CYBERSECURITY

Digital skimming: how to stay protected

Table of contents

Introduction 2

Injection methods 3

Critical software vulnerabilities 4

Safeguarding your digital ecosystem 6

INTRODUCTION

What is a digital skimmer?

A digital skimmers malicious code is designed to steal payment card information and sensitive data from online shoppers during e-commerce transactions. Attackers typically inject the skimmer code into the website's source code, secretly capturing users' information as they make purchases. The stolen data is then sent to the attackers' servers, enabling the cards to be sold and used elsewhere for subsequent fraud.

This stealthy technique poses significant threats to both consumers and businesses. These attacks can have severe consequences for businesses, including financial losses, damaged reputations, and legal repercussions. For customers, the damage comes primarily from compromised personal information, including payment data, when may enable subsequent identify theft or financial fraud, among other risks.

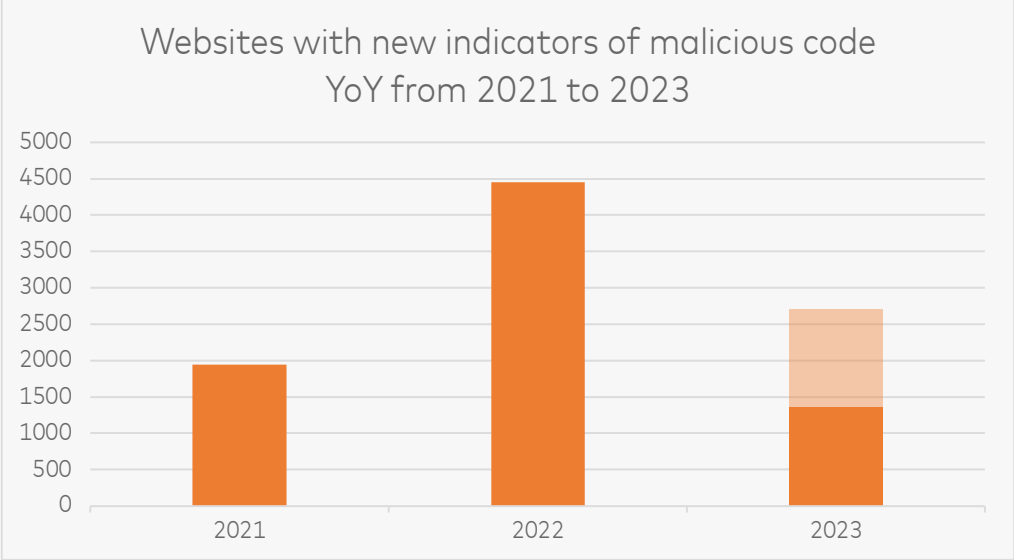
It is crucial for businesses to implement robust security measures and basic cybersecurity best practices to protect their customers and sensitive data. This paper will outline common patterns in digital skimmer injection with a focus on those cybersecurity vulnerabilities that most often lead to compromises. Fortunately, Mastercard has tools in place to identify skimmers and those key vulnerabilities, enabling businesses to proactively ward off injections.

How does Mastercard identify the presence of digital skimmers?

Since its acquisition of RiskRecon in 2020, Mastercard can assess the cybersecurity posture of public URLs. By searching for indicators of compromise associated with digital skimmers—the malicious code scripts through which bad actors send users' data to their servers—Mastercard is able to identify compromised web sites, when the digital skimmer was first detected, how long it stayed on the web page, what other cybersecurity vulnerabilities were present during the breach window, and other findings. Our detailed analysis of the impacted organizations and the nearly 6,500 digital skimming events reveal interesting insights below.

Findings

When looking at the year-over-year trend, the number of digital skimmer infections increased by 129% in 2022, resulting in almost 4,500 new injections in the preceding 12 months. The number for 2023 is expected to rise to about 2,700 new injections.



Digital skimming attacks not only target traditional vulnerabilities but have now extended to other open-source shopping cart software. On average, removing a digital skimmer from the web page takes weeks. However, some

victim web sites did not remove the malicious code for years due to a lack of visibility about third-party scripts running on the website or poor cybersecurity hygiene. Moreover, web site owners take on average nine months to

install patches, as per an analysis of RiskRecon's cybersecurity scans, making them a more likely target for digital skimming attacks.

Digital skimming attacks have grown increasingly popular over the past several years. Tactics among criminals have evolved to both breach sites and evade detection. Digital skimming attacks have become a leading cause of cybercrime in recent years.

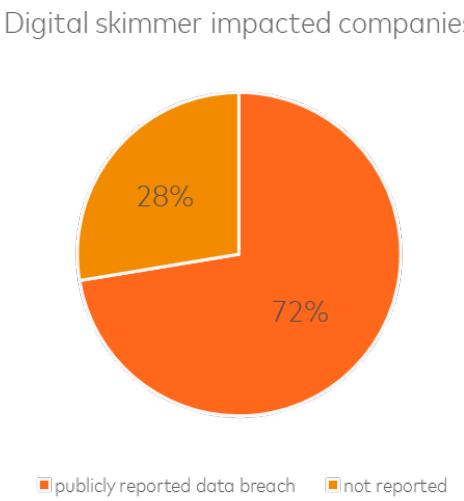
Subsequent fraud and card testing

Based on payment card fraud reported to Mastercard by issuers via the Fraud & Loss Database, Mastercard cards that transacted at infected merchants are 31% more likely to report subsequent fraud. Furthermore, stolen cards are being used fraudulently by criminals and, on average, fraudulent transactions occur five months after the theft. The lag between the theft and the use of the stolen payment credentials for fraud is most likely tied to the compromised payment card lifecycle, which consists of: testing the card for validity before posting it for sale on payment card shops, advertising in criminal marketplaces, purchasing the compromised cards, and eventually attempting a fraudulent transaction.

Data Breach events

Regarding reported data breaches, RiskRecon also provides research on published security breaches and sources data loss events from channels such as public media, regulatory filings, and dark web monitoring. Combined with RiskRecon's cybersecurity assessment data, this data reveals 72% of the entities publicly disclosing a breach were the victim of digital skimming[1]:

INJECTION METHODS



How is a digital skimmer injected?

Criminals embed digital skimmers through a number of different cybersecurity vulnerabilities. These bad actors may replace existing scripts in the source code of the web application or leverage a compromise of the source

[1] The correlation coefficient is 0.64.

code of a third-party tool to attack the primary target. Businesses with insecure admin portals or publicly facing databases are also at risk of having their credentials stolen and utilized to inject digital skimmers. We have also seen use of other methods, such as SQL injection and brute force attacks.

Sometimes the loaded script depends on the referrer header value, i.e., the webpage from which it is fetched. There can be a separate loader script rather than the skimmer itself, meaning that the skimmer code is only loaded if its loader is running on the checkout page.

The skimmer eventually grabs any input, select, and text area elements on the page that are not hidden or empty. Often, we see that the script is encoded using base64 or base16, which is suspicious since benign scripts are not usually encoded. The code can also inject a new malicious form instead of reading the information from the existing form.[2]

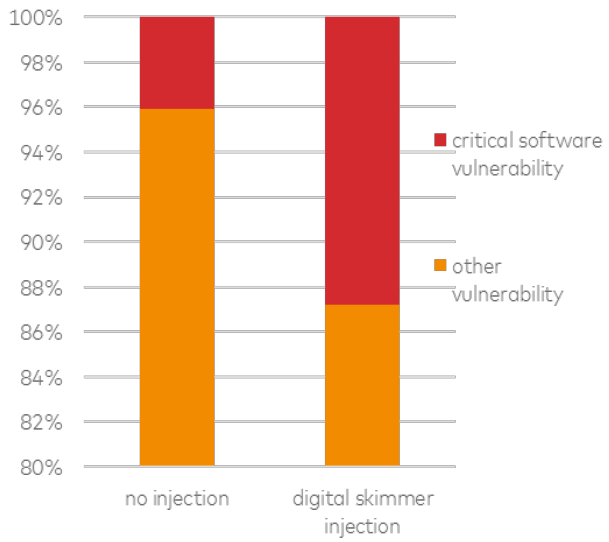
Failure to patch leads to more infections

The Software Patching domain, one of the nine security domains evaluated by RiskRecon, enumerates systems that are running end-of-life and vulnerable software. The Software Patching security domain had the most important findings when comparing impacted entities with a control group. For the infected systems, the cybersecurity rating in the Software Patching domain dropped from A to C, revealing that C-rated merchants on Software Patching are 12x more likely to have a digital skimmer.

For most entities impacted by Magento vulnerabilities, the software became outdated less than a month before the malicious code injection. The number of entities with other cybersecurity vulnerabilities also increased right before the digital skimmer embedding, including missing security headers, the number of systems that are hosting phishing sites, and other outdated content management systems. As soon as other vulnerabilities get resolved, the skimmer code is also removed. Staying current on software patching is a key defense against digital skimming attacks.

CRITICAL SOFTWARE VULNERABILITIES

Critical software vulnerability is an out-of-date software known to have high severity security problems. As per our analysis, enterprises with at least one critical software vulnerability are 3.3x more likely to have a digital skimmer. For entities where a digital skimmer was identified, 13% of vulnerabilities were critical software vulnerabilities versus only 4% in a general population from 2021 to 2023:



[2] See previous Riskrecon white paper: New Digital Skimming Techniques: How RiskRecon Can Keep You Protected, published May 9, 2023.

The abuse of legitimate services for conversion tracking, site analytics, and remarketing provides free infrastructure for threat actors and enhances capability to avoid detection. For example, when leveraging with third-party tools, businesses may mistakenly integrate counterfeit products that would mask a digital skimmer. Therefore, typos in the domain names are typical for an attack. If the tool's proper domain name is tool.analytics.com, a counterfeiter might create decoy tools with domains such as tool.analytsc.com or tool-analytics.com or tool.analytics.ru, etc. Attackers may also use trojanized GTM containers by placing malicious JavaScript within the GTM container.

'Software publishers' and 'Computer Software Stores' are amongst the most common industries targeted by digital skimmers.

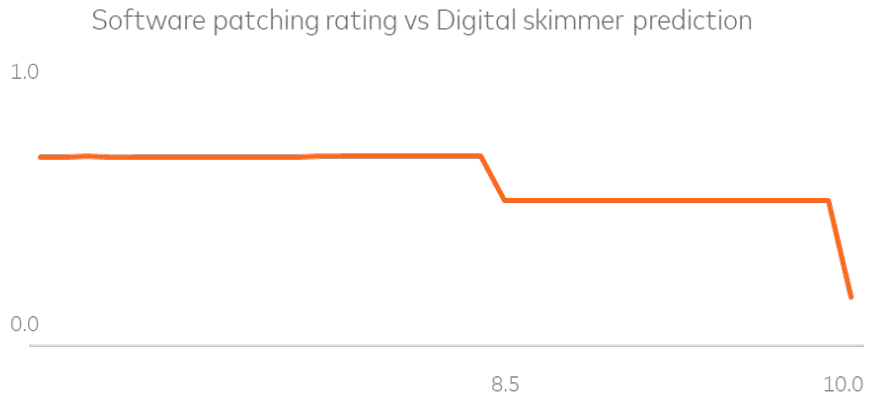
Reinfections

Since 2021, Mastercard has observed that malicious code gets re-injected to the same site for at least 18% of entities, and the same page is being used as a placement for at least 4% of entities, which could be a checkout, authentication, or contact page. Re-infection occurs within 40 days on average and is associated with unpatched software.

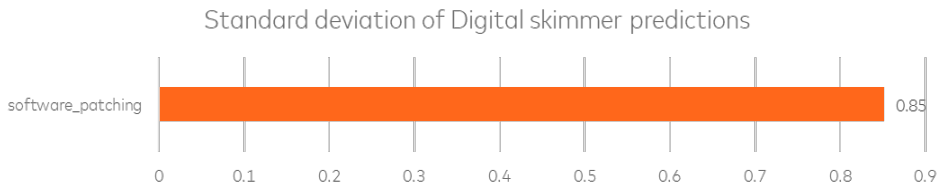
Vulnerability and ratings importance

Since there are hundreds of different cybersecurity findings and data points, the Partial Dependence plot technique can be used to evaluate which vulnerabilities have the most significant contribution to the risk of getting a digital skimmer.

PDPs (Partial dependence plots) are a model-agnostic method which measures feature importance in predictive modelling. To apply PDPs, we build a predictive model to determine the probability of each entity having a digital skimmer. We then vary the value for one of the features and record the resulting predictions. For example, changing the "Software Patching cybersecurity rating" would give us a different prediction. We do this while holding the other features constant at their values. Then, we calculate the average prediction for each changing parameter across all observations. Here is an example of how variation in software patching rating changes the probability of having a digital skimmer:

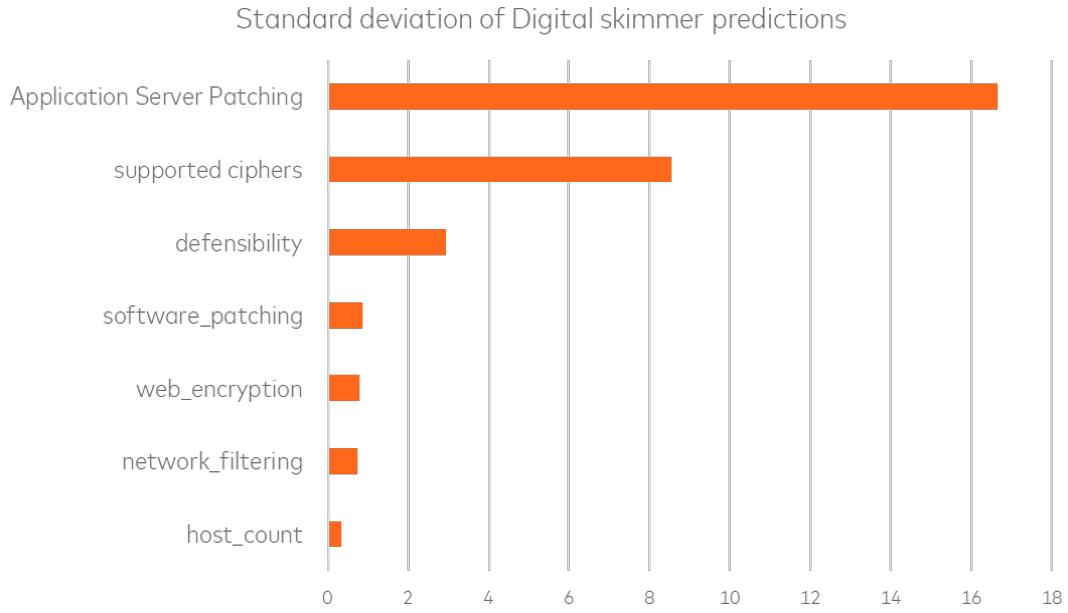


A feature importance score based on PDPs is done by determining the "flatness" of the PDP value for each feature, e.g. if changing the feature does not change the target value, the PDP remains relatively constant. In other words, the y-axis values are always close to their mean value and have a low standard deviation.



PDPs allow us to strip out noise and the effect of other features. However, one of the disadvantages of using PDPs is that it ignores interactions: if interactions are present, the score can underestimate the importance of a feature. Other techniques, such as Individual Conditional Expectation (ICE) plots, can be used to assess such interactions.

Looking at the standard deviation of various predictors, we see the prominence of Application Server related issues, such as outdated PHP, Perl or Magento. In fact, entities with Application Server related issues are twice as likely to suffer from a digital skimmer breach. These include vulnerabilities in PHP, Perl, Magento, MS Exchange, and other operating systems, applications, and database management systems (DBMS).



Using insecure ciphers and outdated protocols—e.g., SSL when TLS can be used—is also associated with a digital skimmer presence.

The number of hostnames is highly correlated with the presence of digital skimmer. In other words, the larger the entity in terms of the number of internet-facing systems, the more likely it will suffer from a digital skimmer. This can include marketplaces, which host hundreds or thousands of micro and small merchants.

SAFEGUARDING YOUR DIGITAL ECOSYSTEM

Although enterprises that utilize open-source e-commerce platforms are at higher risk of digital skimming attacks. Our analysis concludes that with good cyber hygiene, these businesses can achieve greater cyber resiliency and reduce their likelihood of a digital skimming attack.

RiskRecon by Mastercard's cyber risk monitoring assessment tool and threat protection solution can help organizations achieve better risk outcomes through proper cyber health management and real-time threat mitigation.

Cyber Risk Monitoring

RiskRecon offers a comprehensive and proactive approach to third-party risk management that is well-equipped to address the complexities of digital skimming attacks. By providing continuous monitoring, risk assessment, actionable insights, and a focus on vendor ecosystem visibility, RiskRecon helps organizations bolster their security measures and minimize the potential for breaches and their far-reaching consequences.

Cyber Threat Mitigation

RiskRecon Threat Protection helps protect web applications from a variety of application layer attacks—such as cross-site scripting, SQL injection, and cookie poisoning. Plus, it provides additional layers of protection and traffic redirection to prevent bad actors from reaching a business's cyber assets.

Sign-up for a 30-day free trial of RiskRecon by Mastercard to learn the cyber risk standing of up to 50 of your key vendors.

Get started now: **www.RiskRecon.com/KnowYourPortfolio**