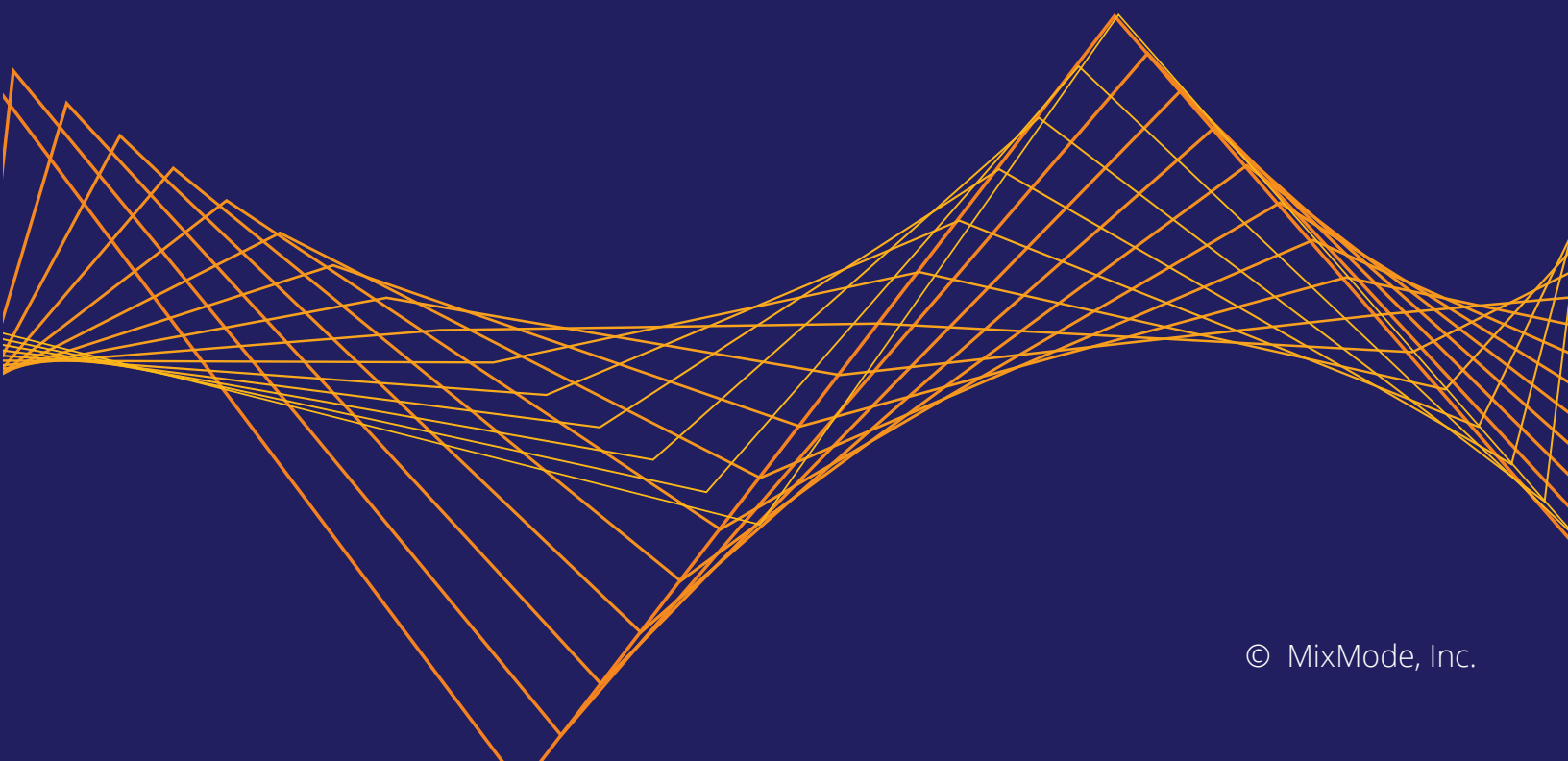
MixMode®

THREAT REPORT

Web Browsers as an Overlooked Risk in Cybersecurity

Michael Yelland
MixMode's Architect & Principal Researcher



Web browsers have transformed from simple tools for displaying static web pages into powerful, interactive platforms that facilitate complex SaaS applications, real-time collaboration, and cloud-based work environments. Initially conceived as “read filters,” browsers once passively interpreted and displayed HTML documents. However, as technology evolved, they became gateways for bidirectional communication, client-side scripting, and interactive applications.

This transformation has introduced significant cybersecurity risks. Despite their widespread use, web browsers remain an overlooked risk vector, offering attackers opportunities to exploit session persistence, cached credentials, and misconfigured security settings.

Building on our previous research into OAuth vulnerabilities, cloud infrastructure laundering, and DeepSeek exploits, this report explores how attackers leverage browser-based vulnerabilities to infiltrate enterprise and government networks. By treating browsers as trusted applications, organizations often fail to implement necessary security controls, leading to breaches that can bypass traditional defenses.

How Web Browsers Increase Cyber Risk

The Problem: Browsers as Silent Data Brokers

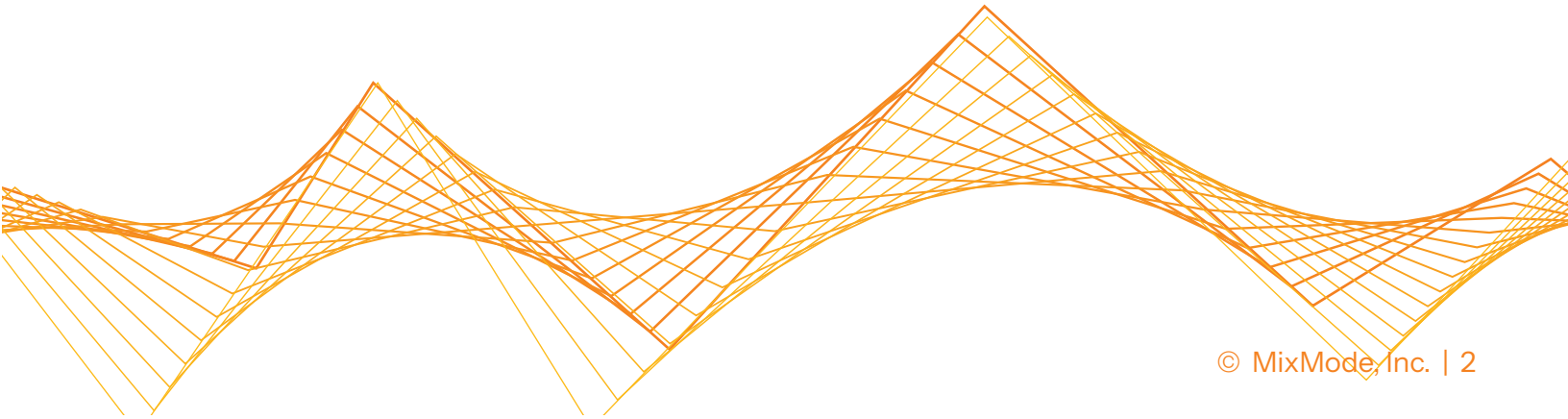
Modern web browsers continuously broadcast information that can be exploited by threat actors, including:

- HTTP Headers: Disclosing browser type, OS, preferred language, and referrer details.
- TLS Handshake Data: Leaking encryption methods and domain-level indicators.
- Local Storage & Cache: Storing session tokens, authentication cookies, and indexed database records.
- WebRTC & Network Discovery: Exposing internal and public IP addresses when improperly configured.

Case Study: The Funnull Network and Cloud-Based Threats

The Funnull Network, linked to Chinese cybercriminals, has demonstrated how cloud environments can be abused to launch phishing campaigns and host malicious content. Similar tactics are now applied within browsers:

- Session Hijacking Attacks: Exploiting stolen cookies to bypass MFA protections.
- Malware Injection via Scripts: Delivering payloads through compromised content delivery networks (CDNs).
- Persistent Tracking Mechanisms: Using third-party cookies and browser storage to maintain unauthorized access.



Confirmed Breaches Due to Browser Insecurity

- SolarWinds (2020): Phishing attacks leveraged browser session data for lateral movement.
- Marriott International (2020): Exploited browser-stored authentication tokens to bypass MFA.
- Colonial Pipeline (2021): Misconfigured browser settings exposed administrative credentials.
- Magecart Attacks (2020-2024): Injected malicious scripts into e-commerce checkout pages.
- LastPass Breach (2023): Cached vault data was accessible via browser automation scripts.

Browser Vulnerabilities and Exploits (2022-2024)

Recent High-Risk CVEs:

- Google Chrome:
  - CVE-2024-0519: Memory corruption in the V8 JavaScript engine.
  - CVE-2024-4058: Critical ANGLE graphics layer security flaw.
- Mozilla Firefox:
  - CVE-2024-9680: Remote code execution vulnerability.
  - CVE-2023-3388: UI spoofing exploit allowing phishing attacks.

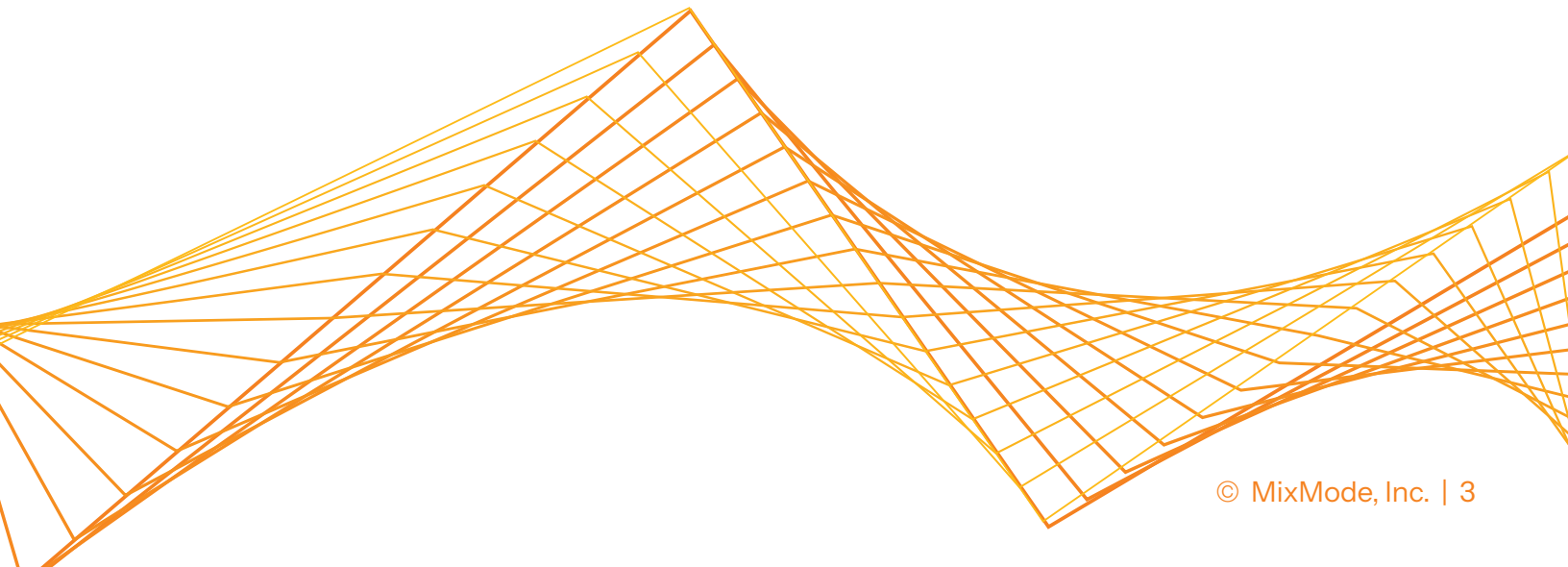
These vulnerabilities highlight how attackers leverage browser flaws for persistent threats that evade traditional endpoint detection and response (EDR) solutions.

The Intersection of OAuth & Browser Security

As detailed in our previous OAuth report, persistent authentication mechanisms create an invisible attack surface within browsers. Web-based authentication flows rely on:

- Long-lived OAuth tokens that remain active across sessions.
- Browser Autofill & Saved Credentials that attackers can extract via malicious scripts.
- Session Hijacking Risks due to poor cookie security policies.

While Zero Trust frameworks are widely adopted, they often fail to enforce continuous authentication monitoring within browser environments, creating exploitable blind spots.



Mitigation Strategies: Securing Browsers Against Emerging Threats

As web browsers continue to evolve into essential tools for enterprise workflows, their security must be treated with the same rigor as other critical infrastructure. Attackers exploit browser vulnerabilities, session persistence, and misconfigurations to infiltrate systems and exfiltrate sensitive data. Implementing the following strategies can help organizations proactively defend against these emerging threats.

1. MixMode's AI-Driven Analysis & Real-Time Monitoring

- Detect abnormal authentication patterns and browser behavior.
- Correlate browser session activity with network and API traffic.
- Provide early threat detection for emerging browser-based attacks.

2. Patch Management & Security Updates

- Enable automatic browser updates for Chrome, Firefox, and Edge.
- Supplement patching with real-time anomaly detection.

3. Harden Browser Security Settings

- Disable WebRTC to prevent IP leaks.
- Enforce Secure Cookie Attributes (HttpOnly, Secure, SameSite).
- Restrict Browser Extensions to approved sources only.

4. Strengthen Authentication Practices

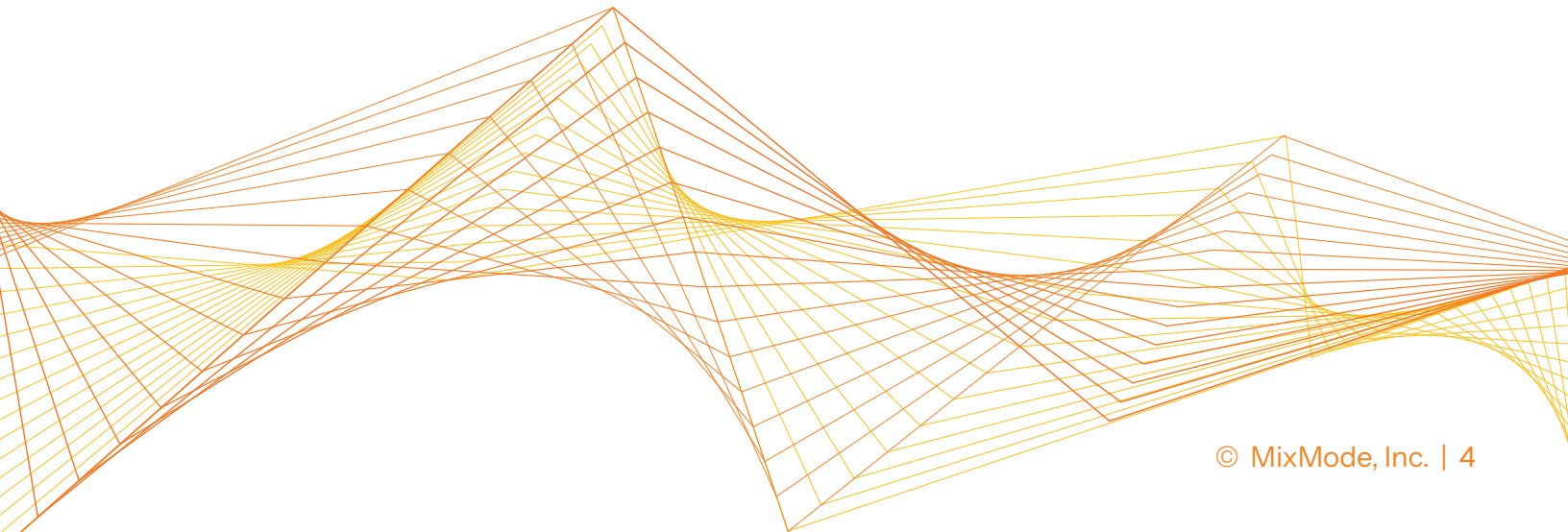
- Enforce short-lived tokens and multi-factor authentication (MFA).
- Use password managers instead of browser-stored credentials.
- Enable secure session expiration policies.

5. Reduce Persistent Data Storage Risks

- Regularly clear cookies, cache, and session storage.
- Block automatic form-filling for sensitive credentials.
- Prevent unauthorized JavaScript execution on login pages.

6. Enterprise Security Policies for Web Access

- Enforce browser isolation for high-risk applications.
- Monitor browser activity for unauthorized login attempts.
- Deploy behavioral analytics to detect anomalies in authentication flows.



The Future of Browser Security in Cyber Threat Detection

Web browsers are an often-overlooked security risk, yet they serve as critical gateways for unauthorized access. Attackers are increasingly using sophisticated techniques—including OAuth session hijacking, infrastructure laundering, and AI-driven reconnaissance like DeepSeek—to exploit weaknesses in browser security.

Organizations must move beyond geolocation-based security measures and implement behavioral analytics, continuous monitoring, and AI-driven detection models. **MixMode's AI-powered security platform offers real-time visibility into browser activity, correlating authentication data with broader network threats to identify risks before they escalate.**