TEVORA™

source DEFENSE

2019 Threat Brief
Tevora and Source Defense Inc.

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

Threat Brief

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.

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

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 as it creates an uncontrolled and highly scalable attack surface.

The Universal Flaw and the Attack Surface

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

Third-party vendors leverage 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 are 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:

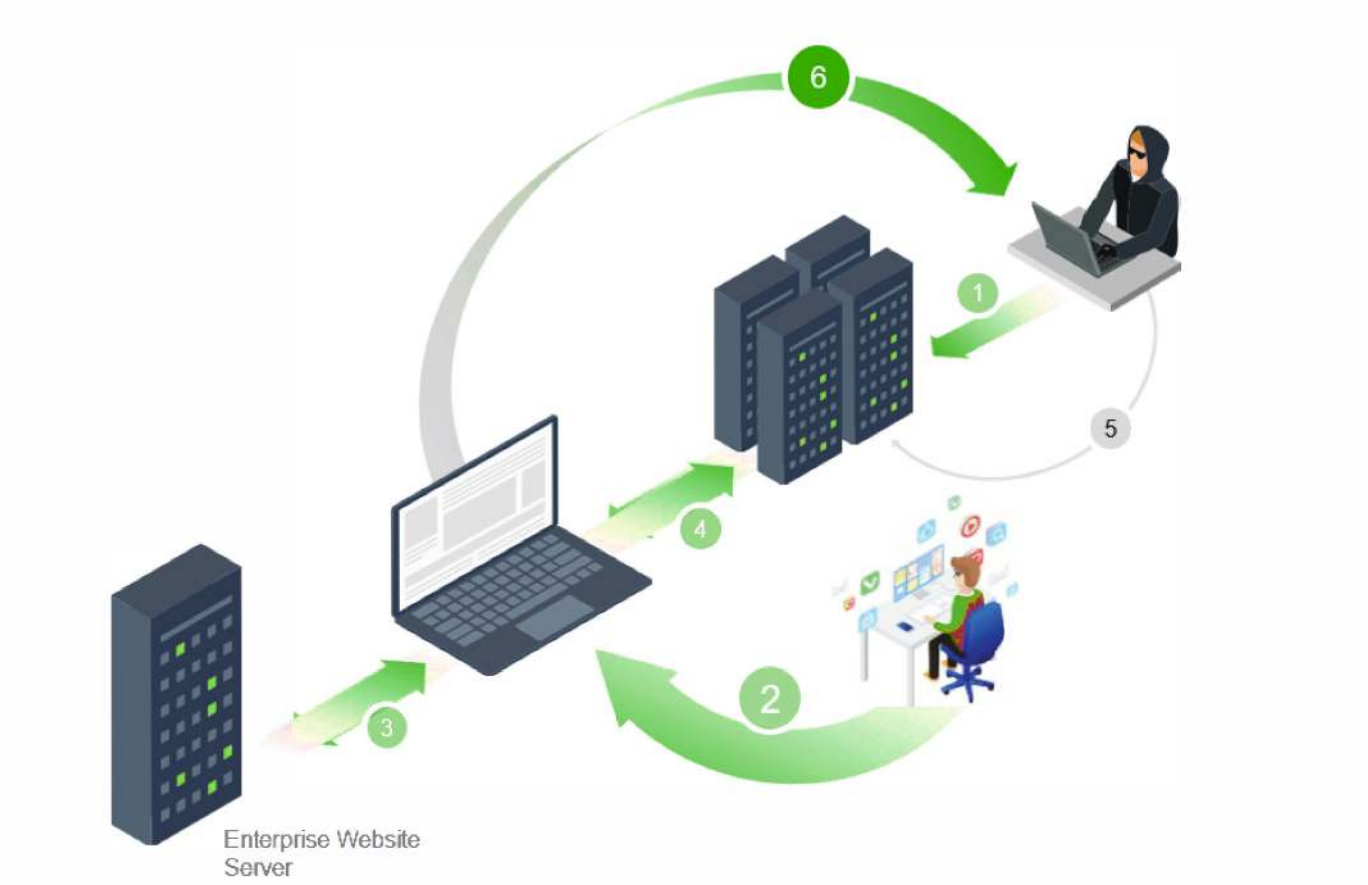
- Banking trojan, ransomware and malware distribution
- Cryptojacking
- Content defacement
- Session redirects (clickjacking)
- Phishing
- Highly Targeted Watering hole attacks
- Malvertising

Supply Chain's Weakest Link and Scalability of Attacks

The uncontrolled access to the webpage and all data transmitted during the user session provides 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 websites and in turn victimize huge user populations during each campaign.

Client-Side Browser Session Attack via Modified 3rd Party Javascript



How a Website Supply Chain Attack Unfolds

1. Attacker compromises a 3rd party vendor & modifies the JavaScript to include 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 3rd party server.
5. The modified JavaScript from the compromised 3rd party is sent directly to the user's browser , requests content from the 3rd party server.
6. The malicious code executes in the user's browser session. In cases of 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 Sub-Resource 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, style sheets, 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.

- 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.

Website Monitoring and Detection

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

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.

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.

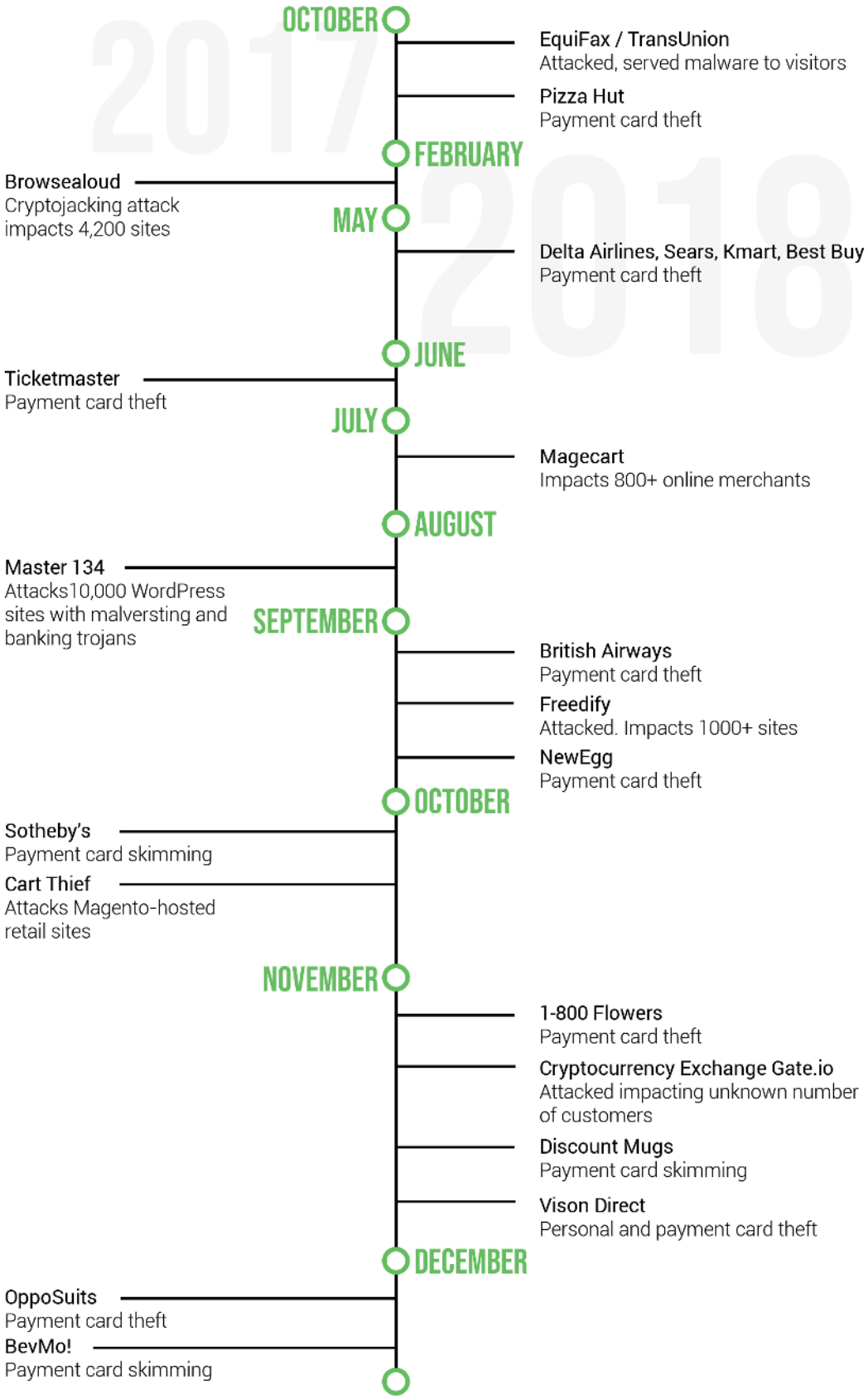
SSL

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



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

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 CW.

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.

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

About Tevora

Founded in 2003, Tevora is a specialized management consultancy focused on cybersecurity, risk and compliance services. Based in Irvine, CA, our experienced consultants are devoted to supporting the CISO in protecting their organization's digital assets. We make it our responsibility to ensure the CISO has the tools and guidance they need to build their departments so they can prevent and respond to daily threats.

Our expert advisors take the time to learn about each organization's unique pressures and challenges so we can help identify and execute the best solutions for each case. We take a hands-on approach to each new partnership and year after year apply our cumulative learnings to continually strengthen the company's digital defenses.

Tevora offers a full range of services designed to anticipate and meet the changing needs of your enterprise

Compliance
We assess, audit, and certify compliance across a comprehensive portfolio of cybersecurity standards.

Enterprise Risk Management
We speak the language of cyber risk and translate it into business impact - giving you rich data to make meaningful decisions.

Data Privacy
We help you craft strategies and plans that work; allowing you to meet the growing demands of domestic and international privacy regulations.

Security Solutions
We help you plan, implement, and integrate cybersecurity products that reduce your risk profile: on-prem, mobile, and in the cloud.

Threat Management
We test your systems, processes, and security with a world class team of certified hackers and security researchers.

Incident Response
We are a team of first responders, threat hunters, and incident containment specialists working with the latest tools and techniques; ready to serve when your business needs it most.