Findings From
the Source Defense
Research Lab

source
DEFENSE

Website Trust & Client-side Security Report 2021

Continuing Client-side Security Intelligence

Website Trust & Client-side Security Report 2021

Continuing Client-side Security Intelligence

eCommerce customers are justifiably worried about security when filling out online forms. They expect that organizations will protect their personal information against attacks, and many would never interact with a business again, either online or in-person, if their personal data were stolen.

Our team at Source Defense conducted a survey this month to gauge consumer thoughts about website trust. The key takeaways from the **Source Defense 2021 Website Trust Survey** performed on a wide audience, emphasize that companies who ask customers to complete online forms are responsible for protecting the information - and brand reputation and loyalty is at stake.

According to the survey, an overwhelming majority of consumers have real concerns about filling out online forms, with **93%** of respondents indicating that they were concerned about data security when filling out forms.

Consumers do it anyway because it’s considered part of the risk they accept in order to reap the rewards and convenience of online shopping.

Survey Finding

93% were concerned with security when filling out forms

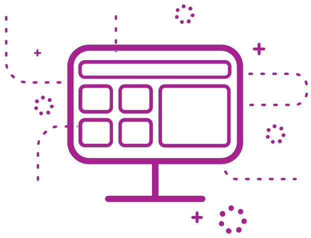
According to the survey

47%

47% of respondents fill out online forms on a weekly or more regular basis

95%

95% of respondents were willing to provide information online when asked to do so



That being said, the devastation of potential form related attacks impacts the majority of people surveyed.

But customers also demand that organizations protect their data -- **91%** of respondents said that companies who ask customers to complete online forms are responsible for protecting their personal information.

And the consequences of failing to protect customer data are severe. Half of respondents (49%) said they would cut ties with that organization and never do business with them again if there were a data breach. Another **28%** said they would stop shopping online and would only make purchases or share data with that company in-person or on the phone.

One of the more alarming findings from the survey is that customers were not familiar with the methods by which attackers steal their credit card information -- **82% of survey respondents indicated they had never heard of terms like formjacking or Magecart.**

Online businesses apparently are not that familiar with client-side attacks either, judging by the ongoing ability of cybercriminals to conduct these types of client-side attacks that seem to slip under the radar of traditional web security defenses.

Survey Finding

91% of companies who ask customers to complete online forms are responsible for protecting their personal

Brand Loyalty at Risk!
28% said they would stop shopping online and only make purchases in person or on the phone information

Describing the Potential Threats

Client-side Attacks Refer to any Attack Utilizing a Web Browser

New online attack occurs every 39 seconds

In the browser, client-side processes are almost always written in JavaScript. According to our team's latest intelligence, there are over 1.7 billion public-facing websites in the world and JavaScript is used on 95% of them.

In order to achieve better performance and experience for end-users in the era of modern web applications, as well as reduce the load from server-side processing, the core logic has shifted from server-side processing to the browser and JavaScript libraries. For example, our team found that over an eight year period, frontend JavaScript code has grown in size over 347% for desktop and over 593% for mobile and keeps growing. JavaScript can be used to interact with the server by performing background requests.

Client-side attacks have been around for a while, but they remain a blind spot for many organizations. Every client-side web attack is different, but they all rely on the fact that the attackers are able to gain access to the browser of the customer who is visiting the website, and they are able to steal the customer's payment details, including credit card information, in real time.

These attacks are rapidly accelerating and they all exploit the trust relationship between a user and the websites they visit. **In fact, according to our research, a new online attack occurs every 39 seconds.** Most client-side attacks are a consequence of a more sophisticated attack chain that eventually affects the visitors of the website.

An online shopping cart is an extremely valuable target to a hacker. All of the payment details from customers' cards have already been collected and are waiting in one place for a hacker to come along with their 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.

Threat Cheat Sheet

Formjacking: The term formjacking got its name because initial attacks were identified by breached forms which caused data loss and stolen credentials on a website. Formjacking occurs when online criminals hack into a website to gain control over its entry point where sensitive information is provided. This type of hack is most commonly associated with cybercriminals who seek to steal credit card details and other forms of payment methods, as well as personal information such as phone numbers and home addresses that could lead to identity theft.

Magecart: Magecart refers to organized criminal groups that steal information from customers' payment cards. They target shopping carts from systems like Magento, which a third-party piece of code, compromised from a systems integrator, can be infected without IT departments knowing about it. This is also known as a supply chain attack.

Cross-site scripting: Cross-site scripting, also known as an XSS attack, involves a malicious script that hackers insert into otherwise benign and trusted websites that might have a flawed and vulnerable validation process. The script, which in many cases infiltrates a highly trusted and heavily used website, convinces innocent end users that the content they are watching or consuming belongs to the main site. XSS attackers are able to make changes to the website and even modify its HTML page information. The XSS malicious script allows hackers to infiltrate the users' cookies data, hijack sessions, redirect links and access personal information.

Spoofing or phishing: Spoofing in this context is when someone or something pretends to be something else in an attempt to gain user confidence, get access to systems, steal data, steal money or spread malware. Spoofing attacks come in many forms. They can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls or re-direct traffic to conduct a denial-of-service attack. Spoofing is often the way a hacker gains access in order to execute a larger cyberattack.

Website spoofing: Spoofing is the act of creating a fake website with the intention of misleading the reader. JavaScript can be used to route web pages and information through the attacker's computer, which impersonates the destination web server.

New Client-side Attacks Put Businesses on the Defensive

Examples of Third-party Scripts

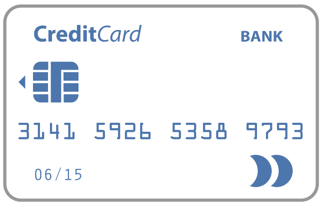
- Social sharing buttons
- Advertising
- Video player embeds
- Analytics & metrics scripts
- A/B testing scripts for experiments

While formjacking is not a new technique, it has become more lucrative and effective in the last few years because of a trend toward web application decentralization. Today, web applications use dozens of third-party services that run in the client browser to deliver mission critical business functions, including payment card processing. Cybercriminals are targeting these third-party services with injection attacks whose malicious payload runs on the client browser. The recent rise of formjacking indicates that any organization accepting payment card information over the web is going to have shopping carts targeted, regardless of sector.

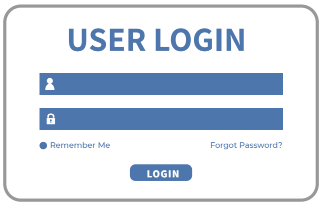
Third-party Scripts Actions

Most Affected Sensitive Pages

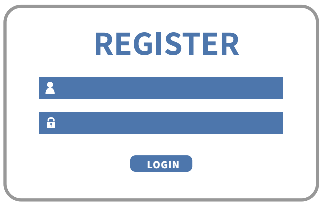
Payment Collection Pages



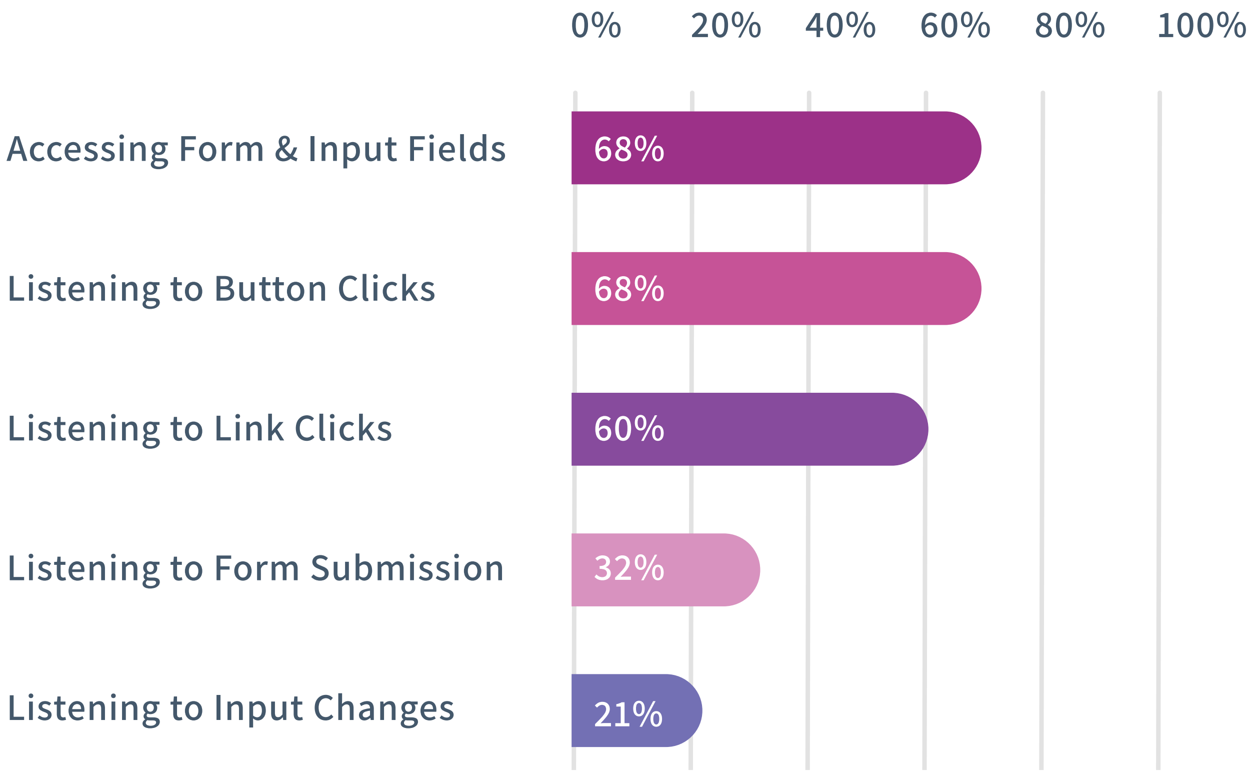
Login/Credential Capture Pages



Account Registratior Pages



Third-party Script Actions Statistics



Formjacking Accounts for 87% of Web Breaches

Formjacking accounts for 87% of web breaches and 17% of total breaches, according to the F5 Labs Application Protection **Report**. The number of attacks doubled early in the pandemic as attackers took advantage of the surge in eCommerce. And the **latest estimate from RapidSpike** is that there are nearly 5,000 formjacking attacks each month. According to **Gemini Advisory's tally**, 570 web sites have been compromised by one Magecart group (Group 8) since 2017.

In September of 2020, hackers compromised more than 1,900 retailers running the Magento software to steal payment details of tens of thousands of customers, making it the largest known Magecart attack ever. Even more exasperating, it was discovered that the stores were running Magento version 1, which was announced as end-of-life three months earlier.

While attackers do claim high-profile victims, such as Macy's and British Airways, researchers warn that 'mom and pop' shops are easy targets because they don't have the sophisticated security defenses of a larger organization. In many cases, they might not even know that credit card skimmers even exist.

Magecart groups are continually improving the methods; they're getting better at hiding their code from detection, better at covering their exfiltration tracks, and coming up with more devious and clever attacks.

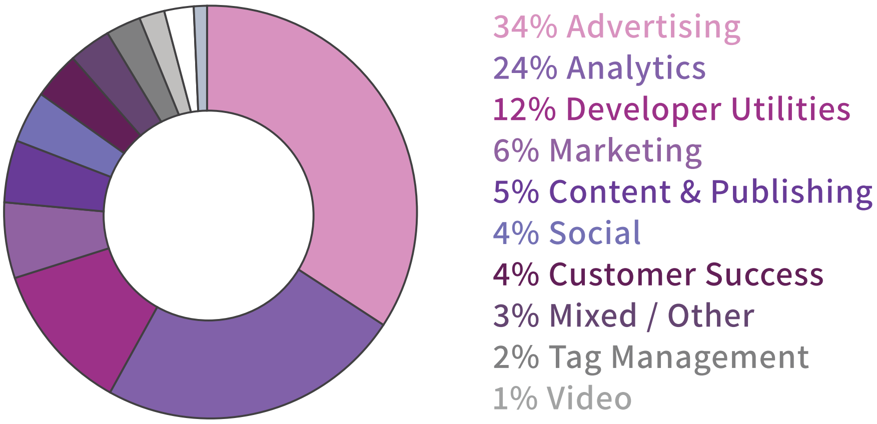
Researchers at Visa recently uncovered a new type of JavaScript skimmer that infected the online checkout pages on at least 17 eCommerce websites to steal payment card data. The skimmer can remove itself from the HTML of a compromised payment website after it executes, enabling it to avoid security detection.

The list of organizations that have been hit with Magecart attacks runs the gamut from the National Basketball Hall of Fame, sportswear brand Fila, gunmaker Smith & Wesson, Warner Music Group, even Australian bushfire donation sites. In other words, no organization is immune.

Why Everyone Should Be Concerned:

Top Industry Affected by 3rd Party Breaches in 2020

1. eCommerce/ Online Retailers



The average consumer today is likely to be doing eCommerce or conducting some manner of online communication involving filling out forms with so many organizations it's probably hard to keep track. And the pandemic has pushed people into conducting more business online rather than in-person.

Examples include online banking and financial services, communicating with healthcare providers, interacting with local, state and federal governments, even ordering a pizza delivery. In these scenarios, a client-side attack could expose credit card information, financial information, medical records or other personal data that could lead to identity theft.

On the other side of the equation, a client-side breach can harm the business in multiple ways, including direct and indirect costs.

Direct Costs of Magecart-style Attacks

Fines: Once a data breach is reported, companies are likely to face fines depending on their location, the location of their target audience and the regulation they must comply with. According to the GDPR that took effect in 2018, a company can be fined up to €20 million or 4% of its global revenue the previous year. Fines can increase if a breach is not announced quickly; a company is likely to incur legal fees in order to handle lawsuits, communication with government organizations, banks, etc. In 2013, Target's data breach affected 41 million consumers. In the years that followed, Target paid over $40 million in legal fees.

Lawsuits: Lawsuits and class-action lawsuits are common following a breach. Legal fees aside, companies often incur additional fees in settlements as a result. That same Target breach resulted in approximately $68.5 million in settlements alone. This doesn't include the $172 million the company paid as part of their settlement with financial institutions.

Hiring more security professionals: Once a data breach is discovered, it needs to be handled by cybersecurity experts. This usually involves hiring additional personnel to investigate the breach, stop it and prevent it from happening in the future.

Hiring public relations firms: PR firms are often hired after a breach to handle the breach aftermath that many times includes a brand reputation crisis. These costs could be enough to bankrupt a company on their own, but they're just the tip of the iceberg. The bigger and more significant costs are indirect, hidden and in many companies go completely under the radar, until it's too late.

Indirect Costs of Magecart-style Attacks

Once a breach occurs, it activates a long chain of events that happen in the background. While you're busy hiring lawyers and dealing with lawsuits, a lot more is going on. Here are a few of the indirect and hidden costs you should consider when evaluating the cost of a data breach.

Reputation Damage:

As we saw in the survey, when a breach occurs, everyone blames the business, and that includes customers, potential customers, supply chain partners and employees. It can negatively affect the personal business reputation of the executive team and affect their own 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. In many cases, the damage is irreparable.

Loss of customers:

Organizations invest a lot of resources to expand their customer base, and even more to retain and upsell to existing customers. As the survey results indicated, a data breach will drive customers to a competitor who promises to do a better job protecting their credit card information, address or other sensitive data. A breach often results in an instant drop in existing customers. It also affects the influx of new customers, which is more difficult to measure. Companies often lower prices or offer additional bonus services to entice customers to choose them. The bottom line is a drop in revenue.

Internal Chaos:

Once a breach is detected, organizations need to alert everyone in the company and try to maintain calm and keep everyone focused on their jobs. This isn't easy to accomplish. Employees start to worry about their jobs and their own reputation. This affects the work environment and everyone's productivity. As soon as the breach becomes public knowledge, there will be an influx of emails, calls, letters and support tickets from concerned customers. Existing employees need to be trained on how to handle calls, speak to customers and communicate about the breach. Existing staff may not be enough to handle this efficiently, which leads to additional costs of hiring and onboarding. Employees start working in "emergency mode," which means that roles can change, usually at the expense of the ongoing business.

Development Delays:

Companies are usually working on new developments, features and upgrades to enhance their products and offerings and keep up with competitors. Dealing with a breach halts this activity in most cases, which leads to significant launch delays.

What Organizations Can Do:

Guidance to Ensure Organizations are Protected from Client-side Security Threats

1 Implement a control system that will identify and control all 3rd party JavaScript on your webpages. It is critical to control the access of all 3rd party JavaScript on your webpages; therefore, making sure the control system is able to identify and control each external JavaScript is crucial to the process.

2 Make sure Nth party JavaScript are either blocked or managed by the system. Many 3rd party JavaScript providers will work in cooperation with other providers to increase their efficiency; these, as their partners have the same unlimited DOM access and therefore should either be blocked or managed in the same manner as a 3rd party.

3 Make sure “whitelisted” 3rd party cannot bypass the security applied policies. Some access policy platforms will use easily bypassed methods to limit 3rd party access such as CSP/SRI or JavaScript Proxying, these are easily bypassed and are considered ineffective.

4 Ensure security controls remain effective even if 3rd party resources change 3rd party resources change rapidly and are often generated dynamically.

5 Implement security controls which protect the entire duration of a visitor’s session Auditing and inventorying known 3rd party resources is ineffective as additional resources can be called into a session at any time, from moments after page load to minutes or even hours later.

6 Ensure controls implemented do not themselves introduce additional vulnerability Security controls introduced to address 3rd party risk may inherently present some risk themselves.

About
Source Defense

Source Defense is the market leader in Client-side Security for websites, providing real-time threat detection, protection and prevention of vulnerabilities originating in JavaScript. The Source Defense patented Website Client-side Security Platform offers the most comprehensive & complete solution addressing threats and risks coming from the increased usage of JavaScript, libraries and open source in websites today.

The ADMIN management console, VICE sandboxing and WiPP data shield offerings utilize patented technology and are deployed by leading Fortune 500 enterprises in the Financial, Retail and Healthcare markets. Headquartered in Israel, with branches across the US and a strong community of global valuable partnerships, Source Defense is the most innovative, reliable and trusted partner in the fight against client-side attacks.