

Browsers Are the New Battlegrounds:

Protecting Your Customers and Web Apps
from Man-in-the-Browser Attacks



Table of Contents

- 1** The Rise of Browser-Based Attacks
- 2** Understanding Man-in-the-Browser (MitB) Attacks
- 3** Malicious Browser Extensions and Info Stealers
- 4** The New Threat Landscape
- 5** Why Traditional Security Measures Aren't Enough
- 6** Real-World Impacts of Browser-Based Attacks
- 7** MirrorTab: Eliminating the Browser Attack Surface
- 8** Strengthening Customer Trust in a New Era of Security
- 9** Resources and Further Reading



1

The Rise of Browser-Based Attacks

A new threat is emerging that targets browsers by leveraging trojan horses, malicious extensions, and info stealers. These new types of attacks, such as Man-in-the-Browser (MitB) attacks, can modify transactions on-the-fly as they are formed in browsers, displaying the user's intended transaction while altering the data that gets sent to the server. This makes them incredibly difficult to detect, as they operate between the user and the browser's security mechanisms.

Unlike traditional phishing attacks that rely on fraudulent websites, these new browser-based attacks use real services, with the user correctly logged in. There is no visible difference to the user, making the attacks nearly impossible to detect. As these attacks evolve, traditional security measures like PKI, advanced authentication methods, and other security protocols are rendered obsolete.

In this whitepaper, we explore the rise of browser-based attacks, the specific threats they pose, and how companies can protect their customers as they interact with web applications.

"CISOs and heads of security have ended up becoming more and more responsible for user behavior and how it impacts the security and privacy inside of applications."



Sounil Yu

Creator of the Cyber Defense Matrix

[linkedin.com/in/sounil](https://www.linkedin.com/in/sounil)



2

Understanding Man-in-the-Browser (MitB) Attacks

Man-in-the-Browser (MitB) attacks are a sophisticated form of cyberattack where an attacker uses a trojan to infect a user's computer, typically by exploiting vulnerabilities in the operating system or applications. This trojan installs an extension into the browser configuration, which is loaded the next time the browser starts.



How a MitB Attack Unfolds as seen on OWASP

1

Infection: The trojan infects the computer's software, either through the operating system or an application.

2

Extension Installation: The trojan installs an extension into the browser configuration, ensuring it loads upon the next browser start.

3

Browser Restart: At some point, the user restarts the browser, unknowingly loading the malicious extension.

4

Handler Registration: The extension registers a handler for every page load, monitoring the user's browsing activity.

5

URL Detection: The extension searches the URL of each loaded page against a list of known sites targeted for attack.

6

Login Detection: The user logs in securely to a targeted site (e.g., a banking site).



7

Pattern Recognition: The extension detects specific patterns in the page's content, such as those associated with financial transactions.

8

Form Field Manipulation: When the user submits a form, the extension extracts all data from the form fields through the Document Object Model (DOM) interface and remembers the values.

9

Data Modification: The extension modifies the values in the form fields through the DOM interface before the data is sent to the server.

10

Submission: The modified form data is submitted to the server, appearing as a legitimate request.

11

Receipt Manipulation: The extension intercepts the server's response, modifying the receipt data to match the original values the user entered.

12

User Perception: The user sees a receipt that appears correct, believing the transaction was completed as intended.

Man-in-the-Browser (MitB) attacks are a sophisticated form of cyberattack where an attacker uses a trojan to infect a user's computer, typically by exploiting vulnerabilities in the operating system or applications. This trojan installs an extension into the browser configuration, which is loaded the next time the browser starts.



3

Malicious Browser Extensions and Info Stealers

While MitB attacks are a significant threat, they are not the only danger lurking in browsers. Malicious browser extensions and info stealers also pose a substantial risk to customers interacting with web applications.



Malicious Browser Extensions

Malicious extensions often masquerade as useful tools or utilities but contain hidden code that can steal data, monitor browsing activity, or even modify web pages in real-time. For example, a seemingly harmless extension might collect login credentials or inject malicious code into web pages, all without the user's knowledge.



Info Stealers

Info stealers are malware designed to extract sensitive information from a user's computer, such as passwords, session tokens, and personal data. This data is often used for further attacks, including credential stuffing, identity theft, and financial fraud.



The Rising Threat



280 Million Chrome Users at Risk

Between July 2020 and February 2023, over 280 million Chrome users installed extensions that contained malware (Stanford University, CISPA).



87 Million Downloads of Malicious Extensions

Malicious extensions in the Chrome Web Store were downloaded around 87 million times (Kaspersky).



A Cyber Attack Every 39 Seconds

On average, a cyberattack occurs every 39 seconds, totaling approximately 2,244 attacks daily (University of Maryland).

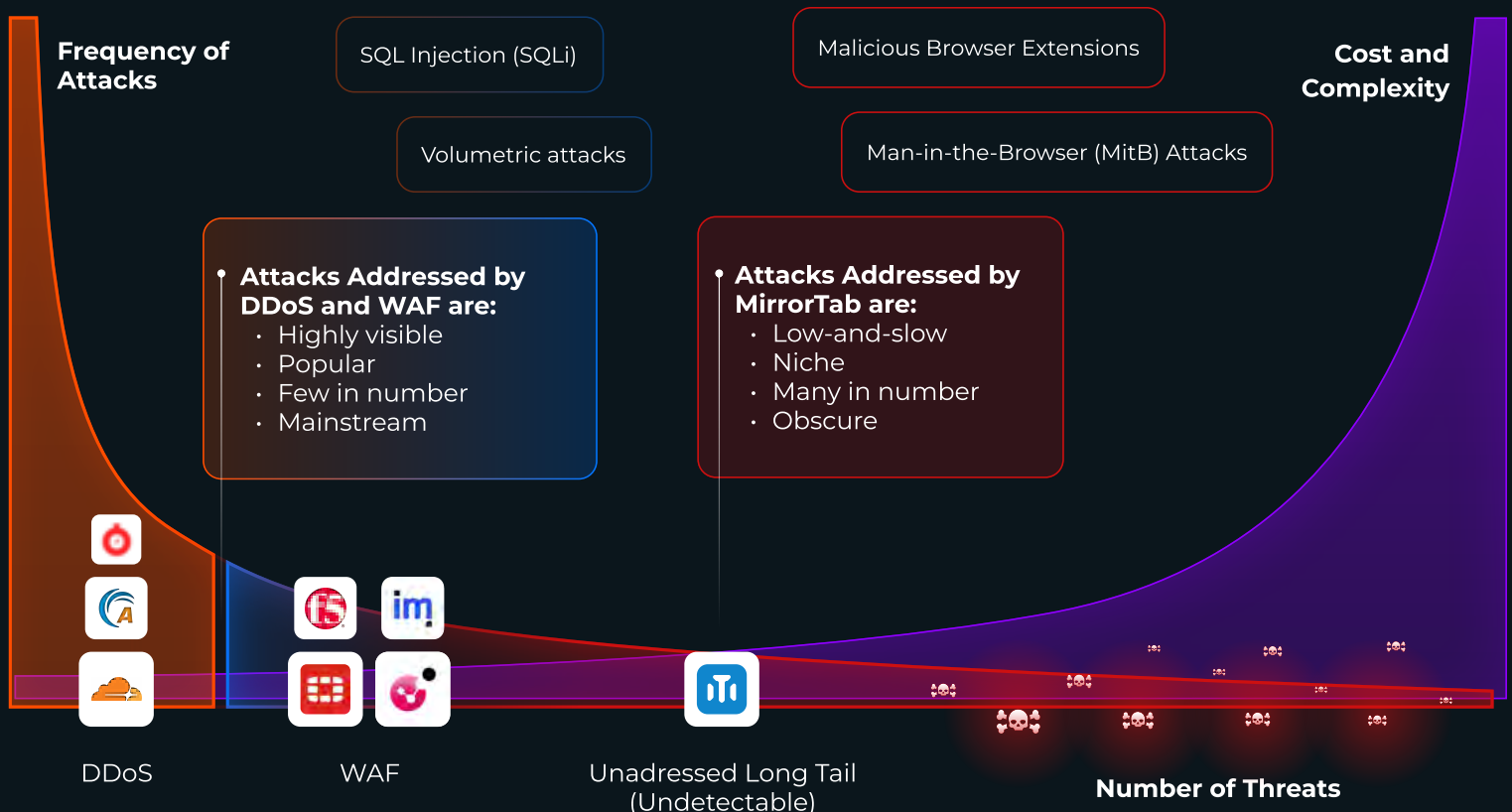
These statistics highlight the growing risk posed by browser-based threats and underscore the importance of securing web applications and the browsers used to access them.



4 The New Threat Landscape

Web applications are the primary online interfaces for businesses, while browsers serve as the gateway through which users access these applications. As more business interactions move online, the browser has become a critical battleground for cyberattacks.

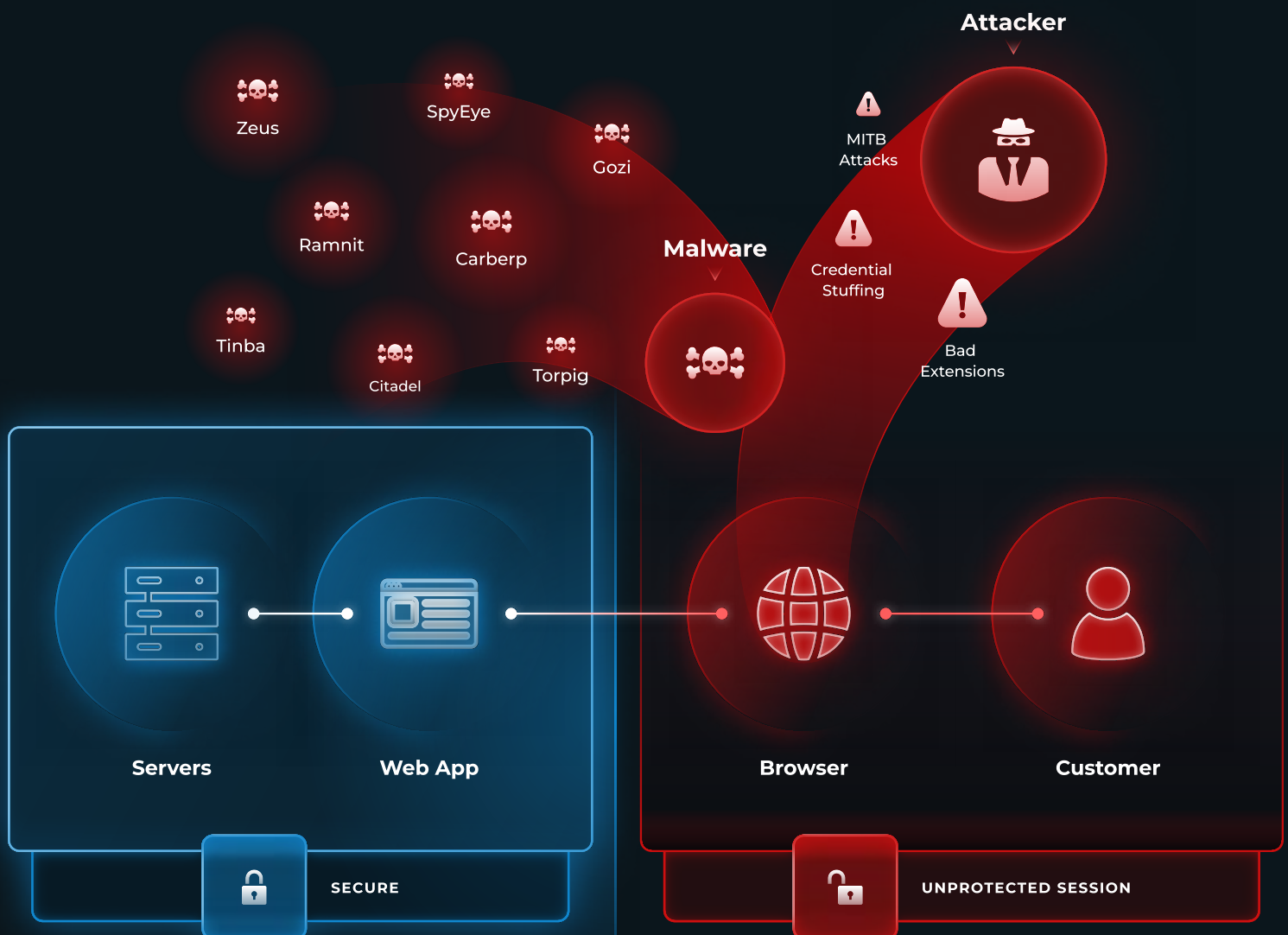
MitB attacks, malicious browser extensions, and info stealers are increasingly targeting users' browsers, exploiting the trust that users place in the websites they visit. These attacks are particularly dangerous because they can operate invisibly, making them nearly impossible for users to detect.





Why Traditional Security Measures Aren't Enough

Traditional security measures, such as Web Application Firewalls (WAFs) and Distributed Denial of Service (DDoS) protection, are essential for defending against direct attacks on web servers. However, they fall short when it comes to protecting the client-side—where browsers operate. This gap in security leaves users vulnerable to attacks that exploit the browser as the weakest link in the security chain.





5

Real-World Impacts of Browser-Based Attacks

Browser-based attacks can have devastating consequences for both businesses and their customers. Some of the most significant impacts include:



Financial Losses

Companies can face significant financial losses due to fraud, as attackers manipulate transactions or steal sensitive data.



Reputational Damage

A successful attack can severely damage a company's reputation, leading to a loss of customer trust and long-term business consequences.



Regulatory Penalties

Organizations may face hefty fines and legal repercussions if they fail to protect customer data in compliance with regulations like GDPR or PCI DSS.



6

Best Practices for Securing Your Web Apps

Given the growing threats posed by browser-based attacks, it's essential for businesses to adopt a comprehensive approach to securing their web applications:

1

Implement Client-Side Isolation

Use technologies like MirrorTab to create a virtual air gap between your web applications and the customers accessing them. This ensures that even if a customer's browser is compromised, the security of your web app remains intact.

2

Regularly Audit and Update Browser Extensions

Encourage customers to use only trusted browser extensions and to regularly review and update them. Provide guidance on how to detect and remove malicious extensions.

**3****Educate Customers on Browser Security**

Inform your customers about the risks associated with browser-based attacks, such as MitB and info stealers. Provide resources and tools to help them secure their browsing environment.

4**Deploy Multi-Layered Security Solutions**

While MirrorTab can eliminate the browser attack surface, it's important to complement this with other security measures like WAFs, DDoS protection, and real-time monitoring to defend against server-side threats.

5**Monitor and Respond to Emerging Threats**

Stay informed about the latest cyber threats and adjust your security strategies accordingly. Regularly update your web applications and security protocols to address new vulnerabilities.



7

MirrorTab: Eliminating the Browser Attack Surface

MirrorTab offers a new approach to securing your customers by removing the browser attack surface entirely. With MirrorTab's advanced pixel streaming technology, your customers can securely interact with web applications even if their browser is compromised by malware, a man-in-the-browser attack, or a malicious extension.

How MirrorTab Works



Client-side Isolation

MirrorTab creates a virtual air gap between web applications and the customers accessing them, ensuring that even if the customer's browser is compromised, the security of your web app remains intact.



Pixel Streaming

Instead of rendering DOM elements, MirrorTab streams secure virtual representations of your web application's content as pixels. This eliminates the attack surface for browser-based threats, including MitB attacks, info stealers, and malicious extensions.



Deployed Server-Side

MirrorTab operates server-side, ensuring a seamless user experience without requiring any changes to client-side behavior. Web applications behave normally and content is presented accurately, maintaining a frictionless user experience.



Why MirrorTab is the Best Browser Security Solution

Protects Against a Wide Range of Attacks

MirrorTab secures your customers from MitB attacks, session token theft, credential stuffing, and other browser-based threats.

Seamless Integration

MirrorTab integrates smoothly with your existing web applications, providing robust security without disrupting the user experience.

Advanced Security for Your Customers

By eliminating the browser attack surface, MirrorTab ensures that your customers can securely access your web apps—even if their browser is compromised.





8

Strengthening Customer Trust in a New Era of Security



As web applications become the primary interface for business operations, securing the browsers that access them has never been more critical. The rise of MitB attacks, malicious browser extensions, and info stealers represents a significant shift in the threat landscape—one that traditional security measures are not equipped to handle alone

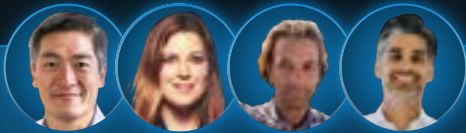
MirrorTab offers a revolutionary solution by removing the browser attack surface entirely, ensuring that your customers can securely access your web apps, regardless of the security state of their browser. By adopting MirrorTab and following best practices for browser security, businesses can protect their customers, maintain trust, and stay ahead of the evolving cyber threat landscape.



9

Resources and Further Reading

To learn more about protecting your customers from emerging browser-based threats, explore the following resources:



Watch CISO Event

Learn about the evolving role of CISOs and how they must protect customers and web apps from MitB attacks.

mirrortab.com/ciso-event

SANS



Watch SANS Cyber Fest

Discover how browsers are the new battlegrounds and how MirrorTab protects web apps and maintains customer trust.

mirrortab.com/sans-cyber-solution-fest

Watch Overview

Watch a demo of how MirrorTab uses advanced pixel streaming technology to enhance customer trust and security.

mirrortab.com/overview

Visit MirrorTab's Website

Find more information on how MirrorTab can help your business stay ahead of the evolving cyber threat landscape.

mirrortab.com



References

"DOM-based vulnerabilities," PortSwigger. Available: <https://portswigger.net/web-security/dom-based>

"Man-in-the-browser (MitB) attack," OWASP. Available: https://owasp.org/www-community/attacks/Man-in-the-browser_attack

"Man-in-the-browser (MitB)," TechTarget. Available: <https://www.techtarget.com/searchsecurity/definition/man-in-the-browser>

Virus attack on HSBC Transactions with OTP Device

Virus attack on ICICI Bank Transactions

Virus attack on Citibank Transactions

Hackers outwit online banking identity security systems, BBC Click

Antisource - ZeuS A summary of ZeuS as a Trojan and Botnet, plus vector of attacks

Man-In-The-Browser Video on YouTube Entrust President and CEO Bill Conner

Zeus: King of crimeware toolkits Video on YouTube The Zeus toolkit, Symantec Security Response

How safe is online banking? Audio BBC Click

Boy-in-the-Browser Cyber Attack Video on YouTube Imperva