# MAGENTO WEBSITE SECURITY REPORT

## CONTACT US

WWW.FOREGENIX.COM/WEBSCAN
TEL: +44 845 309 6232

11TH JANUARY 2021

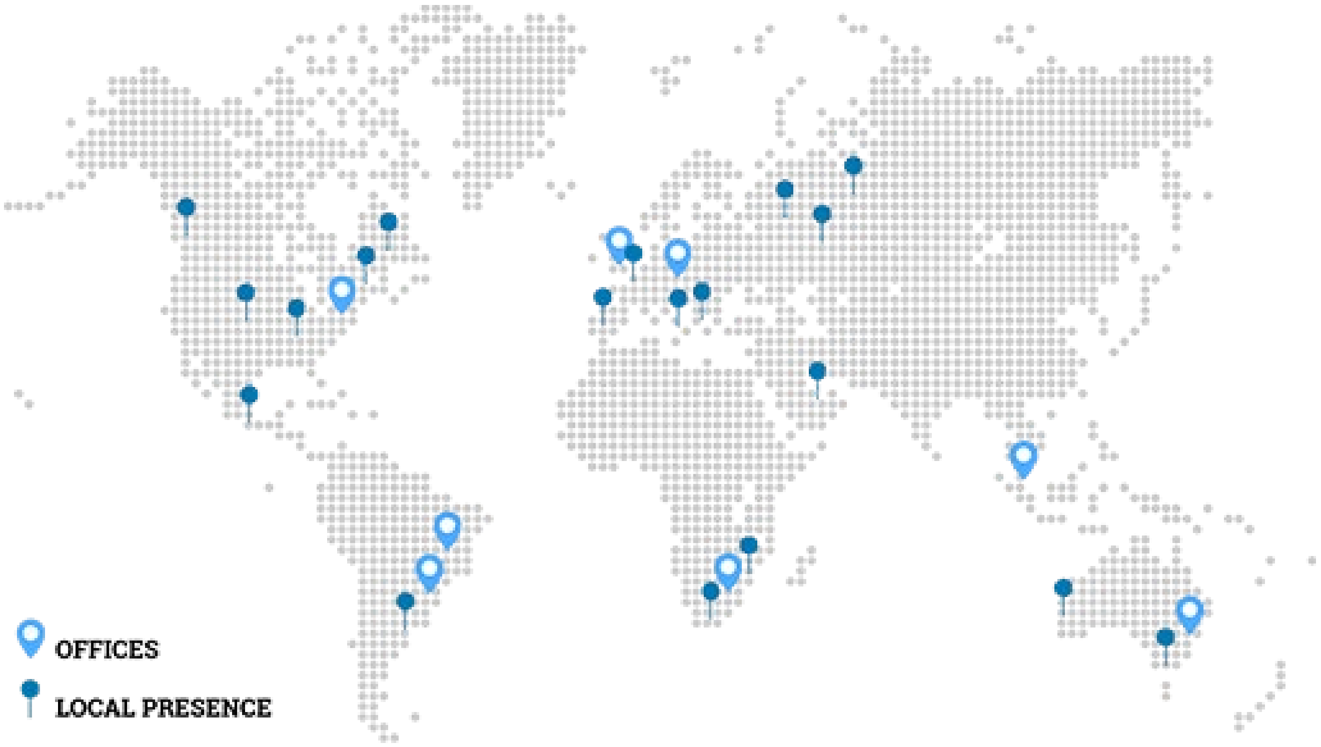
PRODUCED BY FOREGENIX

# 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

11TH JANUARY 2021

# OVERVIEW

## WHAT IS WEBSCAN?

We currently monitor over

**260,000**

Magento Merchants

**GLOBALLY**

WebScan is our comprehensive non-intrusive website scanning solution. It analyses 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

FOREGENIX

11TH JANUARY 2021

# OVERVIEW SUMMARY

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

Magento 1 websites have slightly **DECREASED**

**1,493** Magento websites are hacked, with card-harvesting malware.

**27%** of Magento 2 websites are High/Critical Risk

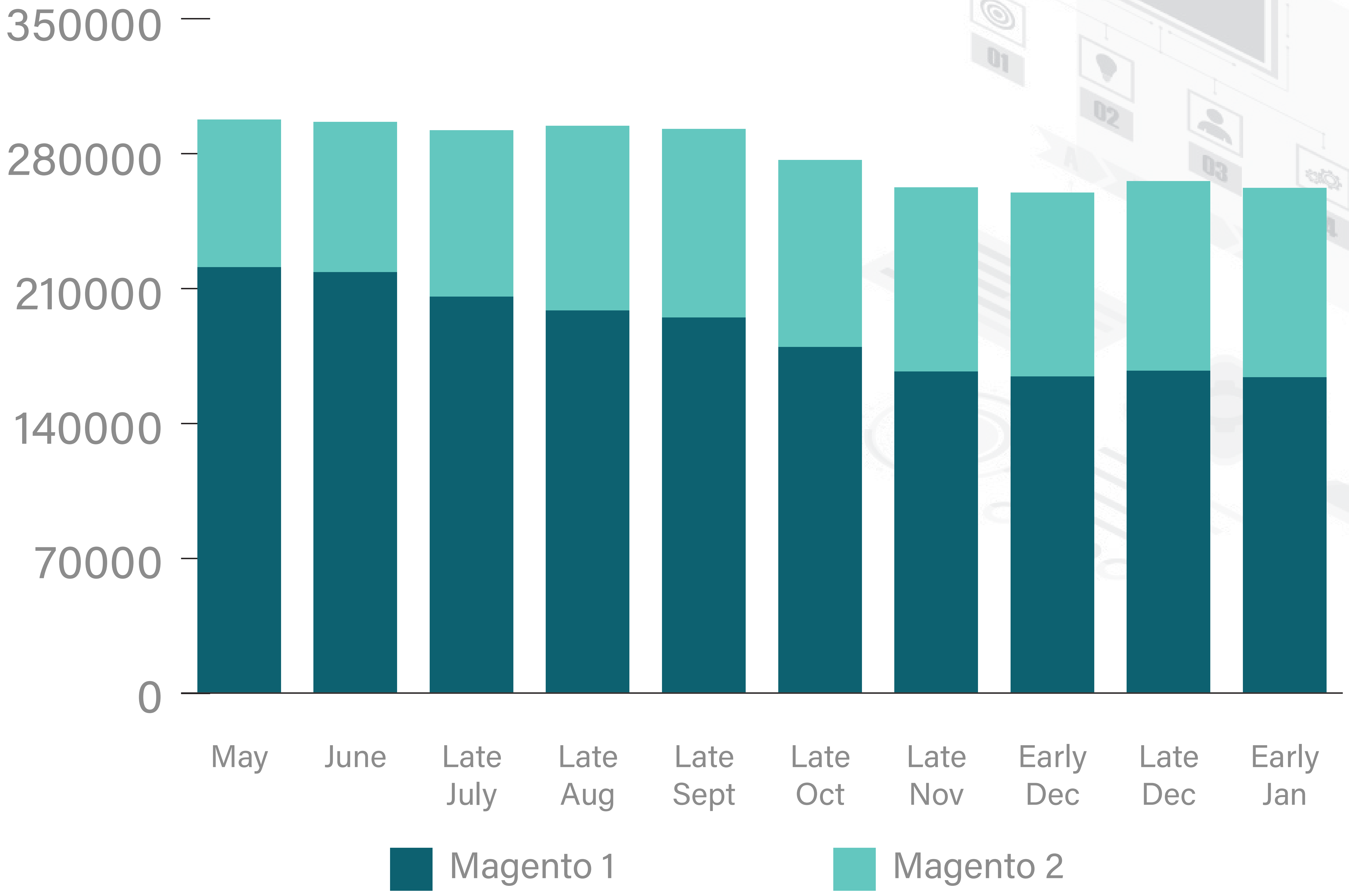
## MAGENTO 1 AND 2 REMAIN THE MOST TARGETED PLATFORMS BY CRIMINALS

Magento

11TH JANUARY 2021

# WEBSCAN RESULTS

## WEBSITE NUMBERS (ALL MAGENTO)



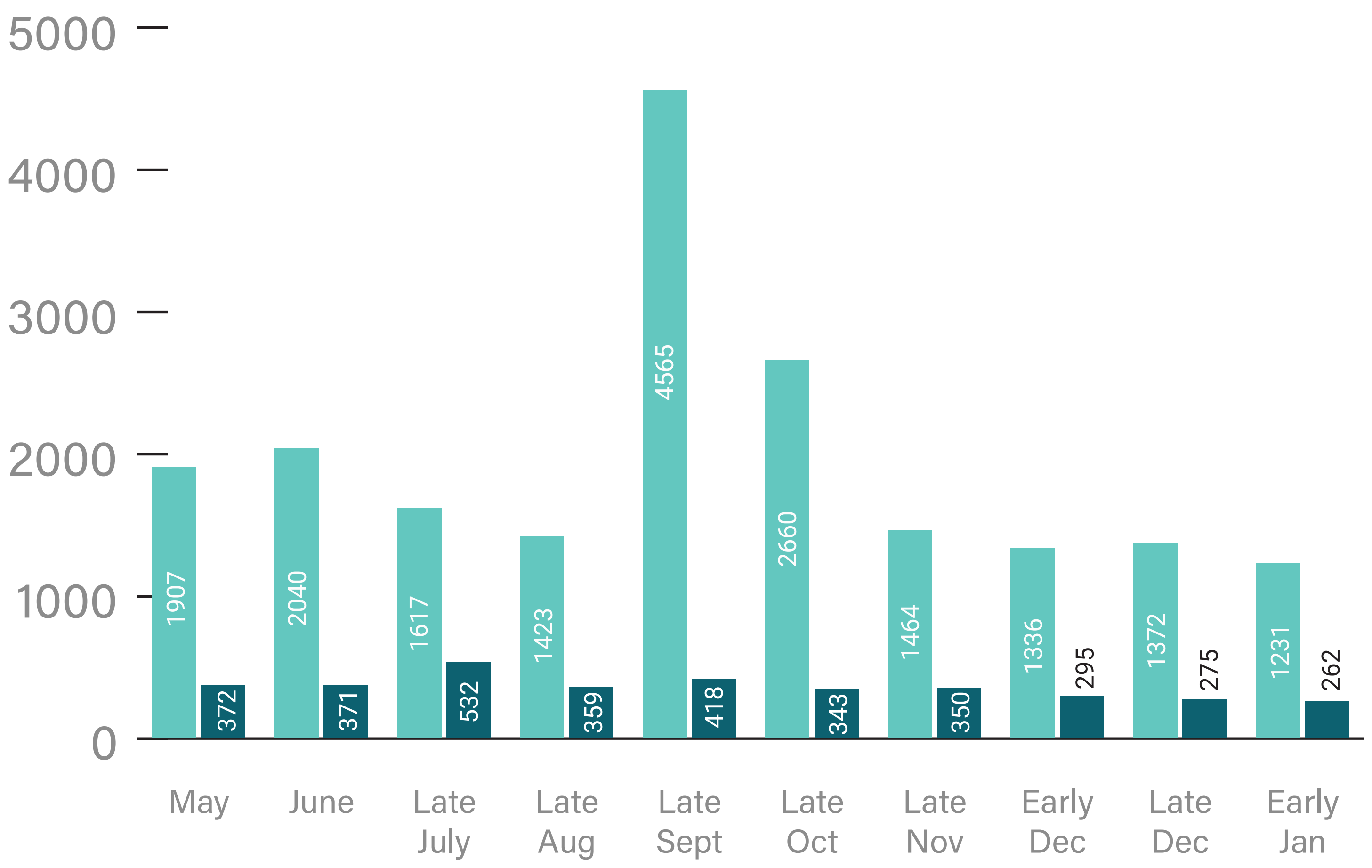
FOREGENIX

11TH JANUARY 2021

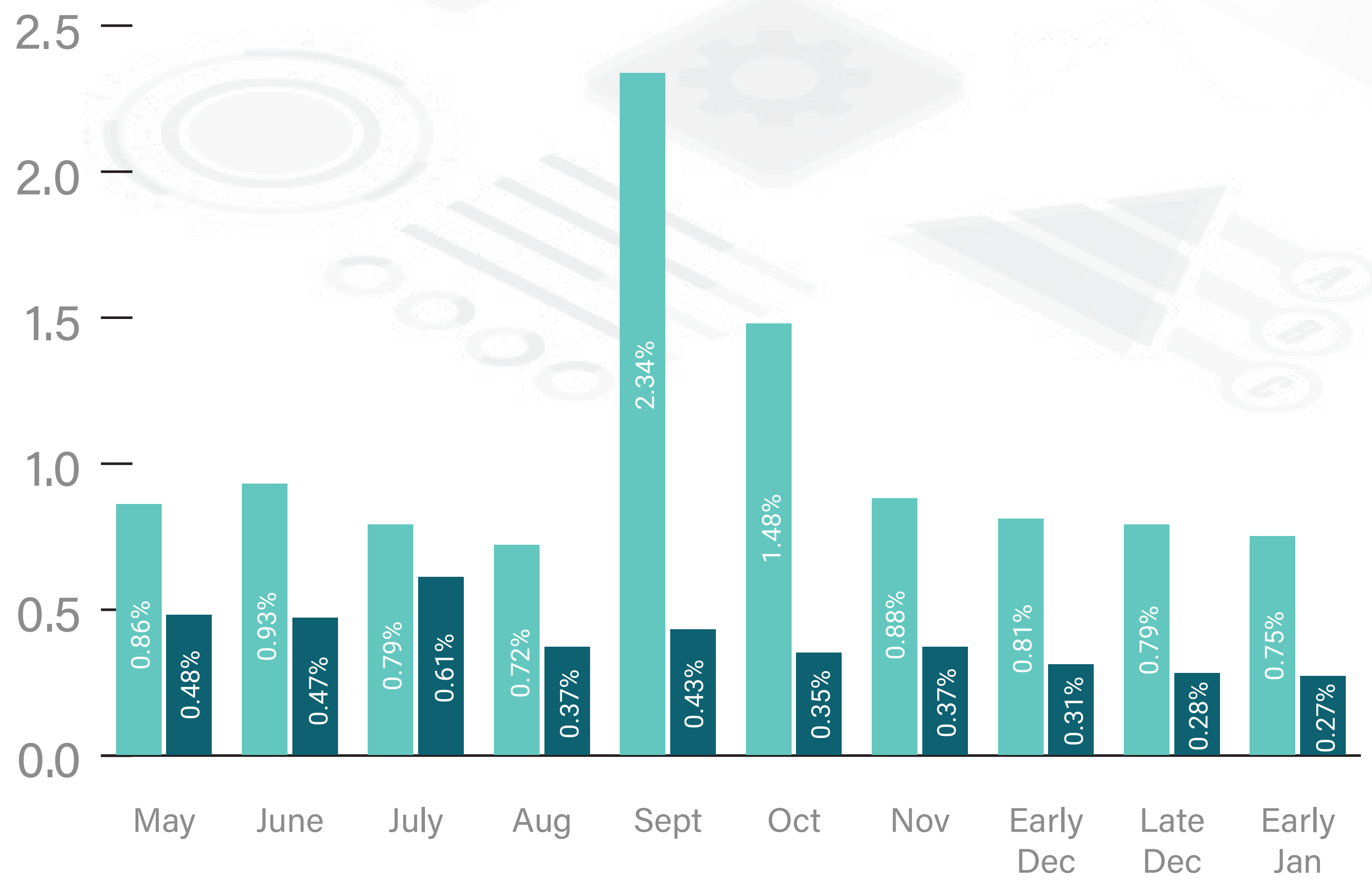
# WEBSCAN RESULTS CRITICAL RISK

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

## ACTUAL NUMBERS



## PERCENTAGE OF TOTAL SITES



🟩 Magento 1 ■ Magento 2

FOREGENIX

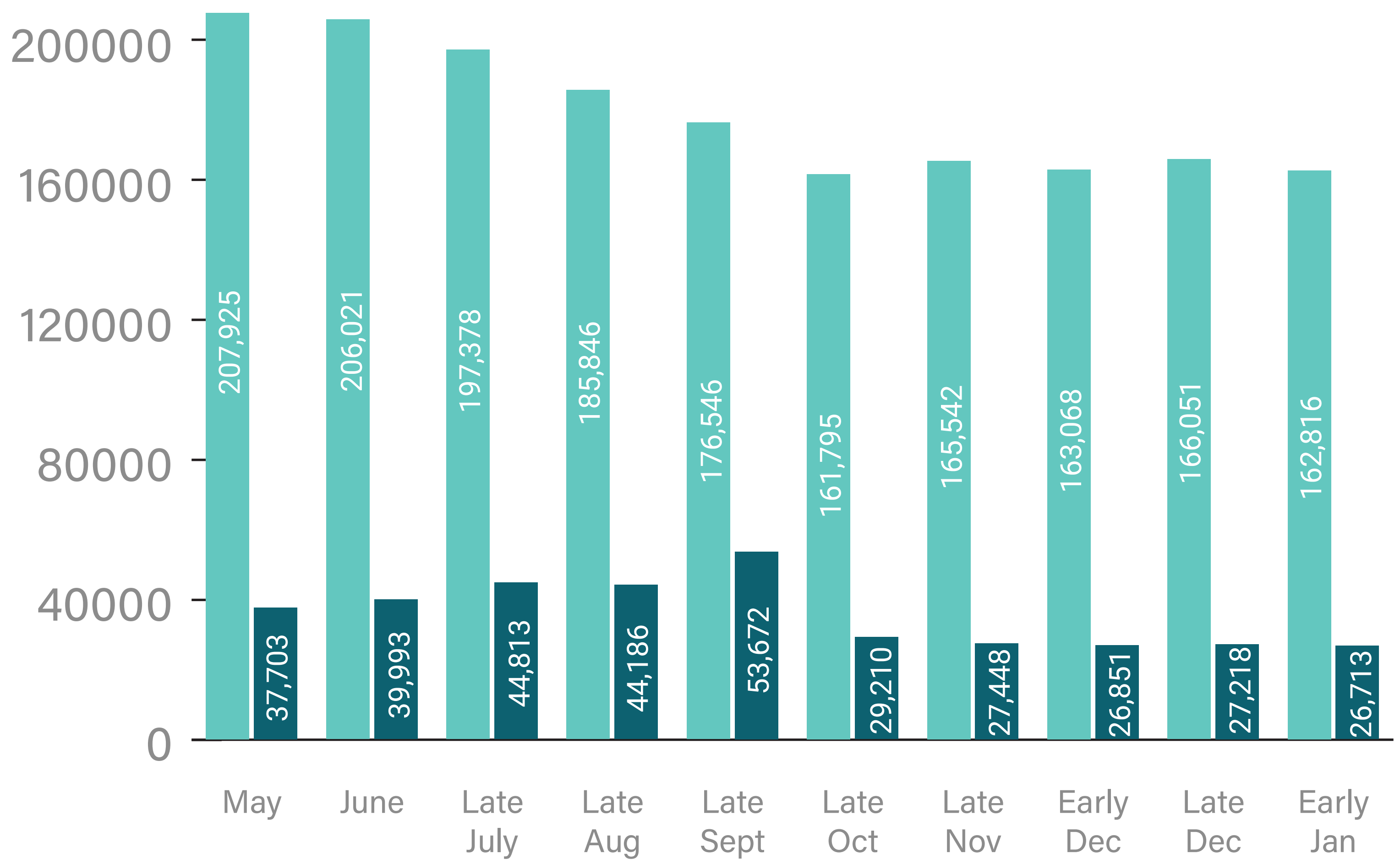
11TH JANUARY 2021

# WEBSCAN RESULTS HIGH RISK

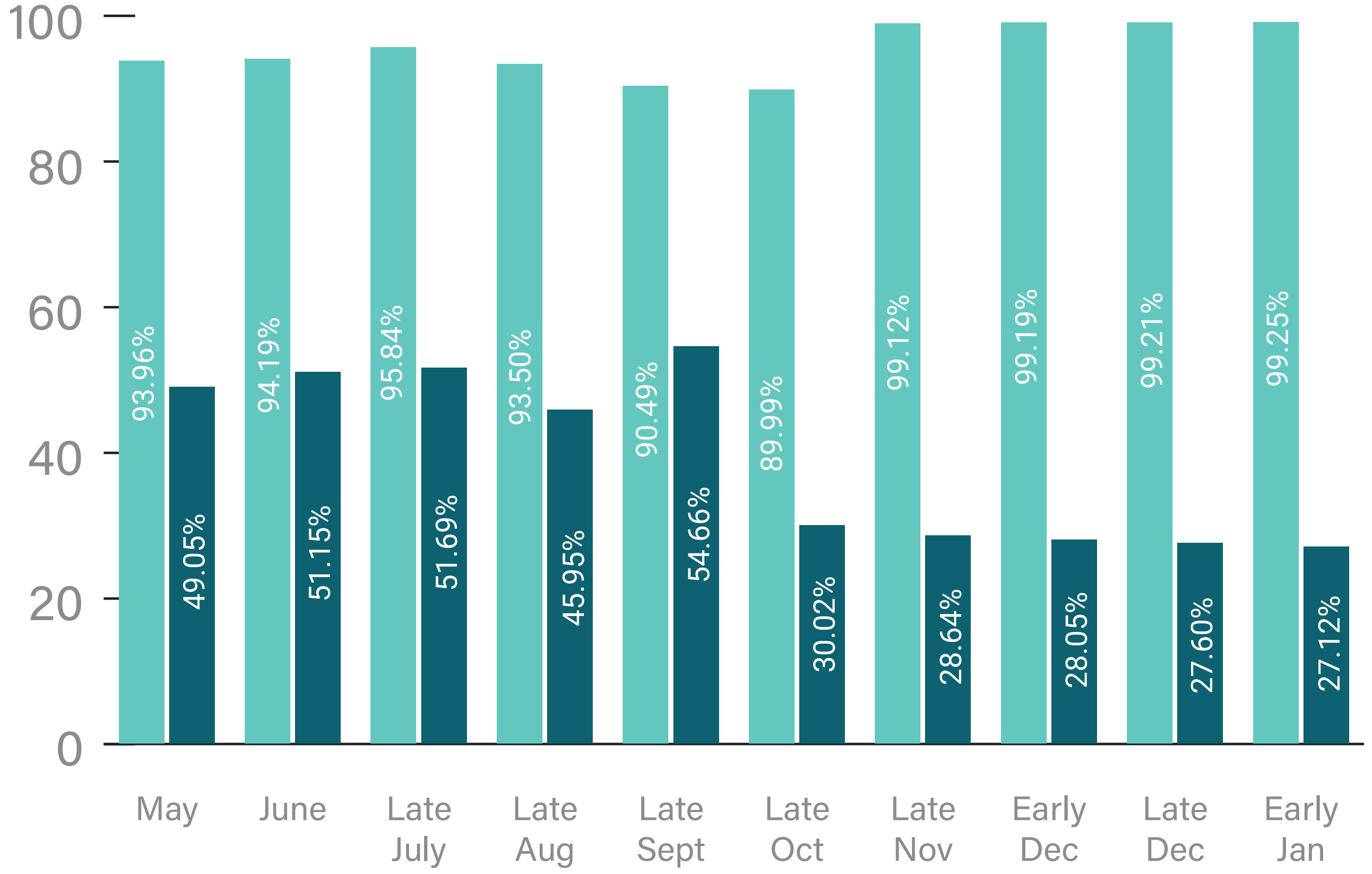
Websites identified as High Risk have significant security issues that make them very vulnerable to criminals. The sites have one or more of the following:

- 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

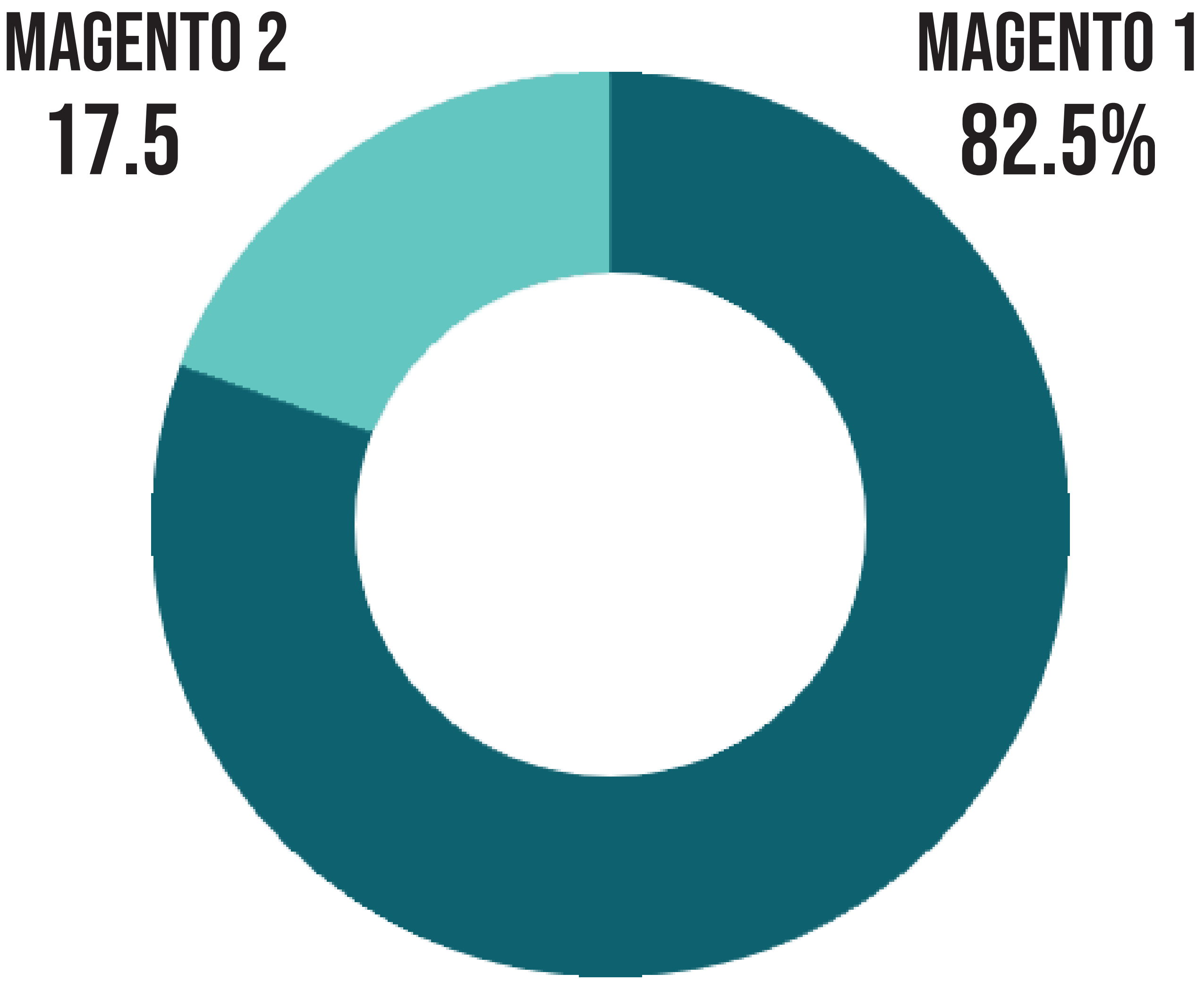


🟩 Magento 1 🟦 Magento 2

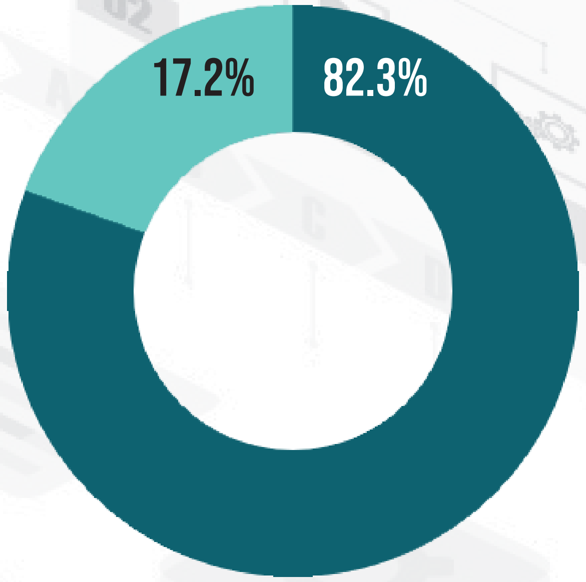
FOREGENIX

11TH JANUARY 2021

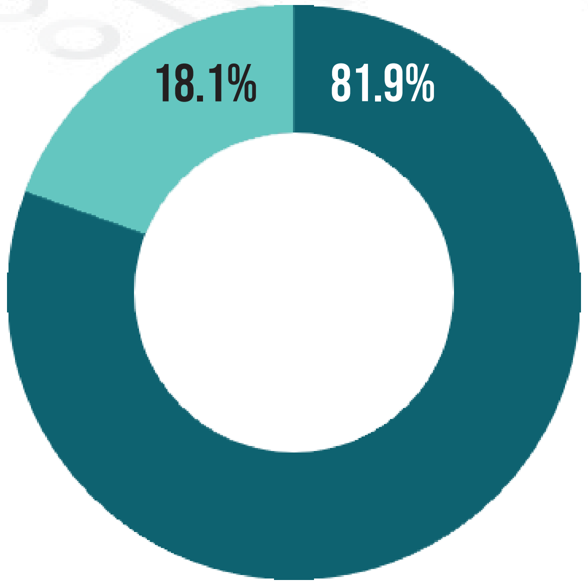
# WEBSCAN RESULTS CARD-HARVESTING MALWARE DISTRIBUTION



TWO WEEKS AGO



ONE MONTH AGO



FOREGENIX

11TH JANUARY 2021

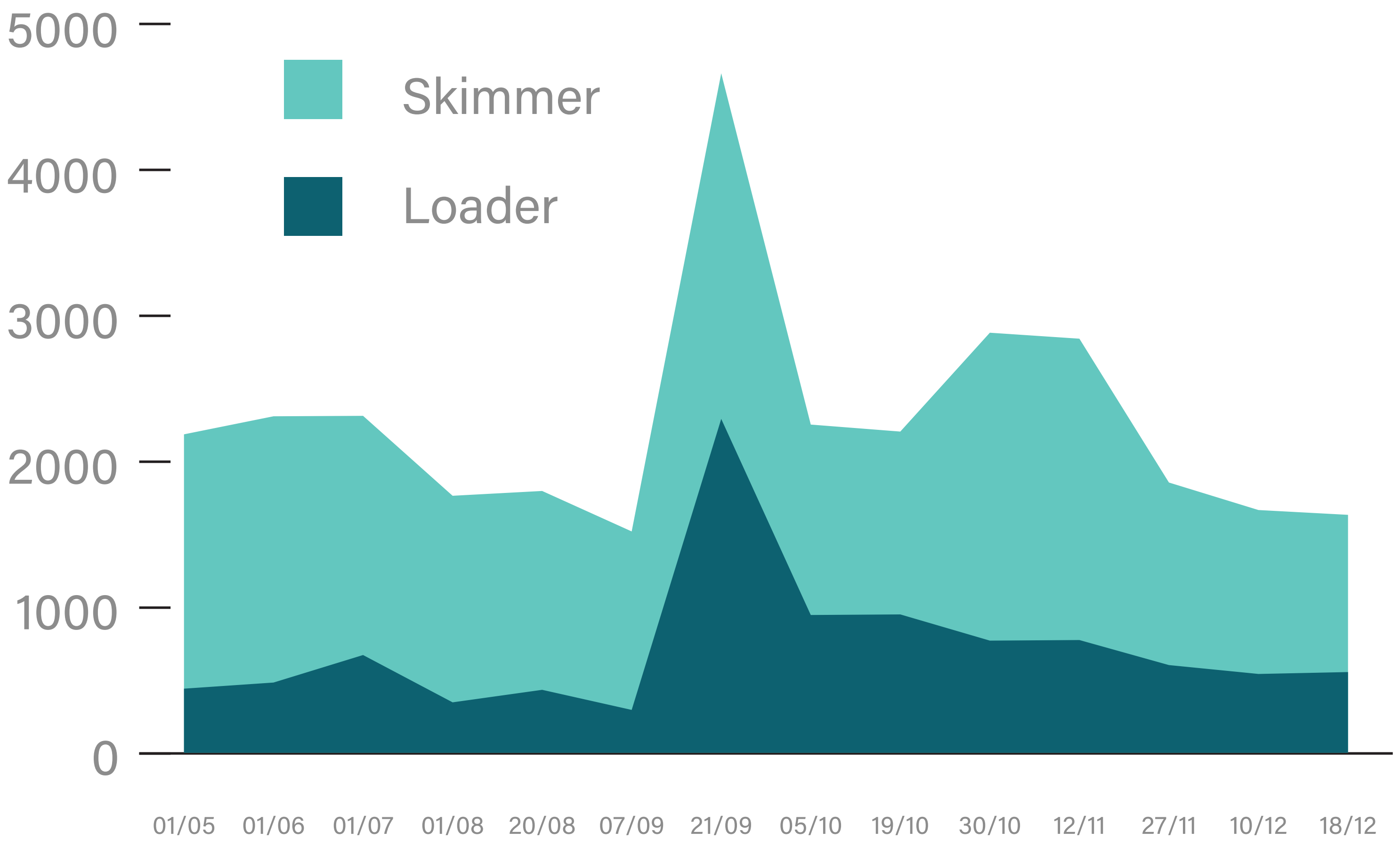
# WEBSCAN RESULTS MAGENTO 1 & 2 - LOADERS & SKIMMERS

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

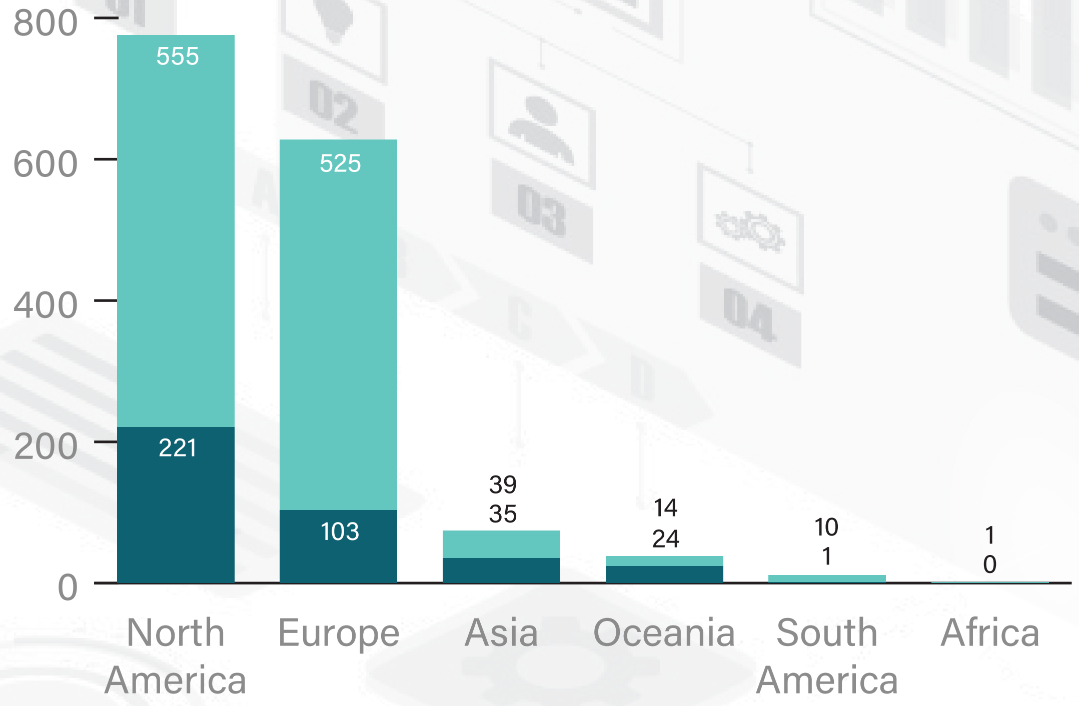
**Loaders** - are small pieces of code designed to load in additional malicious code onto a website.

**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.

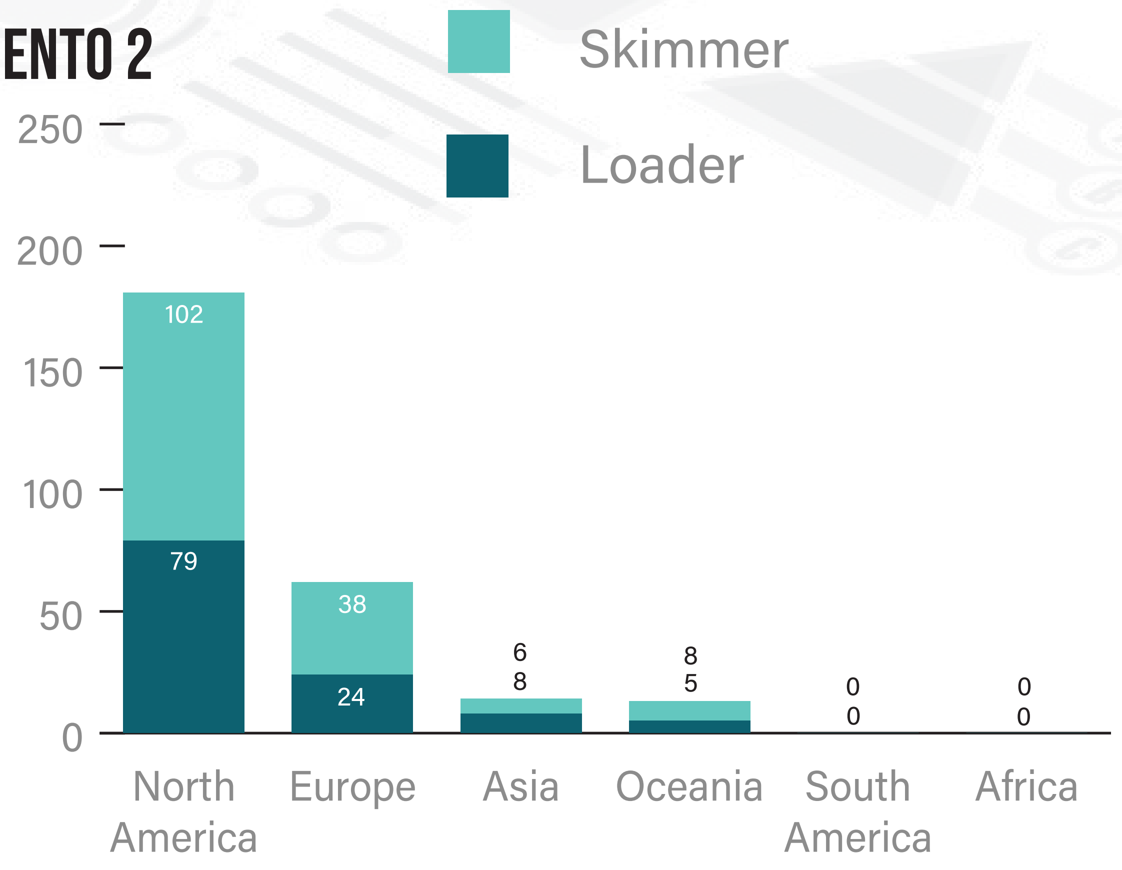
The charts to the right show which regions in the world have the highest infection rate, and below shows change over time.



## MAGENTO 1



## MAGENTO 2



FOREGENIX

11TH JANUARY 2021

# WEBSCAN RESULTS MAGENTO 1 & 2 - FRAMEWORK ISSUES

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

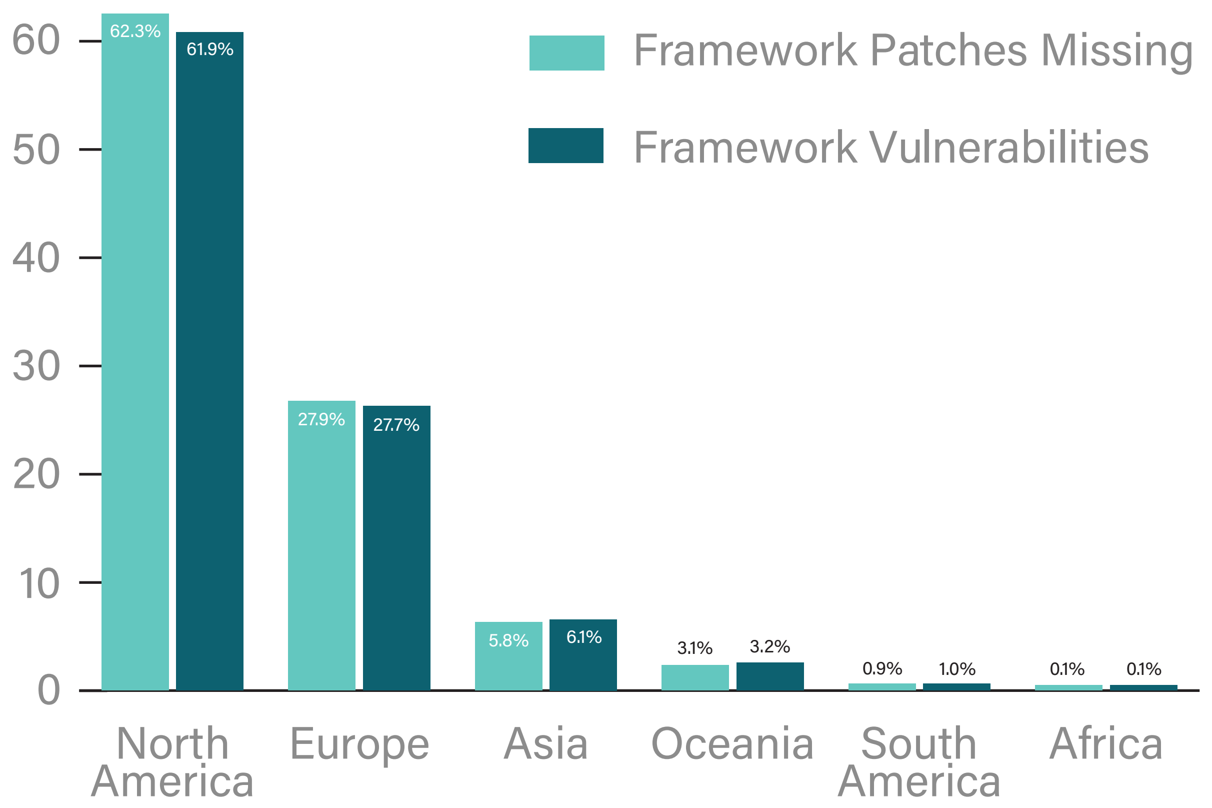
“**Framework security patches missing**” means a website is missing security patches/updates that are already available.

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

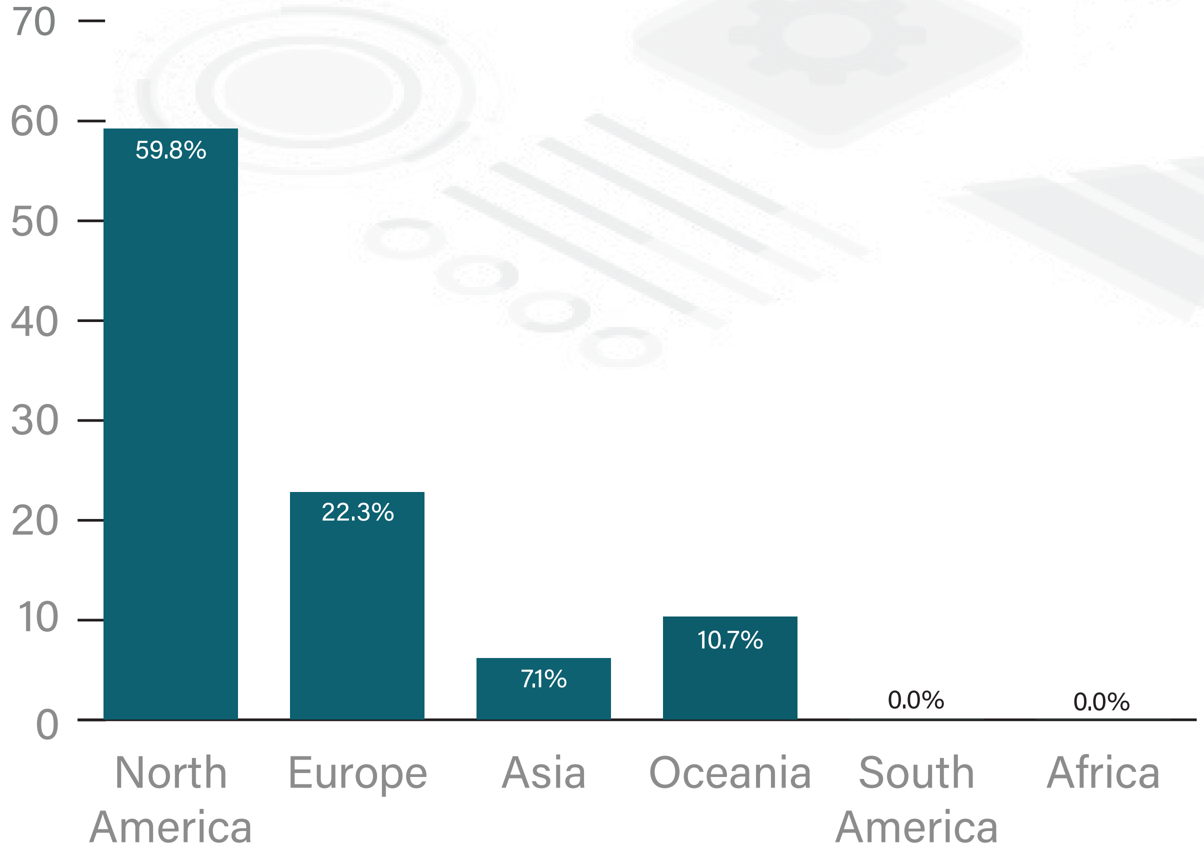
It’s good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having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



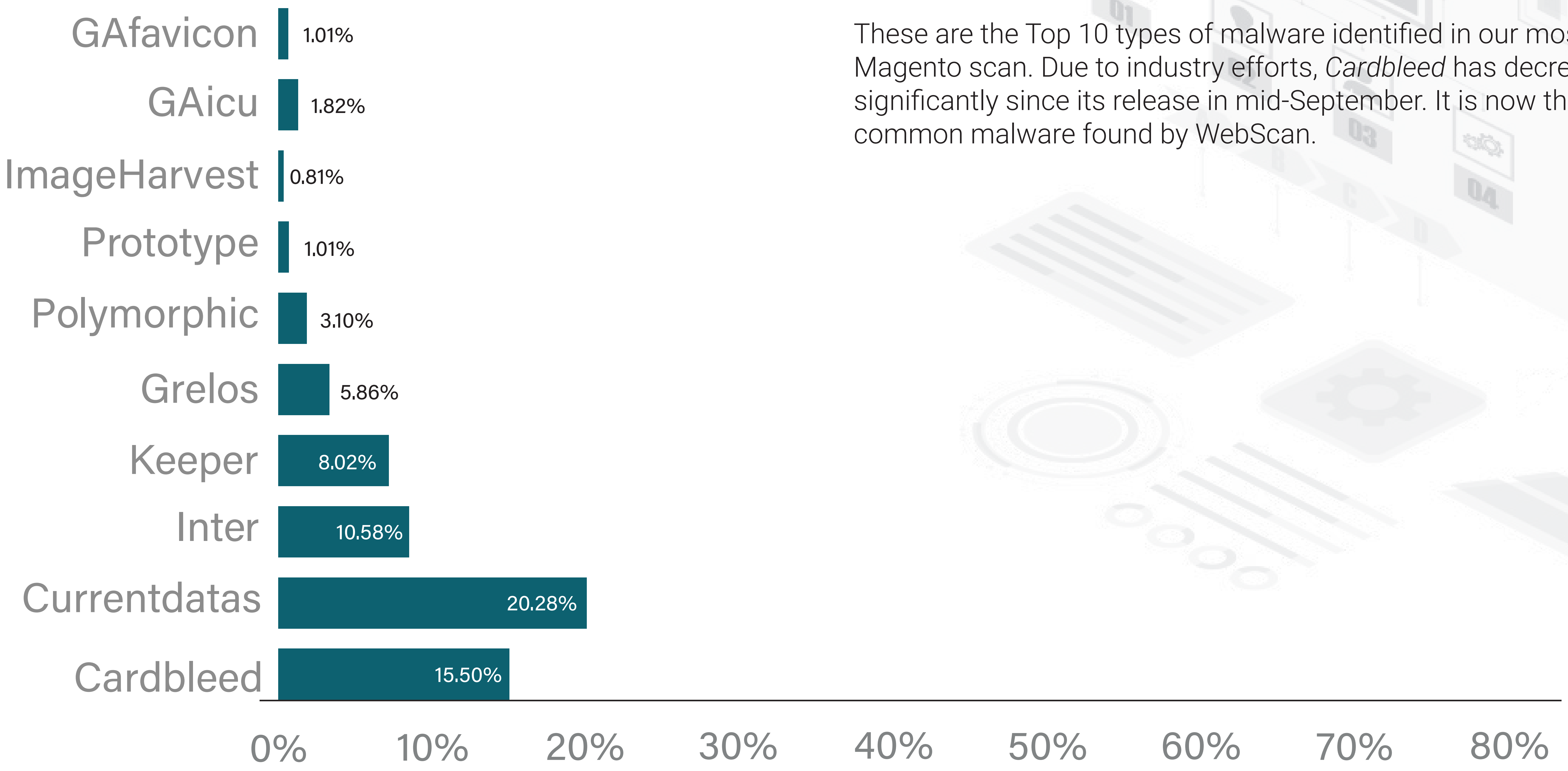
## MAGENTO 2 PERCENTAGES



FOREGENIX

11TH JANUARY 2021

# WEBSCAN RESULTS MALWARE TYPES



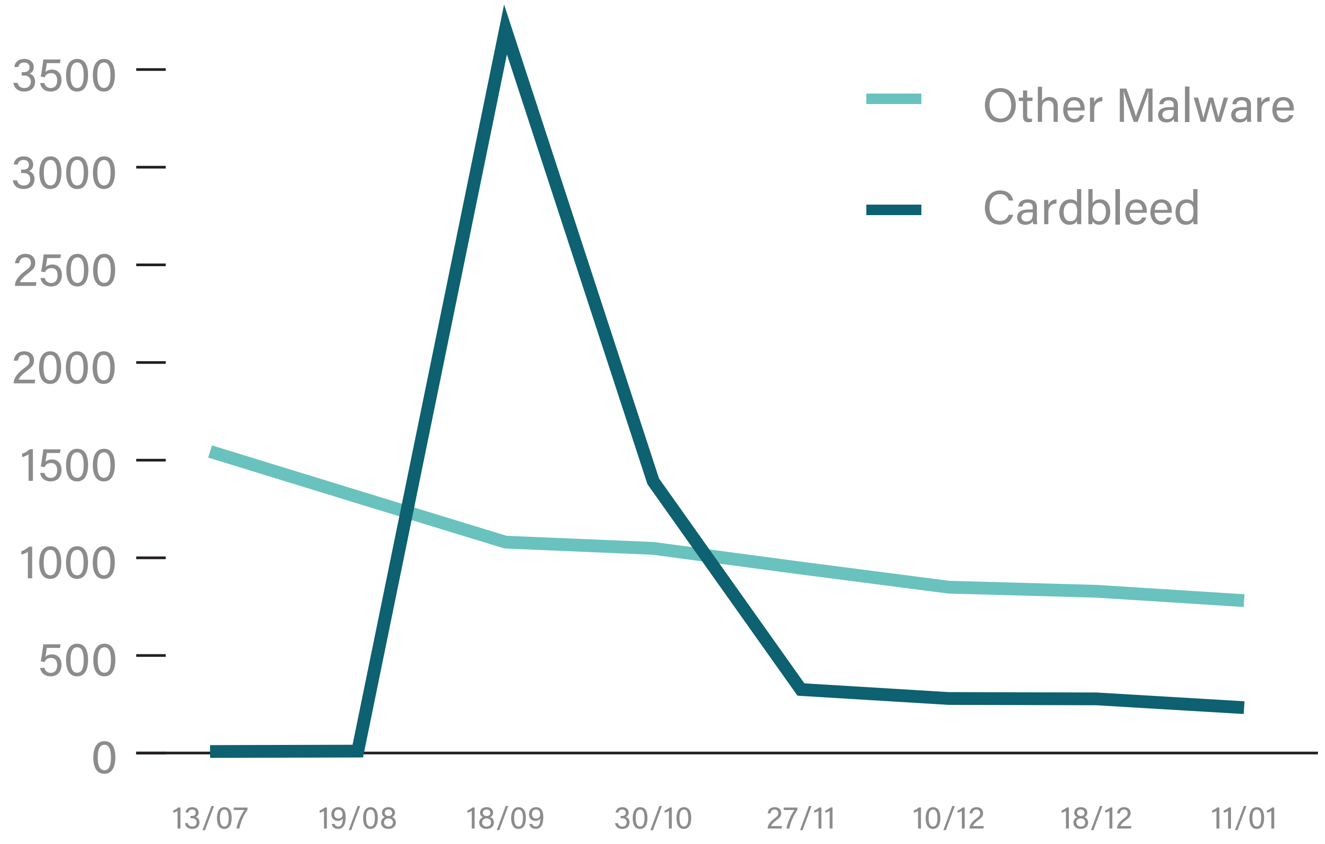
These are the Top 10 types of malware identified in our most recent Magento scan. Due to industry efforts, *Cardbleed* has decreased significantly since its release in mid-September. It is now the second most common malware found by WebScan.

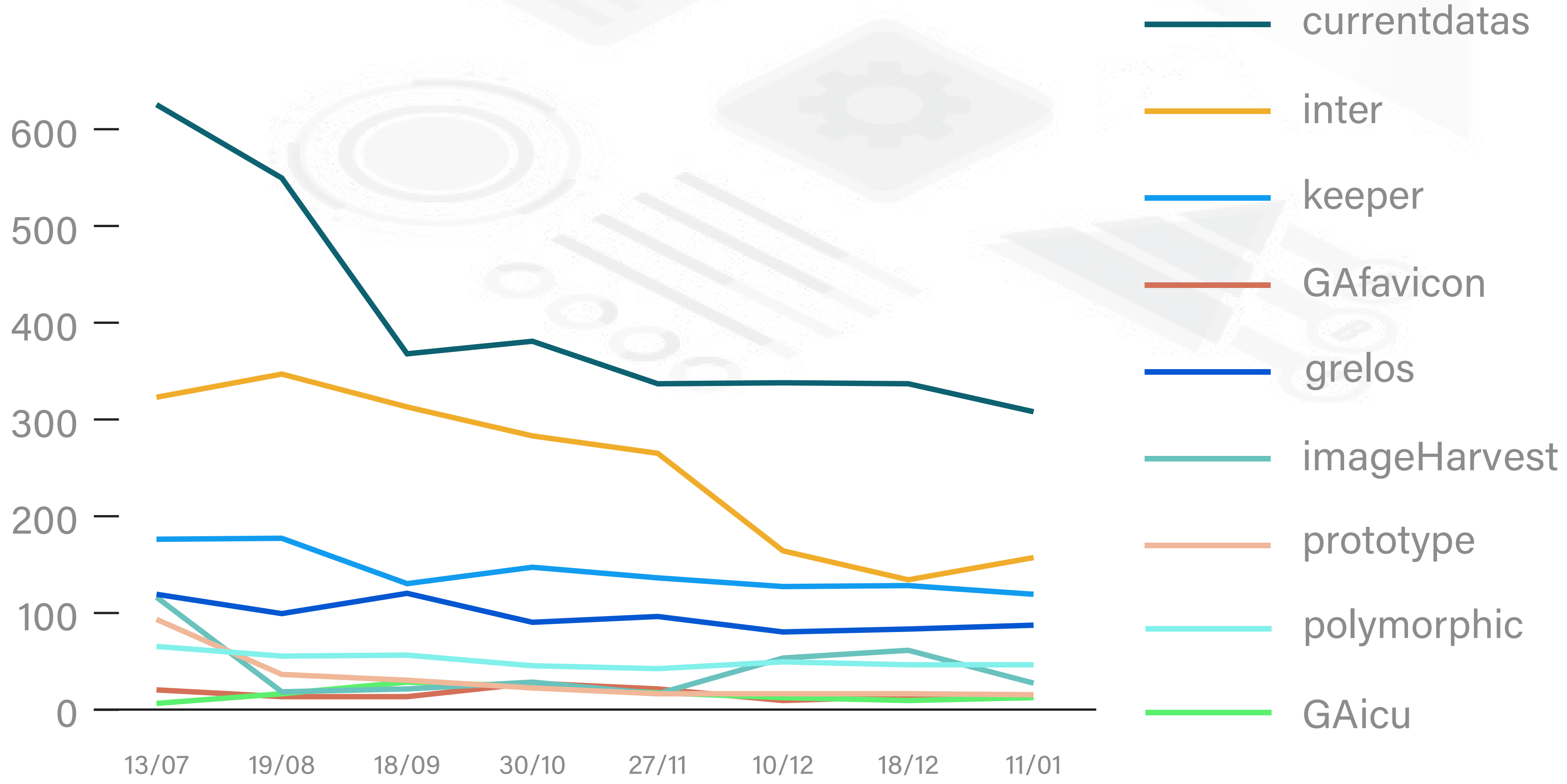
FOREGENIX

11TH JANUARY 2021

# 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

11TH JANUARY 2021

# MALWARE ANATOMY IMAGEHARVEST

Some malware campaigns that we have observed use image tags to exfiltrate the stolen data to the attacker's server. This campaign in particular attempts to harvest both card data and admin credentials.

The skimming code is placed in a JavaScript file on the infected site; either a new file is created or the code is appended to a legitimate JavaScript file. The code first checks whether the web browser's developer tools are open. If they are, then the rest of the code will not execute in an attempt to hide the malicious activity from analysts or developers. Otherwise, the code will search the page's ***`input`***, ***`select`***, and ***`textarea`*** elements for any data inputted by the user. If the current URL contains the word "***`checkout`***" or "***`admin`***", an ***`Image`*** element will be created with the ***`src`*** set to a Base64-encoded URL. The user's data is added to this URL as part of the query string and the data is sent off to the attacker's server when this "image" is loaded.

The full URL is usually in the form ***`https://[domain]/?rnd=[random number]&data=[stolen data]&loc=[infected site]`***. This allows the attacker to see which site the data was stolen from. It also allows the attacker to easily change which domain the data is sent to when they modify the code for future infections, should any of their infrastructure be taken down. This campaign has been seen using both compromised sites and purpose-made sites to receive the stolen data.

# MALWARE ANATOMY GAFAVICON

One popular technique among card skimming malware is to disguise their code as Google Analytics code. This campaign contains a reference to the legitimate Google Analytics URL, however instead of posting the data to this URL it uses this string to generate the malicious script location.

The code will contain an array of numbers and a string containing the Google Analytics URL with some extra characters on the end, e.g.

```
var userID = [26, 26, 9, 11, 9, 11, 16, 15, 14, 15, 16, 16, 19, 18, 19, 23, 21, 22, 23, 24, 25, 26, 27, 15, 28,
19, 23, 24, 14, 22, 19, 23, 24];
l1ll = ‘//www.google-analytics.com/fvrphd’
```

The script location is generated by looking up the nth character of the Google Analytics URL for each number in this array. In the above example, it first looks up the 26th character (/), then the 26th character again (/), then the 9th character(g), etc. The final result is the URL “`//gegelanallitics[.]com/favicon.ico`”. While different domains have been observed as part of this campaign, the URLs all end in “`favicon.ico`”.

Requesting this file directly will just return a fake “Not Found” page. However if the file is requested while the user is on the checkout page, it will serve an image file instead. The skimming code is stored within the EXIF data of this image, in the “Copyright” tag.

# OUR INSIGHTS

After a slight increase in the number of Magento websites, the number is going down once again. As a recap, the number of Magento 1 (M1) fell by 1.99%, and Magento 2 (M2) by 0.14%.

The number of websites with card harvesting malware also decreased, which is a good indication that the industry is moving and improving its cybersecurity.

Even with the slight decrease of M1 websites, the number is still too high, especially if you consider that the platform has far surpassed its end of life; in July of last year. It is just a matter of time before another *Cardbleed*-attack happens once more.

Although it might not be so easy to migrate to M2, it is possible to take some simple steps in improving your website security. Check out for free guidance on how to keep your website secure on our Magento Security Insights page.

And, do not forget that, for extra peace of mind, we recommend using a website security solution, as well as investing in cyber insurance.

## 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