



CROWDSTRIKE SERVICES AND SOURCE DEFENSE INC. THREAT BRIEF

Rapid Increase of Magecart-Style
Browser Session Attacks via a Universal
Website Supply Chain Flaw

EXECUTIVE SUMMARY

Threat actors like the Magecart groups have successfully compromised multiple third parties within the website supply chain that provide critical website capabilities, functionality, and content. These actors have been exploiting a universal website supply chain flaw that leaves personally identifiable information (PII) and payment data exposed to theft from web sessions at mass-scale – repeatedly victimizing hundreds and even thousands of sites per campaign. Based on open-sourced reporting, notable victims have included Ticketmaster, Best Buy, Delta Airlines, NewEgg, Sears, Pizza Hut, Kmart, 1-800-Flowers, Equifax, and TransUnion¹. The frequency of attacks targeting this flaw highlights the inadequacy of current security controls and the nearly universal vulnerability of website owners.

This flaw prevents website owners from controlling what data can be accessed by their website supply chain vendors and the hackers that exploit them. The challenge is that every website that uses third-party JavaScript is susceptible to this attack vector because attacks occur when external third-party web servers send modified JavaScript directly to the client-side browser. Currently, no component of traditional security solutions prevents client-side, third-party JavaScript modification.

The goal of this threat brief is to raise awareness of this universal flaw and summarize why almost all websites remain exposed to this attack vector. This will include highlighting the limitations of various mitigation options and discussing preventative as well as investigative measures that organizations can take to avoid this type of damaging attack.

THIRD-PARTY WEBSITE JAVASCRIPT OVERVIEW

Third-party JavaScript refers to vendor scripts that are embedded into websites to enrich the customer experience, enhance analytics and monetize sites via advertising. For example, websites that include a chat box asking if you have questions or need assistance are demonstrating a third-party feature that operates via JavaScript. These third-party scripts can provide powerful functionality, but they also introduce risks that can impact security, privacy, performance, and page behavior. Therefore, while having more third-party JavaScript enhancements will improve website effectiveness, it also increases risk because it creates an uncontrolled and rapidly expanding attack surface.

This flaw prevents website owners from controlling what data can be accessed by their website supply chain vendors and the hackers that exploit them.

THE UNIVERSAL FLAW AND THE ATTACK SURFACE

Third-party vendors send JavaScript directly to the user's browser session via an unmanaged client-side connection between the user's browser and their third-party servers. Being unmanaged means your company's security defenses will have no visibility into the connection and thus unable to protect the end user visiting your website. Due to JavaScript's designed-in flexibility, this external third-party JavaScript has full developer-level access (i.e., DOM access) to your webpages. This results in website owners being unable to control how the third-party JavaScript modifies and interacts with the webpage during the user session.

The expanding attack surface occurs because the third parties involved routinely chain-in multiple fourth and fifth parties that share the same level of unrestricted access to your webpage. It is these unmanaged connections between the client-side browser and external third-party servers that attackers are increasingly targeting in order to modify the website and exfiltrate PII and payment data.

However, the scope of potential damages far exceeds data skimming. With the unlimited DOM access provided to the third-party JavaScript, this attack vector has also been used for:

- **Banking Trojan, ransomware and malware distribution**
- **Cryptojacking**
- **Content defacement**
- **Session redirects (clickjacking)**
- **Phishing**
- **Highly targeted watering hole attacks**
- **Malvertising**

SUPPLY CHAIN'S WEAKEST LINK AND SCALABILITY OF ATTACKS

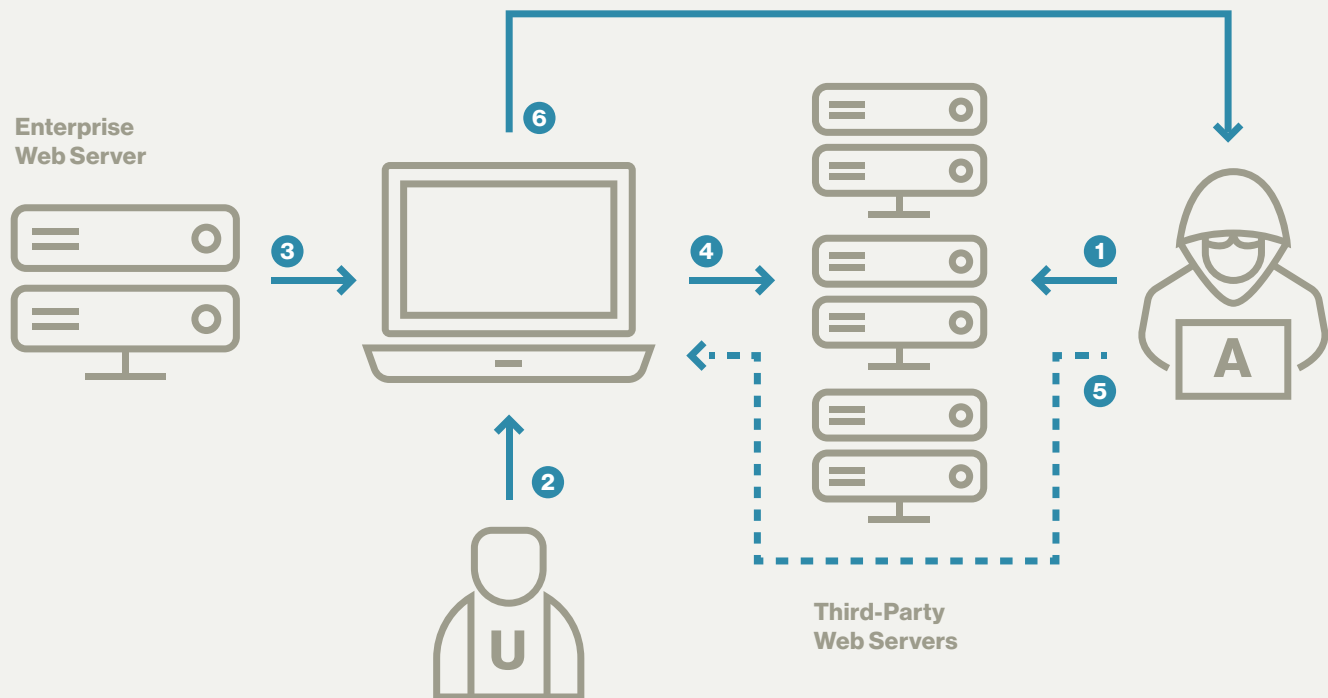
The uncontrolled access to the webpage and all data transmitted during the user session provide threat actors with an easy path to penetrating a website's security and exfiltrating PII and payment data. Instead of directly targeting the defenses of the highly secured website owner, threat actors follow the path of least resistance: targeting the vulnerable third-party vendor's security infrastructure. Once they have breached the security defenses of a third-party vendor (or a linked fourth party), threat actors modify the code served from the external third-party server to the client-side browser. Frequently these modifications involve adding card skimming code or some other means of data exfiltration.

This attack type is extremely scalable because the attackers not only have access to a single website, they immediately gain access to every website served by the compromised third-party JavaScript vendor. This allows threat actors like Magecart to attack hundreds or thousands of organizations and in turn victimize huge user populations during each campaign.

Due to JavaScript's designed-in flexibility, this external third-party JavaScript has full, developer-level access to your webpages.

HOW A WEBSITE SUPPLY CHAIN ATTACK UNFOLDS

CLIENT-SIDE BROWSER SESSION ATTACK VIA MODIFIED THIRD-PARTY JAVASCRIPT



- 1** Attacker compromises a third-party vendor and modifies the vendor's JavaScript to include their malicious code
- 2** A user visits your site
- 3** Your web servers provide your website to the visitor
- 4** Your webpage, while rendered in the user's browser, requests content from the third-party server
- 5** The modified JavaScript from the compromised third-party is sent directly to the user's browser
- 6** The malicious code executes in the user's browser session — in data theft attacks, data is exfiltrated either directly back to the compromised vendor's server or to the attacker's server

LIMITATIONS OF TRADITIONAL CONTROLS

Security teams should diligently evaluate this attack vector because current controls are not capable of preventing these types of attacks. The following describes traditional controls and explains why they are inadequate.

CONTENT SECURITY POLICY (CSP) AND SUBRESOURCE INTEGRITY (SRI)

SECURITY LIMITATIONS

These approaches leave an organization exposed to several variations of this attack type:

- CSP will not protect against a script served from a whitelisted domain that was compromised nor prevent data exfiltration to a whitelisted domain.
- SRI will not protect against fourth-party attacks nor malicious ads served through ad networks.

OPERATIONAL OVERHEAD

These techniques require a prohibitive level of research and development (R&D) resources to implement and manage:

- CSP requires close coordination with third parties to ensure that the proper domains are whitelisted and that the required resources (e.g., scripts, images, stylesheets, etc.) from each whitelisted domain are included within policy definitions.
- SRI requires fingerprinting and validating third-party executable files that change frequently (sometimes multiple times per day). Implementing this technique for third-party JavaScript requires in-depth knowledge of every file loaded from a third-party domain. The personnel and man-hours required make this approach cost-prohibitive.

BUSINESS IMPACT

- CSP restricts scripts to only those originating from whitelisted sources, limiting the business's ability to rapidly integrate with and benefit from newly emerging third-party technologies. Additionally, extending trust outside of the business also introduces risk — for example, even whitelisted sources can be compromised as mentioned above. In addition, fourth parties that provide functionality will be blocked by CSP unless they are explicitly permitted by policy definition. This can erode the intended behavior, downgrade the visitor experience, and ultimately interfere with monetization objectives.
- SRI will block updates and improvements provided by third parties resulting in improper and/or suboptimal third-party functionality. This may impact the website's ability to collect analytics, deliver a consistent user experience, and monetize the website via multiple methods including ads.

CSP restricts scripts to only those originating from whitelisted sources, limiting the business's ability to rapidly integrate with and benefit from newly emerging third-party technologies.

THREAT BRIEF

WEBSITE MONITORING AND DETECTION

- **Inadequate Detection:** In many cases, this attack vector is hyper-targeted to a very small and specific sub-population of users, evading most website-focused detection approaches.
- **Not Scalable:** Website detection technologies are not designed to dynamically monitor every website session and are incapable of scaling to effectively address client-side attacks.
- **Alert Fatigue:** These approaches generate a tremendous amount of false positives, which can result in alert fatigue. The dynamic nature of JavaScript and the difficulty of baselining intended behavior impedes the ability to provide accurate reporting, making it difficult to prioritize anomalous events that require response and remediation.
- **Incident Response:** In all cases, these reactive, non-preventative technologies detect an event that has already had some impact before the detection was made. Such events will require investigation and remediation, and can result in operational disruption, cleanup, disclosure, regulatory response, and corrective action.
- **No Remediation:** Monitoring and detection services do not include remediation options.
- **Persistence:** The most troubling aspect is that detection technologies allow the threat to persist and the underlying flaw, which is related to unmanaged third-party connections, is not addressed.

Website monitoring and detection approaches generate a tremendous amount of false positives, which can result in alert fatigue.

WEB APPLICATION FIREWALL (WAF) AND FIREWALL

These technologies focus on traffic to the web server and do not cover the JavaScript being sent directly from remote servers to the client-side browser.

DAST/SAST/RASP

These methods are deployed on pre-production environments and will not cover scripts on a production site dynamically loaded by external servers.

SSL

In general, TLS/SSL and encrypted point-to-point technologies ensure that information is not compromised as it is communicated between a host serving content and the host providing it. If the host providing content is compromised, the in-flight protection provided by SSL will still be in place; however, it will only ensure that the malicious content is delivered successfully.

PENTESTING

Periodic or even continuous testing of web applications only evaluates the third-party JavaScript that is included as part of the webpage served to visitors. However, this JavaScript is simply the call that initiates the connection between the client-side browser and the third party's corresponding external server. This attack occurs during that third-party server JavaScript response made directly to the client-side browser.

RECENT ACCELERATION OF JAVASCRIPT ATTACKS AT MASS SCALE



THREAT BRIEF

PUBLICLY REPORTED ATTACKS

The following is a summary of the publicly reported attacks cited in this report:

TICKETMASTER ATTACK

A chatbot service used on the website of this major ticket broker was hacked, had its JavaScript modified, and was used to steal credit card information from users of the Ticketmaster's website. Further investigation showed this was part of the largest payment card theft in history, compromising multiple third-party vendors and affecting more than 800 online merchants over the course of three years.

DELTA AIRLINES AND BEST BUY ATTACKS

A third-party chat and support service was hacked and used to distribute malware to its client's users. This resulted in a massive credit card skimming attack on major enterprise online commerce sites including (but not limited to) Delta Airlines, Best Buy, and other large online retailers including Kmart and Sears.

EQUIFAX AND TRANSUNION ATTACKS

A third-party analytics tool used by two of the largest U.S. credit rating agencies was hacked and used to prompt a message to users, simulating a message from Adobe asking users to update their Flash plug-ins. Users who interacted with the message were infected by malware. This breach is a good example of how hard it is to detect this type of attack. Equifax was only weeks away from a very publicized breach and, with a security team on highest alert, they still were not able to prevent this attack from affecting their users.

PIZZA HUT ATTACK

A third-party analytics tool used by a major U.S. restaurant chain was hacked and used to access user-provided information on the webpage. The hacker accessed home and email addresses, as well as credit card information including expiration date and CVV.

WATERING HOLE MALWARE ATTACK ON THE EUROPEAN UNION (EU) PARLIAMENT

This attack illustrates how compromised third-party vendors can be leveraged to launch hyper-targeted attacks. An ad network operating on a news website frequented by Parliament members was breached and used to redirect users to a webpage, which distributed targeted malware directly to members of Parliament visiting the website. When deployed at small scale, attacks leveraging the flexibility of JavaScript to launch client-side attacks are particularly hard to detect. In many cases, these attacks can be implemented, sensitive data exfiltrated and all evidence of the infiltration subsequently removed, as the modified JavaScript is returned to its original state.

BANKING TROJANS AND RANSOMWARE DISTRIBUTED VIA 10,000 WEBSITES

A sophisticated hack illegitimately added an unauthorized third-party JavaScript ad network tool (Adsterra and/or its affiliates) to 10,000 websites. The campaign used malicious JavaScript hosted on the ad network servers to redirect users to the threat actor webpage. This page, in turn, distributed a variety of malware including banking Trojans, ransomware, and bots to visitors of over 10,000 websites.

RESPONDING TO A THIRD-PARTY JAVASCRIPT ATTACK

Forensic investigators can assist both website owners and third-party providers during third-party JavaScript breach investigations. The challenge when investigating these attacks for website owners is that the full attack occurs in the user's browser. Worse, many of these attacks utilize sophisticated targeting mechanisms that make detection and recreation nearly impossible. It is often difficult to tell where and how a website has been compromised.

This is where the Source Defense solution can be critical in aiding in an investigation. By quickly implementing Source Defense on a website, investigators have granular access to understand what is happening in the end user's browser. Source Defense is able to determine precisely what third parties are doing on the webpage, giving the investigator previously unavailable information necessary to confirm the specifics of an attack and provide recommendations for remediation.

Post-investigation, the Source Defense solution can continue to protect the website by giving the website owner control over third-party access and behavior, and preventing future attacks in real time.

ABOUT SOURCE DEFENSE

Source Defense provides an entirely new and unique solution to prevent Magecart-style browser session attacks originating via the website supply chain. Source Defense's real-time prevention isolates all 3rd party JavaScript from the webpage and leverages a fully automated and machine-learning assisted set of policies that control the access and permissions of all 3rd party tools operating on a website (including the 4th and 5th parties they chain-in). The Source Defense solution preserves the user experience, eliminates unnecessary latency introduced by 3rd party tools, and prevents stability issues caused by 3rd parties while ensuring 3rd parties may not be leveraged for malicious data extraction or website alteration.

This real-time prevention also unlocks the potential of digital channels and website marketing by empowering the use of technologies that provide enhanced analytics, competitive advantage through innovation and differentiation, customer retention, and customer conversion.

For a complimentary Risk Assessment & Attack Surface Map:

Info@sourcedefense.com

www.SourceDefense.com



source

DEFENSE

Source Defense provides an entirely new and unique solution to prevent Magecart-style browser session attacks originating via the website supply chain.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging CrowdStrike's world-class threat intelligence and next-generation endpoint protection platform, the CrowdStrike Services incident response (IR) team helps customers around the world identify, track and block attackers in near real time. This unique approach allows CrowdStrike to stop unauthorized access faster, so customers can resume normal operations sooner. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks and ultimately, prevent damage from cyberattacks.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

CrowdStrike Falcon protects customers against all cyber attack types, using sophisticated signatureless AI and indicator-of-attack (IOA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates 1 trillion security events a week from across the globe to immediately prevent and detect threats.

There's much more to the story of how Falcon has redefined endpoint protection, but there's only one thing to remember about CrowdStrike: We stop breaches.

EXPERIENCED A BREACH?

Call +1 855.276.9347

www.crowdstrike.com/services

