

MAGENTO WEBSITE SECURITY REPORT

CONTACT US

WWW.FOREGENIX.COM/WEBSCAN

TEL: +44 845 309 6232

24TH AUGUST 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**



OVERVIEW WHAT IS WEBCAN?

We currently monitor nearly

300,000

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

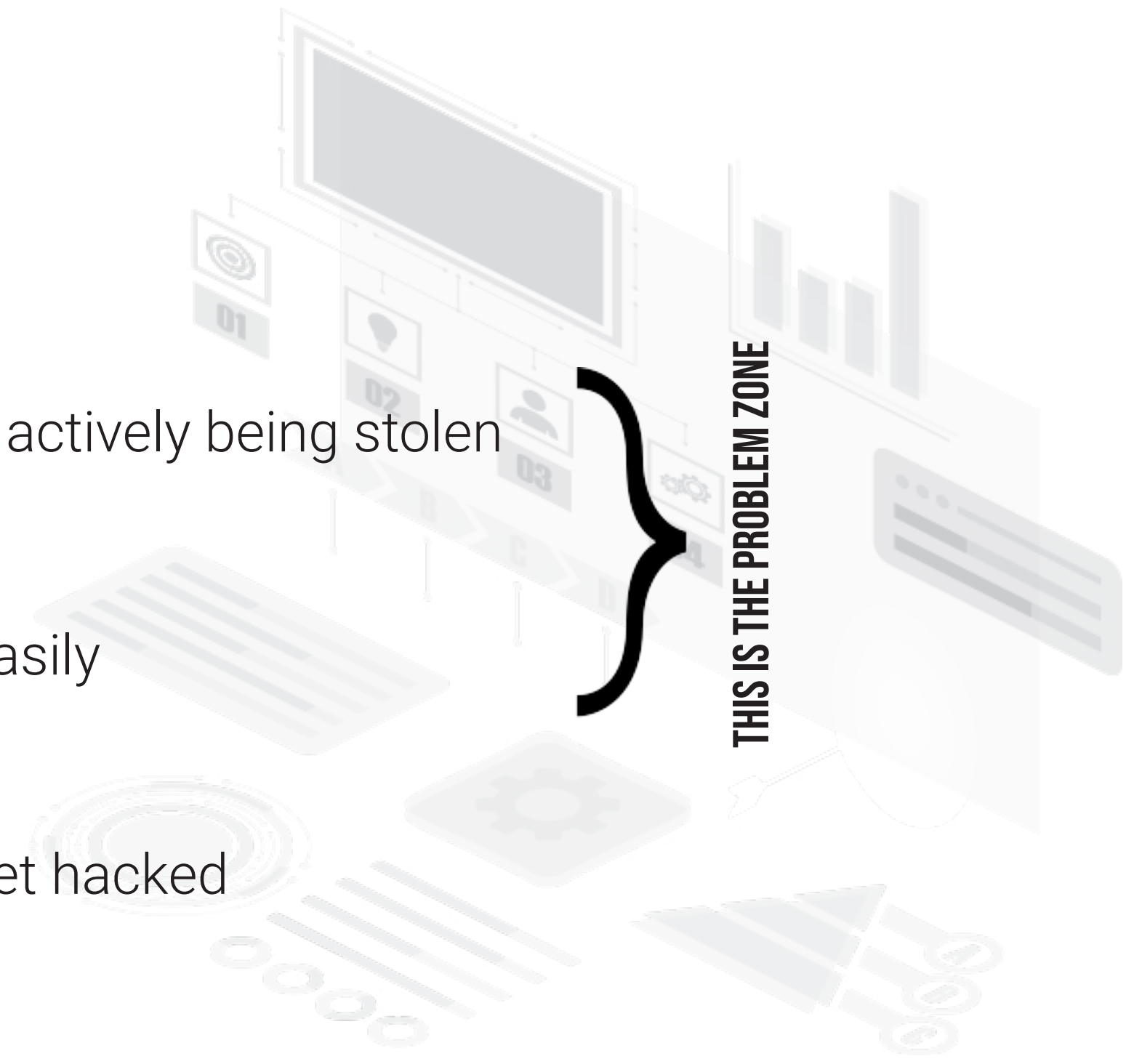


Some issues, unlikely to get hacked

LOW



Hacking unlikely



THIS IS THE PROBLEM ZONE



OVERVIEW WEEKLY SUMMARY

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

DECREASE of hacked Magento 2 websites since last month

94% of Magento 1 websites are High/Critical Risk

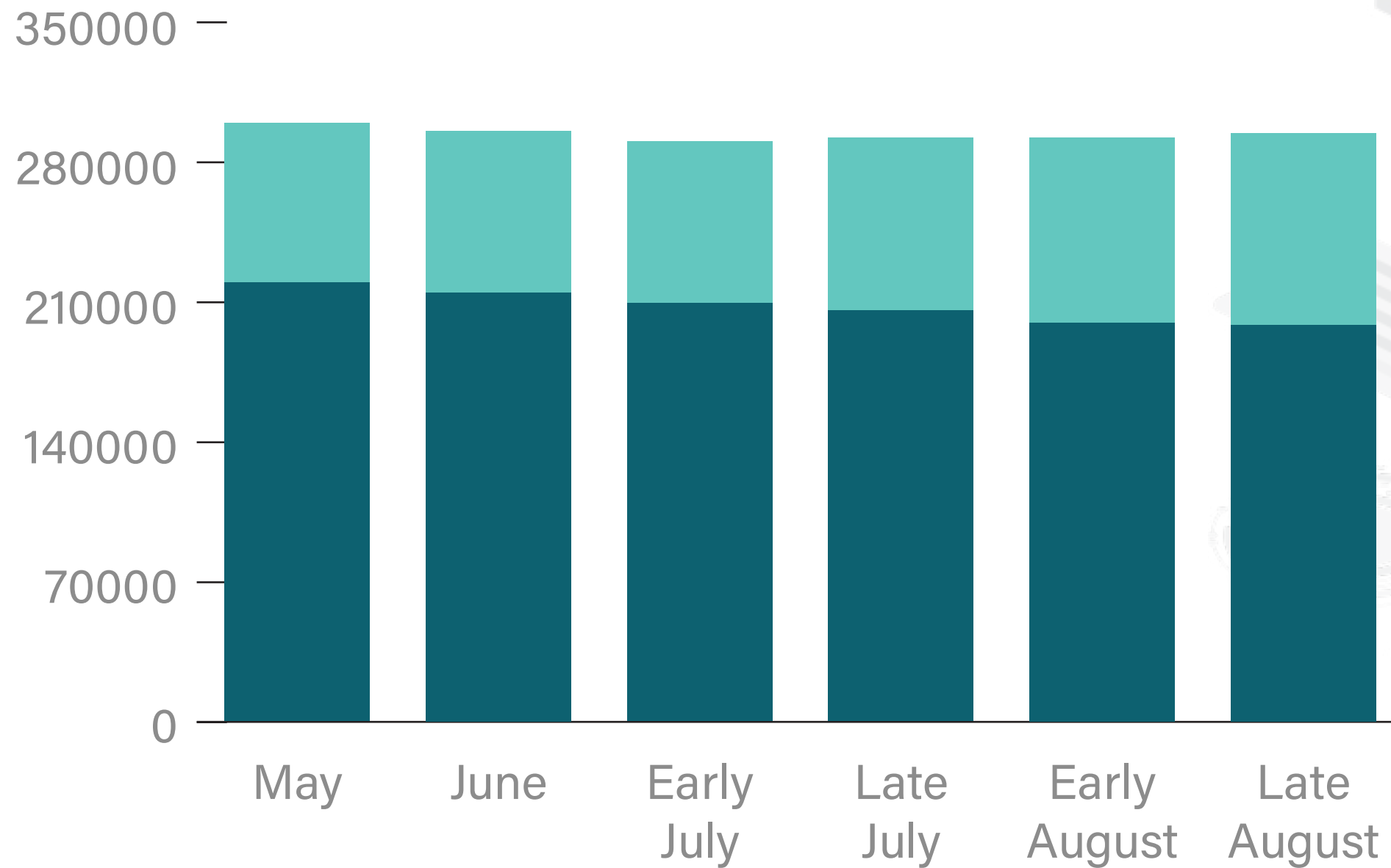
46% of Magento 2 websites are High/Critical Risk

MAGENTO REMAINS THE MOST TARGETED PLATFORM BY CRIMINALS



WEBSCAN RESULTS

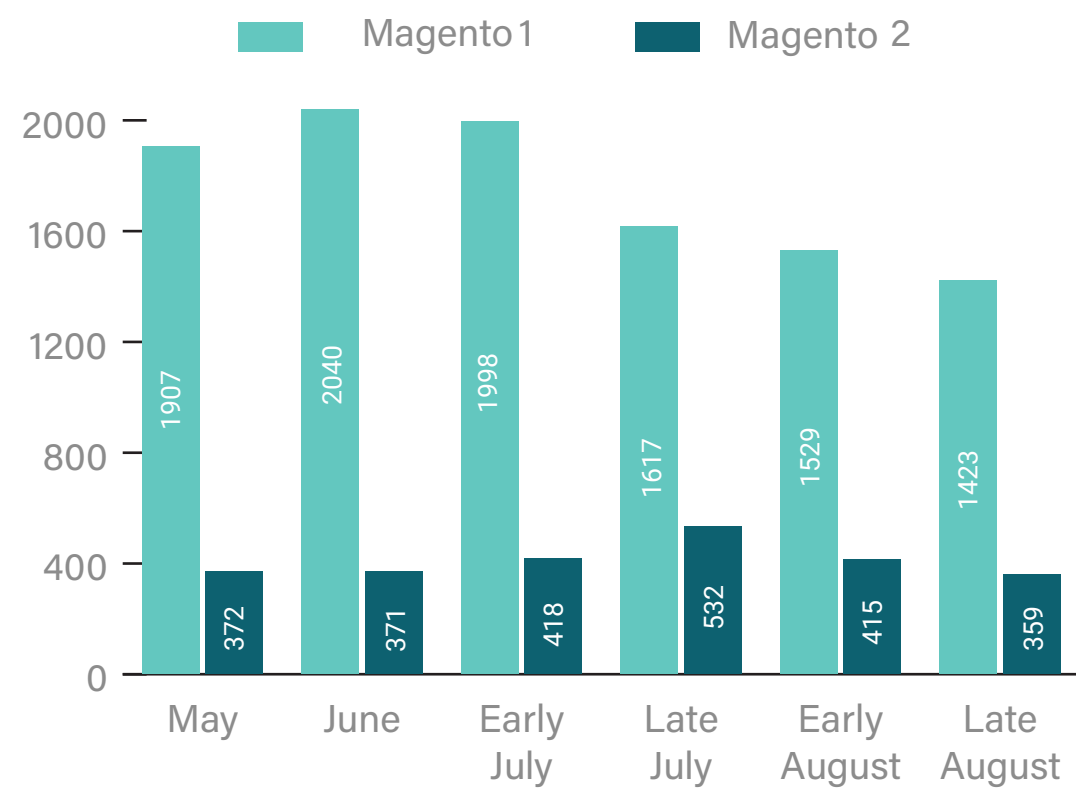
WEBSITE NUMBERS (ALL MAGENTO)



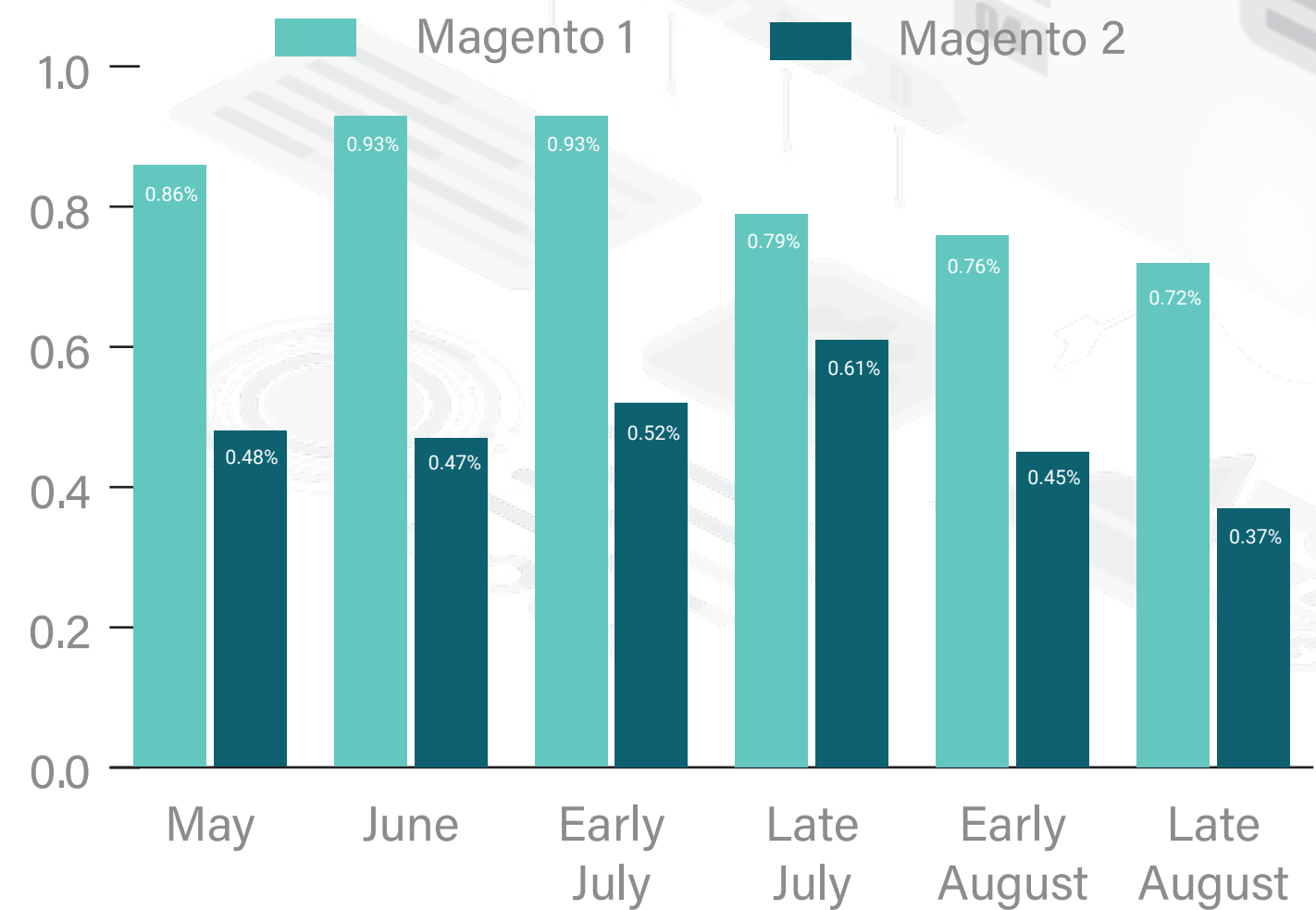
WEBSCAN RESULTS **CRITICAL RISK**

Websites with Critical Risk have already been hacked (with card data being actively stolen). This month we have seen a marginal decrease in the percentage of hacked Magento 1 and 2 websites. Magento 2 decrease of Critical and High risk websites seems to be due to a patch released in late July.

ACTUAL NUMBERS



PERCENTAGE OF TOTAL SITES

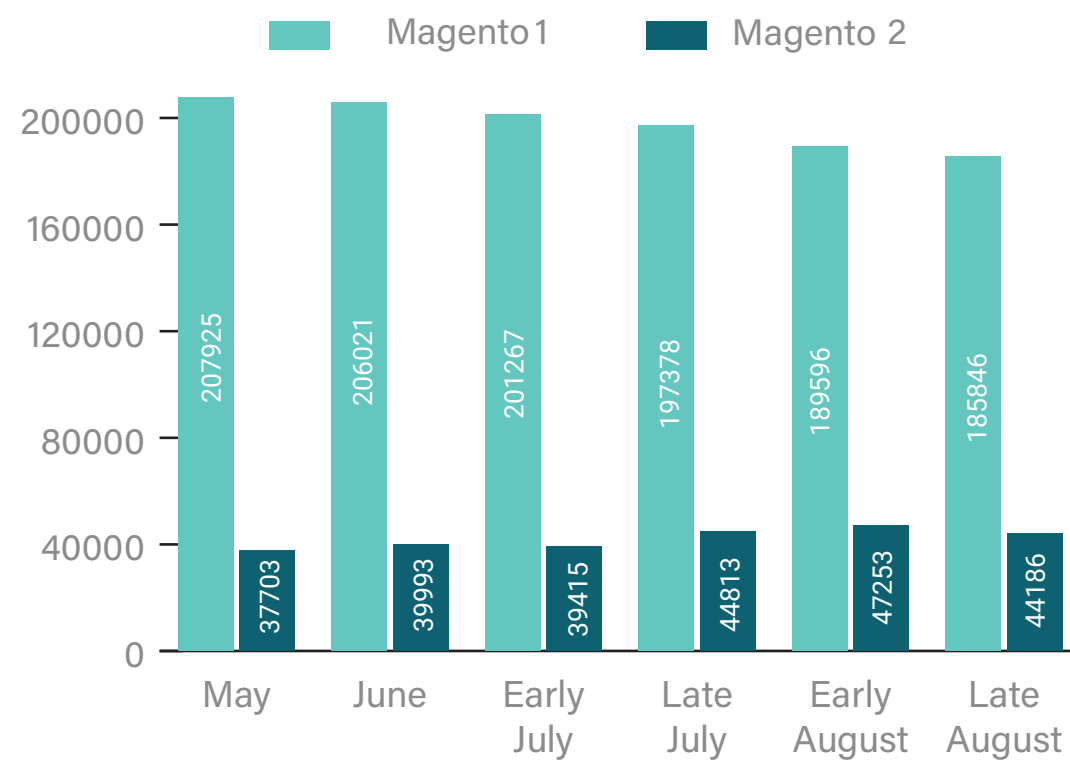


WEBSCAN RESULTS HIGH RISK

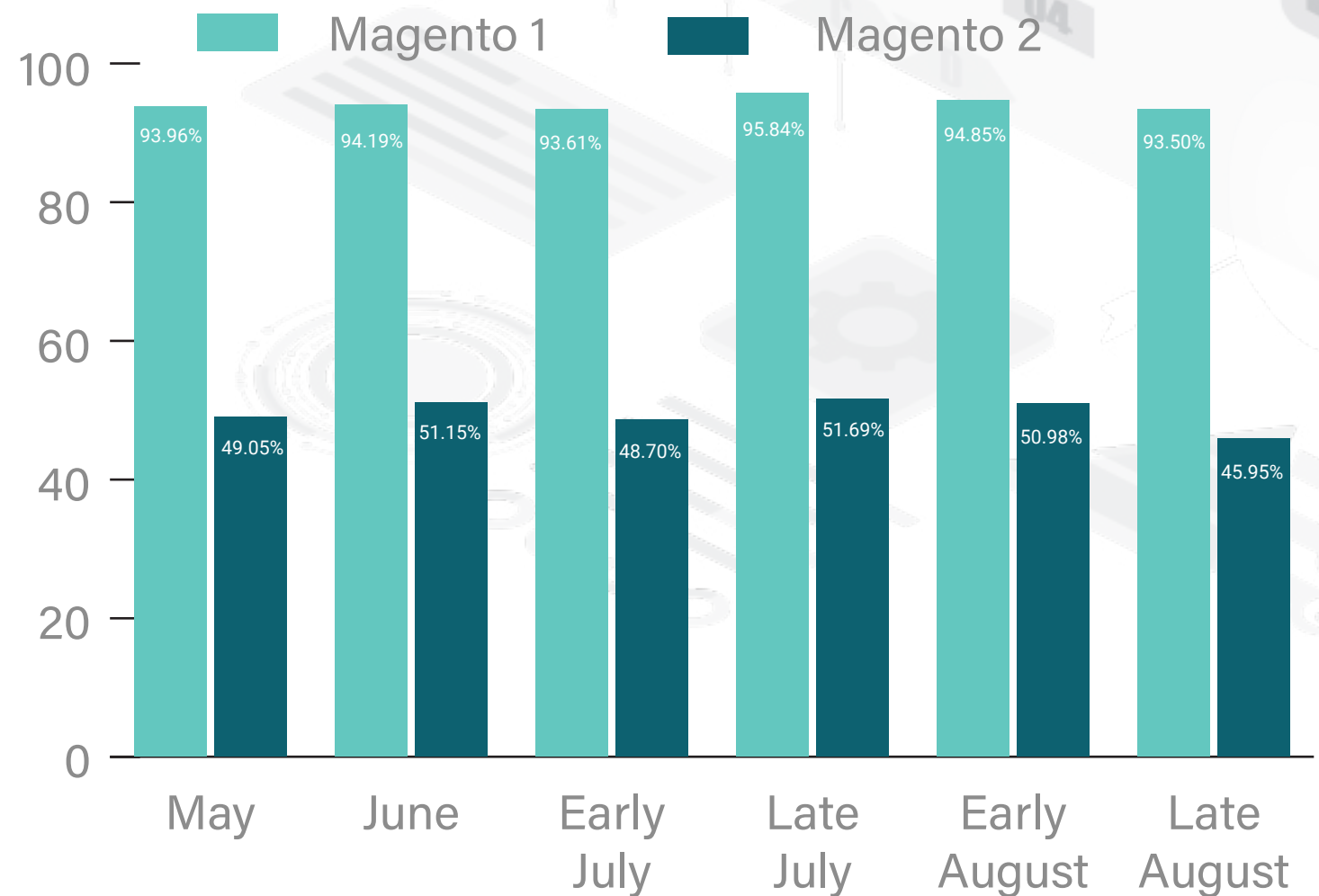
Websites with High Risk have significant security issues that make them very vulnerable to criminals. The sites have one or more of the following:

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

ACTUAL NUMBERS

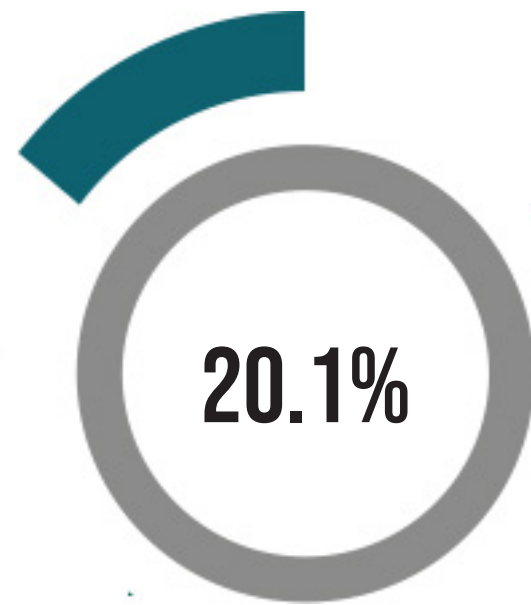


PERCENTAGE OF TOTAL SITES

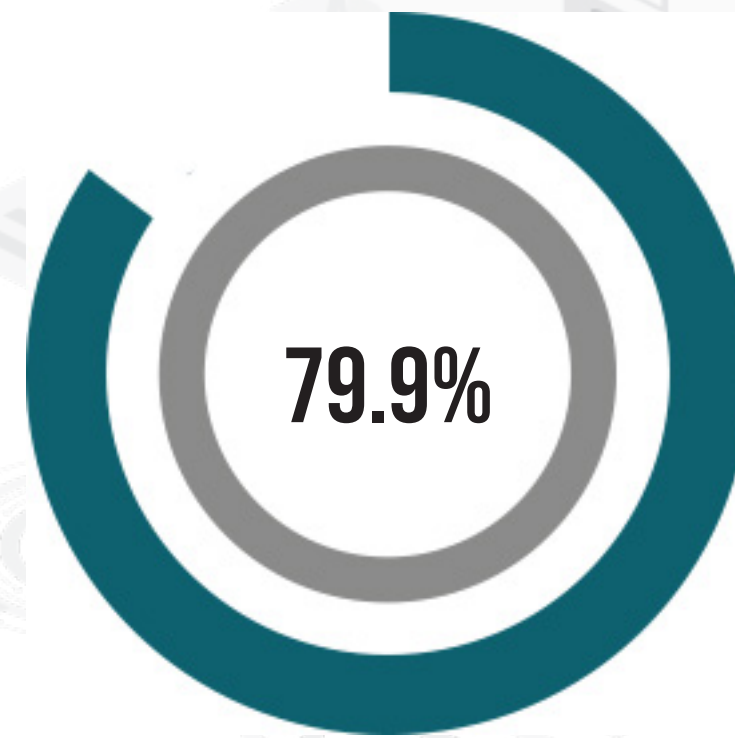


WEBSCAN RESULTS

CARD-HARVESTING MALWARE DISTRIBUTION



MAGENTO 2



MAGENTO 1

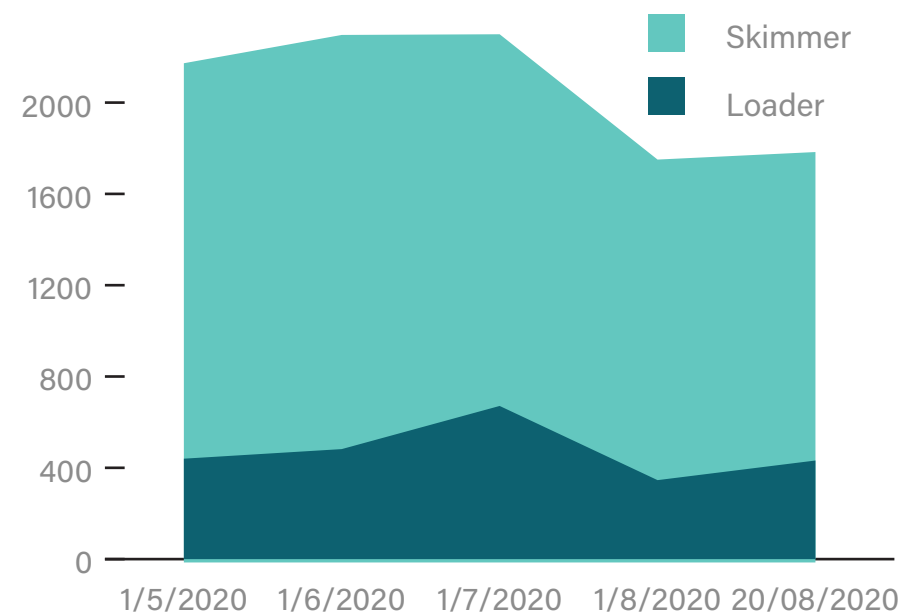
WEBSCAN RESULTS MAGENTO 1 & 2 - LOADERS & SKIMMERS

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

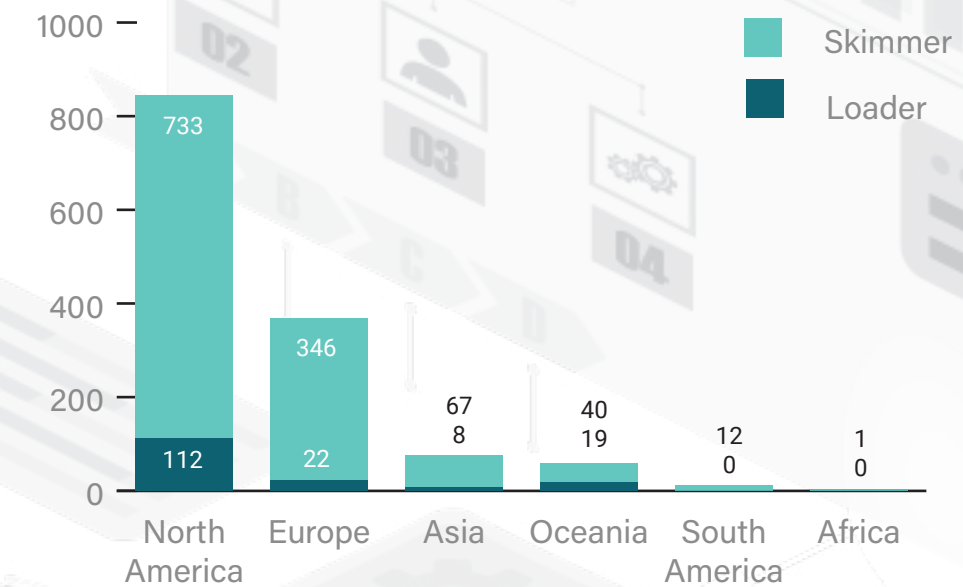
Loaders - are small pieces of code designed to load in additional malicious code onto a website.

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.

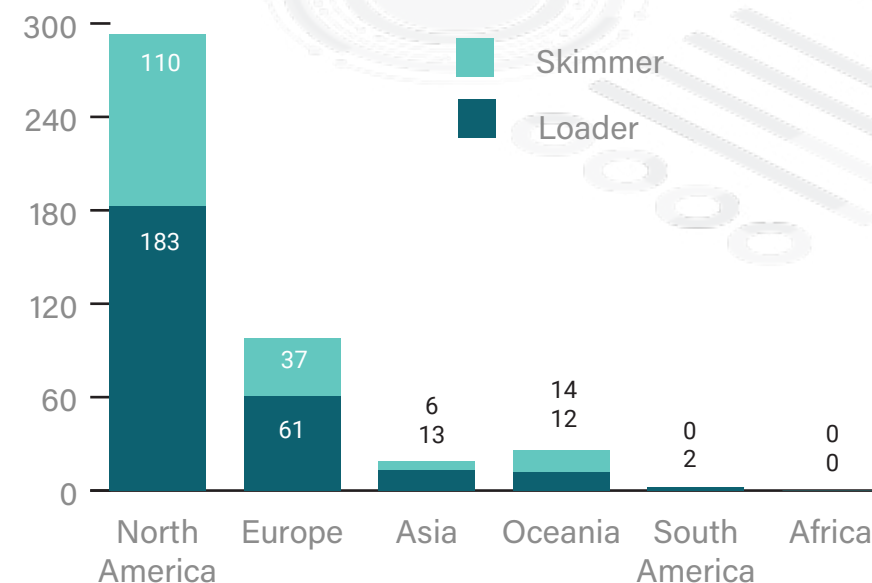
The charts to the right show which regions in the world have the highest infection rate, and below shows change over time.



MAGENTO 1



MAGENTO 2



WEBSCAN RESULTS MAGENTO 1 & 2 - FRAMEWORK ISSUES

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

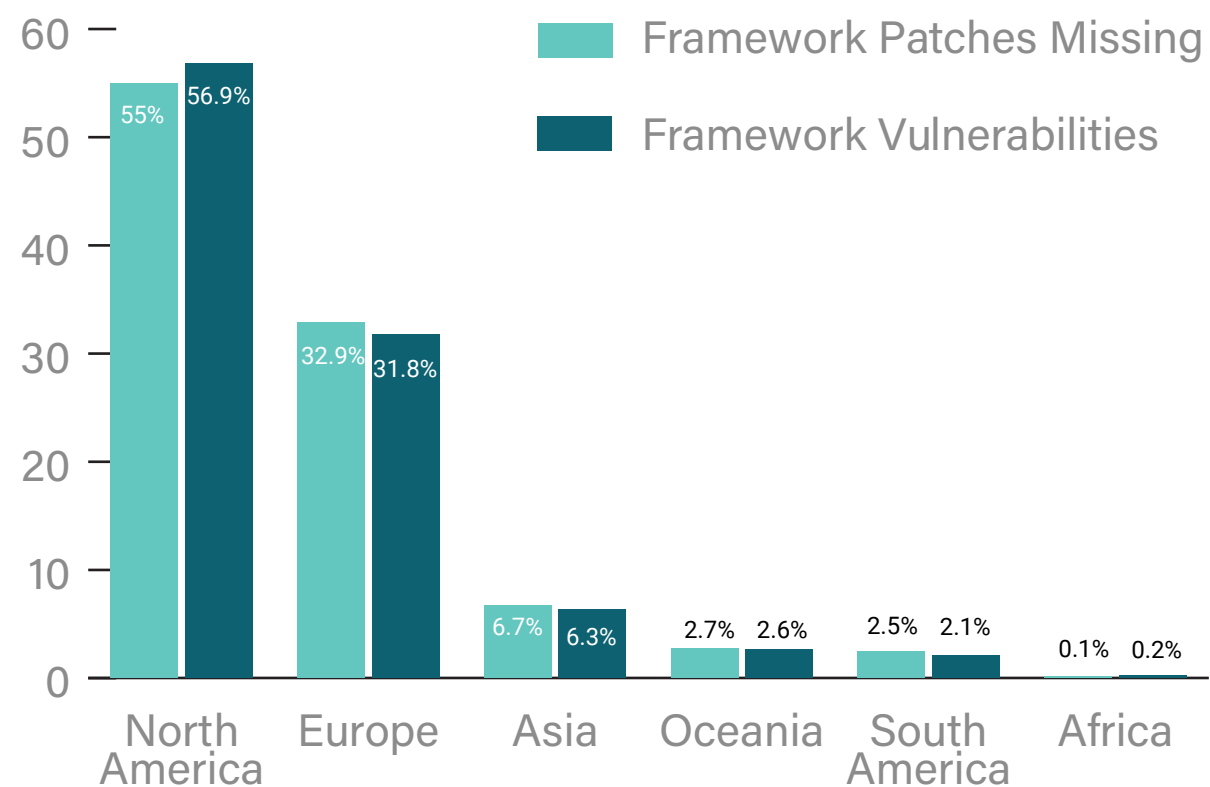
“Framework security patches missing” means your website is missing security patches/updates that are already available.

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

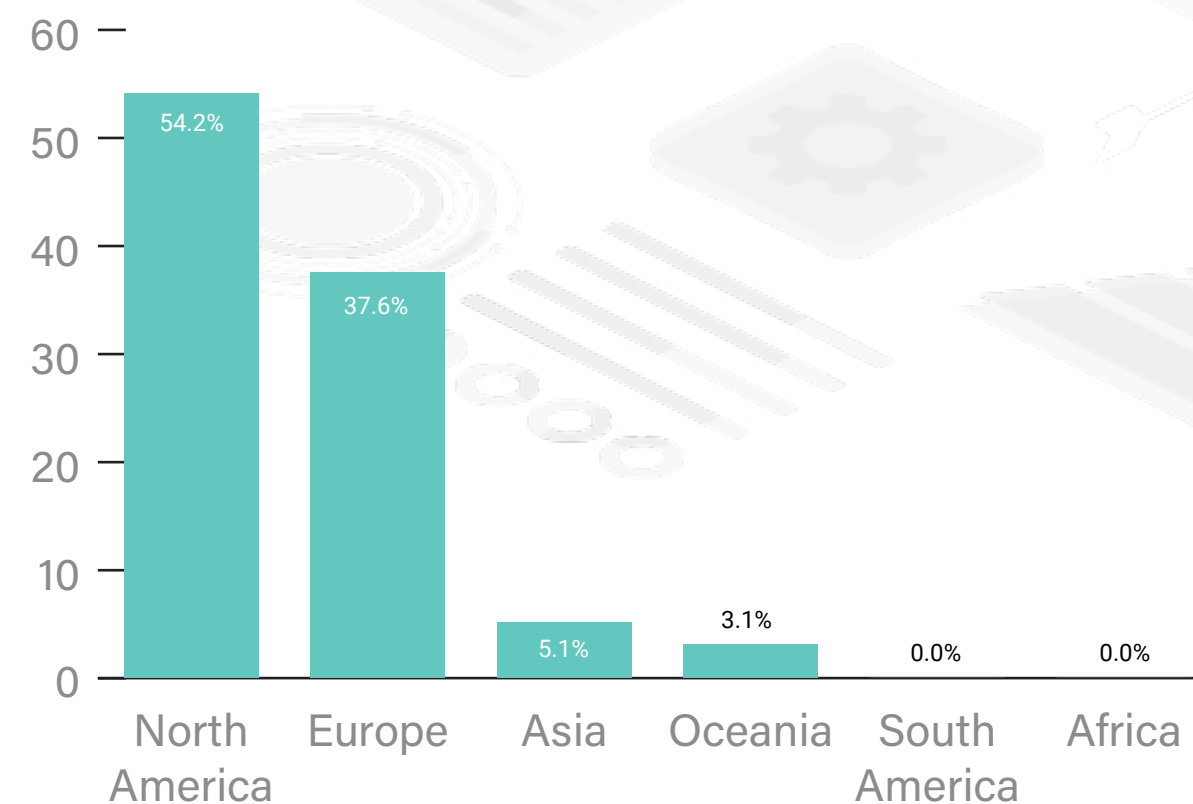
It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having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



OUR INSIGHTS

Since our last report which showed a decrease in Critical Risk Magento 2 websites due to a security patch, it appears risk has continued to decrease. This shows the importance of keeping your Magento installation up to date, as this has resulted in a marginal decline in hacked websites.

The High Risk numbers show that Magento 1 websites are at significant risk of being breached, while the number of High Risk Magento 2 websites is slowly decreasing. Simple - and mostly free or low cost - security controls will significantly reduce the risk of data compromise on these websites. Please see our Magento Security Insights page for guidance on the simple changes that can change a website's risk posture.

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