IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Combating the Risk of Web Browser Attacks

Jonathan Lee

Jonathan Lee
Senior Product Manager
Menlo Security

Biography

Jonathan Lee is a Senior Product Manager at Menlo Security (https://www.menlosecurity.com), a leader in cloud security. In this role he serves as a trusted advisor to enterprise customers, and works closely with analysts and industry experts to identify market needs and requirements, and establish Menlo Security as a thought leader in the Secure Web Gateway (SWG) and Secure Access Service Edge (SASE) space.

Experienced in leading technical development, launch and adoption of innovative security products, including email security, data loss prevention and end point security, Jonathan previously worked for Proofpoint and Websense. As an industry expert, media commentator and speaker, Jonathan is well versed in data protection, threat analysis, networking, Internet isolation technologies, and cloud-delivered security.

Keywords Web browser security, Cyber security, Zero trust, Cyber awareness, Browser attacks, Cyber threat
Paper type Reference

Abstract

The widespread shifts to more flexible working that we saw take hold during the pandemic and prevail post-Covid have seen organizations shift their operating models and IT infrastructure to the cloud, paving the way for the browser to become one of the most critical business tools. But as research by Menlo Labs has found, many attackers are now adapting their methods of attack directly to capitalize on a series of new opportunities which are arising as people spend most of their day in the browser doing their work. The mitigate the risks, companies are now faced with a new set of challenges, as the author of this article explains.

Introduction

Until only recently, most of us knew work as a place where you went. As children, our parents would leave the house and return nine hours later, having physically ‘gone to work’. Today, however, work isn’t a place you go, but something you do. We’re no longer tied to an office or worksite in the new normal. Today, many of us have the freedom to log onto our company network as it suits us – from the office, at home, or on the go.

Widespread shifts to more flexible working that we saw take hold during the pandemic and prevail post-Covid have seen organizations shift their operating models and IT infrastructure to the cloud, paving the way for the browser to become one of the most critical business tools. Almost all work is now carried out on the internet. Indeed, Google has reported[1] that end users spend an average of 75% of their workday using a web browser.

From a greater work life balance to boosted productivity and improved staff retention, both employees and employers have seen the benefits of remote and hybrid models. However, this shift has also presented a series of new and evolving risks that companies are now faced with managing and mitigating.

Where users can use the internet to access sensitive data within applications and Software as a Service (SaaS) platforms using a variety of devices in a variety of locations, the web browser has become the biggest attack surface available to threat actors, who are actively leveraging and exploiting it.

Indeed, many attackers have been adapting their methods to capitalize on a series of new opportunities. At Menlo, we have witnessed a significant ramp up in the deployment of techniques specifically designed to evade traditional layers of detection, such as firewalls, secure web gateways (SWGs), malware analysis engines, and phishing detection tools, enabling the efforts of threat attackers to slip under the radar.

Web browser attacks

Four browser-based attack methods which we are frequently observing include:

1. **HTML smuggling** – HTML smuggling and/or JavaScript trickery is often used within browser environments as a means of bypassing content inspection engines, enabling attacks to deliver malicious payloads to target endpoints. This technique relies upon the malicious file being dynamically constructed inside the browser to ensure there are no resource requests for a remote file that can be inspected. Significantly, even file types that would typically be blocked by SWG engines can still make it to the endpoint without any user interaction.

2. **Malicious links** – Malicious links are a common tactic used by threat actors, sent not just via email but equally through social media, SMS messages, shared documents and more. When these methods are used in combination with HTML smuggling, content inspection engines become blind to any risk, incapable of identifying the dynamic generation of a file within the browser beyond typical network security perimeter controls.

3. **'Good2Bad' websites** – 'Good2Bad' websites are a third technique that see attackers leveraging benign websites for malicious activities to circumvent web categorization. Specifically, these are used to support malicious intent for brief periods before reverting to their original benign state. Notably, between 2019 and 2021, Menlo Labs identified a massive 958% increase in the use of Good2Bad sites.

4. **Evasive HTTP traffic inspection techniques** – Several browser exploits such as phishing kit code, crypto-mining code and the impersonation of brand logos can be generated using JavaScript in the browser to avoid detection from static signatures that typically examine web page source code and HTTP traffic. Such methods again render traditional detection tools that are deployed prior to web page execution largely useless.

Defending against browser-based threats

Attackers are finding new ways to bypass legacy security solutions that are simply not equipped for modern ways of working. Indeed, the most common tools used in current security stacks were created in the era before De-parameterization, when work was a place that could be walled off from malicious actors and aren't fit for modern cloud- and browser-led operating environments.

Today, we're seeing web content of all kinds is evolving at rapid speed. New websites are being spun up faster than they can be categorized by URL filters, and threat intelligence can't keep up with the amount of content being created and compromised by attackers. Even those solutions leveraging artificial intelligence and machine learning need reputational evidence to detect malicious activity, and by then it's often too late.

Some vendors are working to respond by adding security controls directly within the browser. Google and Microsoft, for example, are providing built-in controls inside Chrome and Edge to secure at the browser level rather than the network edge. However, with attackers developing new evasive attack methods like HTTP Smuggling at increasing rates, new approaches are needed. For this reason, it is vital that organizations take a Zero Trust approach to security to stop zero-day malware and credential phishing sites in their tracks and avoid false positives that can drain IT resources and disrupt productivity.

In achieving Zero Trust in the truest sense, remote browser isolation is a logical option, preventing all content – be it good or bad – from executing on a local device. Keeping potentially malicious code away from the endpoint is the only way to stop browser-based attacks with certainty. If malicious content cannot be delivered, threat actors can't traverse to network and execute attacks.

Reference

[1] Tabriz, P. (15 September 2020), The future of enterprise: Your business, in the browser. Google Cloud. Available at: https://cloud.google.com/blog/products/chrome-enterprise/chrome-is-helping-it-teams-support-cloud-first-workforce