source DEFENSE

SOURCE DEFENSE

THE RISK OF CLIENT-SIDE ATTACKS IN **THE E-COMMERCE INDUSTRY**

www.sourcedefense.com

| info@sourcedefense.com

TABLE OF CONTENTS:

The Risk of Client-Side Attacks in **the eCommerce Industry**

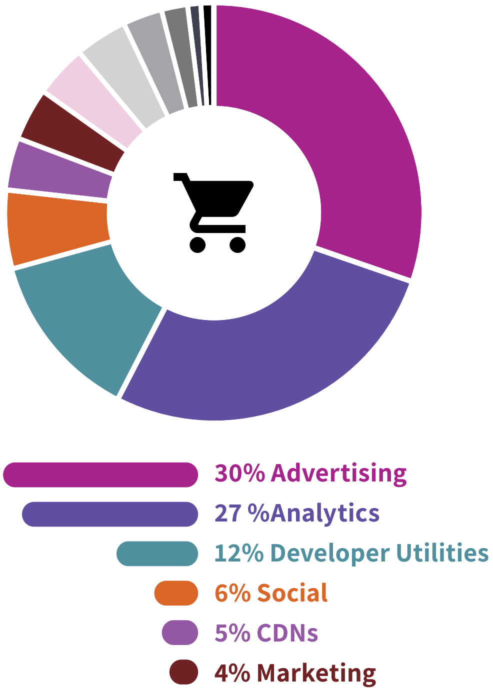
INTRODUCTION

eCommerce websites are experiencing a surge in cyberattacks. They hold a lot of customer data, which makes them a prime target for attackers. Not only are cyberattacks on the rise, but the hacks are now more lucrative than ever for cybercriminals. This is due to the fact that stealing physical credit card data is much harder today than ever before.

Online competition is fierce, making customer experience and maintaining a feature-rich website critical success factors. Online retailers rely on an ever-expanding ecosystem of 3rd party suppliers to enhance and personalize user customer experience, increase engagement, monitor their customers' journey and behaviors, monitor monetization and so on.

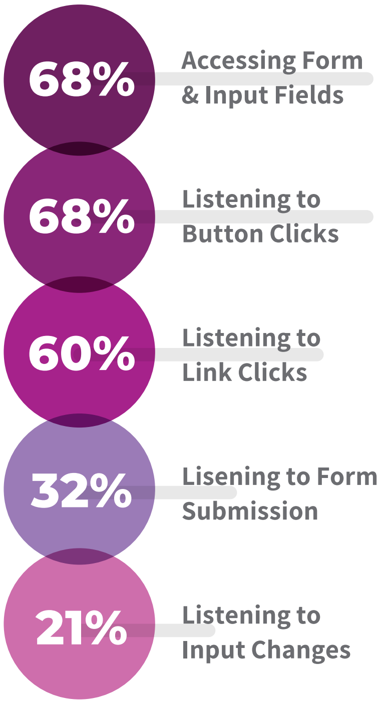
The average eCommerce website uses 40-60 3rd party tools, with retailers saying they plan to add an average of 3-5 new 3rd party technologies to their sites annually.

Usage in eCommerce industry



3rd Party website enhancement tools introduce a universal client-side vulnerability that provides threat actors with unmanaged access to critical business and customer data.

Third-party scripts action statistics



Alongside the benefits of these 3rd party tools, they also provide attackers with an attractive gateway for malicious activity (aka Formjacking, Magecart, JS Skimming). Unfortunately, this means that the more such tools are used, the more risks eCommerce websites take upon themselves. Instead of hacking the eCommerce websites themselves, hackers often attack the 3rd party plugins and use their Javascript to hitchhike the eCommerce website. Checking the security perimeter of an eCommerce site is just not enough. A website is affected by the security perimeter of all of the 3rd party tools it uses. Moreover, it has no control over what's happening outside the 3rd party circle: there are 4th party circles, 5th party circles and so on, that most website owners are not even aware of. Despite this, eCommerce sites have exponentially increased their dependency on 3rd, 4th and 5th party technologies, sharing confidential and sensitive information with a staggering 583 outside parties on average.

ATTACK VECTOR OVERVIEW

Web sites rely heavily on 3rd party vendors to provide functionality and behavior expected of visitors. 3rd parties provide analytics, user behavior analysis, customer engagement, display advertising and, in general, monetization of a website's content and brand. Although 3rd parties provide immense value, they also introduce a broad security risk to the visitor of an organization's web site.

JavaScript, the programming language which enables interactivity on the web and facilitates the functionality of these 3rd party tools has very poor inherent security controls. In fact, it would be fair to say that there are no controls available at all. Every line of JavaScript which is executed by a web browser has the same level of access, permission to run and interaction with the user that any other line does. The consequence of this is that there is no way to control the behavior of any particular script within any given web session using standards-based approaches.

Each script in a traditional computer programming context may be thought of as its own application running within the browser. Unlike traditional applications, however, each piece of JavaScript is accessed in real-time as the visitor requests a web page. There is no concept of compilation, bundling or package delivery within the browser -- each script arrives fresh on each pageview with whatever behavior it contains at that particular moment.

The combination of these factors leads to a serious security flaw, namely, that 3rd parties which drive monetization can and do introduce unintended behavior into the visitor experience. And, if a third party is compromised, that unintended behavior may take the form of malicious exploitation: credit-card skimming, defacement, PII disclosure, etc.

In essence, an enterprise hosting content through a web server is extending unlimited trust to each 3rd party as it relates to the visitor's experience. In the context of modern cybersecurity, this is untenable from the perspective of due diligence, reputation management and compliance.

eCommerce Industry Vulnerabilities

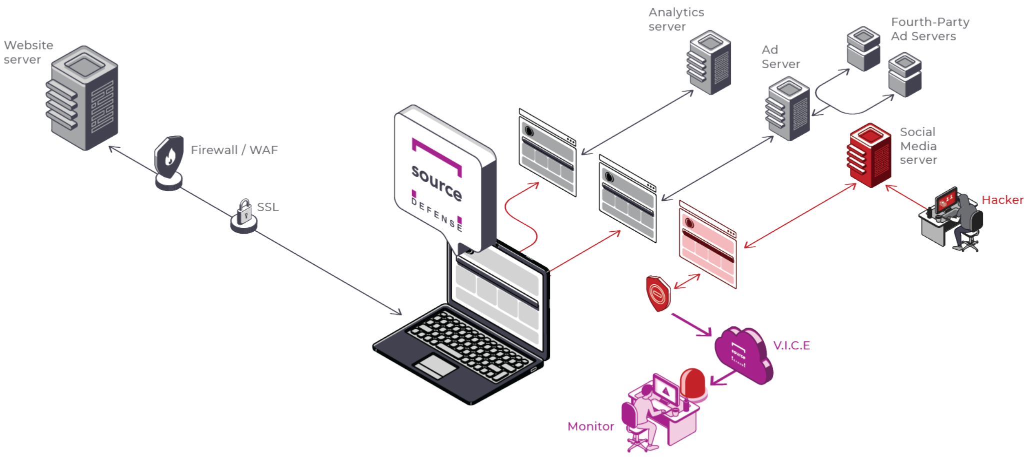
- Gift Card Abuse
- Slowdowns
- Card Cracking
- Visibilty and Metrics
- Unauthorized Scanners
- Formjacking

CLIENT-SIDE ATTACKS

Hundreds of external 3rd party tools (and the hackers that exploit them) are allowed nearly unlimited access to nearly 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.

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. 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 your website, new features and code may be pushed into the remotely hosted 3rd party JavaScript server at any time. JavaScript gets the same privileges since this is how browsers works, the JavaScript is being rendered in the client-side no matter where did it come from. 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 the existing security infrastructure and goes beyond its control without dynamic and continuous per-session monitoring of website activity. You are actually facing an impossible task!

Diagram of Client-Side Attack



Web security solutions including WAFs and firewalls are designed to deliver communication between the browser and the server by filtering requests. 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 Application 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. These technologies can test your own code but CANNOT test the code in the third-party remote server. 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 if only "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 EVOLUTION OF MAGECART

Magecart is a group of unscrupulous hackers who make up a consortium in order to steal information online from customers payments cards. They target shopping carts from systems like Magento, where a third-party piece of software is compromised from a systems integrator, or a VAR or an industrial process can be infected without being picked up by IT. This is known as a supply chain attack.

An online shopping cart is an extremely valuable target to a hacker due to the fact that all the payment details from customer's cards have already been collected and are sat waiting in one place for a hacker to come along with their malicious malware and take it right out of the cart. Virtually all eCommerce websites do not thoroughly vet the code which is used by these third- parties, therefore making the job of a hacker quite simple using their sophisticated malware.

Magecart is becoming more and more prolific since it's inception 5 years ago. It was featured in Wired Magazine on their list of Most Dangerous People On The Internet in 2018 following an analysis by RisqIQ which showed that Magecart was creating hourly alerts where websites were compromised by its skimmer code.

THE MAJOR IMPLICATIONS OF ATTACKS

The major implications of such attacks include:

Compliance: An eCommerce business is required to meet certain standards to be considered "in compliance," and fines can be levied against a business or its owner if it does not comply with them.

Financial solvency: If breached, a business has a whole host of other problems that will impact its bottom line. It may have to pay for a forensic investigation, data recovery services, credit monitoring for impacted parties, and more.

Customer trust: Customers put a lot of trust in the online retailers they shop with, providing them with personal data and sensitive payment information with every purchase. Earning customers' trust is critical to a long-lasting relationship, and once lost, earning it back is a very difficult task. That's why breaches can have a big impact on long term customer loyalty and retention: 64% of consumers say that they are **unlikely to do business**[1] again with a company from which their personal data was stolen.

Damage to brand reputation: Reputation is a fragile thing. It takes years to build, and moments to destroy. When a breach occurs, the target audience feels betrayed and angry. The initial cost can be seen in the form of lawsuits, but there is a far greater cost that can last for years. Furthermore, this can negatively affect the business reputation of each person on the executive team and affect their future endeavors. Stocks drop, the team is affected, and revenues plummet. Unlike a fine, which can be paid and forgotten, reputation cannot be fixed so easily.

[1] https://safenet.gemalto.com/resources/data-protection/customer-loyalty-data-breaches-infographic/

SUMMARY

3rd party risk presents, in many ways, a novel challenge to traditional enterprise security strategy. Because of the combination of clear business necessity, poor security architecture and rapidly accelerating exploitation, the attack vector presented by 3rd party JavaScript within the browser requires a unique approach and careful consideration from any organization providing content to visitors.

Standards-based approaches towards mitigating this attack vector are well-engineered and logically sound, however, they fail in the sense that they take the perspective of a web application developer or maintainer. In other words, technologies like CSP and SRI work well in the context of a self-developed application: if you know everything about how your application works then surely you can know what other code it incorporates and how that code functions. You may even deploy technologies like dynamic application testing or application monitoring to further secure that application. This, however, is not the challenge presented by 3rd party JavaScript.

The landscape of a contemporary customer-facing website is wholly unlike an internally developed web application. The participants contributing code in an average visitor's browsing session number in the dozens, if not more. As such, it is impossible for an enterprise to know, let alone control, the entirety of the attack surface.

In summary, it may be possible to partially address the risk presented by 3rd party vendors through traditional approaches, but only at great cost to the organization and with limited effectiveness in terms of mitigation. Unfortunately, traditional security technologies and techniques are proving to be an insufficient response to this emergent and accelerating threat.

Source Defense

Source Defense is the market leader for Client-Side and End-User attack prevention. Traditional security methods focus on website protection and with new attacks such as Magecart and Formjacking, they have found ways to penetrate websites before ever getting to your WAF.

With their patented VICE platform, Source Defense protect web pages from vulnerabilities in third-party scripts. Source Defense's solution isolates those scripts from the web page and allows them to read and write according to a given permission either defined by Source Defense's recommended standards, or specific company policies.

Source Defense extends the traditional security perimeter to protect your customers and fortify your security stack in real-time.