MAGENTO WEBSITE SECURITY REPORT

CONTACT US

WWW.FOREGENIX.COM/WEBSCAN

TEL: +44 845 309 6232

5TH OCTOBER 2020

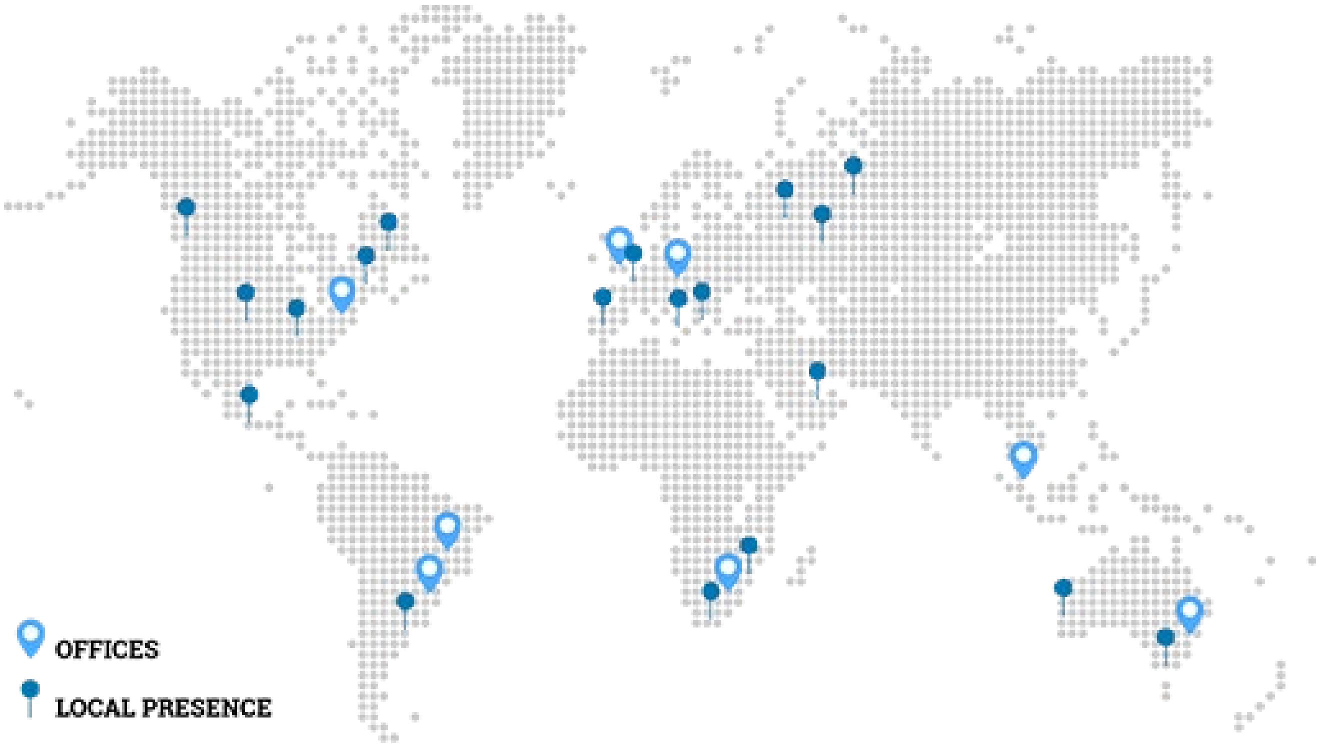
PRODUCED BY FOREGENIX

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

5TH OCTOBER 2020

OVERVIEW WHAT IS WEBSCAN?

We currently monitor over

300,000

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:

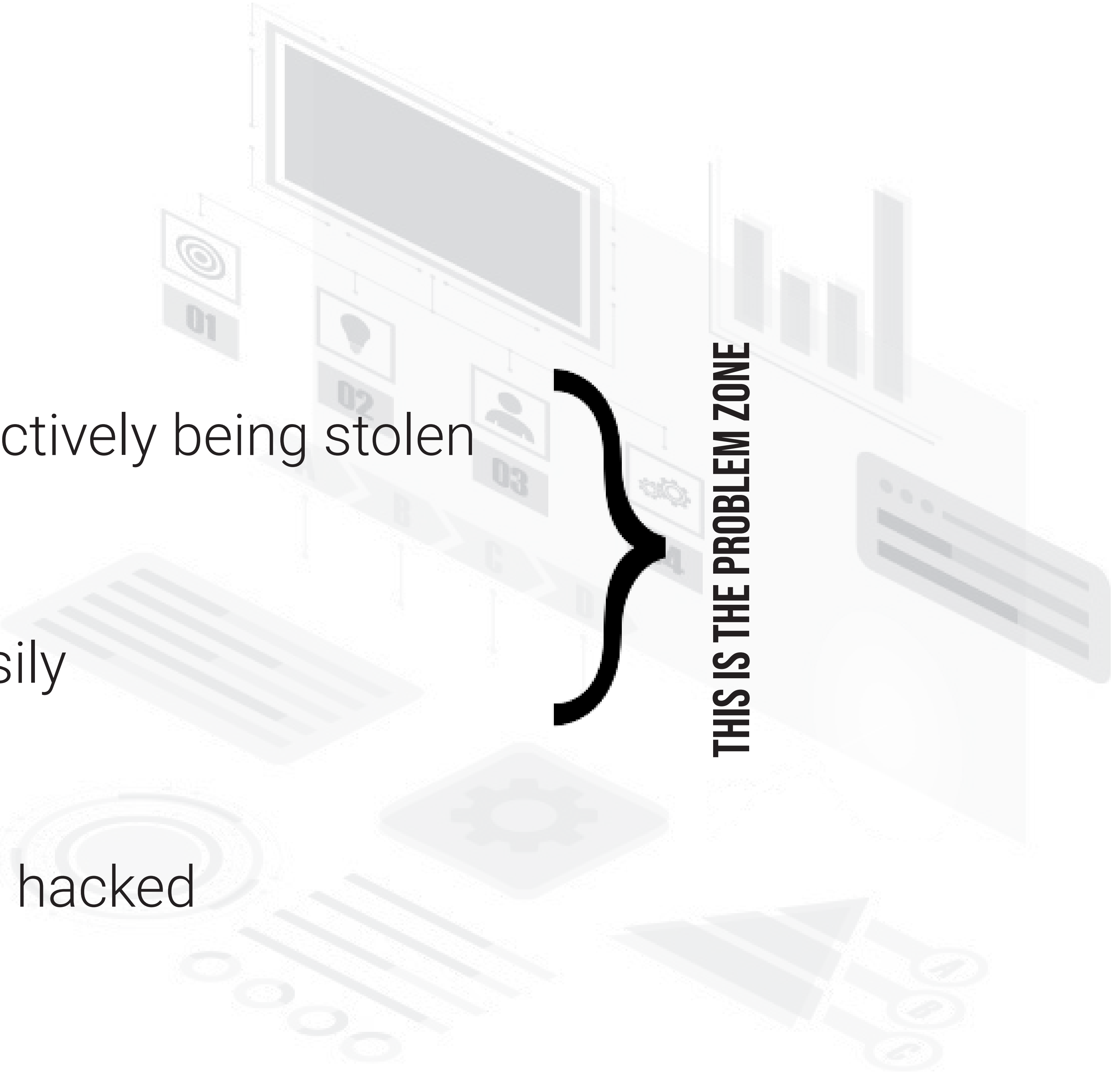
- Malware (including card skimmers)
- Platforms and patching information
- SSL issues

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



FOREGENIX

5TH OCTOBER 2020

OVERVIEW SUMMARY

Nearly **200,000** websites remain on the Magento 1 Platform

Significant **DECREASE** in the number of Magento websites

93% of Magento 1 websites are High/Critical Risk

55% of Magento 2 websites are High/Critical Risk

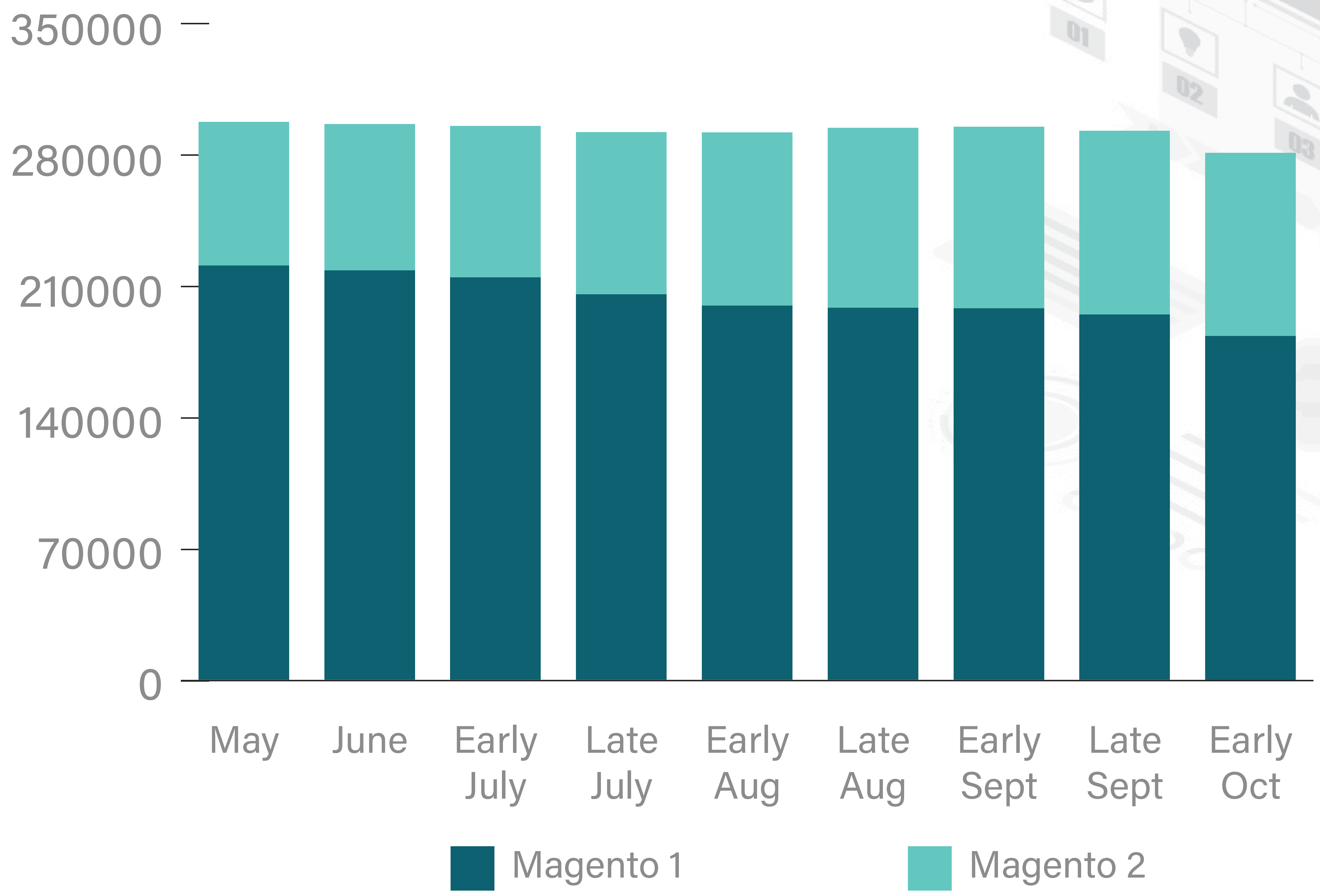
MAGENTO REMAINS THE MOST TARGETED PLATFORM BY CRIMINALS

Magento

FOREGENIX

5TH OCTOBER 2020

WEBSCAN RESULTS WEBSITE NUMBERS (ALL MAGENTO)



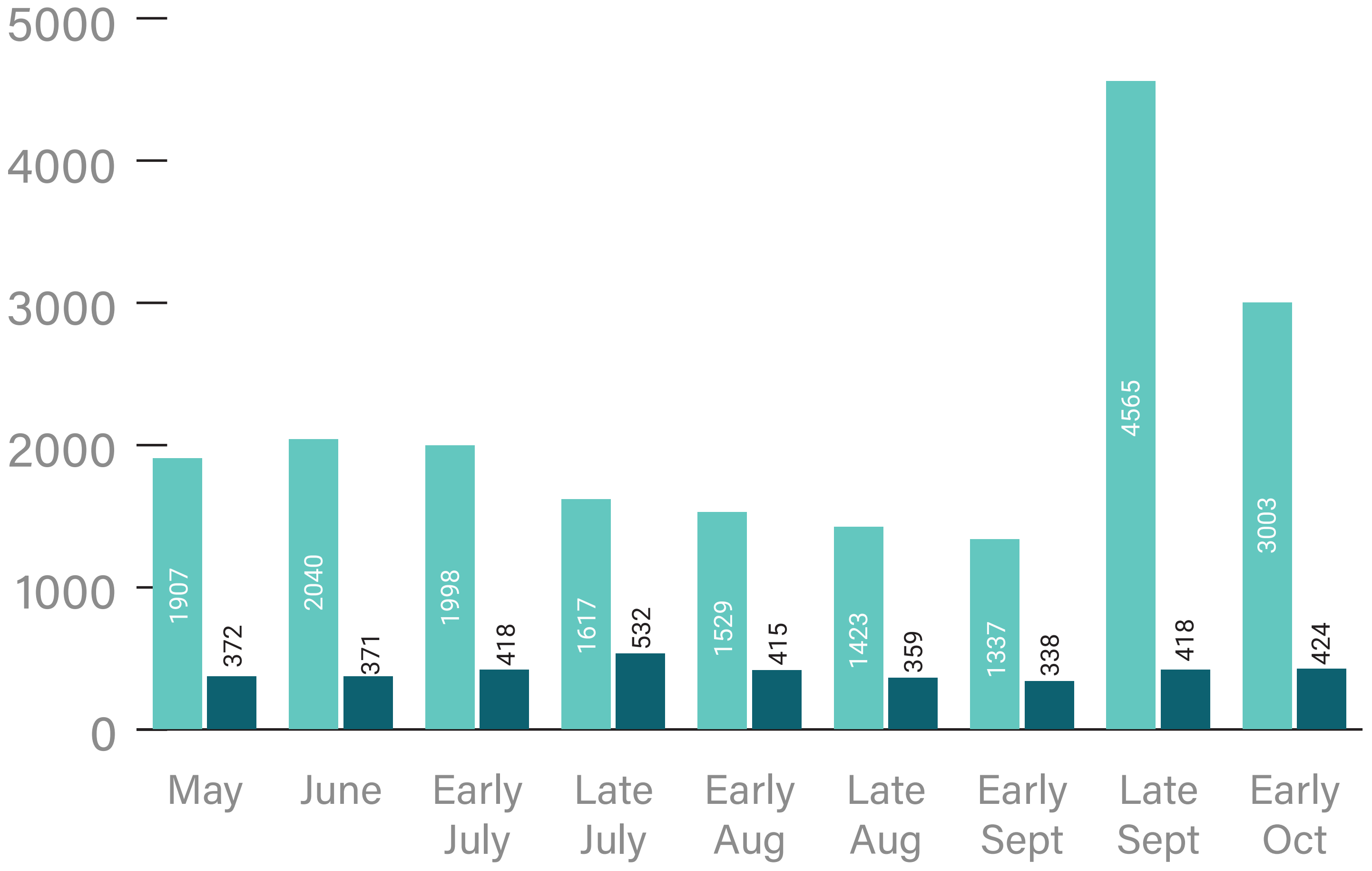
FOREGENIX

5TH OCTOBER 2020

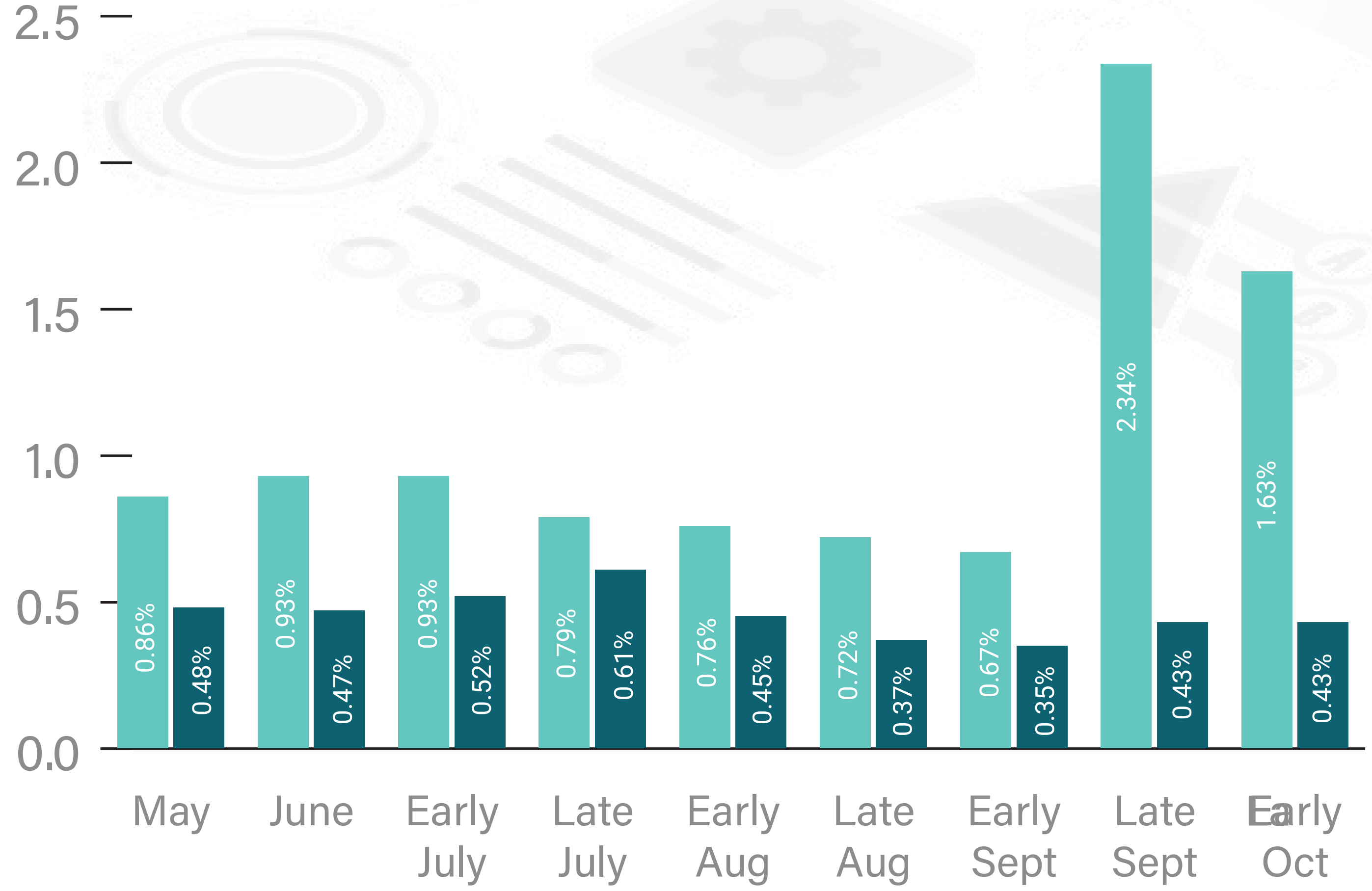
WEBSCAN RESULTS CRITICAL RISK

Websites with Critical Risk have already been hacked (with card data being actively stolen). This month we have seen a significant drop in the % of hacked Magento 1 and 2 websites, but this number is still much bigger than usual.

ACTUAL NUMBERS



PERCENTAGE OF TOTAL SITES



▨ Magento 1 ■ Magento 2

FOREGENIX

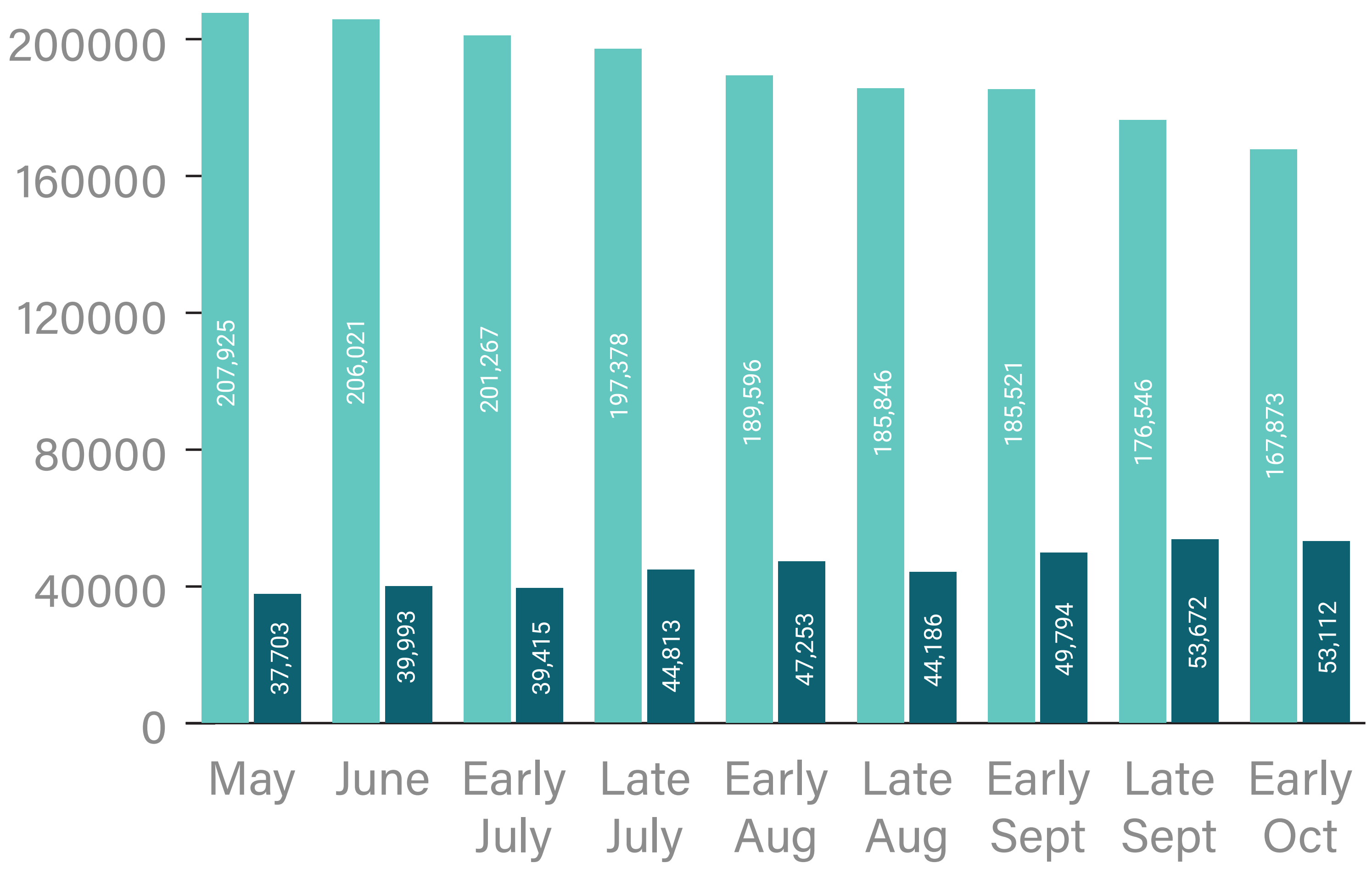
5TH OCTOBER 2020

WEBSCAN RESULTS HIGH RISK

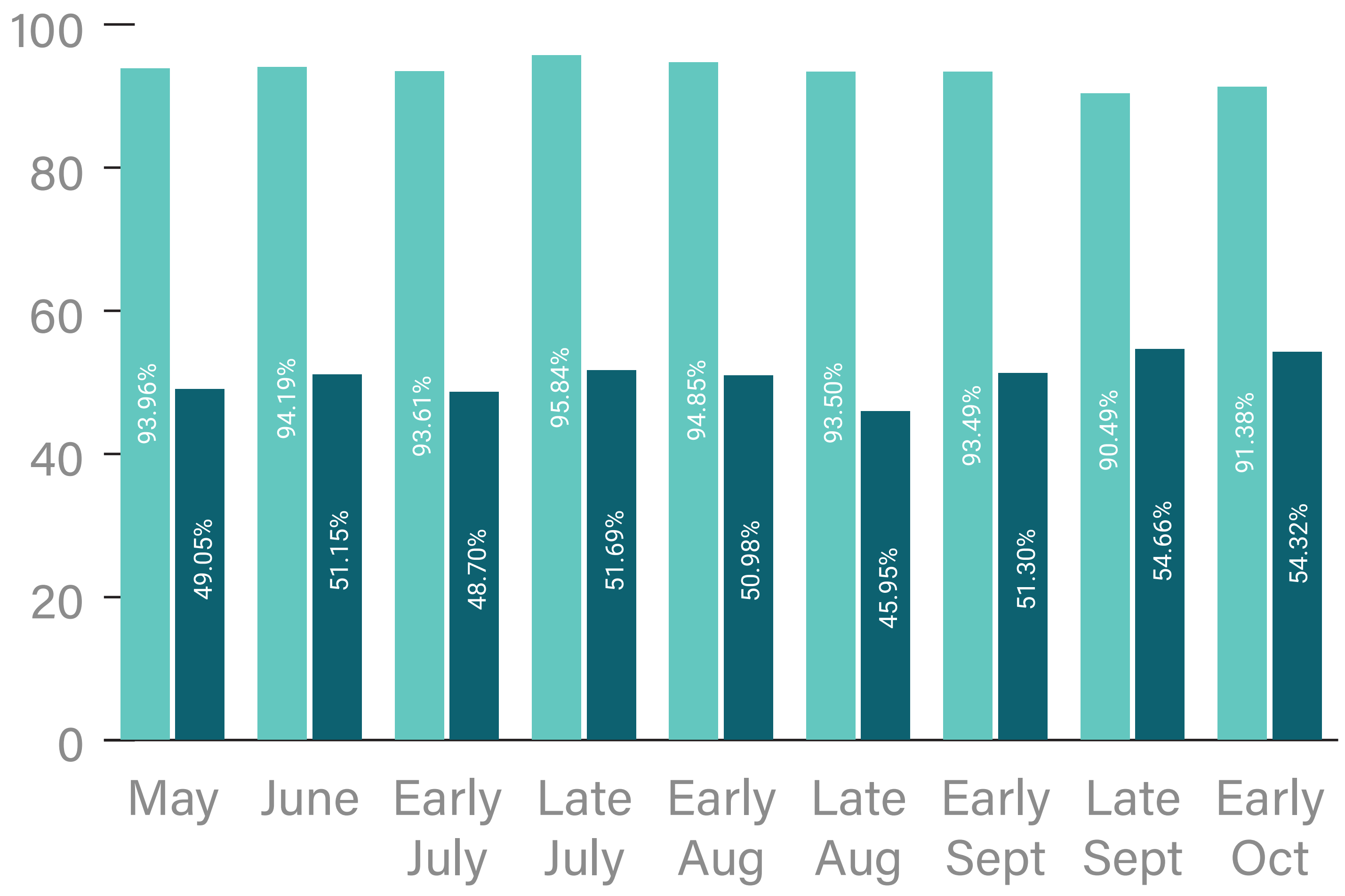
Websites with High Risk have significant security issues that make them very vulnerable to criminals.
The sites have one or more of the following:

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

ACTUAL NUMBERS



PERCENTAGE OF TOTAL SITES



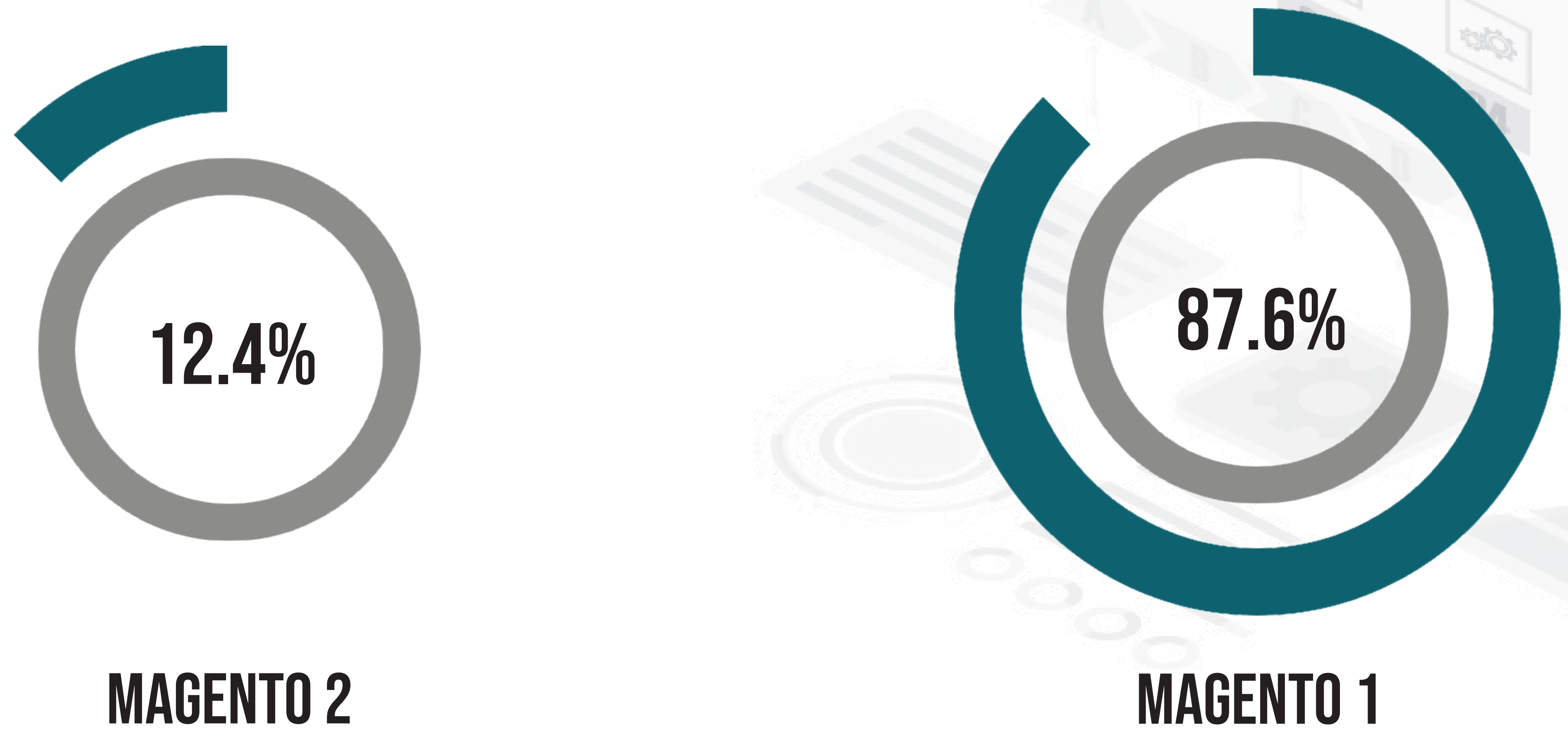
🟩 Magento 1 ■ Magento 2

FOREGENIX

5TH OCTOBER 2020

WEBSCAN RESULTS

CARD-HARVESTING MALWARE DISTRIBUTION



5TH OCTOBER 2020

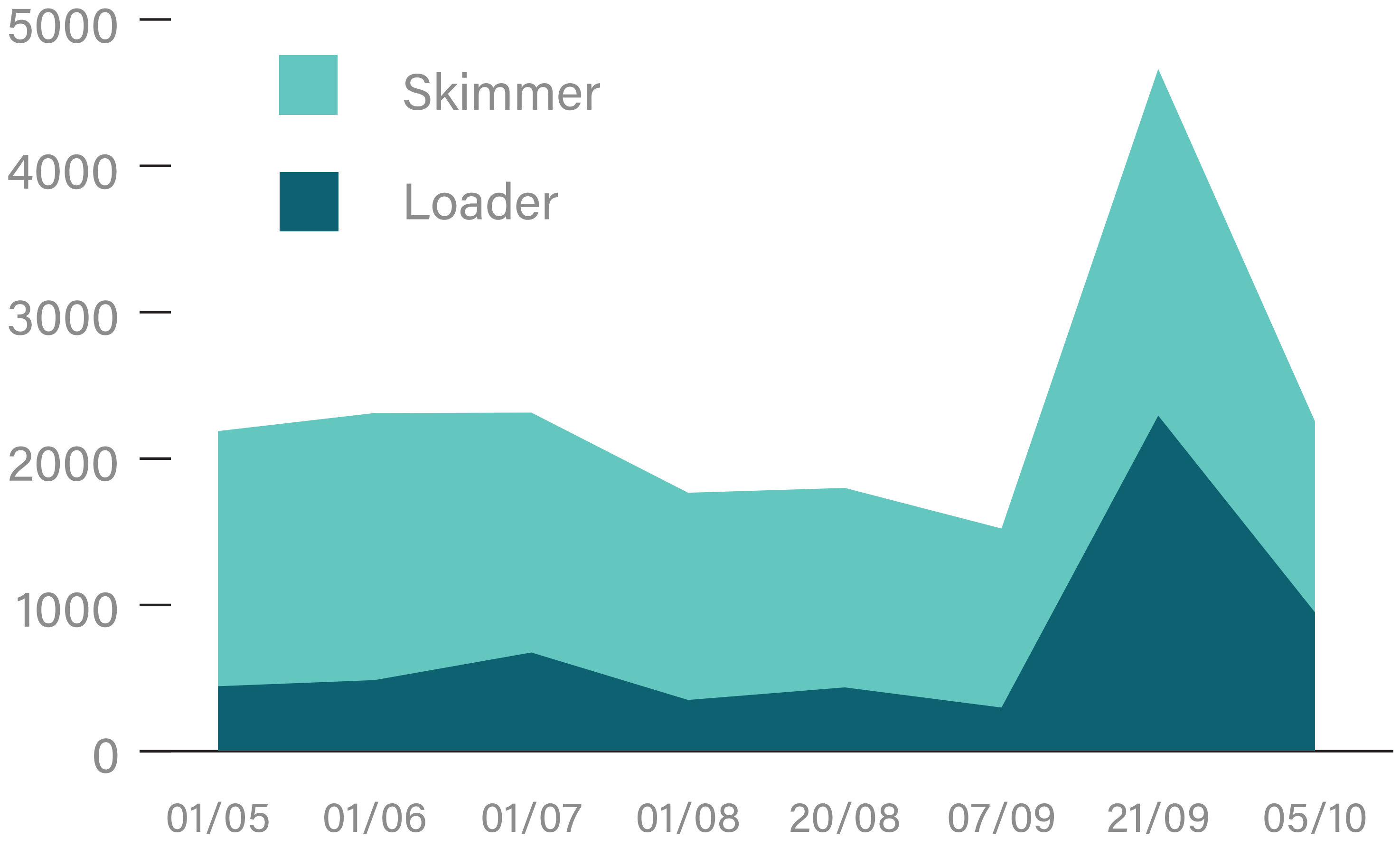
WEBSCAN RESULTS MAGENTO 1 & 2 - LOADERS & SKIMMERS

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

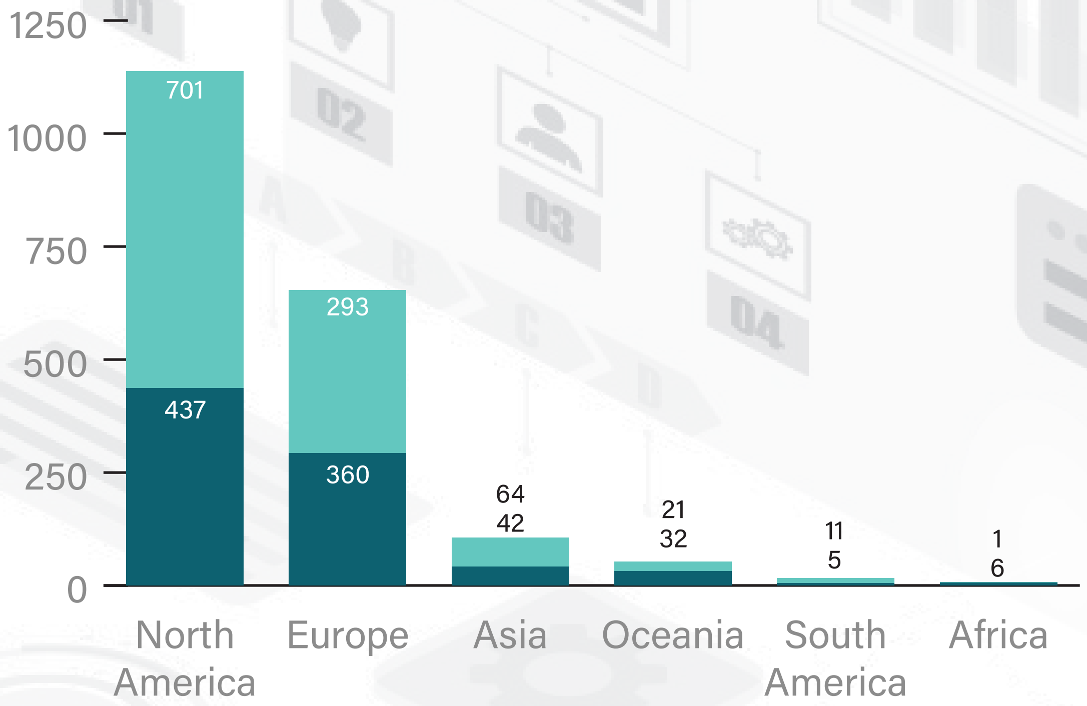
Loaders - are small pieces of code designed to load in additional malicious code onto a website.

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.

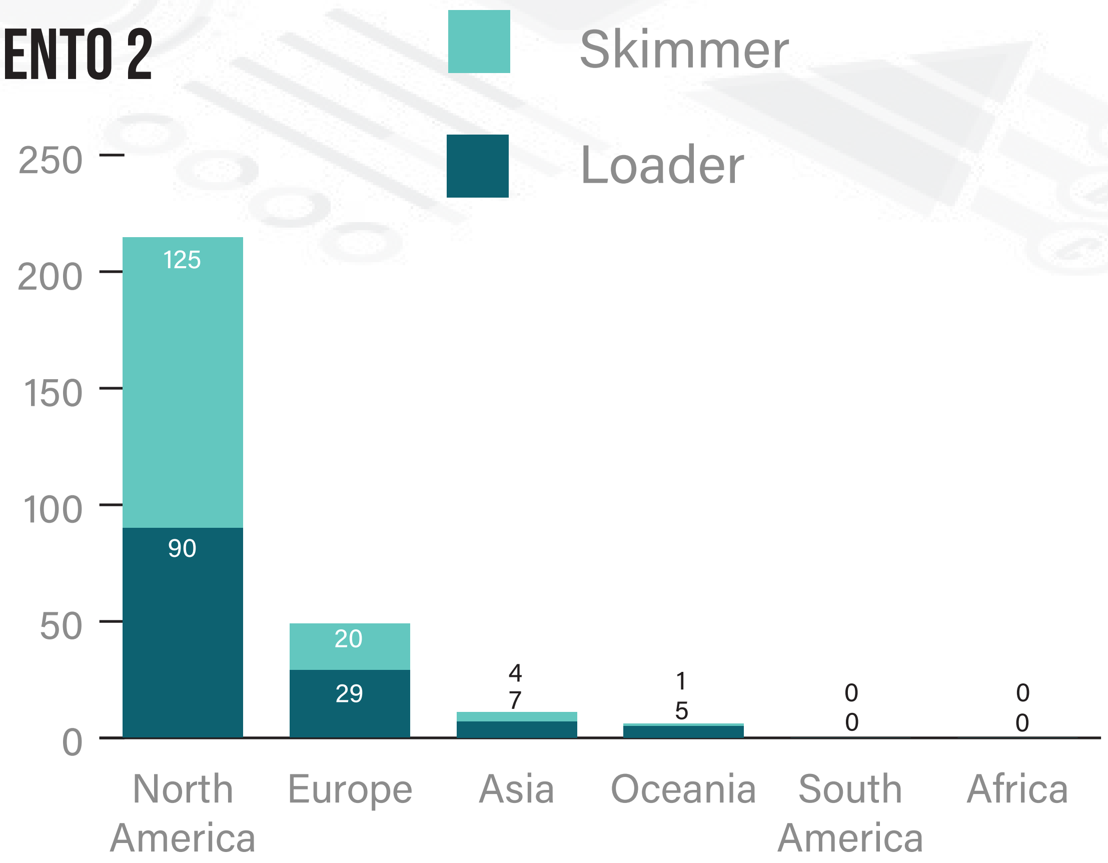
The charts to the right show which regions in the world have the highest infection rate, and below shows change over time.



MAGENTO 1



MAGENTO 2



FOREGENIX

5TH OCTOBER 2020

WEBSCAN RESULTS MAGENTO 1 & 2 - FRAMEWORK ISSUES

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

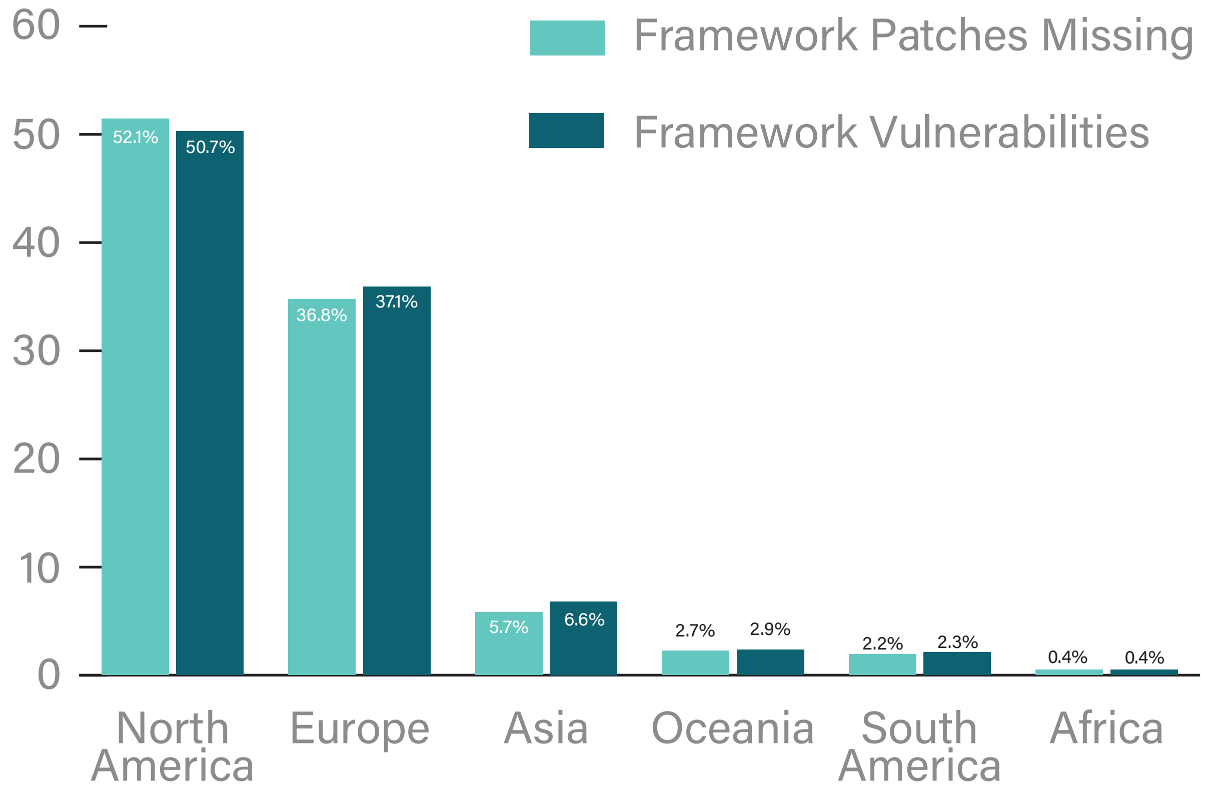
"**Framework security patches missing**" means a website is missing security patches/updates that are already available.

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

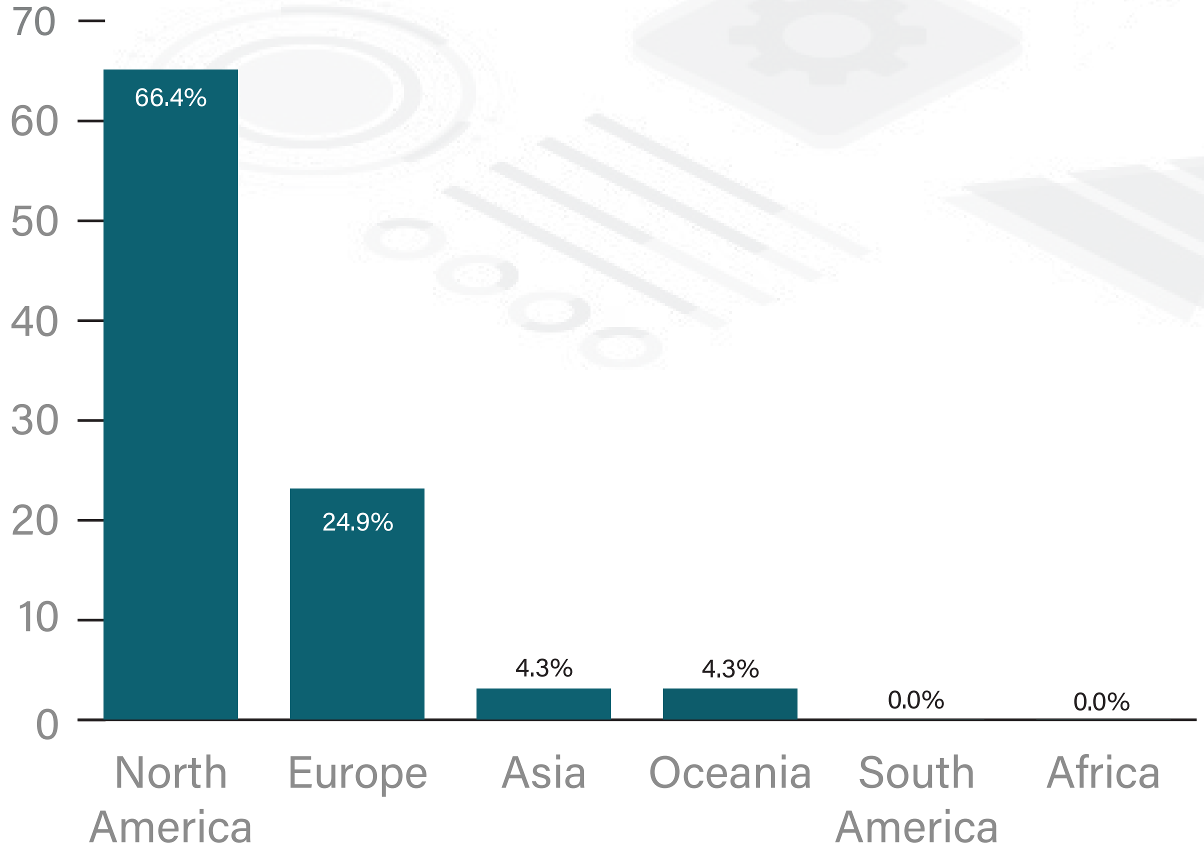
It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having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

With Magento 2, they abandoned this practice and websites are expected to upgrade to the latest version of Magento should they want to stay secure.

MAGENTO 1 PERCENTAGES



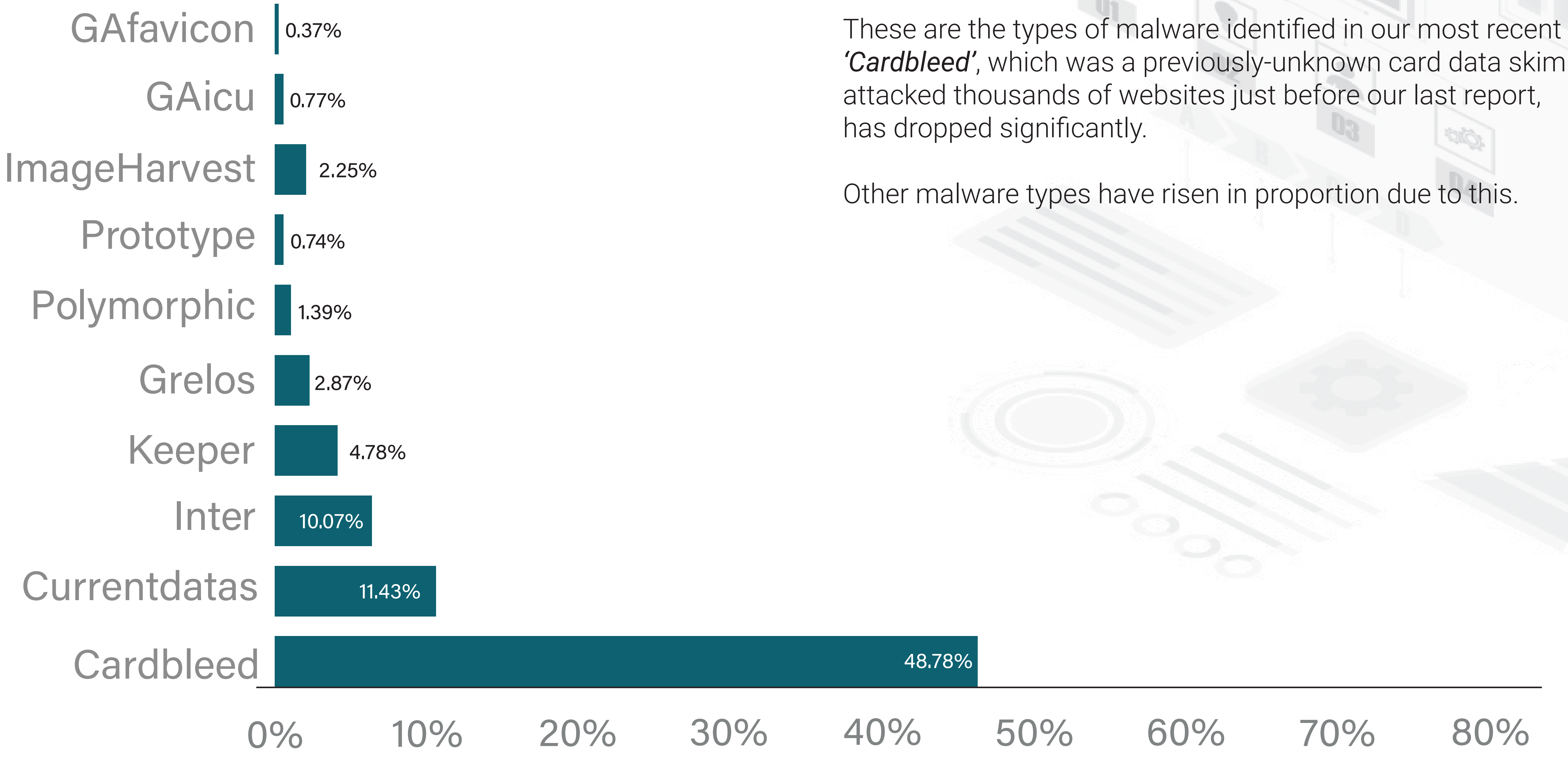
MAGENTO 2 PERCENTAGES



FOREGENIX

5TH OCTOBER 2020

WEBSCAN RESULTS MALWARE TYPES



These are the types of malware identified in our most recent Magento scan. *'Cardbleed'*, which was a previously-unknown card data skimmer that attacked thousands of websites just before our last report, has dropped significantly.

Other malware types have risen in proportion due to this.

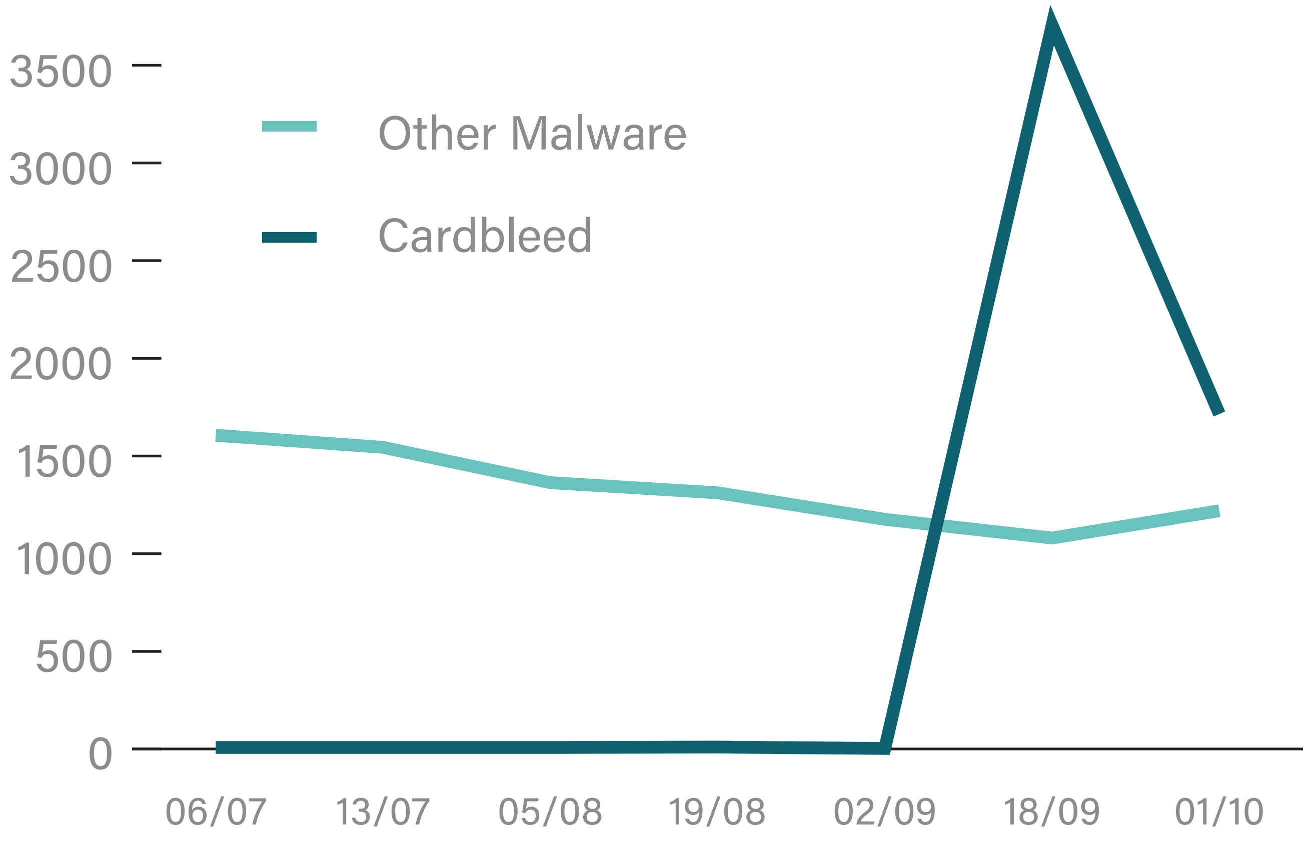
FOREGENIX

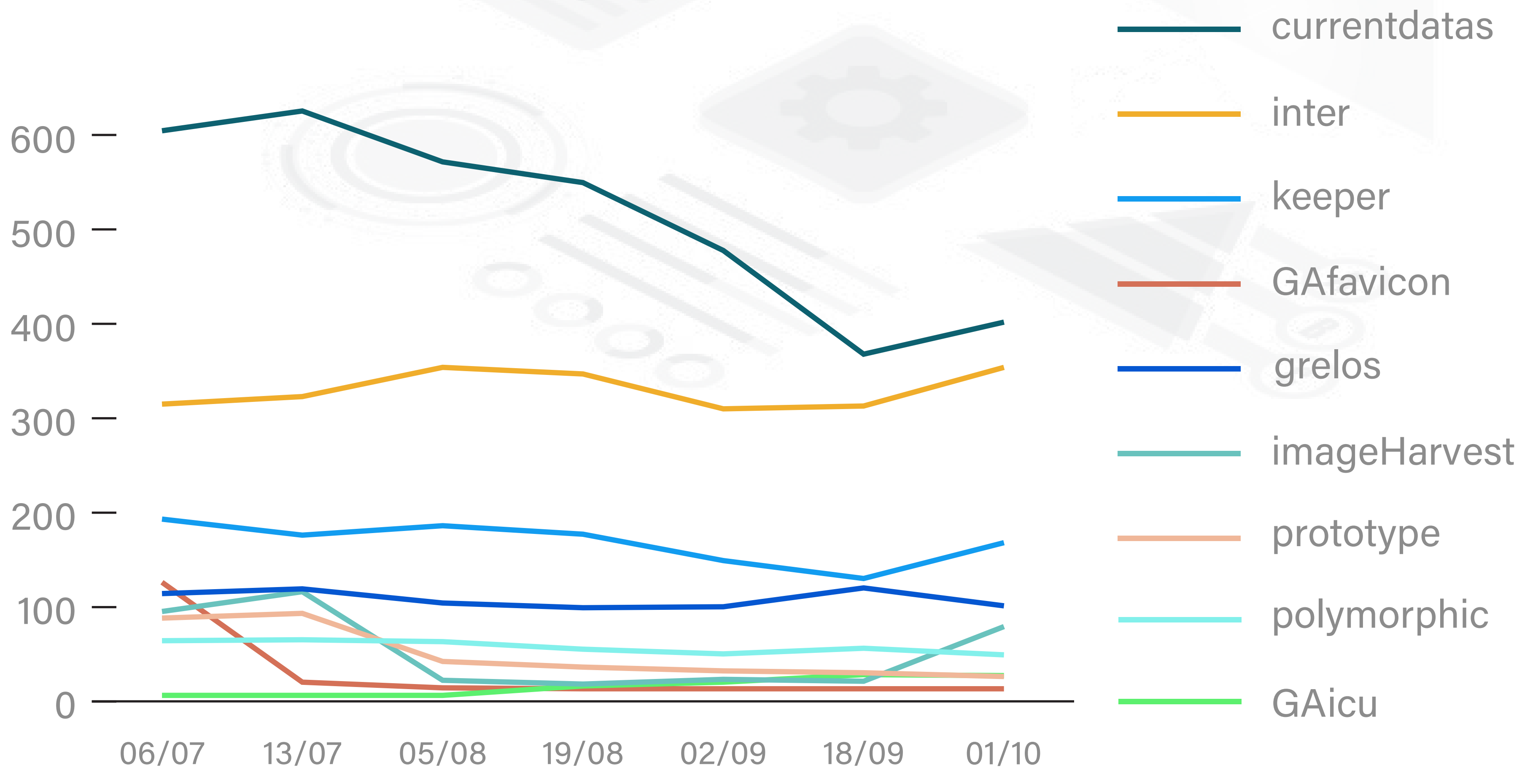
5TH OCTOBER 2020

WEBSCAN RESULTS MAGENTO 1 & 2 - MALWARE TRENDS

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

This month, we can see a significant decrease of *Cardbleed* malware, which may correlate with the decline in Magento websites. However, it is still the biggest threat to Magento websites and is bigger than all other malware combined.





FOREGENIX

5TH OCTOBER 2020

OUR INSIGHTS

The *Cardbleed* attack affected a lot of Magento websites in September. We have seen a good recovery, however there are still plenty of hacked websites. Being candid, we expect more large scale attacks to happen as all Magento 1 websites are extremely vulnerable at the moment (as there are no security patches due to being at its end of life).

The increase of hacked Magento 2 websites is not a good sign either. We believe that the owners/administrators of these websites should review their configuration/set-ups, as a large percentage of Magento 2 sites could significantly reduce risk by having their websites set up securely in the first place. Additional advice would be to invest in website security **and** cyber insurance to mitigate the risk of having a breach.

For free guidance, check out our Magento Security Insights. Many of the simple changes we have been advising are precautions that could prevent *Cardbleed's* exploit, or any exploit for that matter -- though not for certain.

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