MAGENTO WEBSITE SECURITY REPORT

CONTACT US

WWW.FOREGENIX.COM/WEBSCAN

TEL: +44 845 309 6232

14TH DECEMBER 2020

PRODUCED BY FOREGENIX

OVERVIEW

WHO IS FOREGENIX?

We are a leading independent cybersecurity company with a focus on keeping the world's payment systems secure.

With over a decade of experience in the Payment Card Industry (PCI), we help merchants, payment processors, banks and other operators to ensure they are securing their environments effectively while complying with industry security standards.

We won the Queen's Award for Enterprise in 2019.

WHAT DO WE DO?

COMPLIANCE & RISK

DIGITAL FORENSICS & RESPONSE

CYBERSECURITY TECHNOLOGY

THE QUEEN'S AWARDS FOR ENTERPRISE: INTERNATIONAL TRADE 2019

FOREGENIX

14TH DECEMBER 2020

OVERVIEW

WHAT IS WEBSCAN?

We currently monitor over

260,000

Magento Merchants

GLOBALLY

WebScan is our comprehensive non-intrusive website scanning solution. It analysis websites for specific security vulnerabilities to produce a risk score.

The scans are passive, meaning it looks for publicly available information (just like criminals do), and at no point does it try to exploit vulnerabilities.

WebScan looks for:

- Malware (including card skimmers)
- Platforms and patching information
- SSL issues

We like to say that WebScan is the most up-to-date website scanning solution in the market, as it is constantly updated by both our forensic team and Threat Intelligence Group.

OVERVIEW

THE RISK CATEGORIES

CRITICAL — Already hacked, card data actively being stolen

HIGH — At risk of being hacked - easily

MEDIUM — Some issues, unlikely to get hacked

LOW — Hacking unlikely

THIS IS THE PROBLEM ZONE

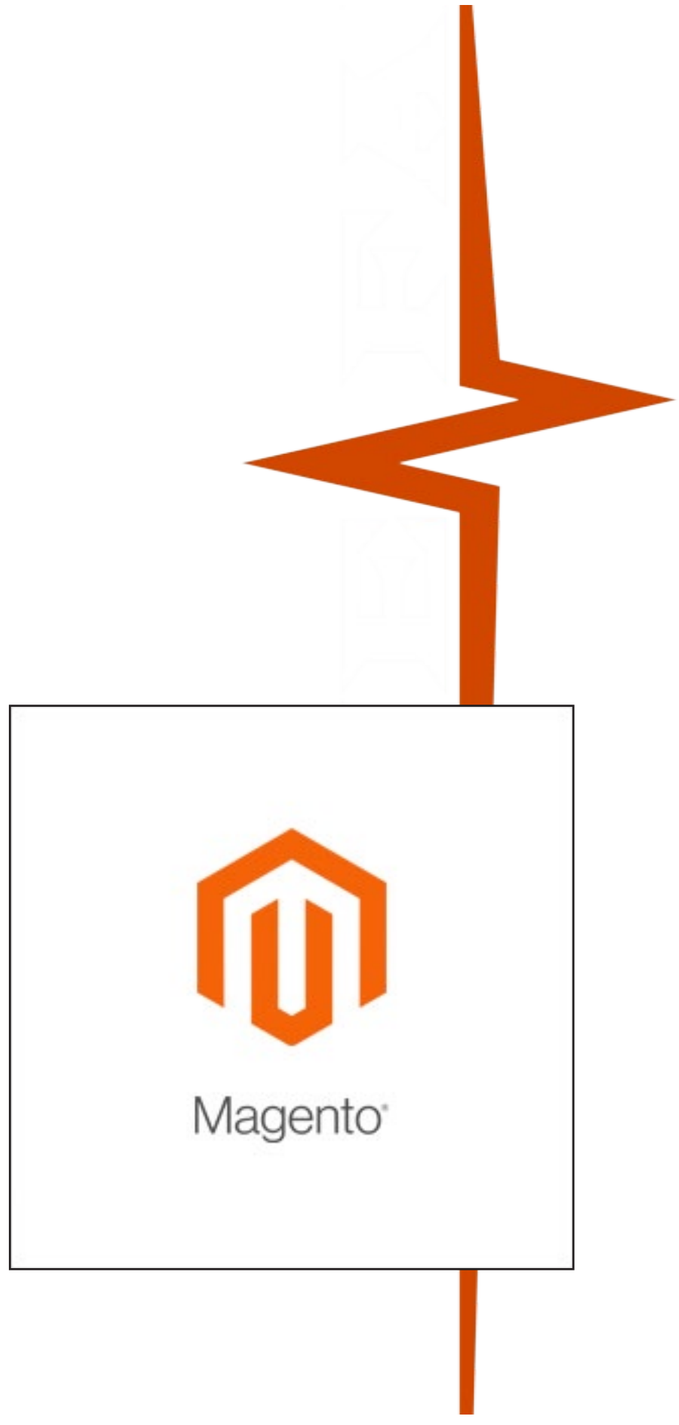
OVERVIEW SUMMARY

Over **160,000** websites remain on the Magento 1 platform

Magento 1 websites continue to slowly **DECLINE**

1,631 Magento websites are hacked, with card-harvesting malware.

28% of Magento 2 websites are High/Critical Risk



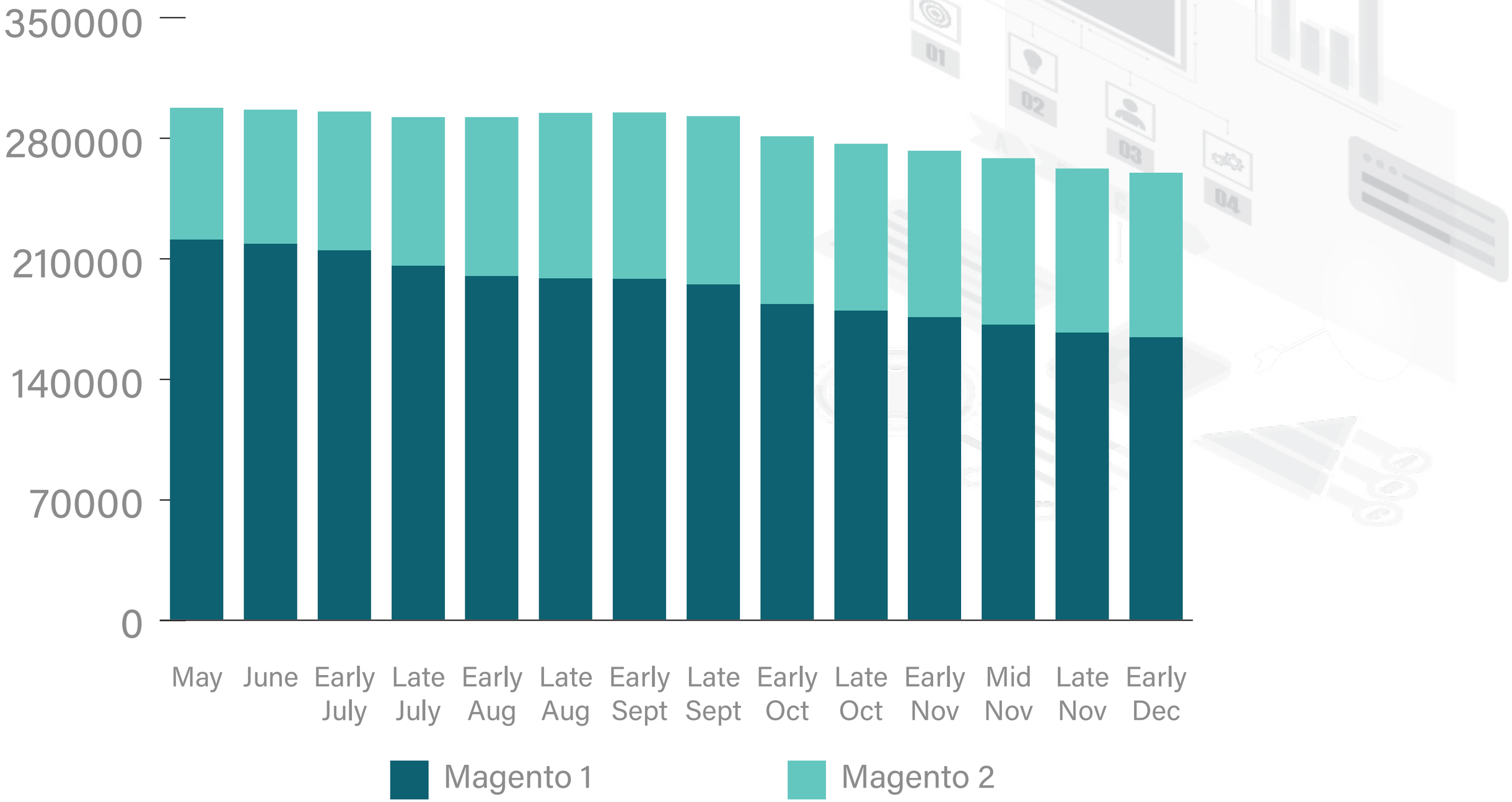
MAGENTO 1 REMAINS THE MOST TARGETED PLATFORM BY CRIMINALS

FOREGENIX

14TH DECEMBER 2020

WEBSCAN RESULTS

WEBSITE NUMBERS (ALL MAGENTO)



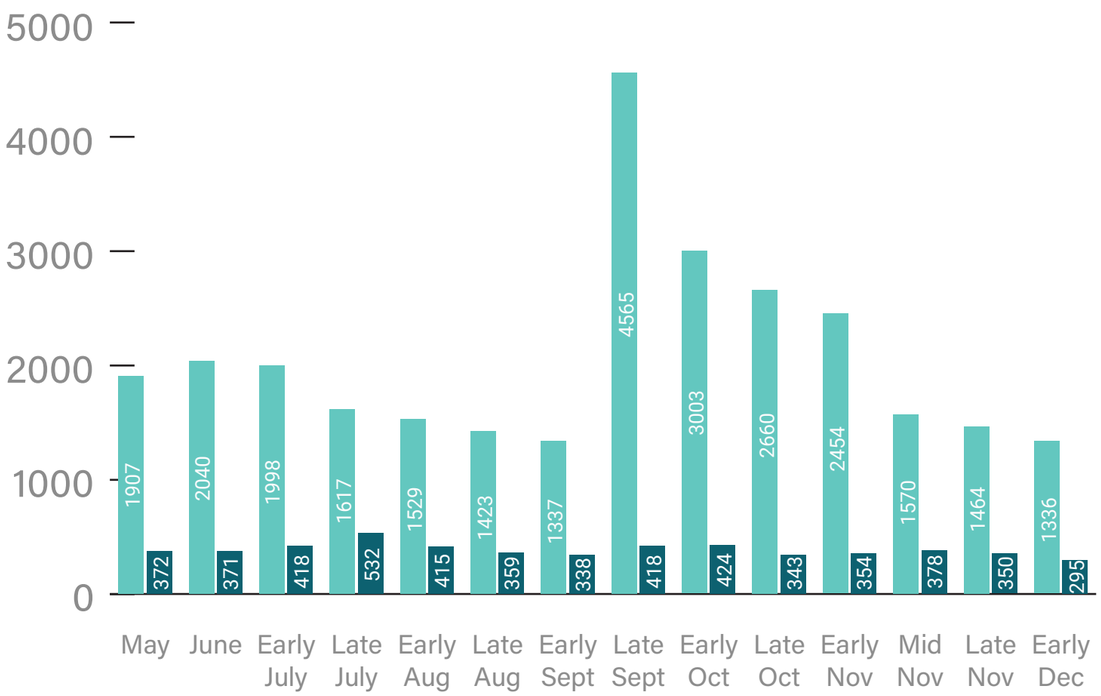
FOREGENIX

14TH DECEMBER 2020

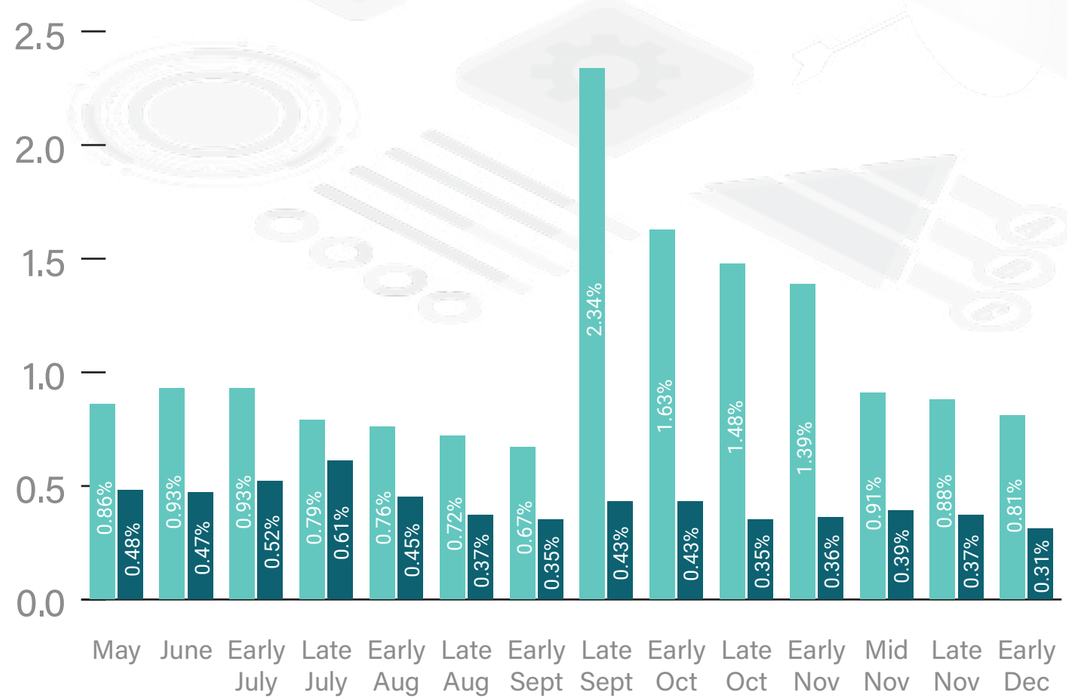
WEBSCAN RESULTS CRITICAL RISK

Websites with Critical Risk have already been hacked
(with card data being actively stolen).

ACTUAL NUMBERS



PERCENTAGE OF TOTAL SITES



Magento 1 Magento 2

FOREGENIX

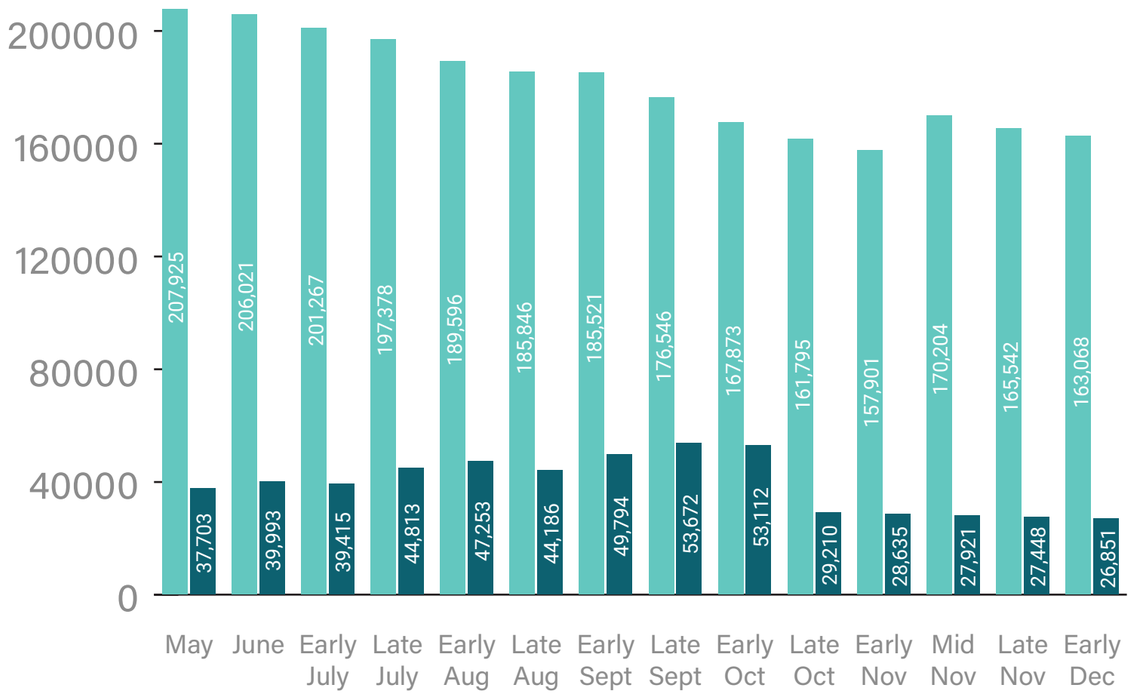
14TH DECEMBER 2020

WEBSCAN RESULTS HIGH RISK

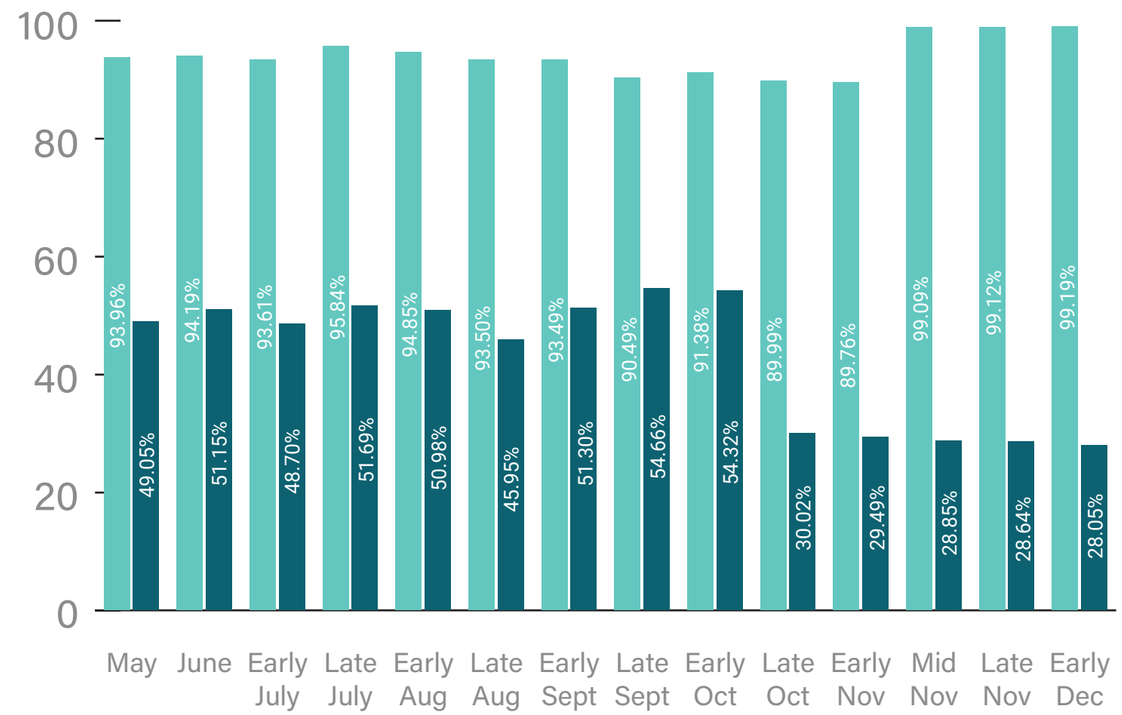
Websites with High Risk have significant security issues that make them very vulnerable to criminals.
The sites have one or more of the following:

- Missing critical framework security patches
- Has known framework vulnerabilities
- Security issues with website setup
- Non Card Harvesting Malware

ACTUAL NUMBERS OF HIGH RISK SITES



PERCENTAGE OF TOTAL SITES



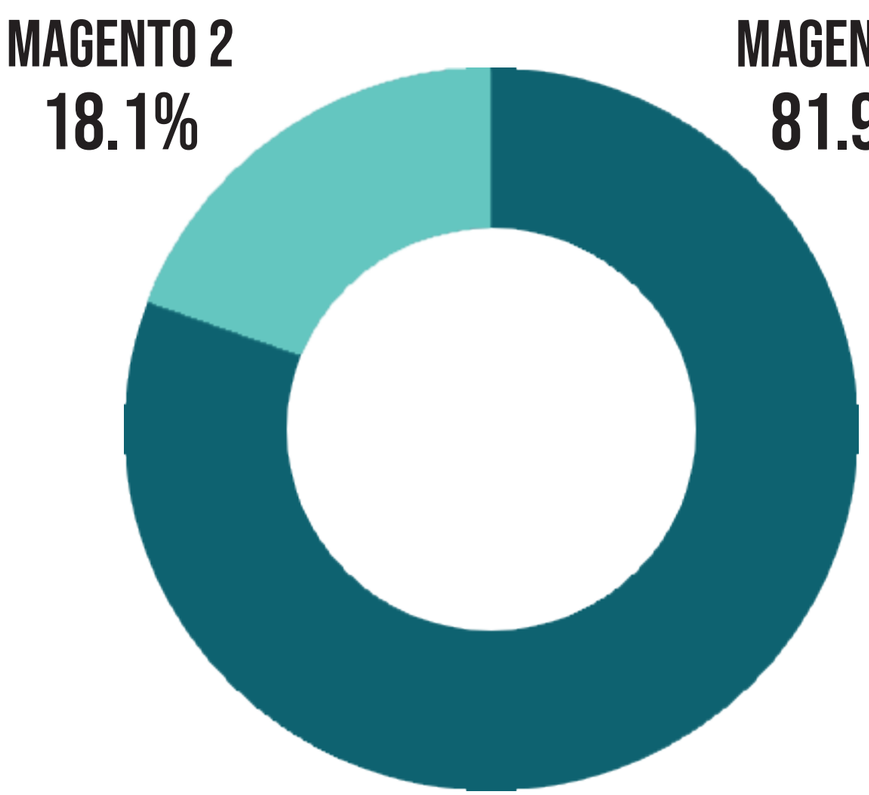
Magento 1 Magento 2

FOREGENIX

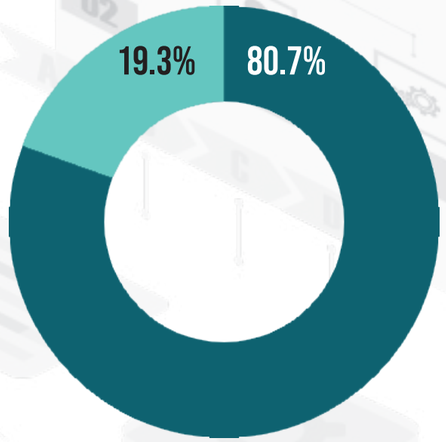
14TH DECEMBER 2020

WEBSCAN RESULTS

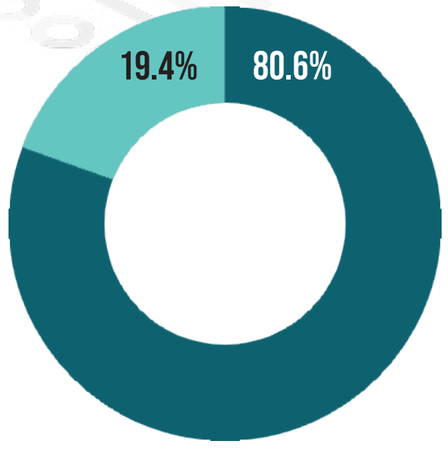
CARD-HARVESTING MALWARE DISTRIBUTION



TWO WEEKS AGO



ONE MONTH AGO



FOREGENIX

14TH DECEMBER 2020

WEBSCAN RESULTS

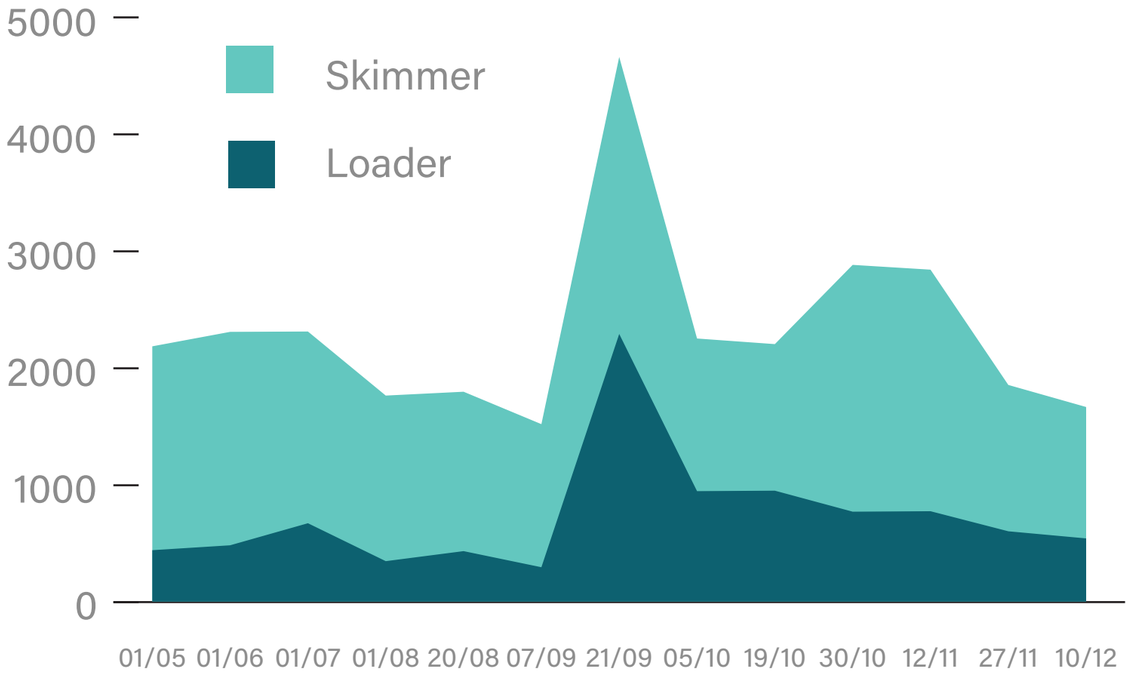
MAGENTO 1 & 2 - LOADERS & SKIMMERS

We also track how many websites are infected with loaders and skimmers.

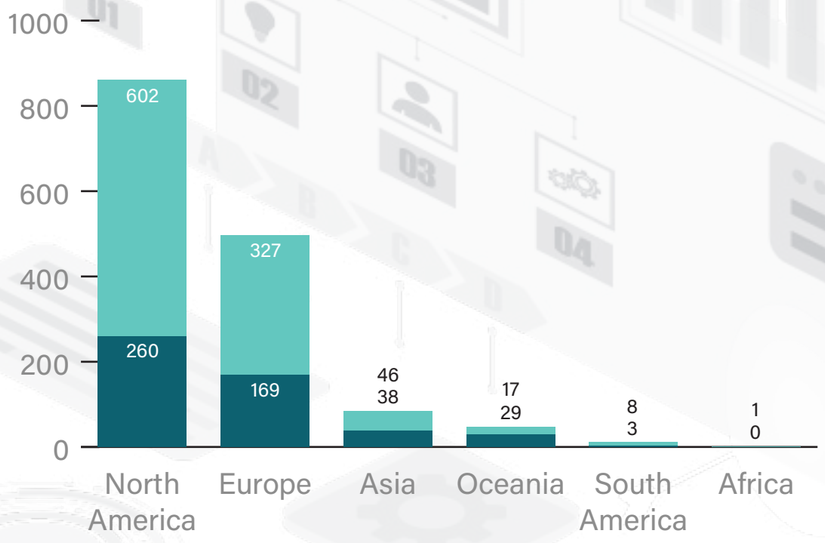
Loaders - are small pieces of code designed to load in additional malicious code onto a website.

Skimmers - are malicious scripts designed to scrape card data and customer information from a site's payment page before sending them off to the attacker.

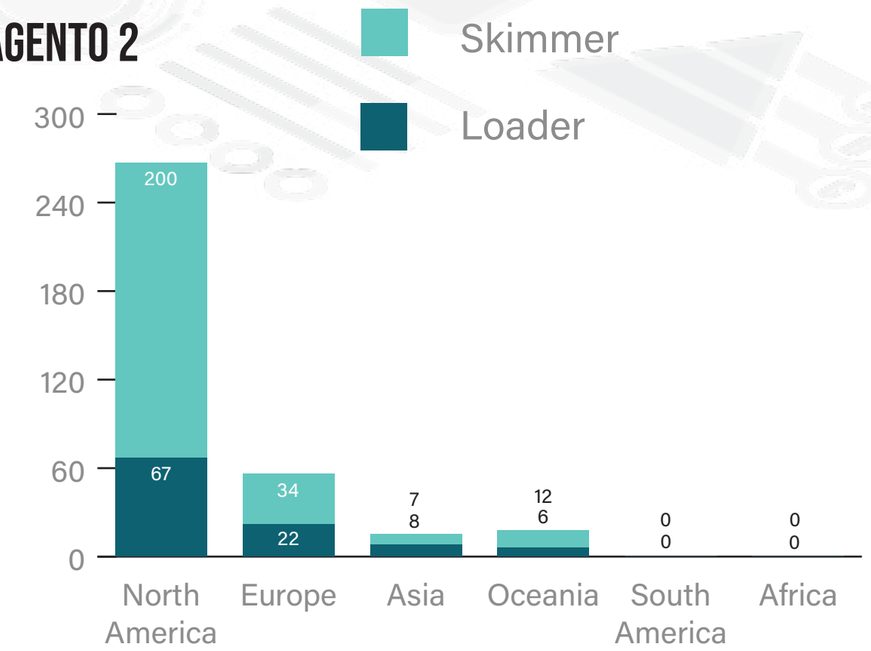
The charts to the right show which regions in the world have the highest infection rate, and below shows change over time.



MAGENTO 1



MAGENTO 2



FOREGENIX

14TH DECEMBER 2020

WEBSCAN RESULTS MAGENTO 1 & 2 - FRAMEWORK ISSUES

Framework vulnerabilities are usually bugs in the software used to run your website.

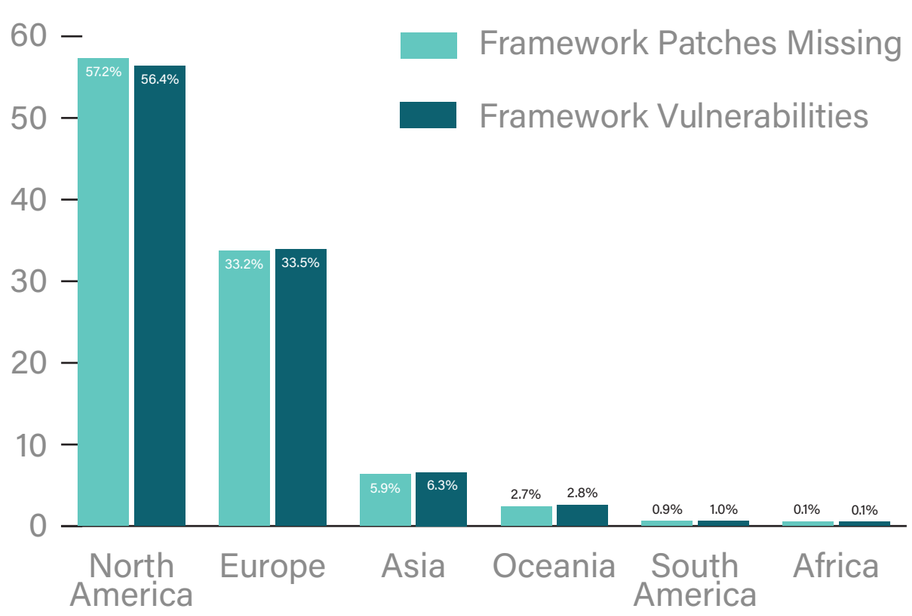
"**Framework security patches missing**" means a website is missing security patches/updates that are already available.

Framework issues also include insecure website set up, such as leaving default settings in place (e.g. admin panel location, etc)

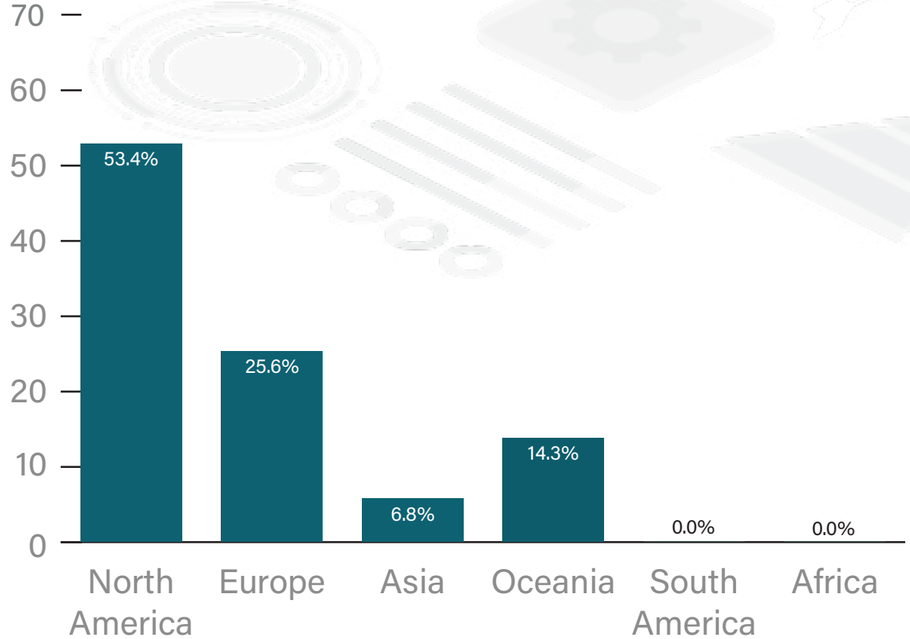
It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having to update the entire website.

With Magento 2, Adobe typically offers a single security patch for the previous version, whenever a new version is released. This gives merchants some flexibility when it comes to upgrading their sites, however they will eventually need to perform a full version upgrade to remain secure.

MAGENTO 1 PERCENTAGES



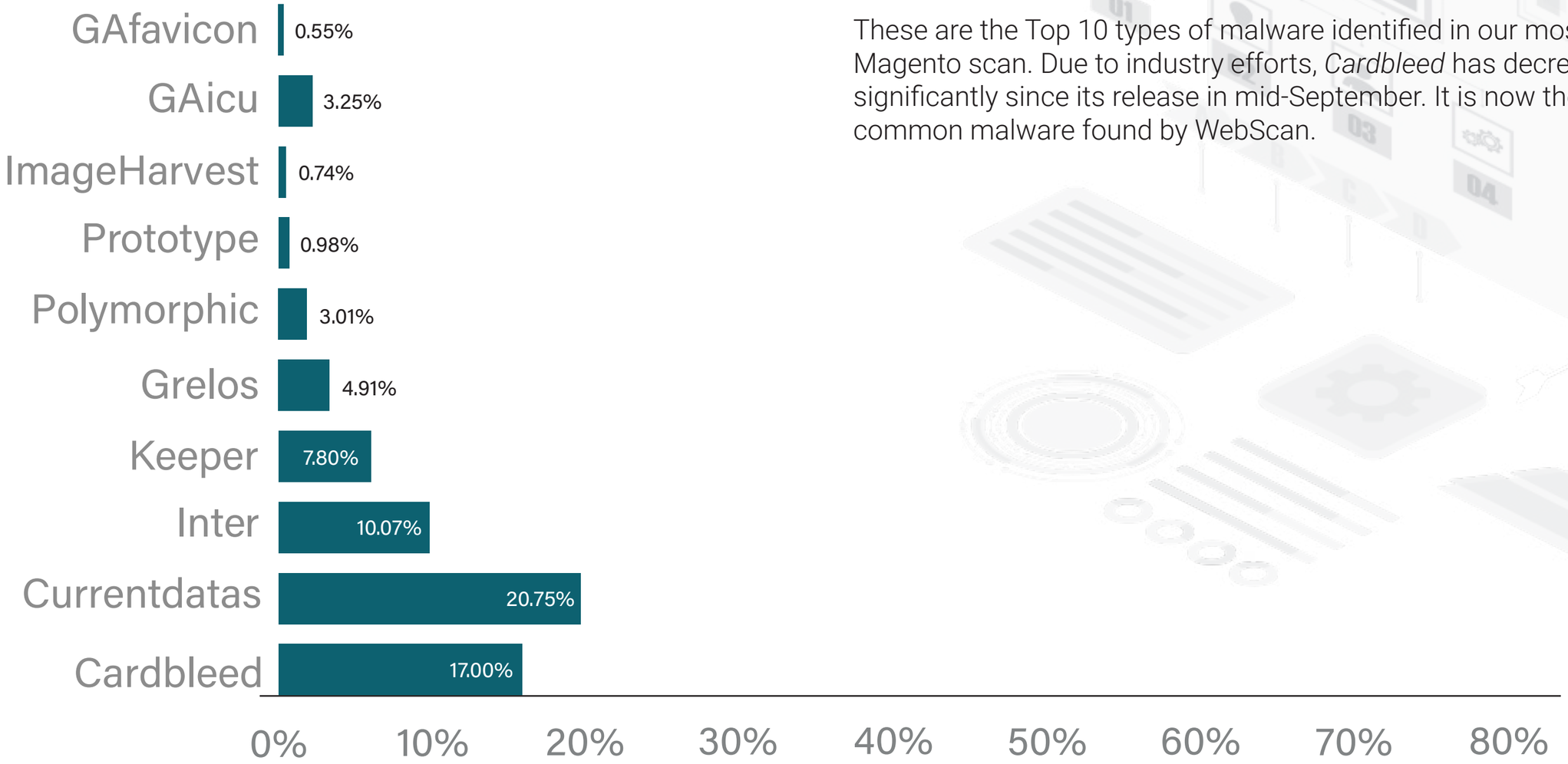
MAGENTO 2 PERCENTAGES



FOREGENIX

14TH DECEMBER 2020

WEBSCAN RESULTS MALWARE TYPES



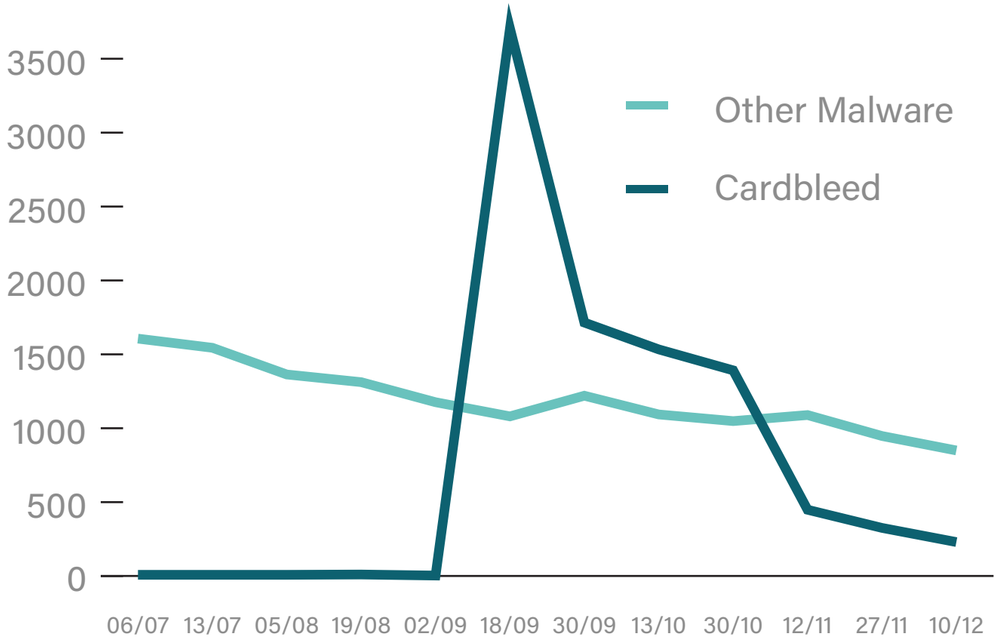
These are the Top 10 types of malware identified in our most recent Magento scan. Due to industry efforts, *Cardbleed* has decreased significantly since its release in mid-September. It is now the second most common malware found by WebScan.

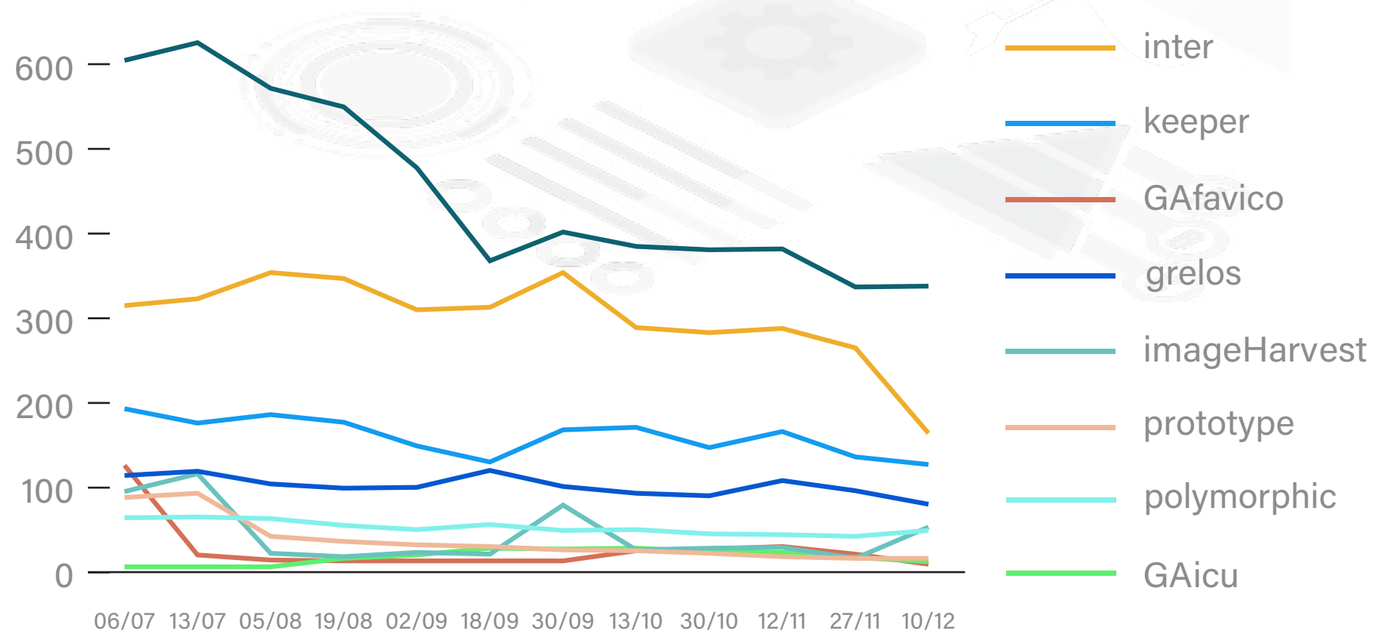
FOREGENIX

14TH DECEMBER 2020

WEBSCAN RESULTS MAGENTO 1 & 2 - MALWARE TRENDS

We are tracking the malware types that are infecting Magento websites.
Due to the *Cardbleed* attack in September, we have broken the data into two graphs.
The first graph shows how all the top 10 malware combined compares with the spike of *Cardbleed,* while the second graph shows the trend over time without it.





FOREGENIX

14TH DECEMBER 2020

MALWARE ANATOMY INTER

Inter is a skimming kit available for purchase on underground forums. It has been used by several different threat actors. It was developed by an actor known as "*Sochi*", who previously went by the name "*poter*". The kit includes everything an attacker needs to compromise an online store and steal card data.

Typically, the Inter skimming code will create an object with a number of adjustable properties, including *Number, Holder, Month, Year, CVV, Gate and Data*. The `Gate` property is used to store the exfiltration URL. Other properties can be defined to target specific elements on the checkout form, the customisability of the skimmer allows it to target a large number of different checkout forms.

The object contains the method `SaveAllFields`, which will read the contents of all the `input`, `select` and `textarea` fields on the page. It then looks through these values, identifies any card data and stores it to the `Data` property. To exfiltrate the data, the skimmer creates an image element with the `src` set to the location specified in the `Gate` property. The data is encoded and appended to the end of this URL as part of the query string, resulting in the stolen data being posted off to the attacker's server via a GET request when the "image" is loaded.

A lot of the time, the exfiltration URL ends in `gate.php`. However we have seen versions of this skimmer post to other URLs, many of which seem to mimic Google-related websites.

While the underlying skimming script is mostly the same across many sites, a few different methods to load the malware have been seen. Some attackers just inject the skimming code directly into the bottom of every page on an infected site. Other attackers have taken a much stealthier approach, ensuring the skimmer is only loaded when the user is on the checkout page.

One version of this skimmer has removed all references to the exfiltration URL completely from the skimming script. Instead, a separate loader is used to fetch the skimming code from an obfuscated location somewhere on their site. This loader then sets a variable `ld`, which is equal to the base64-encoded exfiltration URL. The main skimming script then sets the `Gate` property to this location, which allows it to send the data off to this URL.

MALWARE ANATOMY KEEPER

Keeper is the name given to a group of hackers that have been targeting online stores with the goal of planting card skimming malware. They have a large network with several registered domains used to serve card skimming malware and receive the stolen card data. The name "*Keeper*" was derived from one of the domains this group used regularly: ***`fileskeeper[.]org`***.

A few different methods have been used to load the main skimming script in this campaign. In some cases, the script is hosted on one of the attacker's domains (typically stored in the directory ***`/src/`*** or ***`/js/`***) and a script tag referencing this location is added to the infected site. In other cases, the skimming code itself is injected into every page, or a single JavaScript file that is loaded during the checkout process (such as Magento's ***`prototype.js`*** file) is modified to contain the skimming code.

The skimming code itself is typically obfuscated with a custom encoding function. The function is used to convert an encoded string into an array of strings, which is referenced throughout the rest of the script. By encoding most of the keywords this way, it helps the code to hide its functionality and evade anti-malware scanners. A few variants of this skimmer have been observed. On some sites the skimming script was split across two files, the first file would generate a fake payment form while the second file would perform the exfiltration of card data.

When the skimmer has been loaded and the customer has entered their details on the checkout page, the skimmer scrapes this data from the checkout form. It encodes this data and replaces some of the characters so that it cannot be easily decoded, then it sends the data off to the exfiltration URL. While the attacker has used several different domains to receive the card data, many of them end with ***`/tr/`***.

OUR INSIGHTS

The number of Magento websites continues to decrease, the amount of High and Critical Magento websites found throughout 2020 may explain why many eCommerce websites have closed their doors.

On a positive note, the number of websites infected with card-harvesting Malware decreased once again. Since mid-November, the number of Critical websites has been decreasing, now at 1,631; way below 2,808 in Early November. This is great news, however Christmas is approaching and many people are yet to buy presents online, this leads us to believe that more attacks are likely to happen.

We ask website owners/administrators using Magento, to check their configuration/set-ups, and make sure their site is secure. For extra peace of mind we recommend using a website security solution and getting cyber insurance.

We'd love to hear from you. Call us or send us an email at Magento Security Insights.

ADDITIONAL RESOURCES

Magento

Magento Security Insights Page

foregenix.com/magento

Use our free scanner to understand your website security posture

foregenix.com/webscan

Try out our website security solution, FGX-Web

foregenix.com/fgx-web

FOREGENIX

14TH DECEMBER 2020