ENSIGHTEN

Ensighten eGuide

15-Minute Guide to Client-Side Online Skimming Protection

Online skimming protection is a critical component of a well-implemented website security strategy

June 2020

Introduction

Website skimming protection secures a website against a new and growing range of malicious attacks which target an organization's online presence at the most vulnerable point, at render time, in the user's browser.

Ultimately, skimming protection is designed to stop the theft of sensitive data, such as credit card numbers, social security numbers, home addresses and more. Although not as well-known as attacks like SQL (Structured Query Language) injection or distributed denial of service attacks, criminal gangs such as Magecart have successfully stolen millions of credit card numbers from some of the largest retailers, including Macy's, TicketMaster, Forbes, Nutribullet and more.

Skimming attacks are not just about stealing PII. Numerous researchers and even government agencies have published documentation proposing that website skimming has been used to steal user credentials to be later used for gaining access to an organization's infrastructure.

What you need to know about online skimming

What is website skimming?

Website skimming is an attack method designed to steal user data by injecting malicious JavaScript into a web page, often by compromising a third-party technology that is used by a site developer. Skimming incidents have increased dramatically over the past few years and a number of significant brands have experienced breaches, resulting in millions of consumers having their personal information stolen.

How a skimming attack happens

For a skimming attack to be successful cybercriminals will inject malware into a website. This malware can be injected into a website directly if an exploitable hole exists, or the attackers can target one of many third-party JavaScript libraries which developers and marketers utilize.

Once injected, the malware is delivered to a user's browser along with the organization's own website code where it will run and watch for data being entered by users; data such as names, addresses and credit card numbers. The malicious code will take a copy of it when such data is entered and relay the data to a server owned by the attackers to be later sold on the dark web.

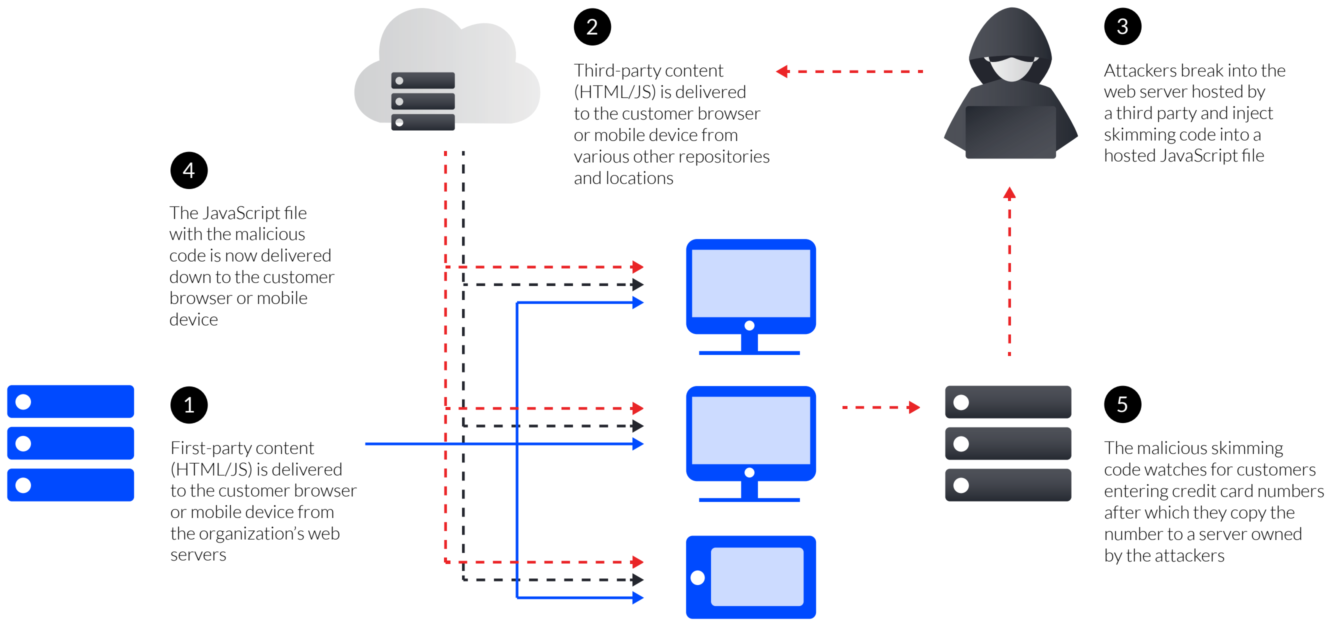
> *Any business accepting online payments on their website is at risk of an eskimming attack. This threat has impacted ecommerce companies in the retail, entertainment and travel industries as well as utility companies and third-party vendors.*
>
> — Unites States Computer Emergency Readiness Team (US-CERT)

Prerequisites for a successful attack

While web skimming attacks vary greatly in their approaches, they still revolve around a basic principle of exfiltrating user data from a website when the site is being rendered by a user's browser. In order for an attack to take place, there needs to be two things possible:

- An attacker needs to be able to inject malicious code either directly into a website or into one of the third-party components in use
- The malicious code when running within a user's browser needs to be able to send the data it captures to a remote network location

How a web skimming attack happens



1 First-party content (HTML/JS) is delivered to the customer browser or mobile device from the organization's web servers

2 Third-party content (HTML/JS) is delivered to the customer browser or mobile device from various other repositories and locations

3 Attackers break into the web server hosted by a third party and inject skimming code into a hosted JavaScript file

4 The JavaScript file with the malicious code is now delivered down to the customer browser or mobile device

5 The malicious skimming code watches for customers entering credit card numbers after which they copy the number to a server owned by the attackers

Protection and prevention

There are two main requirements to prevent and protect against website skimming: strong security at the origin to *prevent* the introduction of malicious code and strong security at the point of render to *protect* against the actions of code injection.

Most organizations have put technologies and policies in place to address the first aspect. But with the common use of third-party tags within website code and a myriad of plugins and extensions, the browser remains a substantially large attack surface.

Online skimming protection operates at the website code level, monitoring and filtering the way in which JavaScript interacts with a web page and any data entered into it to prevent malicious actions such as data theft, cryptomining, ad injection and more.

⚠

Any site which allows user to enter sensitive or personal information is a target for web skimming attacks

Key benefits of online skimming protection

Any site which allows users to enter sensitive or personal information is a target for website skimming and protecting against such attacks is essential for organizations of all sizes.

Fraud prevention

Most organizations learn they have been impacted by a website skimming attack when a financial organization contacts them following the discovery of fraudulent charges affecting their customers. Online fraud is a concerning problem leading to substantial financial implications, higher business insurance premiums and consumer worry and stress.

Businesses have a legal but also moral duty to protect their customers' information to the best of their ability and to strive to prevent fraud resulting from the usage of their online property.

Brand protection

Data theft does not just affect a business' customers but also has a significant negative impact on the organization's brand. With both legal disclosure requirements and vast availability of public forums through social networking, breaches are well publicized and often heavily litigated.

When an organization loses their customers' data, customer trust and loyalty to their brand decreases, resulting in direct impact to the bottom line. In an ever-competitive marketplace, it takes a short time to lose a customer's confidence and a lifetime to regain it.

81% ***of consumers would stop engaging with a brand online if they experienced a data breach***

Compliance protection

An increasing number of privacy-focused laws are putting emphasis on data protection requirements and calling out malicious data loss. The CCPA and Europe's GDPR allow consumers to take action when their data has been stolen, resulting in substantial penalties for the organizations involved.

With businesses having a legal requirement to safeguard their customers' data, website skimming protection helps them prevent data theft beyond their perimeter, where the data is most vulnerable but where they still need to protect it.

Increased customer confidence

As online skimming attacks increase, so does the public awareness of them – and just like customers expect to see SSL (Secure Sockets Layer) while shopping, they will soon expect to see skimming protection too. Online checkouts contain numerous logos today, demonstrating a focus on security which in turn results in an increased customer confidence.

Customers also need protecting from themselves with an abundance of malware from viruses to malicious browser plugins looking to steal their data. By ensuring their interaction with a business' website is secure, customers continue to have the confidence in the organization.

The three types of website skimming protection

There are generally three approaches to provide protection against skimming attacks:

Edge protection

Many content delivery networks offer the ability to scan both incoming and outgoing traffic for anomalies or malicious content, either alerting when discovered or outright blocking. These solutions are effective against already-known attack methods or specific malware signatures which have been obtained through research or other sources.

The biggest challenge that edge protection faces is the rapid evolution of website skimming, both in the malware used and the attack methodologies. Over the past couple of years, attacks have become complex – often obfuscated and hidden and exceptionally creative. As one method is discovered and added to an edge protection solution, a new one emerges.

Website skimming attack software is also readily available through the dark web, creating unique malware not contained in any known databases in seconds. This means that solutions which rely on databases of known bad content are essentially rendered mute in these scenarios.

The biggest challenge that edge protection faces is the rapid evolution of website skimming, both in the malware used and the attack methods

Browser security controls

Modern browsers have inbuilt security capabilities, including Content Security Policy (CSP) and Sub Resource Integrity (SRI), which are designed to limit or prevent the impact of rogue and malicious code. For sites with minimal changes or few to no third-party technologies, these measures are effective at preventing website skimming.

The challenge with this approach is that the management burden is often directly associated with the website complexity and for most modern ecommerce websites, usage of the controls is impractical.

Some solutions look to combine edge protection with browser security controls by dynamically setting page policies or applying resource hashing, for example when the page is delivered to a user. While certainly more effective than the standard application of browser controls, these approaches still rely on a fundamental knowledge of the existing threat landscape and are often defeated with new attack techniques.

Solutions which rely on browser security controls find themselves at the mercy of the browser vendor with respect to updates and being able to respond to threats

Solutions which rely on being able to configure browser security controls find themselves at the mercy of the browser vendor with respect to updates and being able to respond to threats. Consider a flaw being discovered in the security component of a popular browser; the security vendor is reliant upon not only the browser vendor fixing the issue quickly, but also users then updating to the new version before an organization can effectively be protected against skimming attacks.

Client-side enforcement

Client-side security approaches are relatively new when it comes to protecting websites, but similar techniques have been used in areas such as application performance monitoring (APM). Client-side enforcement works by including additional code alongside the normal website code which is designed to protect the website as it is being rendered within the browser.

With client-side enforcement, a JavaScript library or JavaScript code is included within a website, normally at the top of each page so that it gets loaded first. Once the code is processed by the browser, it *shims* certain functions, such as those for reading or writing to form fields, so it can control who or what can use them.

When implemented correctly, client-side enforcement will prevent 100 percent of online skimming attacks while having an unnoticeable impact on perfomance

The technique is similar to that used by APM technologies which often hook into network functionality so they can measure how long certain requests take – although, newer browsers now expose this data, making this easier. The challenge with this approach is that if it is not done correctly or is applied to the wrong parts of a website, then it will have a negative impact on performance.

Client-side enforcement is the most secure method of protecting a website from client-side attacks but the technology used must be battle-tested and mature. When implemented correctly, client-side enforcement will prevent 100 percent of online skimming attacks while having an unnoticeable impact on performance.

Client-side enforcement – choosing the most effective option

If you have decided to look at utilizing client-side enforcement, it is important to ensure that the solution you adopt takes the right approach – bad implementations can lead to poor website performance.

DOM element control

Some client-side approaches look to control data access at the document element level, for example intercepting a read operation on a specific text field. These approaches normally use CSS (Cascading Style Sheet) selectors to determine which document elements to monitor, creating a list of fields to protect.

For a website with minimal elements under protection and one that does not change often, this approach can be effective against data skimming – at least where currently known methods of reading data are concerned. Performance can be impacted if the list of monitored elements increases or a highly utilized element is included and as such, organizations utilizing this approach should ensure they conduct adequate testing of their website.

49% ***of companies have experienced a data breach caused by a third-party technology***

63% ***of all cyberattacks could be traced directly or indirectly to third-party technologies***

Network control

Another client-side approach looks to control data theft through preventing it leaving the web page and being sent to an unknown, remote location by controlling network connections. This approach works by hooking into the functionality that transmits or receives data and ensures the remote party is trusted.

This is the most robust method of client-side enforcement because:

1. It does not matter how the data is read or what technique is used; the transmission to the attackers will be prevented, meaning that even yet unknown methods of skimming will be mitigated
2. By limiting the enforcement action to the network there is no heavy burden with respect to monitoring individual document elements and thus, no performance impact or degradation

Network-based client-side enforcement is suitable for websites of all complexity levels as it rarely needs changing once implemented and configured.

About Ensighten

Ensighten is the global leader in website client-side security, bringing next generation protection against data theft through website skimming, malicious ad injection, CSS injection and more. With Ensighten's technology, organizations can assess their security and privacy risk and stop unauthorized leakage or theft of data, as well as comply with the CCPA, GDPR and other data privacy regulations. Ensighten's MarSec^{TM} platform protects some of the largest brands in the world.

Ensighten's client-side protection is effective against 100 percent of skimming attacks and brings the following benefits:

Network allowlist

Prevents data from leaving the web page except to approved destinations

Modern filtering

Stops emerging attack methods, including mutating resources and image injection

Performant and lightweight

SaaS-delivered technology from highly scalable cloud infrastructure protects your website while maintaining the very best user experience

Intelligent analysis

Identifies specific types of data, such as credit card numbers and social security numbers, and prevents transmission to unknown destinations

Real-time analytics and reporting

Monitors all network requests and provides visibility into attack attempts, alerting you to potential issues

Comprehensive user interface

Allows easy configuration, rapid onboarding and low-maintenance protection

Ensighten is headquartered in Menlo Park, US with the European HQ in London, UK. To learn more, get in contact or join the conversation on LinkedIn and Twitter.