MAGENTO WEBSITE SECURITY REPORT

CONTACT US

WWW.FOREGENIX.COM/WEBSCAN

TEL: +44 845 309 6232

21ST SEPTEMBER 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

21ST SEPTEMBER 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.

FOREGENIX

21ST SEPTEMBER 2020

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

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

Significant **INCREASE** of Hacked Magento 1 & 2 websites since our last report

93% of Magento 1 websites are High/Critical Risk

55% of Magento 2 websites are High/Critical Risk

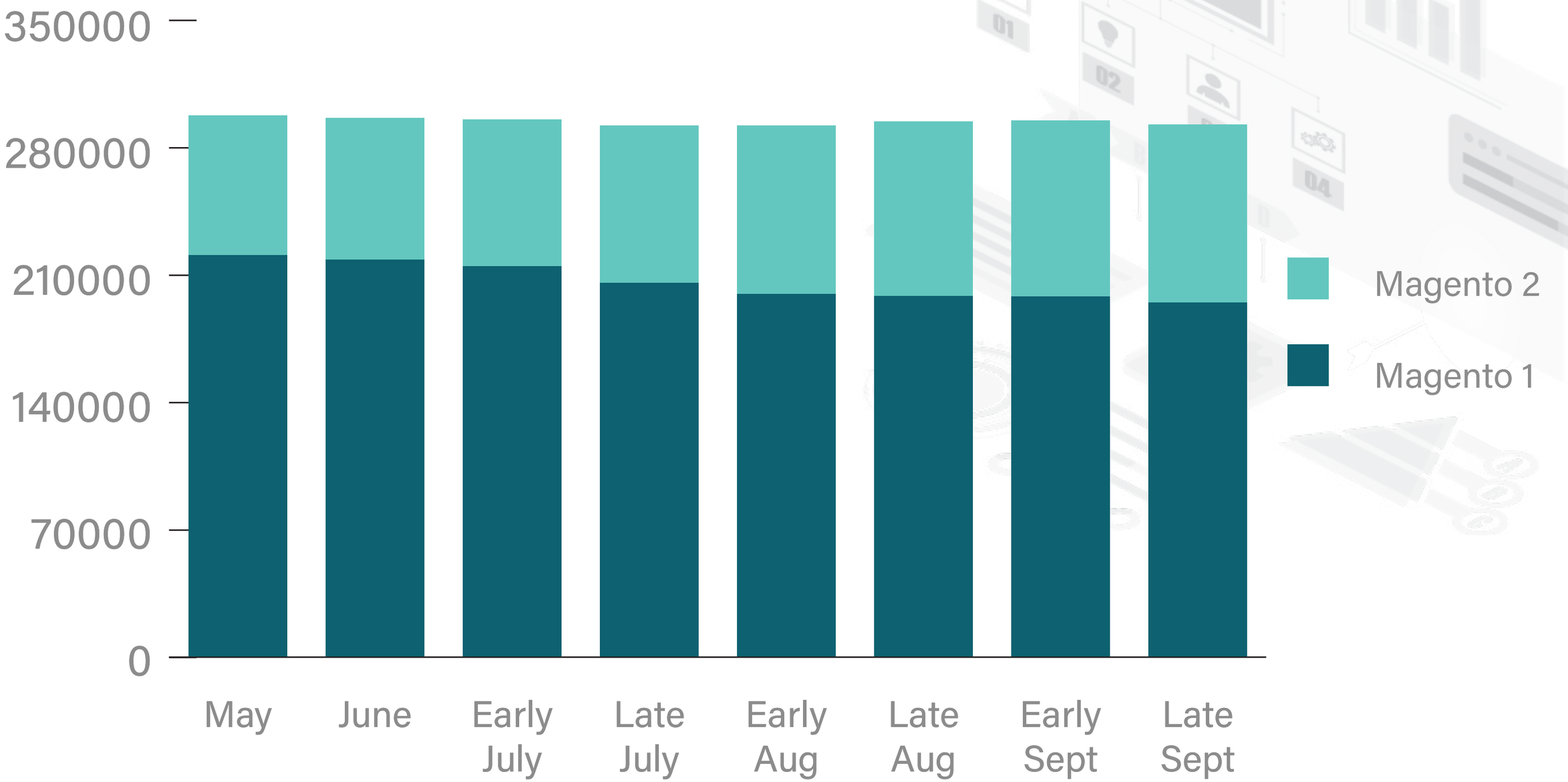
MAGENTO REMAINS THE MOST TARGETED PLATFORM BY CRIMINALS

FOREGENIX

21ST SEPTEMBER 2020

WEBSCAN RESULTS

WEBSITE NUMBERS (ALL MAGENTO)



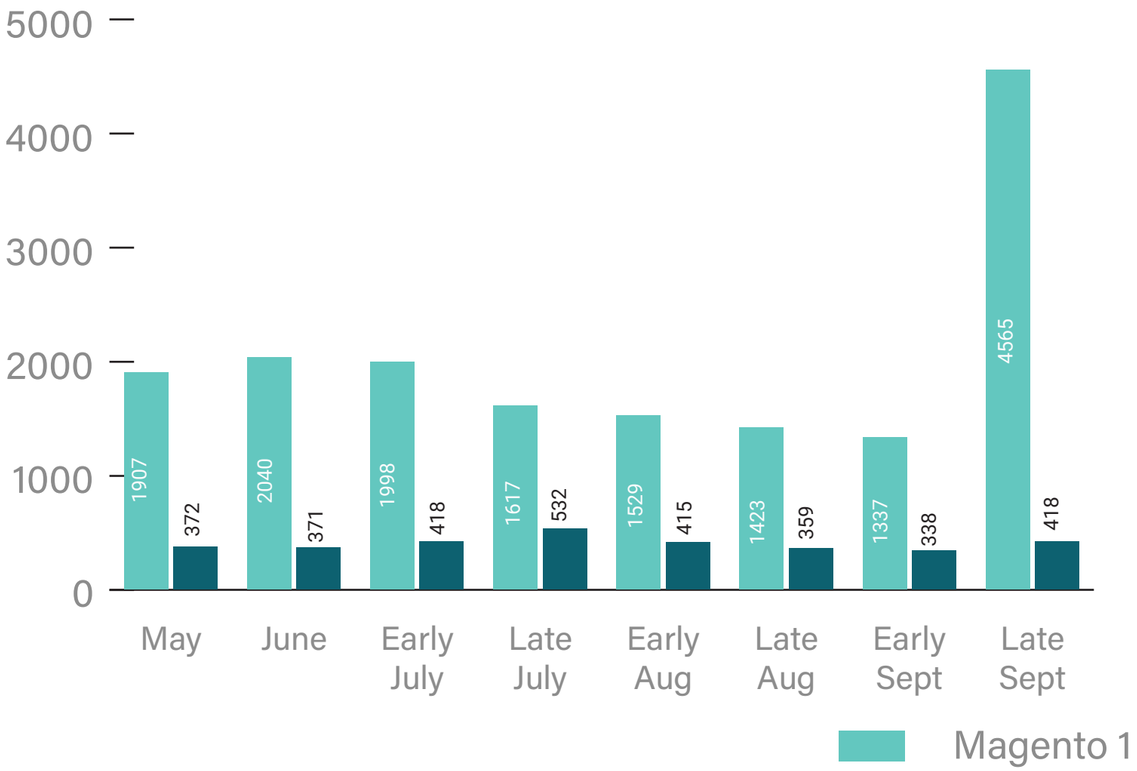
FOREGENIX

21ST SEPTEMBER 2020

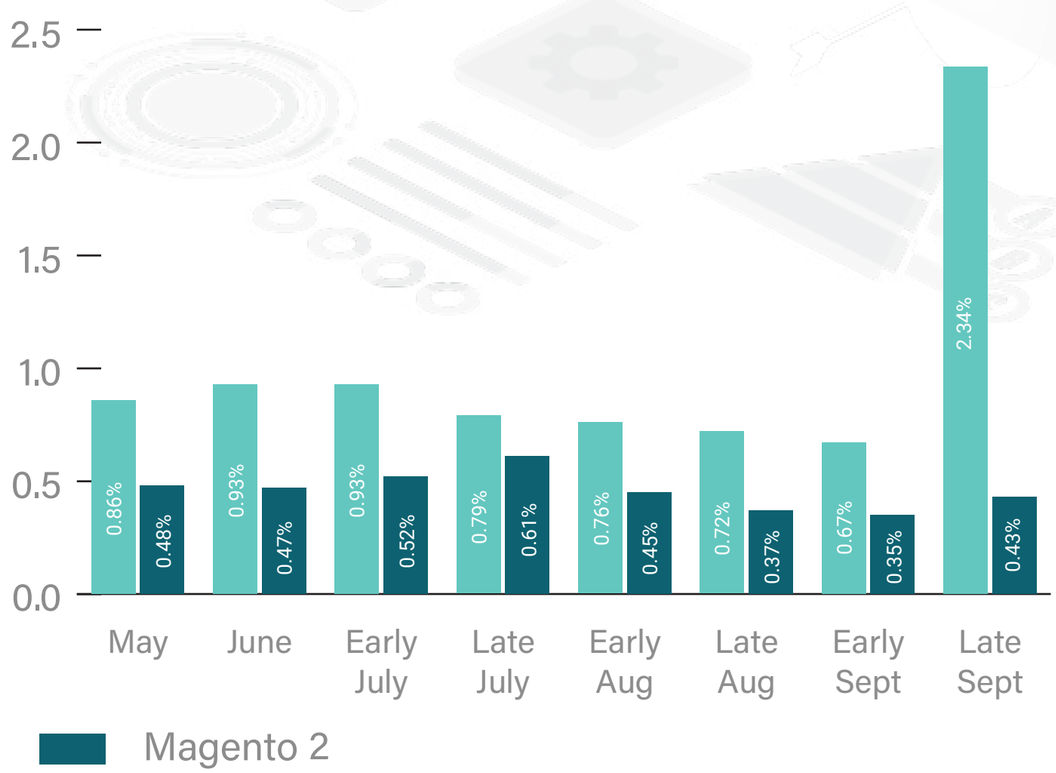
WEBSCAN RESULTS CRITICAL RISK

Websites with Critical Risk have already been hacked (with card data being actively stolen). This month we have seen a huge increase in the % of hacked Magento 1 and 2 websites and Magento 2 also saw a ~3% increase in High Risk websites.

ACTUAL NUMBERS



PERCENTAGE OF TOTAL SITES



FOREGENIX

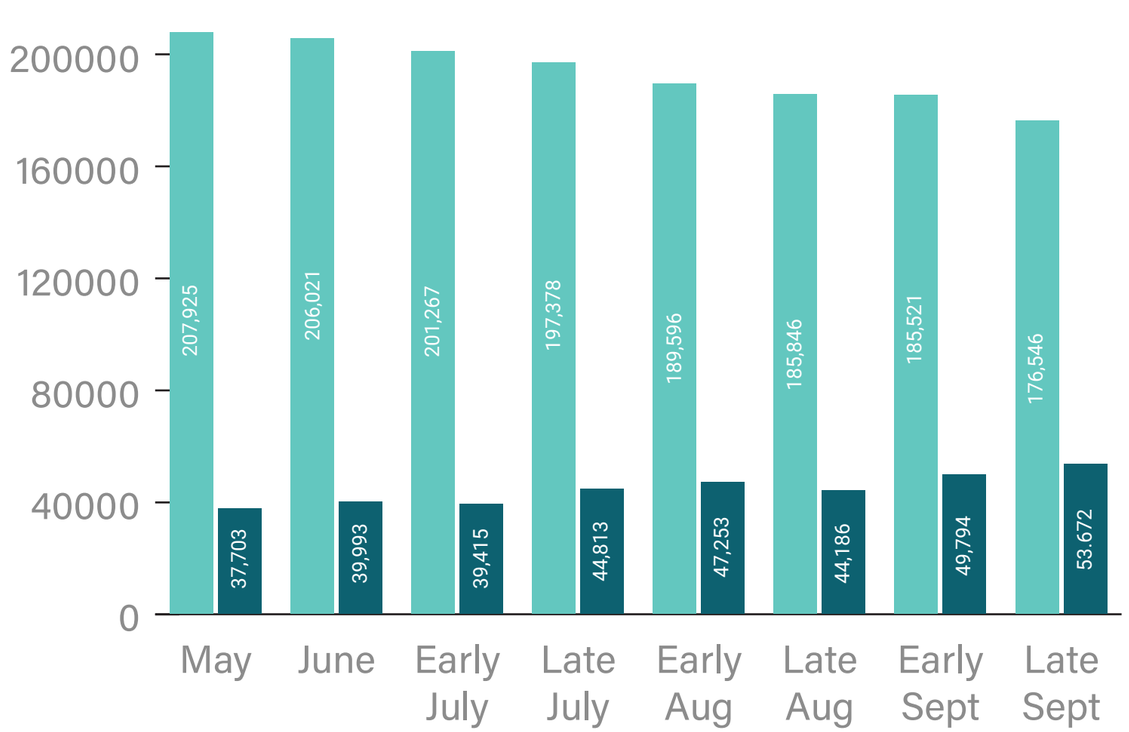
21ST SEPTEMBER 2020

WEBSCAN RESULTS HIGH RISK

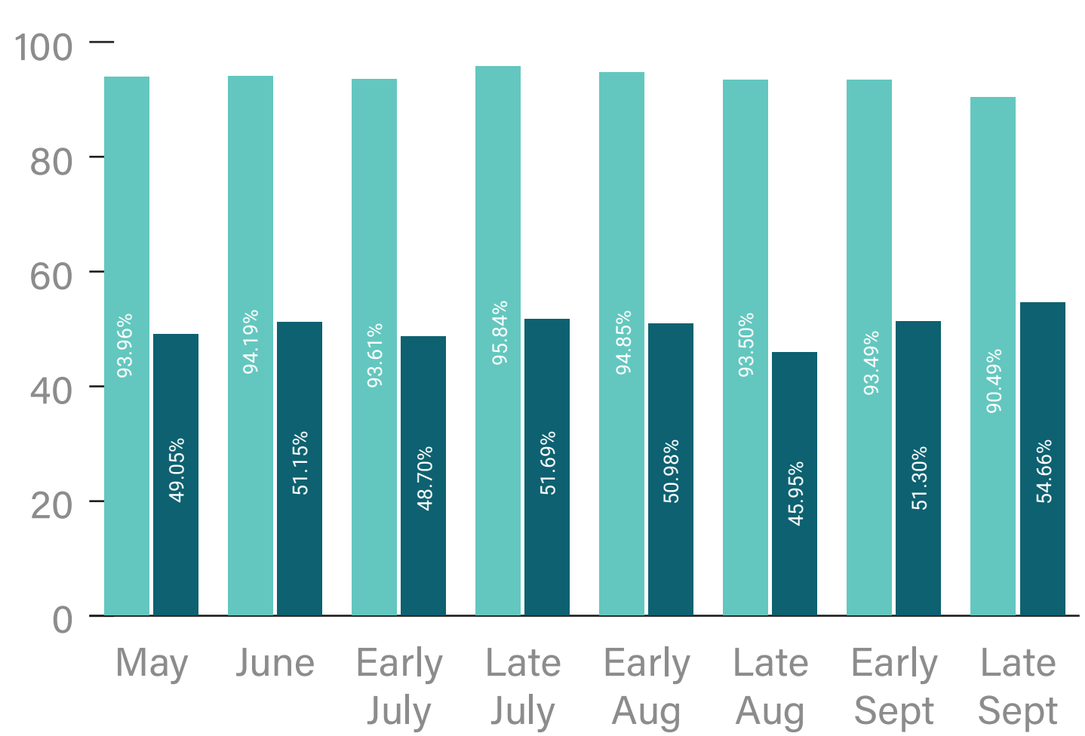
Websites with High Risk have significant security issues that make them very vulnerable to criminals.
The sites have one or more of the following:

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

ACTUAL NUMBERS



PERCENTAGE OF TOTAL SITES



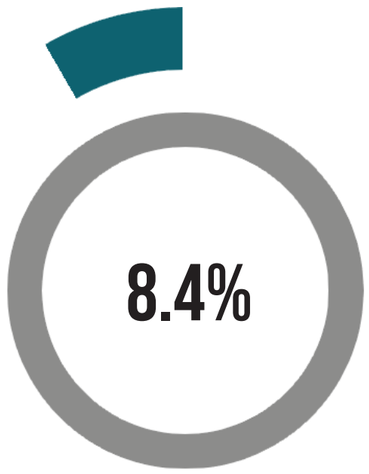
Magento 1 Magento 2

FOREGENIX

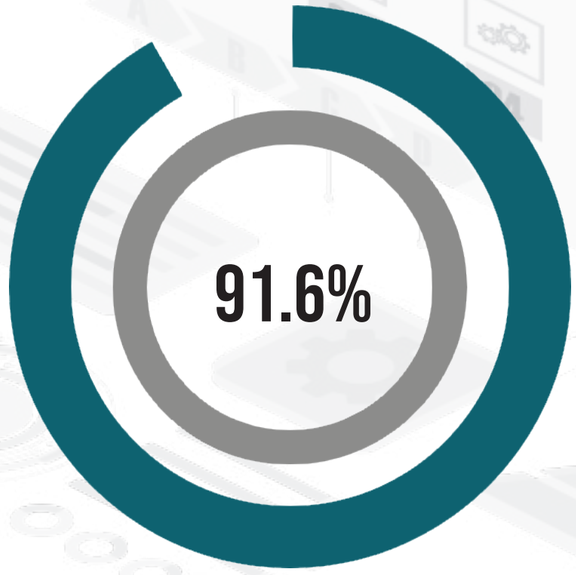
21ST SEPTEMBER 2020

WEBSCAN RESULTS

CARD-HARVESTING MALWARE DISTRIBUTION



MAGENTO 2



MAGENTO 1

FOREGENIX

21ST SEPTEMBER 2020

WEBSCAN RESULTS

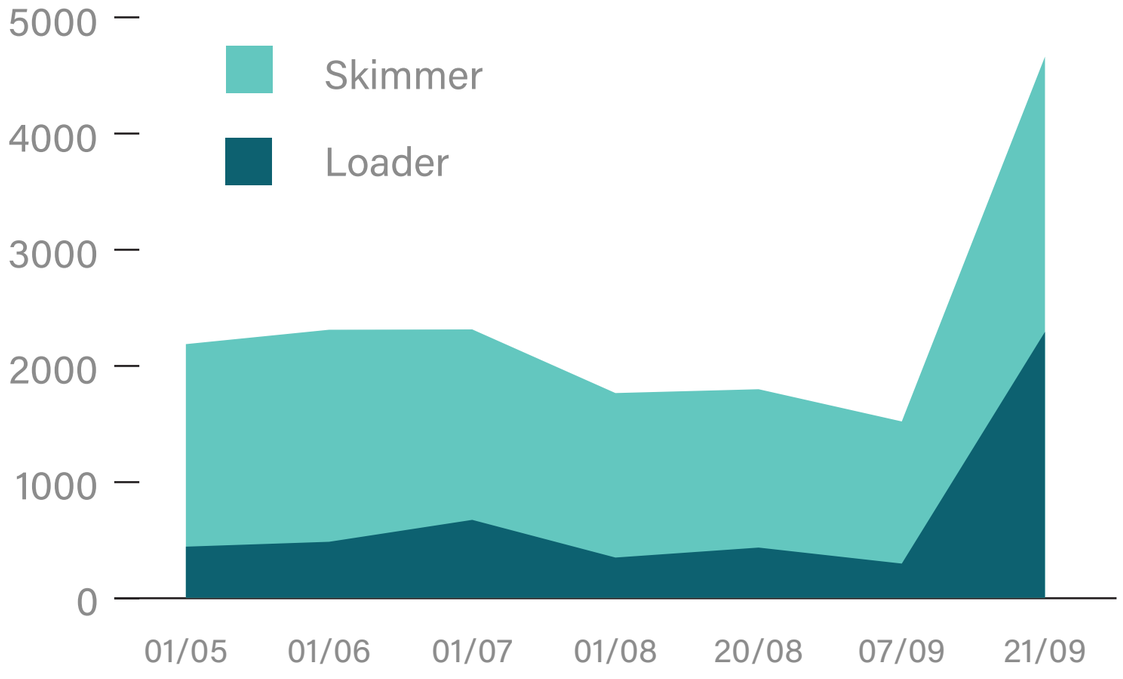
MAGENTO 1 & 2 - LOADERS & SKIMMERS

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

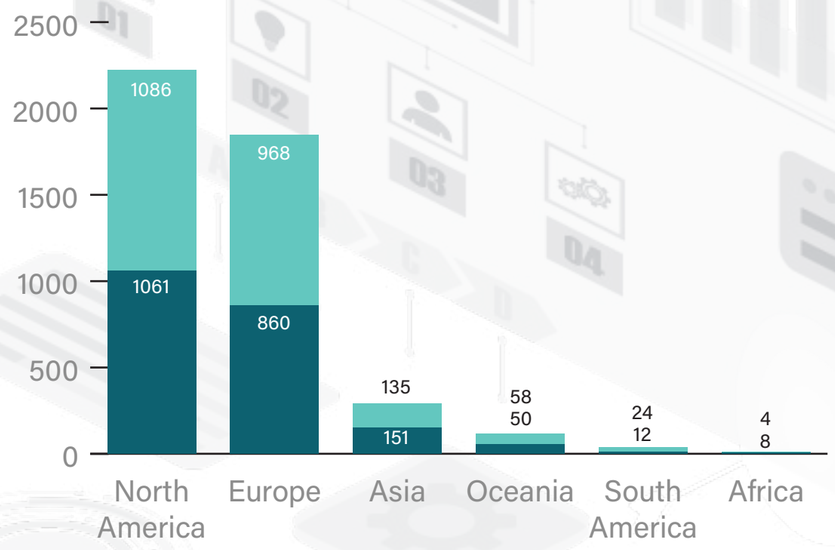
Loaders - are small pieces of code designed to load in additional malicious code onto a website.

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.

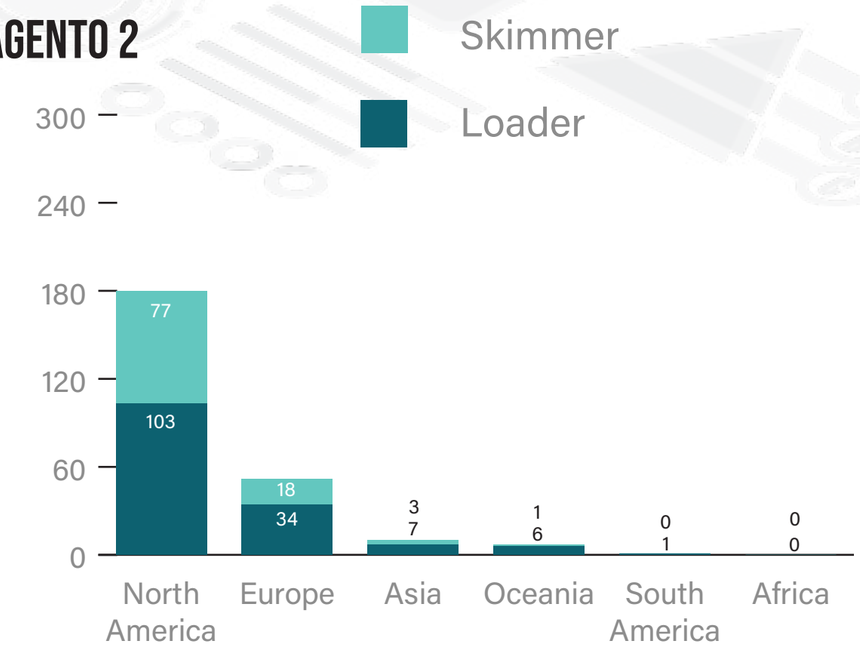
The charts to the right show which regions in the world have the highest infection rate, and below shows change over time.



MAGENTO 1



MAGENTO 2



FOREGENIX

21ST SEPTEMBER 2020

WEBSCAN RESULTS

MAGENTO 1 & 2 - FRAMEWORK ISSUES

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

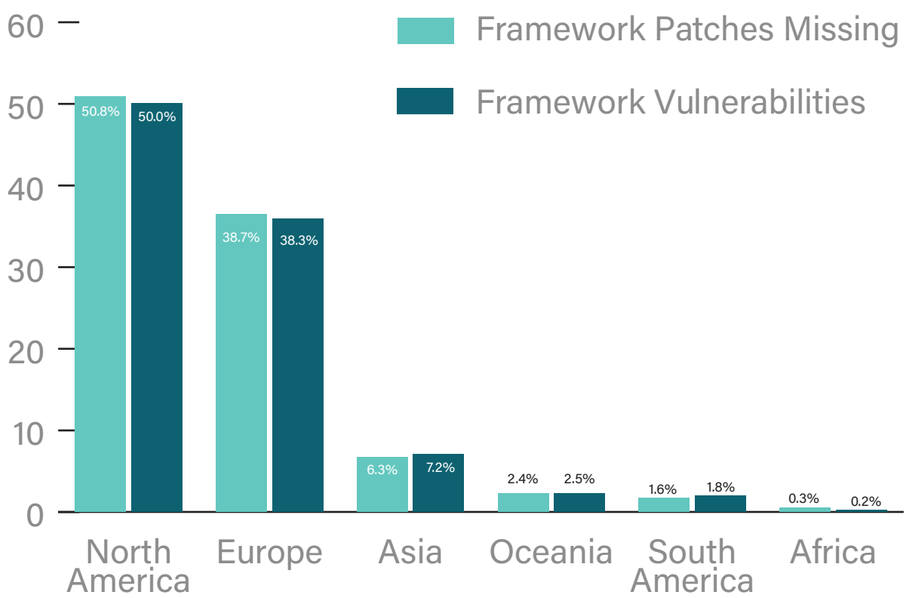
"**Framework security patches missing**" means your website is missing security patches/updates that are already available.

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

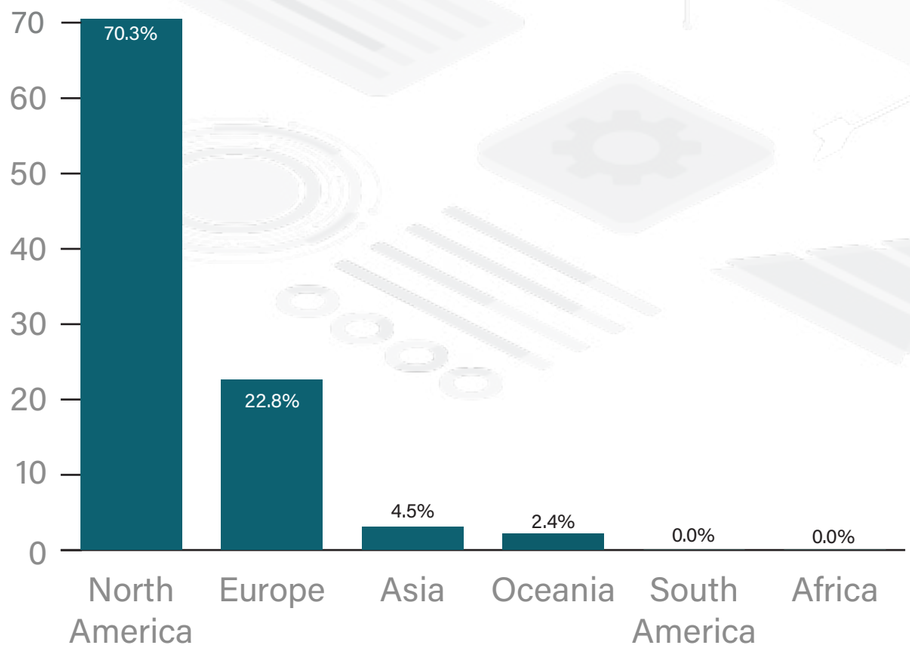
It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having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

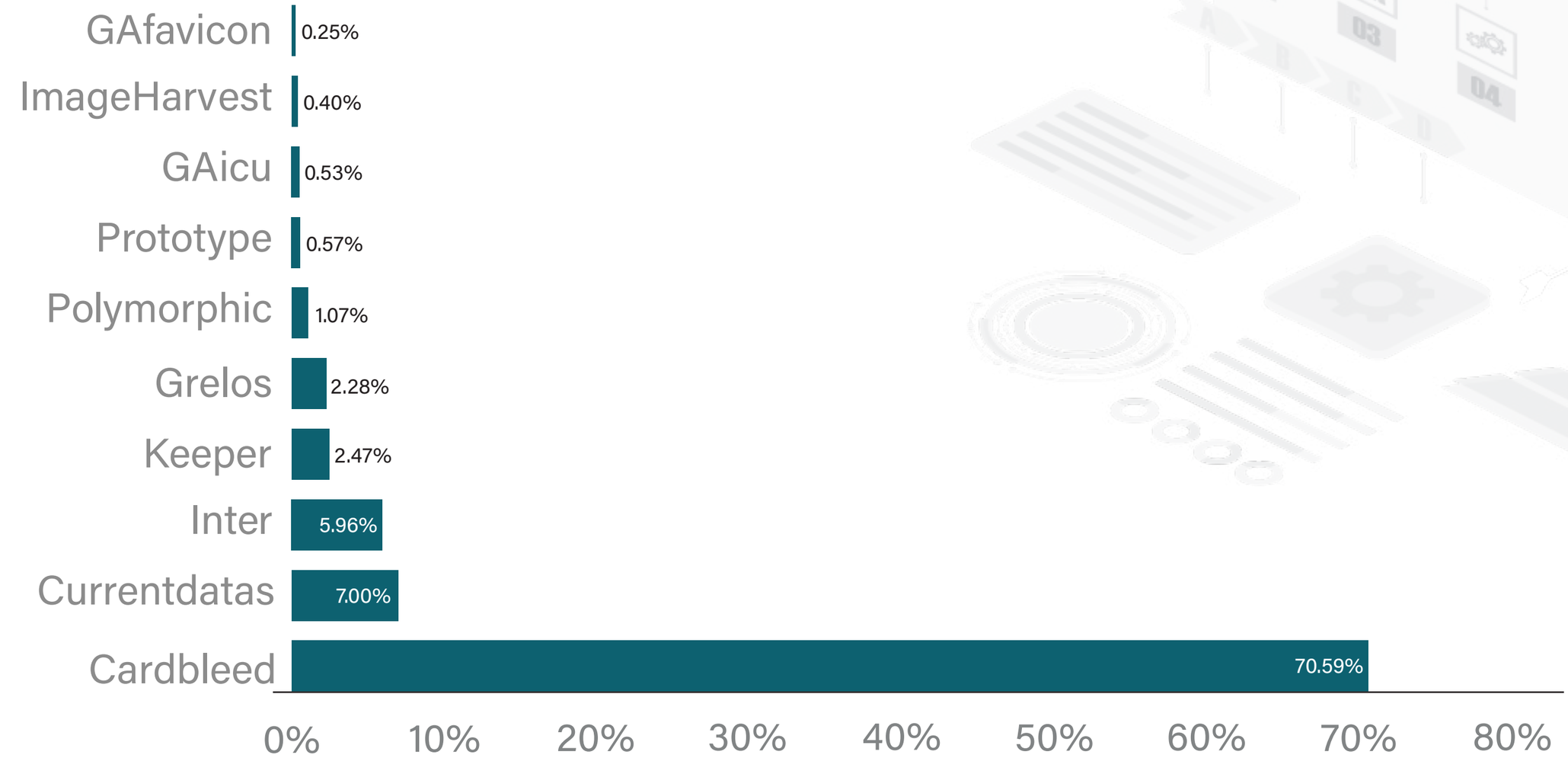


FOREGENIX

21ST SEPTEMBER 2020

WEBSCAN RESULTS MALWARE TYPES

These are the types of malware identified in our most recent Magento scan. *'Cardbleed'*, the previously-unknown card data skimmer that attacked thousands of websites last week, was by far our most common detection, at around 70% of all identified malware.



FOREGENIX

21ST SEPTEMBER 2020

OUR INSIGHTS

Since June, there has been a trending decrease of High and Critical risk websites for Magento 1. However, there has been an unprecedented spike in hacked websites, which seems to have slightly affected Magento 2 as well.

This is due to the recent 0-day exploit which has infected over 4,500 websites with card data skimmers. While Magento 1 was the primary target of this attack (especially after reaching its End of Life), it has slightly affected other platforms such as Magento 2, OpenMage, ASP.net and some PHP sites. We have written more on this in our blog if you would like to learn more.

Also, please see our Magento Security Insights page for guidance. Many of the simple changes we have been advising are precautions that could prevent this exploit -- though not for certain.

ADDITIONAL RESOURCES

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

21ST SEPTEMBER 2020