The Skimming Threat

Learn About Digital Skimming Attacks, How They Work, and How to Stop Them

feroot

There are dozens of methods that cyber threat actors can use to steal Private Identifiable Information (PII), financial transaction data, and other confidential and proprietary data from businesses. Traditionally this involved breaching a target's corporate network to accomplish this goal. Today, there are a multitude of new vectors that can be used to steal data from companies; including use of malicious scripts directly on the front-end of a website or web application to start skimming the data when a user enters information into a form. ***Digital skimming is a client-side cyberthreat that requires organizations who interact with their customers via websites and web applications must secure their business from.***

What is Digital Skimming?

Digital Skimming, web skimming or e-skimming attacks infect websites with malicious code; specifically designed to exfiltrate data. ***Skimming malware comes in a variety of flavors that are commonly referred to as skimmers, sniffers, or JavaScript sniffers, all of which are very difficult to detect.*** An infected website skims user information from payment checkout forms, login pages, marketing forms, or anywhere else companies collect personal information. Most of the time the business and the website user are not aware that their information is being skimmed by threat actors, who likely have the intent to use that information for their own financial gain.

Threat actors use skimming attacks to collect a wide variety of information that they can either use immediately for financial gain, or sell the information on the dark web for profit later. This information might include:

Payment Skimming*

- Usernames
- Passwords
- Email address
- Credit card information
- PayPal or Venmo Credentials

PII Harvesting*

- First and last names
- Billing address
- Email address
- Phone numbers
- Social security numbers
- Healthcare information

What is E-skimming?

E-skimming, commonly referred to as a 'Magecart*' attack, is a process in which malicious threat actors, nation-state sponsored hackers, and financially motivated hackers gain access to an online store of a company. These threat actors inject skimming code onto payment card processing pages of the website in order to make financial gain.

Who is at Risk?

Threat actors love to exploit the obvious. So, at this point in time, a better question to ask is "who is ***not*** at risk?" To do business with any consumer, businesses must have a digital presence. Marketers like to say "our website is the center of our universe," and this definitely holds true. If a business does not have a website, consumers quickly question the validity of the business. Buying behaviors today dictate that a business must have an online presence available for the consumer to evaluate the goods and services sold as the first step in the consumers' decision making process.

That being said, threat actors also don't like to waste their time or money. They tend to go after low hanging fruit in order to maximize their return on investment, especially if they purchased malware on the dark web and need to recoup that initial investment. Threat actors also try to attack lots of targets at once in order to hedge their bets. All they need to recoup their initial investment is to breach one business's website. There are a number of industries who are at risk to e-skimming attacks. Below is a sample of industries and their estimated e-skimming risk level.

High Risk

- Financial Services & Banking
- Insurance
- Healthcare & Medical
- eCommerce & Retail
- Travel & Hospitality
- Communication, Social Media & Content Producers
- Cryptocurrency Exchanges & Blockchain

Medium Risk

- Real Estate
- Technology & Cybersecurity
- Distribution & Transportation
- Education
- Entertainment

Low Risk

- Manufacturing
- Energy
- Distribution & Transportation
- Consulting & Legal Services

How do Skimming Attacks Work?

Skimming attacks occur on the end-user's web browser. Threat actors conduct these client-side or front-end attacks by compromising third-party, and sometimes fourth-party, software libraries on the target websites code. Threat actors inject malicious code, also known as a JavaScript Injection Attack, into the client-side code base, which is executed within the end-user's browser session. The result is that information that the user enters into a form on the website is copied and redirected to a malicious host* or command & control server*, where the threat actor collects the information for future use.

Examples of third-party applications targeted by attackers include:

- Live chatbots;
- Customer service functions;
- Advertising scripts;
- Marketing forms;
- Marketing tags;
- Open source code libraries; and
- Various other elements loaded by the user's browser.

What is a JavaScript Injection Attack?

During a JavaScript Injection Attack a hacker or malicious user gains website or web application parameters information and can change their values. This allows the threat actor to manipulate the website or application and collect sensitive data, such as PII or payment information.

Today, websites aren't built by a team of developers line by line. They are assembled like a sophisticated jigsaw puzzle. Chunks of pre-written code with varying functionality, that were built by multiple developers with varying capabilities, are pieced together to create the final product. Modern web applications load an average of over 20 third- and fourth-party scripts as part of the user experience. On account of this, compromising one of these third- or fourth-party elements with malicious JavaScript allows an attacker to compromise multiple websites simultaneously. This attack type is commonly referred to as "drive-by web skimming*."

There are a few variants of web skimming codes that are notoriously difficult to detect and remediate. Pipka is a web skimming code with anti-forensic, self-cleaning, and stealth capabilities. It is able to remove itself from a web page's code after it has been executed, thereby making it exceptionally difficult to detect.

Digital skimming continuously evolves and is a persistent threat that cyber security teams need to keep a close eye on. It has been reported that one in five Magecart's victims are re-infected within days.

How do I Detect Skimming Attacks?

The first step in detecting digital skimming attacks is having a full inventory of all your web assets. This includes websites, marketing forms, payment portals, web applications, etc. Your cybersecurity team needs to know what their client-side attack surface looks like, so that they know where threat actors might attack your digital assets and your customers.

The next step is to determine what scripts are running on those assets and which scripts have access to sensitive data. Threat actors love to target 'zombie scripts,' scripts that collect sensitive data but are not being used by the business. To detect skimming attacks, businesses need to be 100% aware of what data is being collected or exchanged via the client-side of the website, and what application elements or third-party elements have access to the data, or are touching your data (i.e., scripts and libraries). Once these basics have been covered, security teams must follow the five steps below on a continuous basis to detect skimming attacks.

1. Review code and security control configurations to identify potential vulnerabilities and misconfigurations.
2. Perform security and vulnerability assessments of all scripts and code elements that your websites or web applications load into the browser.
3. Test web applications for vulnerabilities using assessment tools.
4. Protect your website by using security control-integrity monitoring, file-integrity monitoring, and change-detection automation systems.
5. Implement client-side intrusion detection to detect run-time and browser-level intrusions.

How do I Prevent Skimming Attacks?

The best prevention and defense strategy for skimming attacks is to use a layered security strategy, also commonly referred to as Defense-in-Depth*. Businesses need to deploy and nurture a multi-layered defense against web skimming attacks in order to prevent or significantly minimize the impact of client-side cyberthreats.

1. Harden and tamper-proof the client-side of your web applications.
2. Grant data access only to those websites and web applications which absolutely require access to that data.
3. Carefully restrict access to prevent all unsanctioned scripts and JavaScript libraries from accessing data, to ensure unauthorized access of sensitive data is contained at the browser-level.
4. Continuously analyze all scripts from the client-side to detect unauthorized activities.
5. Deploy vulnerability and malware monitoring technologies and processes on the client-side of your web applications.
6. Implement client-side intrusion prevention policies and procedures to prevent run-time browser-level intrusions in real-time.

Conclusion

Regardless if you are a marketer, a customer service professional, a security professional, or an application developer, you are responsible for protecting your most critical assets — your customers. In order to grow your business and avoid costly data breaches, it's your responsibility to prevent skimming attacks and the associated data exfiltration. The ultimate goal is to deliver a customer experience without risk or compromise. The dangers that come through the client-side are significant, as are the historic challenges to defeat them; complexity, a lack of visibility and an inability to uncover, remediate and prevent client-side security threats. But with knowledge of what is needed, it can be done and not just said.

Appendix

Definitions

What is Payment Skimming?

Payment Skimming or e-skimming is a digital attack method used by financially motivated threat actors and hackers to capture payment information and PII from credit card holders. Hackers utilize a variety of malicious tools to take advantage of web application or website vulnerabilities to collect information for financial gain.

What is PII Harvesting?

PII harvesting is a type of attack in which cyber criminals manipulate forms within web pages, such as login or shopping cart pages, to collect PII or other data that users submit. PII may include social security numbers, email addresses, usernames, passwords, pin numbers, payment information, and physical addresses.

What is Magecart?

Magecart is a group of malicious hackers who target digital or ecommerce businesses who sell their products via online shopping cart systems to steal customer payment card information. These threat actors are financially motivated and like to take advantage of ecommerce websites that are not properly protected.

What is a Malicious Host?

A Malicious Host is a Network Host turned against the network. It's an agent server that attacks mobile agents to achieve a malicious goal.

What is a Command & Control Server?

Command & Control (C&C) Servers are servers owned and operated by threat actors. Threat actors use C&C servers as the place to exfiltrate data when they are conducting a cyber attack such as skimming or other malware related attacks. Essentially, C&C servers allow threat actors to capture and retain stolen data for future use.

What is a JavaScript Injection Attack?

During a JavaScript Injection Attack a hacker or malicious user gains website or web application parameters information and can change their values. This allows the threat actor to manipulate the website or application and collect sensitive data, such as PII or payment information.

What is Drive-by Web Skimming?

In Drive-by Web Skimming a threat actor compromises third- or fourth-party code with malware, with the hope that multiple organizations use this code and infect their websites and web applications inadvertently. Modern web applications load an average of over 20 third- and fourth-party scripts as part of the user experience. On account of this, compromising one of these third- or fourth-party elements with malicious JavaScript allows an attacker to compromise multiple websites simultaneously.

What is Defense in Depth?

Defense in Depth is an approach to cybersecurity in which a series of technologies, processes and procedures are layered in order to protect valuable data and information. If one piece of the puzzle fails, another is already there to stop a cyber threat actor from continuing his attack. Defense in Depth is designed to have multiple layers and redundancies to increase the chances of successfully stopping a breach from happening or a threat actor moving laterally to attack other systems.

About Feroot

Feroot Security believes that customers should be able to do business with any company online securely, without risk or compromise. Feroot secures front-end web applications so businesses can deliver flawless digital user experiences to their customers. Leading brands trust Feroot to protect their client-side attack surface. Visit www.feroot.com.