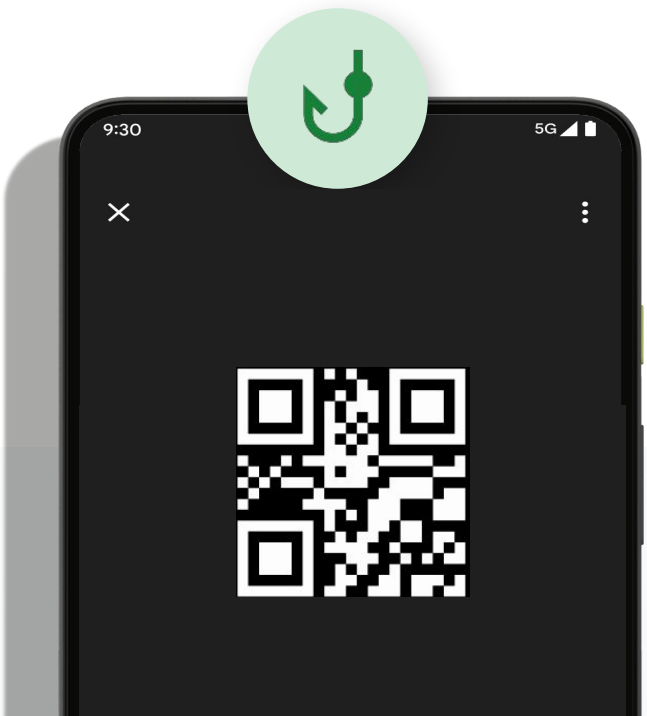
The attacker initiated the compromise through a QR code phishing attack (Quishing or QR Phishing), which bypassed company security when the targeted employee scanned the malicious QR code with his personal phone.

The threat actor used a reverse proxy phishing infrastructure to circumvent multifactor authentication and conditional access policies. After gaining access to the victim's cloud account, the attacker registered their mobile phone as a trusted device to maintain access. The investigation revealed that the attacker spent time browsing the contents of the compromised employee's mailbox. The attacker's primary goal was to locate and extract documents that contained sensitive information regarding past financial transactions, including invoices and payment records. Once the attacker had gathered sufficient information, they proceeded to leverage this knowledge to create fraudulent payment orders.

These payment orders were meticulously crafted to appear legitimate to exploit the trust within the finance department. The attacker then submitted these fraudulent payment orders to employees in the finance department via email. The orders often included urgent requests to expedite processing, resulting in significant financial loss.

With email phishing attacks on the rise, it's crucial to understand how these threats are evolving and impacting cybersecurity. In 2024, BEC attacks accounted for 73% of all reported cyber incidents according to the FBI's IC3 (IC3, 2024).

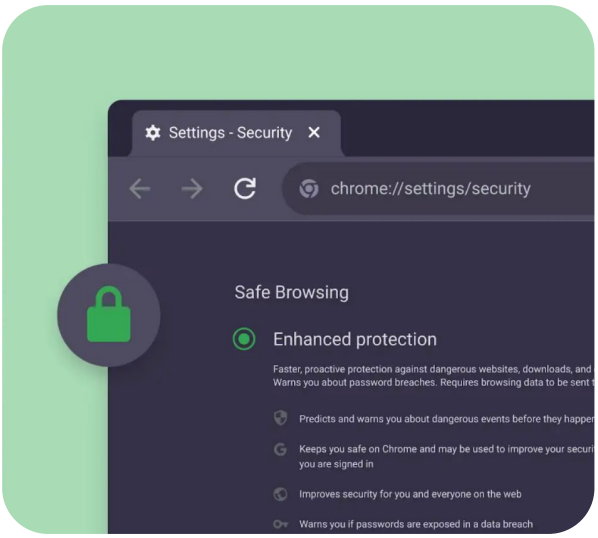
The increasing sophistication of evasive phishing tactics, such as QR Code phishing, coupled with Adversary-in-the-Middle (AiTM) frameworks, is rendering traditional security tools less effective. These tactics allow attackers to bypass Multi-Factor Authentication (MFA), by stealing login session tokens, and evade detection. In a recent publication, the Google Threat Intelligence Group (GTIG) detailed how Russian-aligned threat actors attempted to compromise Signal accounts. The threat actors exploited Signal's "linked devices" feature, which allows the app to be used on multiple devices simultaneously by scanning a QR code.



It started with a click

Chrome Enterprise Premium offers several layers of defense against QR infection. First, even if the initial malicious QR code was scanned on a personal device, if the employee subsequently accessed company resources or internal web applications through a managed Chrome browser, Chrome Enterprise Premium's real-time URL risk evaluation would assess the legitimacy of the linked website. Administrators can configure policies to warn users or outright block access to sites flagged as risky by Google Safe Browsing or through custom internal risk assessments.

Furthermore, in scenarios where attackers leverage reverse proxy phishing to circumvent Multi-Factor Authentication (MFA), Chrome Enterprise Premium's enhanced security features, such as context-aware access controls and deep integration with identity management solutions (IdP), are critical. These capabilities can help identify anomalous login patterns, enforce device trust requirements, and flag attempts to register unauthorized devices. Should a user inadvertently navigate to a phishing site and attempt to enter credentials, Chrome Enterprise Premium's AI-powered phishing and malware protection, including real-time URL scanning and Safe Browsing technologies with advanced threat intelligence, would actively work to block the malicious site or warn the user.



In the event of an attempted download of a malicious document, its real-time file scanning and advanced malware detection capabilities are designed to identify and prevent such threats, rather than relying on traditional DLP rules which focus on outbound data exfiltration.

Upon detecting policy violations indicative of phishing or recognizing known phishing behaviors through its advanced threat intelligence, Chrome Enterprise Premium enables swift and targeted responses. Rather than directly isolating the user's session and documents within the browser itself, administrators can leverage its capabilities to effectively mitigate the threat. This includes actions such as dynamically moving the affected user into a restricted access group with more stringent policies, globally blocking access to the malicious domain across the organization, and remotely triggering the clearing of browser data on the compromised device. Furthermore, through the rich telemetry provided by 'Chrome signals,' security teams gain deep visibility into user activity and associated documents. The Evidence Locker feature can capture records of files and user actions, preserving crucial data for forensic analysis, advanced malware scanning, and a comprehensive understanding of the event's scope. This combination of proactive detection, granular response actions, and detailed audit trails significantly mitigates the financial and operational risks associated with sophisticated phishing attacks.

Data Breach from Home

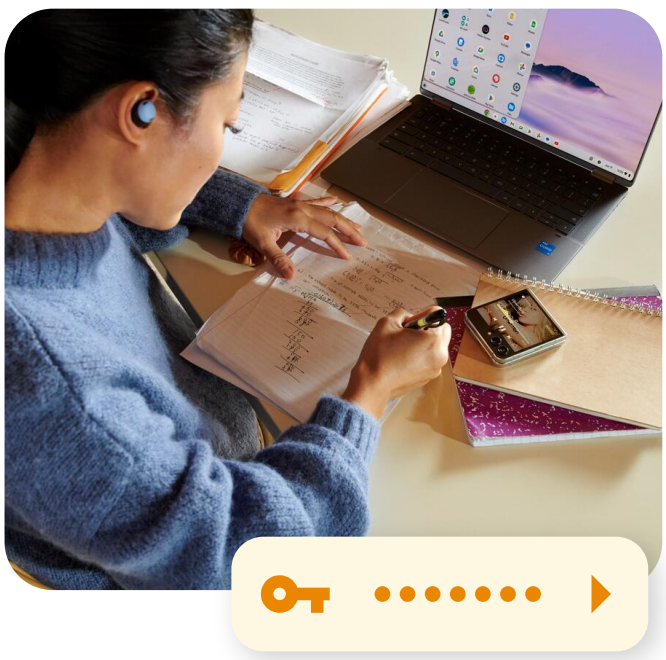
A client engaged Mandiant Consulting after a threat actor published several dozen gigabytes of their internal data on a criminal forum. The attacker gained initial access through stolen web access credentials from a personal computer that had been compromised by password-stealing malware.

The attacker initially logged on to the internal Confluence web portal and also used the same credentials to access the Jira and Bitbucket web portals.

Over two days, the attacker's activity was focused on accessing and downloading data via the applications' web interface. This included exploring Confluence spaces and downloading page attachments, as well as accessing and downloading source code from Bitbucket repositories. The attacker then deleted the Bitbucket repositories.

BYOD policies can make companies more attractive to employees, save time, and cut costs, but they also introduce vulnerabilities. Mandiant has responded to numerous incidents over the past several years where valid accounts were used as the initial access vector. These accounts could have been compromised by threat actors through phishing or infostealer malware. In some cases, Mandiant discovered that personal laptops had been compromised and used to access enterprise accounts. Personal devices allowed under BYOD policies are not covered by EDR solutions. Additionally, the reuse of valid accounts is undetectable by network security solutions without context.

Chrome Enterprise Premium directly addresses the vulnerabilities highlighted in this data breach by enforcing a Zero Trust security model. Even with compromised credentials, Chrome Enterprise Premium's principle of least privilege, coupled with continuous user and device context evaluation, would significantly limit the attacker's actions upon accessing internal portals like Confluence, Jira, and Bitbucket. By leveraging device signals, it could have identified the login attempt originating from an unmanaged and potentially compromised personal computer, potentially blocking or restricting access altogether. Furthermore, Chrome Enterprise Premium's robust data protection features could have prevented the attacker from downloading sensitive data from these web applications onto the unmanaged device. Policies could have been configured to block downloads, disable copy/paste functionality, and restrict other data exfiltration methods. Finally, the ability to capture and monitor critical user actions within these applications provides valuable insights for security teams, enabling quicker detection of malicious activity and a more effective response to contain and remediate the breach.



Insider Threat

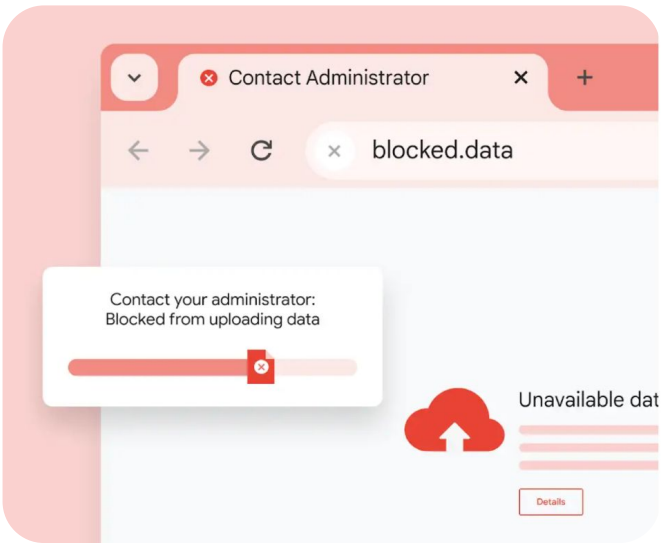
Mandiant Consulting was engaged by a client to investigate a potential data theft incident involving a recently resigned employee suspected of copying proprietary documents to personal devices.

Forensic analysis revealed that the former employee accessed the company's SharePoint and OneDrive servers to download corporate files to his personal device.

Evidence indicated that the employee had used various cloud storage services and a network storage device to store business-related documents. The former employee had also created multiple ZIP archives containing business-related documents, which were then uploaded to a non-company-issued device, representing a clear breach of data security protocols and a potential risk of data misuse.

Today, the majority of work takes place in web browsers, using multiple SaaS applications. Employees frequently handle sensitive data, writing, copying, pasting, uploading, and transferring information within these browser-based environments. Traditional Data Loss Prevention (DLP) solutions, which were designed to monitor email, endpoints, and network traffic, have not kept pace with this shift. As a result, DLP strategies might struggle to effectively monitor and protect sensitive data within the browser and SaaS applications.

Chrome Enterprise Premium's DLP rules directly address this type of insider threat by providing comprehensive visibility and control over data handling within the browser. In this instance, it could have captured and recorded every download and copy action the former employee performed in SharePoint and OneDrive. These rules can be configured to identify proprietary documents or sensitive data based on content, and administrators could have monitored the volume and speed of the data being accessed to detect the unusual exfiltration pattern. Crucially, Chrome Enterprise Premium offers preventative measures by enabling policies to block downloads to personal devices, redirect them to secure company storage, or stop them entirely. This level of control would have directly countered the employee's attempts to copy corporate files. Furthermore, integrating these browser-level DLP logs with a Security Information Event Management (SIEM) like Google Security Operations would provide a holistic view of the employee's activities across applications and their local device, allowing for a more thorough investigation and response to the data theft.



Malicious Browser Extension

A client engaged Mandiant Consulting to investigate a series of security alerts that had been triggered by access attempts to suspicious domains that were blocked by the organization's internet-facing firewalls.

Through a thorough forensic analysis, Mandiant discovered that the source of these suspicious requests were deleted browser extensions. Unfortunately, due to the fact that these browser extensions had been deleted prior to the commencement of the analysis, Mandiant was unable to conduct a code analysis of the extensions themselves.

During the course of their investigation, Mandiant also uncovered unusual pattern activity on a separate system. This activity was characterized by suspicious access to a domain every time the user of the workstation logged into a particular website. Mandiant suspected that this activity was related to token exfiltration and was also linked to browser extensions that had been deleted before Mandiant began their investigation.

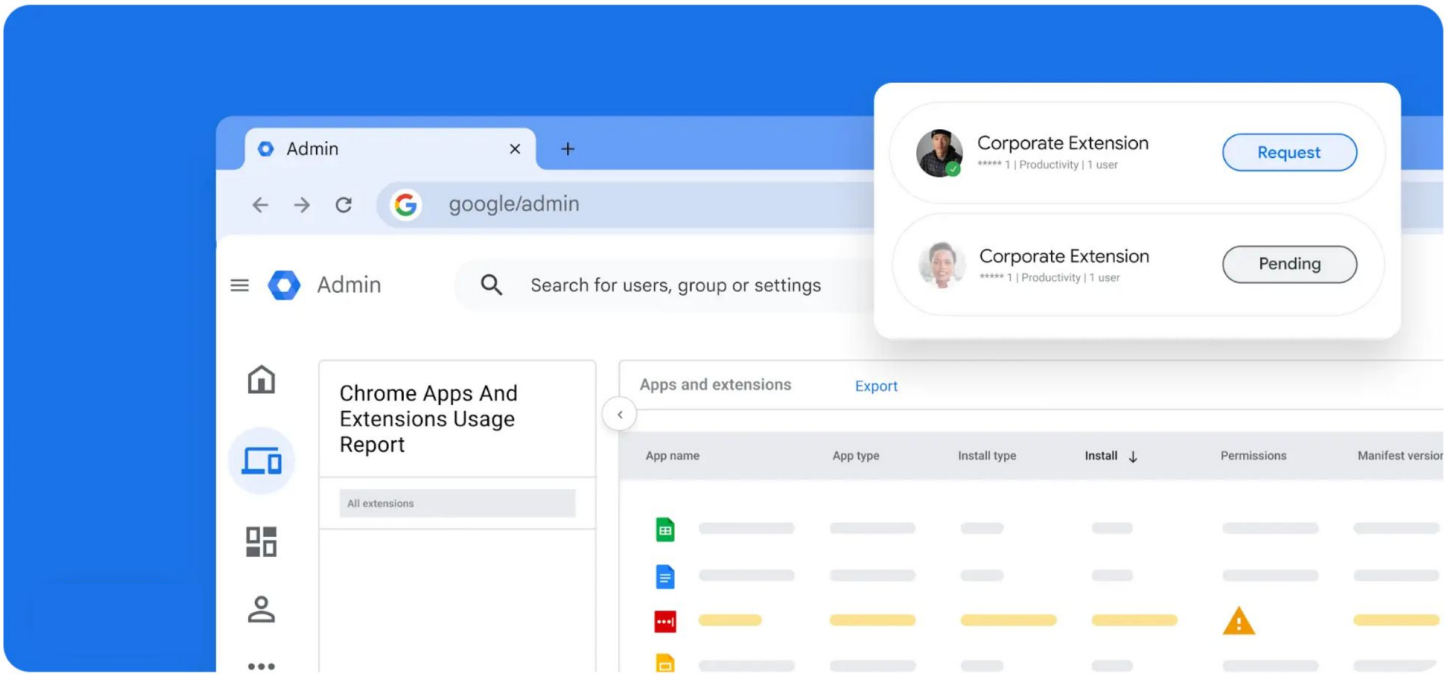
Despite these findings, Mandiant's forensic analysis did not reveal any signs of system-level compromise, suggesting that the suspicious activity was confined to the browser extensions themselves. However, the inability to analyze the code of the deleted extensions left many questions unanswered, including the specific functionality of the extensions, the nature of the data being exfiltrated, and the ultimate goal of the threat actor.

This incident highlights the potential security risks associated with browser extensions, particularly those that are downloaded from untrusted sources. Even seemingly innocuous extensions can be used for malicious purposes, such as data exfiltration, credential theft, and malware distribution.

On the same subject, in late December 2024, a Data Loss Prevention (DLP) company, reported that a threat actor used a phishing attack to compromise an employee's access to the Google Chrome Web Store. The threat actor then used this access to publish a malicious version of one of the company's Chrome extensions. It was revealed that this attack was part of a larger supply chain attack campaign targeting Chrome extension developers in various industries.

Malicious browser extensions are increasingly using sophisticated techniques such as dynamic configuration and modular, obfuscated structures to modify behavior, evade detection, and bypass endpoint protection.

Malicious Browser Extension



Additionally, malicious actors are increasingly hosting content on trusted cloud platforms to evade detection at the network level.

Chrome Enterprise Premium offers a robust defense against the threats posed by malicious browser extensions highlighted in these scenarios. By providing a comprehensive risk assessment for every extension within the Chrome fleet, administrators can proactively identify potentially harmful extensions before they are deployed. Chrome Enterprise Premium's dynamic extension controls and browser policies allow for granular management, including the ability to limit or prevent users from sideloading extensions, ensuring that only approved and vetted extensions are used. Beyond controlling what extensions are used, Chrome Enterprise Premium enables administrators to control what permissions and website access any extensions have.

The isolation of extensions within Google Identity Profiles further enhances security by limiting the scope of any potential compromise. Moreover, the extension telemetry captured by Chrome Enterprise Premium provides crucial visibility into extension behavior, enabling administrators to monitor network communication with suspicious remote IPs or detect unusual activity indicative of data exfiltration, as demonstrated by the firewall alerts and unusual domain access patterns. This continuous monitoring and control framework allows organizations to effectively mitigate the risks associated with increasingly sophisticated and evasive malicious browser extensions.

Essential Browser Security

These real attacks shine a light on an aspect of security that is overlooked and underinvested in: security within the browser. Now more than ever, the browser needs to be placed at the center of security architecture to simplify and defend your organisation's perimeter.

Traditional security tools and categorization are no longer sufficient, attackers can easily bypass them using techniques like CAPTCHA verification and multiple redirection. Website categorization and URL filtering alone are not reliable for security teams, because attackers are now hosting phishing and payload on legitimate cloud service providers.

The Security teams needs real-time browser telemetry that can be exported into their SIEM, reducing the blind spot of the other security tools. This provides context awareness and, when with the ability to leverage threat intelligence data, will ultimately improve the company's overall security posture.

To improve your organization's browser-based security, we recommend taking the following steps:

1 Manage Your Browser

Improving visibility and enhancing control through browser management is crucial for organizations. By gaining better insight into browser activity and implementing granular controls, organizations can first identify blind spots that need to be addressed. There are security insights available within the Chrome Enterprise browser that provide a clear view on how your browser is being used so it's possible to detect risky behavior such as potential insider threats and data exfiltration attempts. The reports and analytics can guide your decisions to implement targeted security controls and new policies. Managing your browser is an essential first step to empower your organization to move beyond reactive measures and implement a proactive, data-driven approach to securing your environment.

2 Contextualization and Enrichment

A crucial step in enhancing your organization's security is the ingestion of browser telemetry data, along with additional signals, into a SIEM system. This integration allows for the detection of suspicious activity that might otherwise be overlooked by traditional security tools. By correlating browser telemetry with other security data, SIEM systems can provide a more comprehensive view of potential threats, enabling security teams to identify and respond to browser-based attacks more effectively. This approach not only strengthens the overall security posture but also helps close the blind spot that often exists in security, ensuring that potential threats in the browser are identified and addressed promptly.

Essential Browser Security

3 Automation and Orchestration

Organizations can leverage Security Orchestration, Automation and Response (SOAR) capabilities to enhance their incident response capacity and speed when dealing with browser-based attacks. By utilizing SOAR, security teams can create custom remediation and playbook workflows that automate and streamline various aspects of the incident response process. This automation allows for faster and more efficient response times, freeing up valuable resources and enabling security professionals to focus on more complex tasks. Additionally, SOAR playbooks can be tailored to specific types of browser-based threats, ensuring that the appropriate actions are taken in a timely manner.

4 Technical Controls

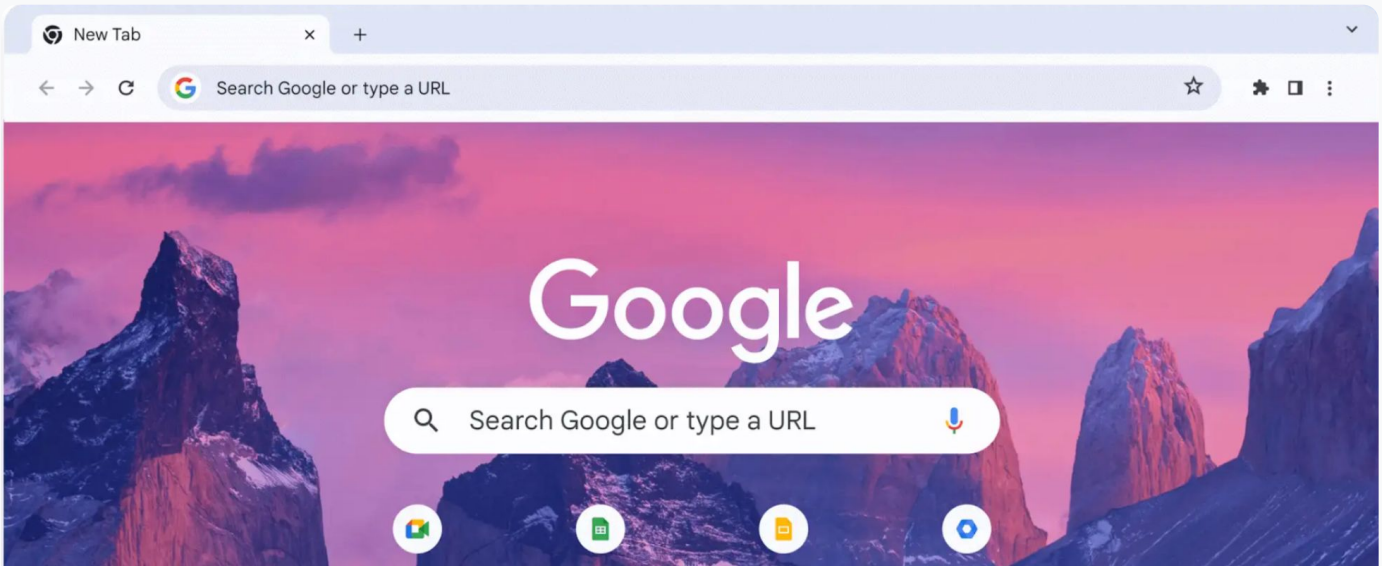
Make the most of browser controls to protect your environment. Use browser hardening to configure browser settings to minimize attack surfaces. Browser extensions are another attack surface that can be used to infiltrate your systems. Take steps to control browser extensions and add-ons. Patch management is essential to ensure all software and plugins are up to date; explore whether it's possible to automate regular updates.

5 User Awareness and Training

One of the most important aspects of user awareness and training is educating users on how to recognize and avoid phishing scams and social engineering tactics. These tactics are commonly used to trick users into divulging sensitive information or clicking on malicious links. Providing guidance on practicing safe browsing habits, such as avoiding suspicious websites and downloads, is also crucial. By educating users on these risks and providing them with the knowledge and tools to identify and avoid them, organizations can significantly reduce their risk of a successful cyberattack.

6 Incident Response

When responding to browser-based attacks, organizations need to be prepared to take swift and decisive action. Detection and containment are paramount; organizations should implement strategies to quickly identify and isolate browser-based attacks to prevent further damage. This may involve monitoring browser activity for suspicious patterns, blocking access to malicious websites or downloads, and quarantining infected devices. Forensic analysis is equally essential to gain a deeper understanding of the attack, including its origin, scope, and the specific tactics used. By conducting a thorough investigation, organizations can attribute the attack to specific threat actors, identify potential vulnerabilities in their browser, and take steps to prevent similar attacks in the future. Understanding the full scope of an attack through forensics is essential for informing future security strategies and hardening defenses against evolving threats.



Close the Blindspot

Browser-based security is often overlooked in traditional cybersecurity strategies. The increasing reliance on browsers for daily operations makes them a prime target for sophisticated attacks, including phishing, data exfiltration, and malware infections.

Attackers exploit user trust, leveraging legitimate browser features for malicious purposes and bypassing conventional security measures. Real-world examples, such as QR code phishing, stolen credentials leading to data breaches, insider threats exfiltrating data through web applications, and malicious browser extensions, demonstrate the significant risks associated with neglecting security in the browser. These attacks highlight the inadequacy of relying solely on network and endpoint security and the necessity of real-time browser telemetry to detect and respond to threats.

Solutions like Chrome Enterprise Premium offer advanced features that provide the necessary telemetry, contextual awareness, and granular controls to mitigate the risks of an advanced attack. Organizations must recognize the browser as a critical entry point and take immediate action to utilize the features and policies available to close this security gap to protect against evolving cyber threats.

Additionally, security professionals need to stay informed about emerging browser threats to ensure that their organization's security posture is equipped to handle the latest attack techniques. Robust incident response plans focusing on detection, containment, and forensic analysis are crucial. The browser, once seen as a simple tool for accessing information, has become a complex battleground in the war against cybercrime; by recognizing this shift and prioritizing browser-based security, we can ensure the browser is a formidable line of defense against even the most sophisticated attacks. The future of cybersecurity lies not just in protecting our networks and devices, but in safeguarding the very portals through which we interact with the digital world. By prioritizing security in the browser today, we lay the foundation for a safer and more resilient tomorrow.