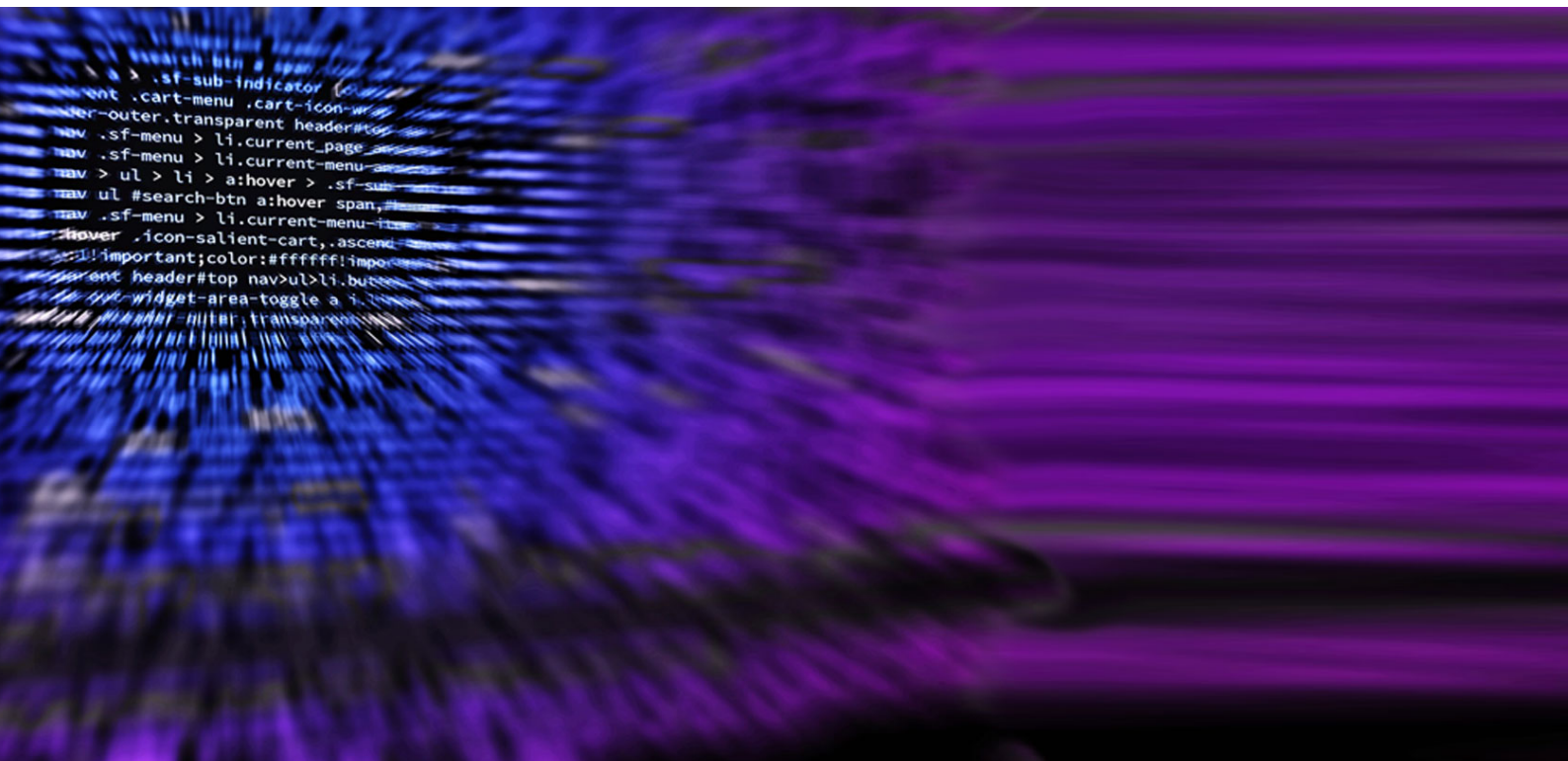
source DEFENSE

SOURCE DEFENSE

2018

SAFEGUARDING THE CRITICAL WEB

Preventing an Unaddressed, Universal Website Supply Chain Vulnerability



Securely Maximize Website Potential & Performance

Security teams face a complex challenge. To drive business performance, marketing teams demands web enhancements that put the onus on security teams to adequately safeguard the business. Unfortunately, it's an impossible challenge. Marketing driven web enhancements introduce a universal client-side supply chain vulnerability that provides threat actors with unmanaged access to your critical business and customer data. Concerned about the tenuous position your organization's website enhancements have left you in? This impacts you.

WEBSITE ENHANCEMENTS INTRODUCE A UNIVERSAL SUPPLY CHAIN VULNERABILITY THAT PROVIDES THREAT ACTORS WITH UNMANAGED ACCESS TO CRITICAL BUSINESS AND CUSTOMER DATA.

The corporate website is one of an organization's most valuable assets serving as a significant revenue channel, an efficient path for customers to interact with your business, and the way your establish and communicate your brand. It is critically important to secure this tremendous tool and ensure its availability.

EVERY WEBSITE TODAY IS VULNERABLE TO THIS CLIENT SIDE SECURITY FLAW.

Providing a deeply engaging user experience and extracting insightful analytics is the goal of marketing who often claim ownership of the web site. Safeguarding this property is the goal of security. This creates organizational friction as the goals are somewhat diametrically opposed. Exacerbating this departmental rift is the pace marketing requires to remain competitive and differentiated which overwhelms security's capacity to verify and secure. Enabling the business demands innovation, speed, and responsiveness and security is often viewed as a bottleneck. As such, many organizations adhere to business goals and defer to the needs of marketing while inadequately involving security or, in some cases, leave them out of the review process entirely.

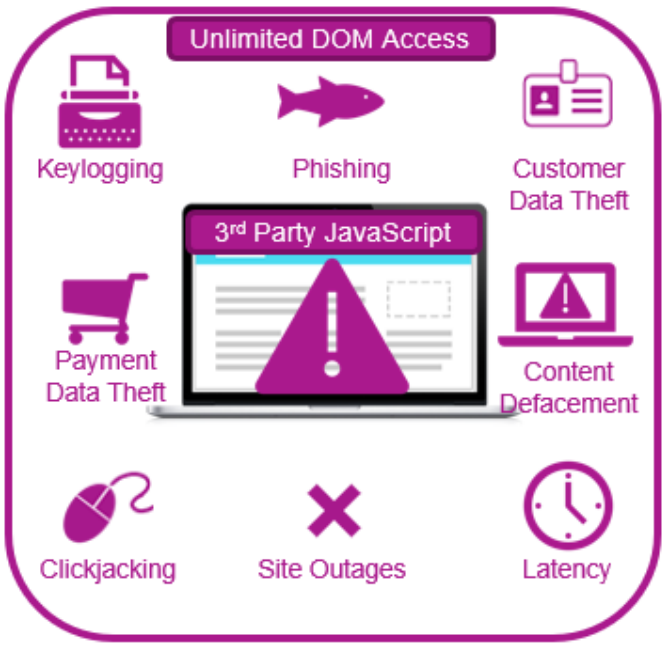
The Easy Target Becomes Your Problem

A perfect example of such a dynamic is the use of 3rd party website tools that enhance the user experience and drive critical analytics (ex. Google Analytics, social media tools, and chat tools). Marketing requires these tools to deliver on the overall and shared goals of the business. These tools, integrated via JavaScript, introduce a universal, client-side website vulnerability that current security tools and process are incapable of securing. Nearly every corporate website today includes dozens of 3rd party JavaScript tools as they deliver rich content, experience, and analytics data.

These external 3rd party tools (and the hackers that exploit them) are allowed nearly unlimited access to every element of your web pages on the client side through completely unmanaged connections with corresponding external 3rd party servers. Making matters worse, these 3rd party website supply chain vendors are almost certainly less secure, on average, than the typical enterprise. This provides hackers with a comparatively simpler path to access website content, data and customers. As if this situation was not concerning enough, once a hacker compromises a single 3rd party vendor, they have unmanaged and unlimited access to every web page that runs that tool.

A recent example of threat actors exploiting this vulnerability is the recent breach of multiple global enterprises, including airlines and mass merchants. Reportedly, a website chat tool vendor was breached, unmanaged access to the multiple websites running the tool was leveraged, and unlimited access to the client-side website DOM was exploited to steal credit card information from site visitors. These websites simply endeavored to engage their visitors through chat functionality but ended up victimized by this website supply chain vulnerability they were left powerless to prevent.

What Are the Potential Damages?



THESE DOZENS OF EXTERNAL 3RD PARTY TOOLS (AND THE HACKERS THAT EXPLOIT THEM) ARE ALLOWED NEARLY UNLIMITED ACCESS TO EVERY ELEMENT OF YOUR WEB PAGES ON THE CLIENT SIDE THROUGH COMPLETELY UNMANAGED CONNECTIONS WITH THEIR CORRESPONDING EXTERNAL 3RD PARTY SERVERS. THIS MEANS EVERY WEBSITE TODAY, INCLUDING YOURS, IS INESCAPABLY VULNERABLE

As these unmanaged JavaScript connections provide unlimited client-side access to the website DOM, the significant, universal vulnerability allows threat actors to steal customer and corporate data via keylogging, web injections, form field manipulation, click jacking, malware distribution, malvertising, and phishing. At risk is:

- Business and Customer Data Theft
- Reputational & Brand Damage
- Lost Revenue
- Fines & Compliance Violations (ex. GDPR, PCI, HIPAA)

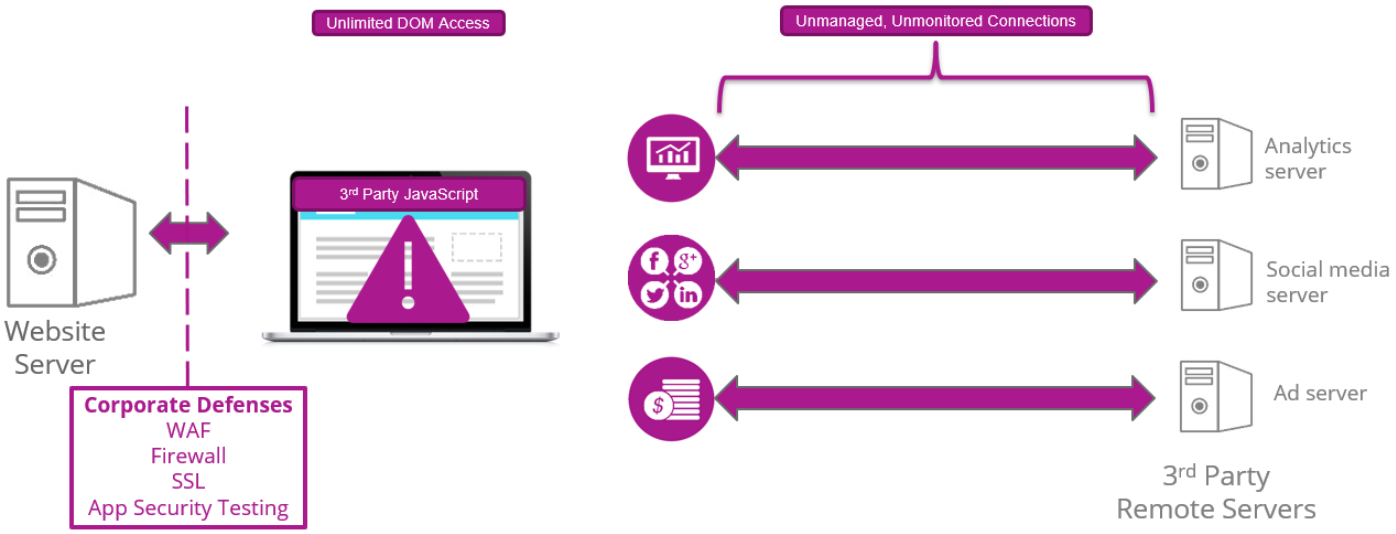
This universal vulnerability can also significantly degrade the critical user experience. This introduces increased risk of:

- Website Content Defacement
- Increased Cost of New Customer Acquisition
- Low Customer Conversion Rates
- Lower Revenue per Customer
- Fewer Repeat Customers

The Universal Website Supply Chain Vulnerability that Current Security Can't Stop

This client-side attack occurs when a 3rd party JavaScript server is compromised and malicious JavaScript code is injected into the original JavaScript. The flexibility and lack of control over JavaScript enables threat actors to access and assume near total control of any and all websites that have integrated this, now compromised, JavaScript tool. Today, this is nearly every commercial website.

The challenge lies in the fact that there is no guarantee that the JavaScript code hosted at the 3rd party will remain static, unimpacted by new or malicious JavaScript. Although the original JavaScript may be reviewed prior to insertion into the client application new features and code may be pushed into the remotely hosted 3rd party JavaScript server at any time. This grants the 3rd party code the exact same privileges as those granted to the website owner. Unfortunately, the designed flexibility of JavaScript works against its security capability to create a significant vulnerability as the 3rd party JavaScript can assume control. This is completely invisible to and beyond the security controls of the existing security infrastructure without dynamic and continuous per-session monitoring of website activity. This is an impossible task.



Before Source Defense, there were no viable controls for this attack vector. Web security solutions including WAFs and firewalls are designed to deliver security on the server-side of the web session. They fail to address the client-side vulnerability when the web session traverses beyond the tightly controlled corporate security perimeter. Web sites operate extensively outside of this security framework and leave your organization vulnerable to threat actors endeavoring to initiate a client-side attack.

Some organizations invest in application security validation testing or dynamic application security testing including *AST testing (IAST, RASP, SAST, DAST, Web Applocation Scanning, etc.). This testing process, while effective for its designed purpose, evaluates the integrity of the designed JavaScript call function and isn't designed to test every use case and operate dynamically as would be required to thoroughly secure this growing attack vector. At best, these types of solutions may operate as a "Detection" approach. They are incapable of providing real-time scanning of all web traffic across the entire user population. This results in successful attacks that are never detected. Furthermore, even if an attack is detected, damage has already occurred. Even is "some" customer data was compromised this constitutes a compliance violation and necessitates disclosure. The fines, brand damage, ensuing PR crisis, and operational firefighting erode the entire value proposition of detection approaches.

The Source Defense Solution: Prevent Website Supply Chain Attacks - Eliminate Vulnerabilities Introduced by the Vendors You Rely on for Website Enhancement, Personalization and Analytics

"We now have complete control over every 3rd party with access to our website and can control what every individual 3rd party JavaScript can see and do"

- Cleanly CTO, Alex Prober

Source Defense provides an entirely new and unique approach focused on preventing vulnerabilities introduced through the website supply chain via 3rd party JavaScript vendors. Through first-of-its-kind isolation and segmentation technology, Source Defense leverages a fully automated and machine-learning assisted set of rules and policies that define the access and permission of all 3rd party JavaScript code operating on a website. The Source Defense solution ensures 3rd party JavaScript may only deliver the intended website experience and that these JavaScript tools may not be leveraged for malicious data extraction or website alteration.

The Source Defense solution was purposefully built for deployment ease and administration simplicity. Integration is simple and our Auto-Config Technology automatically identifies all 3rd party tools operating on the site (including those added in the future), categorizes them, and automatically applies intelligent security settings. These can be customized at the customer's discretion, but the machine-learning process does not require it. Lastly, the Ultra Low-Touch design operates in the background as a prevention solution. All alerts are FYI-only with client-side vulnerability prevention running silently. Alerts may be accessed as desired, but the system does not require ongoing management, monitoring or interaction once installed.

- ✓ **Copy & Paste Integration** requires only minutes to complete
- ✓ **Auto-Config Technology** effortlessly completes system setup
- ✓ **Ultra Low-Touch System Design** operates silently and requires no management

Source Defense provides a compelling security and data privacy compliance solution as well as a critical business enablement tool. It provides security controls and visibility to provide confidence in operating websites securely and does so without introducing additional latency that is the common burden of the majority of other security tools focused on securing the corporate web experience.

Prevent Website Supply Chain Attacks

Find out more:

- What is My Risk?
  - Many Source Defense customers wish to understand their specific risk level. Contact us to receive an assessment of current website exposure to 3rd parties. (https://www.sourcedefense.com)
- Learn More?
  - Read the whitepapers (https://www.sourcedefense.com)
- How Does it Work?
  - Link to how it works (https://www.sourcedefense.com/technology)
- See it in Action?
  - Schedule a demo (https://www.sourcedefense.com/contact)

2018

source DEFENSE

SOURCE DEFENSE