MAGENTO WEBSITE SECURITY REPORT

CONTACT US

WWW.FOREGENIX.COM/WEBSCAN

TEL: +44 845 309 6232

16TH NOVEMBER 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

16TH NOVEMBER 2020

OVERVIEW

WHAT IS WEBSCAN?

We currently monitor close to

270,000

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

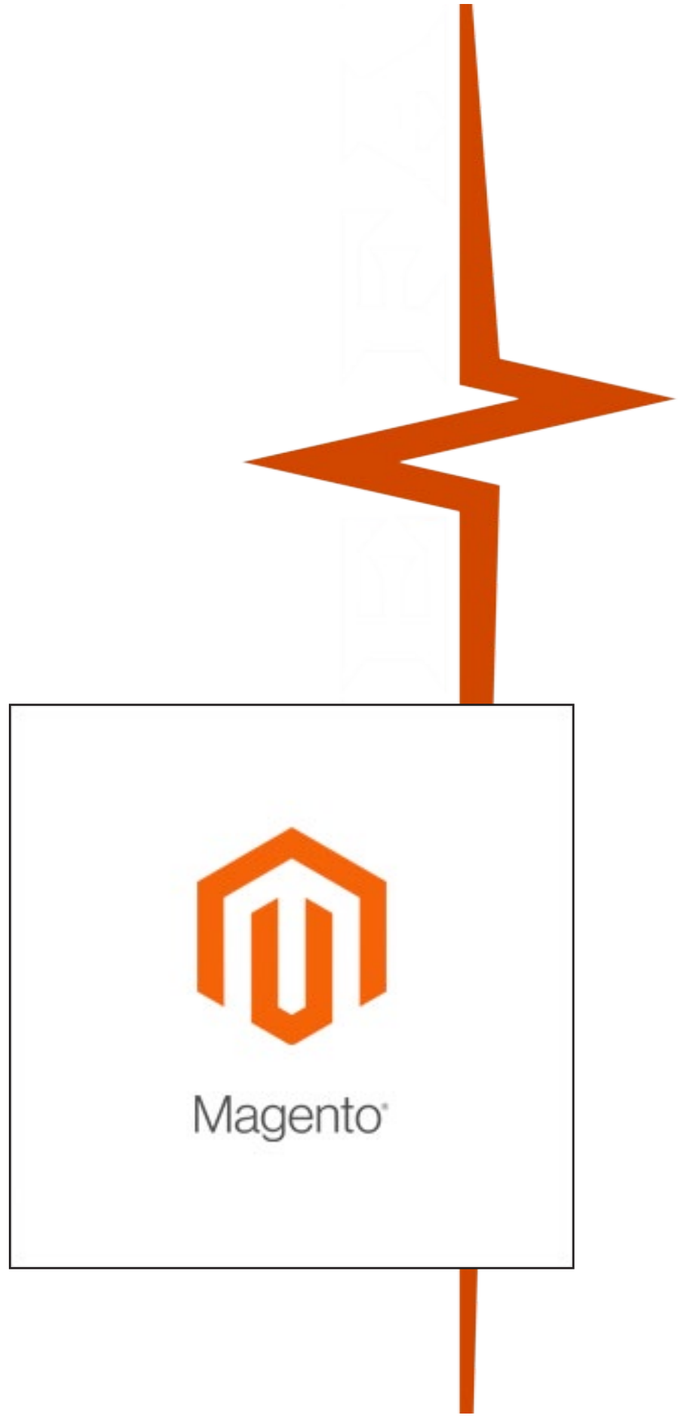
Over **170,000** websites remain on the Magento 1 platform

Magento 1 websites continue to slowly **DECLINE**

1,570 Magento 1 websites are hacked,
with payment data being stolen transaction by transaction

29% of Magento 2 websites are High/Critical Risk

MAGENTO 1 REMAINS THE MOST TARGETED PLATFORM BY CRIMINALS, FOLLOWED BY MAGENTO 2

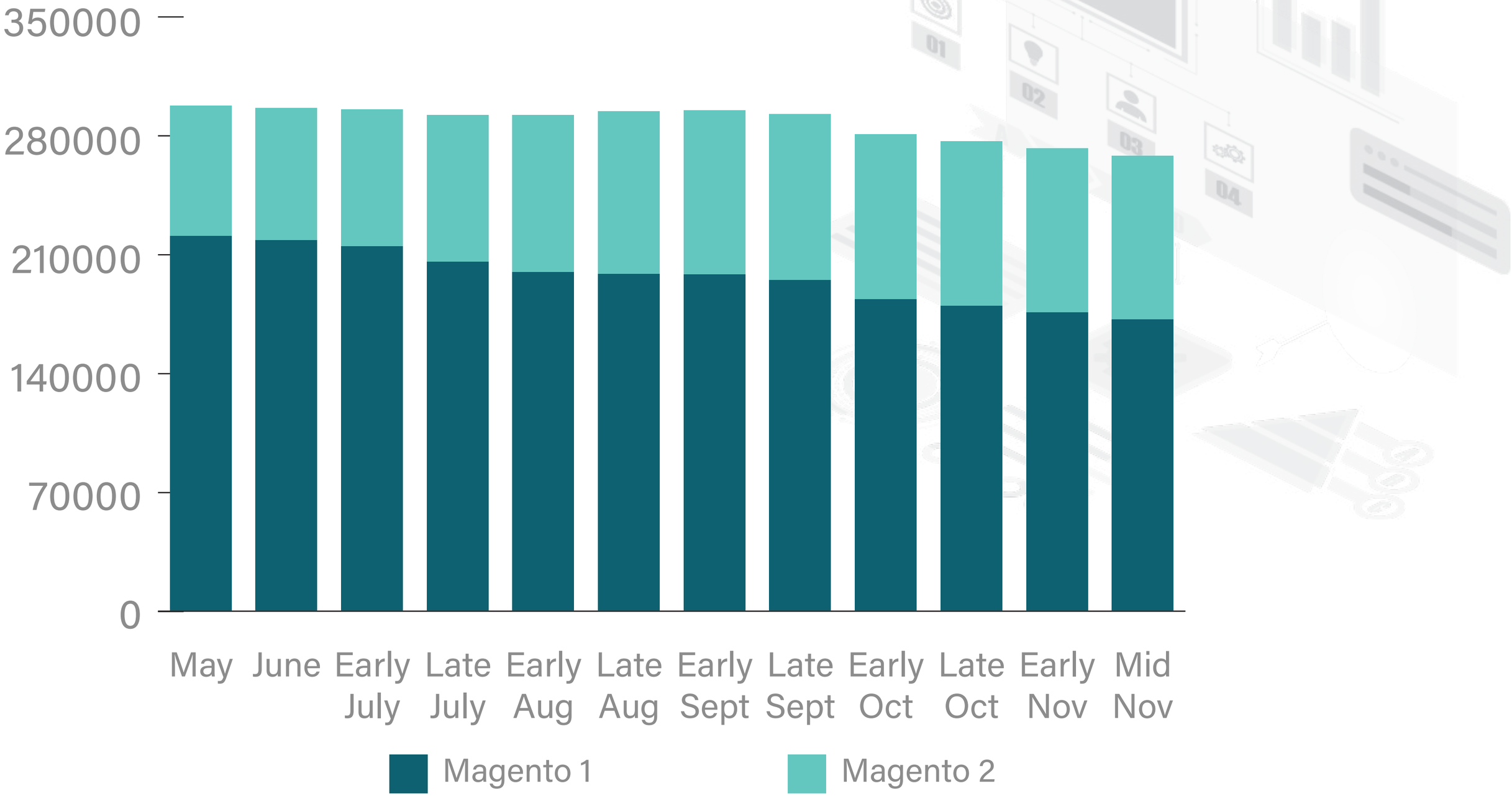


FOREGENIX

16TH NOVEMBER 2020

WEBSCAN RESULTS

WEBSITE NUMBERS (ALL MAGENTO)



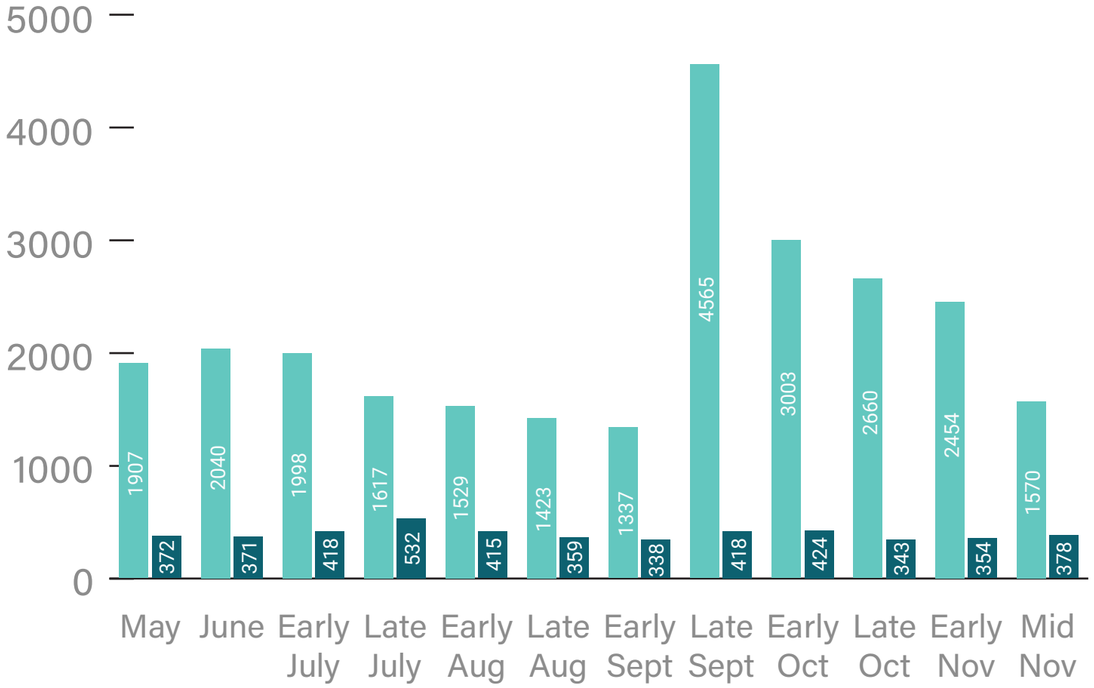
FOREGENIX

16TH NOVEMBER 2020

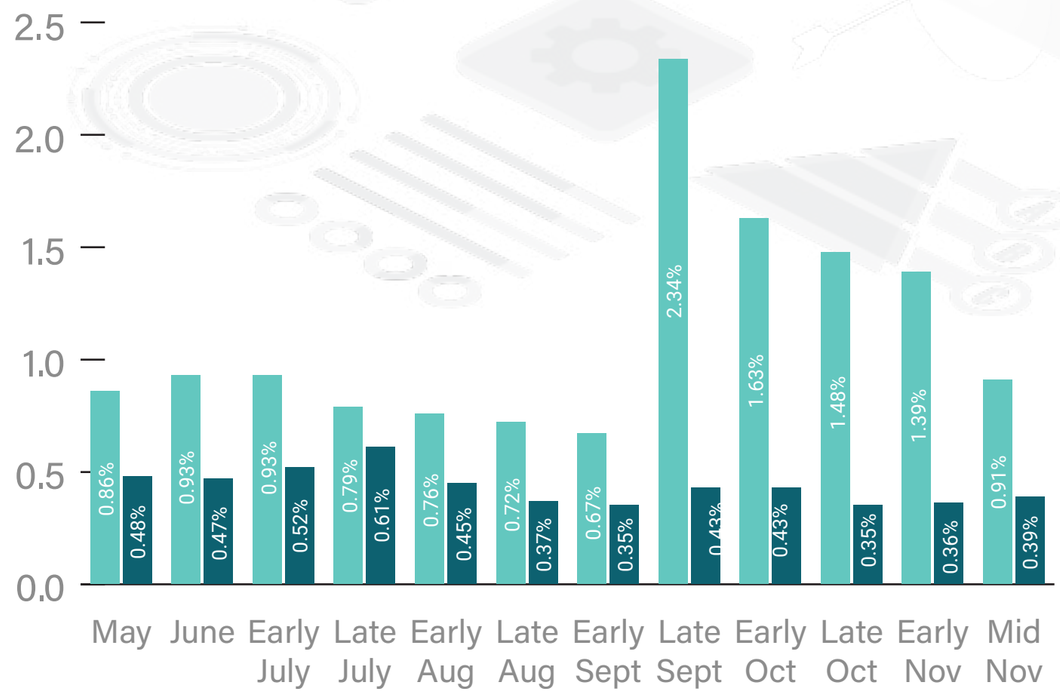
WEBSCAN RESULTS CRITICAL RISK

Websites with Critical Risk have already been hacked (with card data being actively stolen). Critical risk websites decreased massively for Magento 1, which correlates to the halving of '*Cardbleed*' malware reports. Numbers are now just a bit higher than pre-*Cardbleed* attack level.

ACTUAL NUMBERS



PERCENTAGE OF TOTAL SITES



FOREGENIX

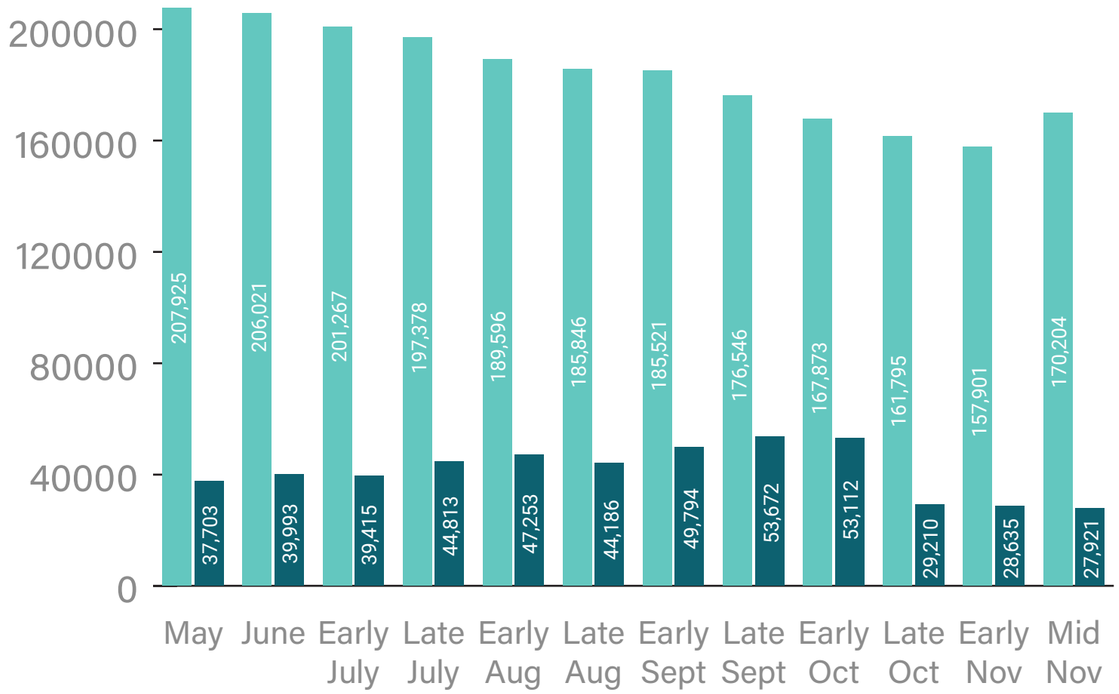
16TH NOVEMBER 2020

WEBSCAN RESULTS HIGH RISK

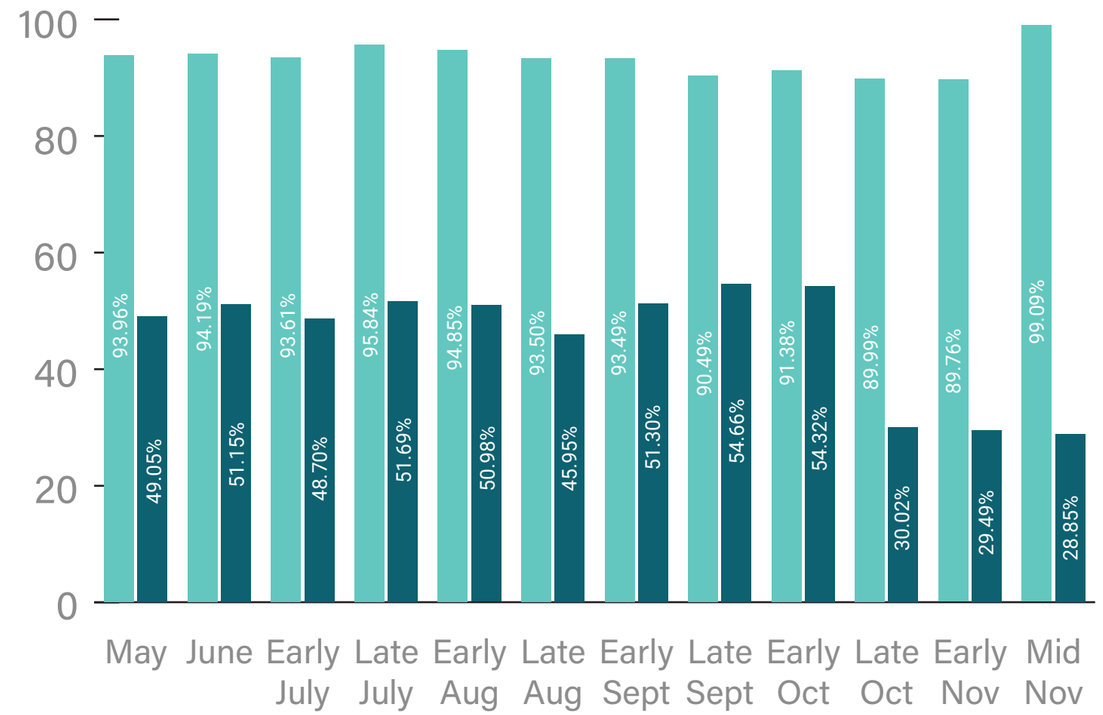
Websites with High Risk have significant security issues that make them very vulnerable to criminals.
The sites have one or more of the following:

- 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



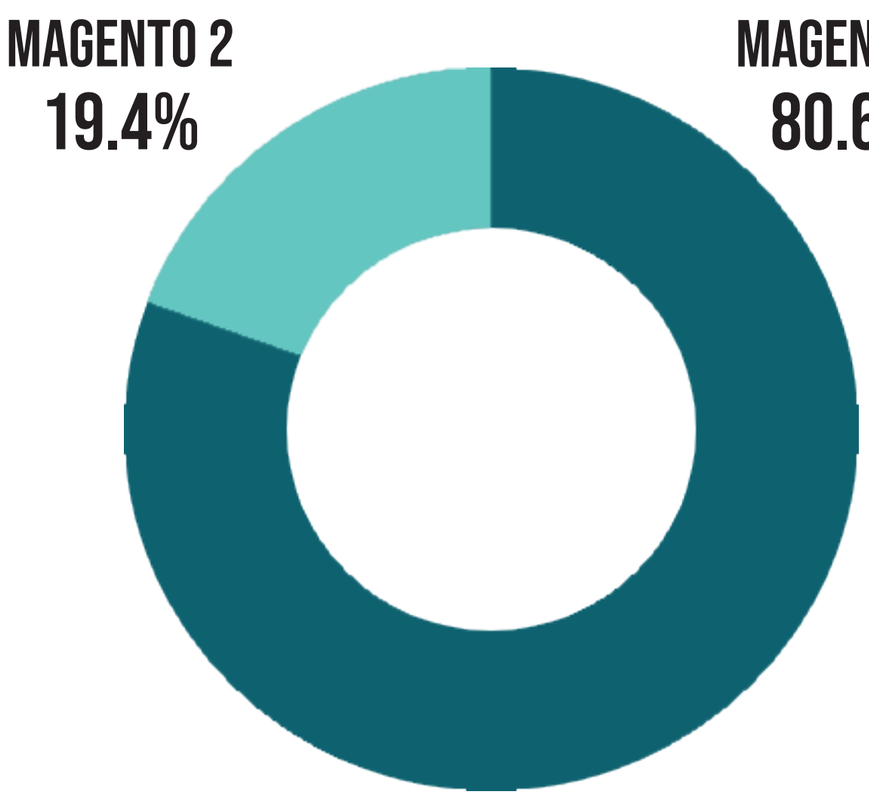
Magento 1 Magento 2

FOREGENIX

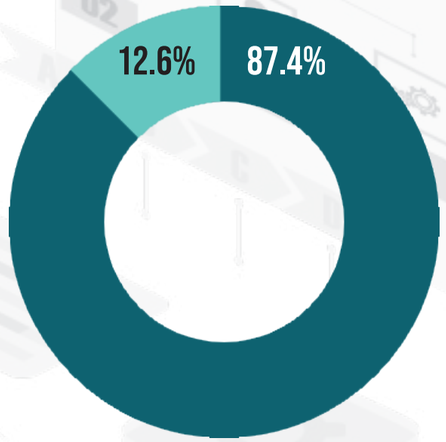
16TH NOVEMBER 2020

WEBSCAN RESULTS

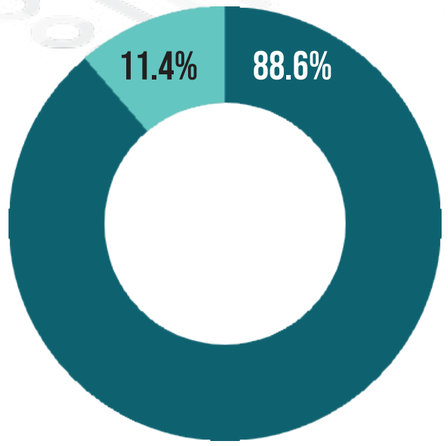
CARD-HARVESTING MALWARE DISTRIBUTION



TWO WEEKS AGO



ONE MONTH AGO



FOREGENIX

16TH NOVEMBER 2020

WEBSCAN RESULTS

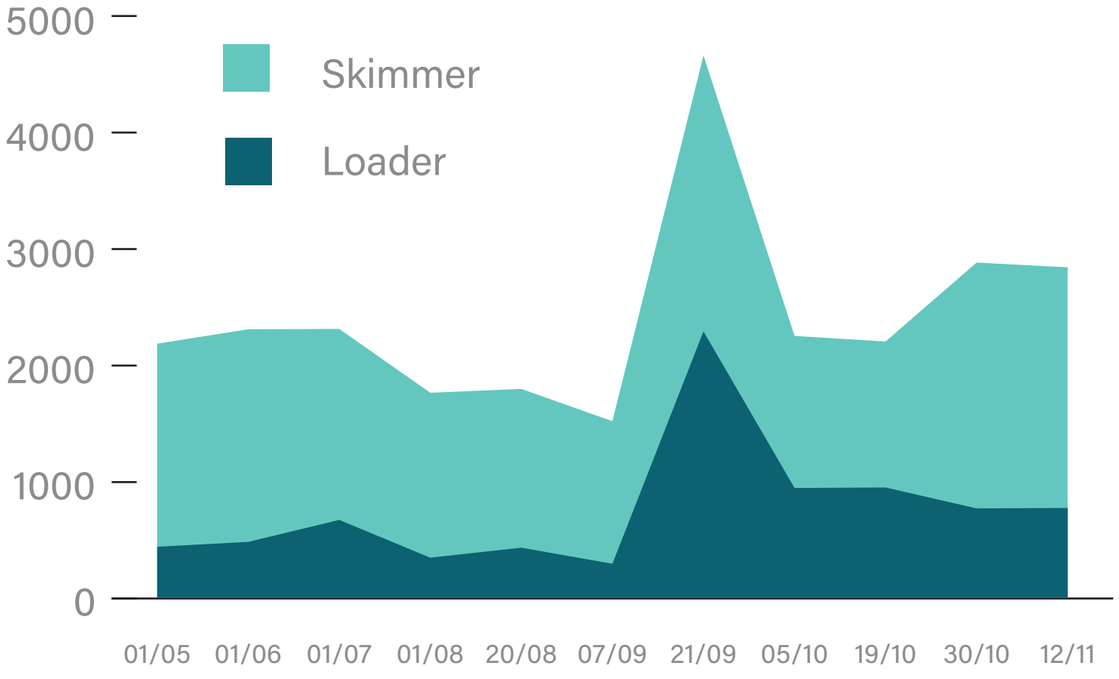
MAGENTO 1 & 2 - LOADERS & SKIMMERS

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.

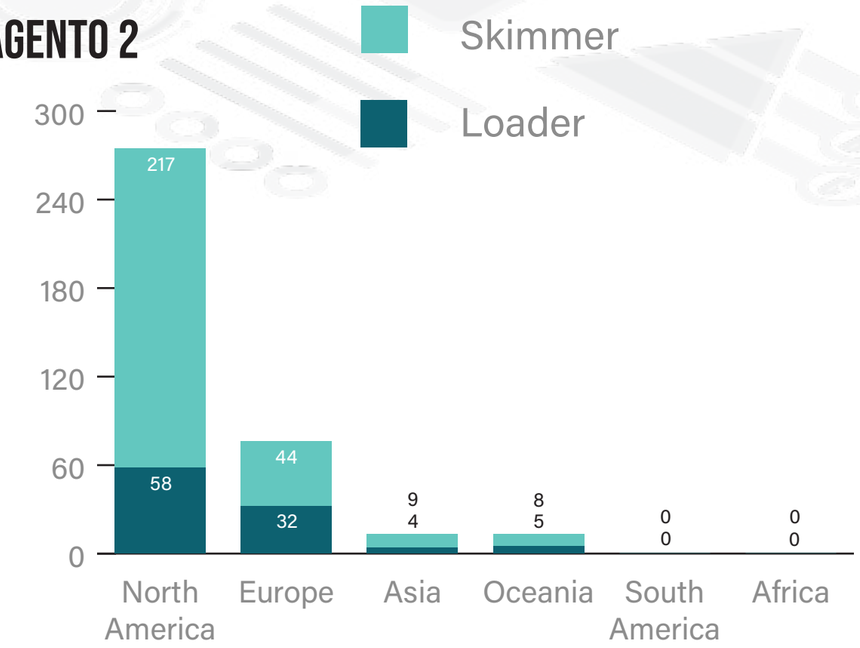
Skimmers - are malicious scripts designed to scrape card data and customer information from a site's payment page before sending them off to the attacker.

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

16TH NOVEMBER 2020

WEBSCAN RESULTS MAGENTO 1 & 2 - FRAMEWORK ISSUES

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

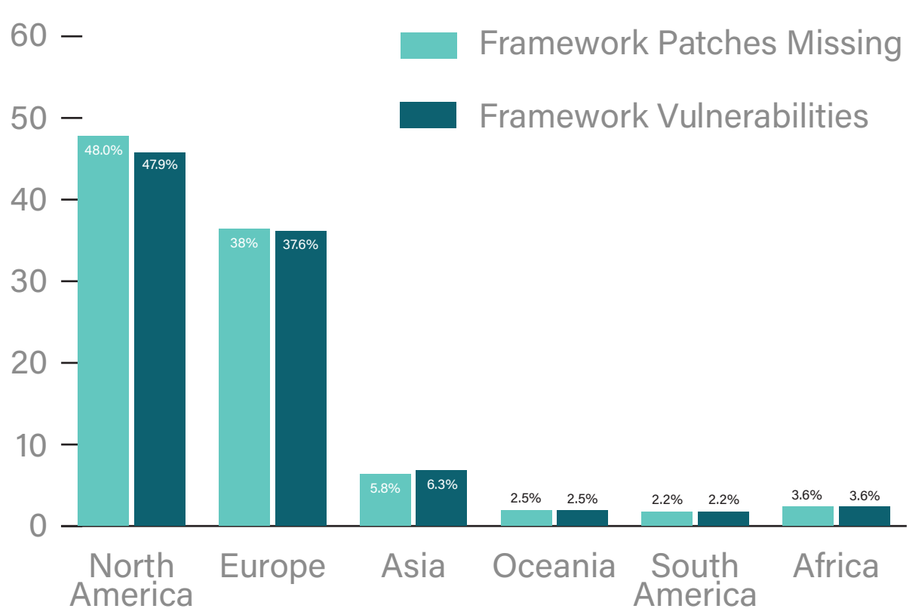
"**Framework security patches missing**" means a website is missing security patches/updates that are already available.

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

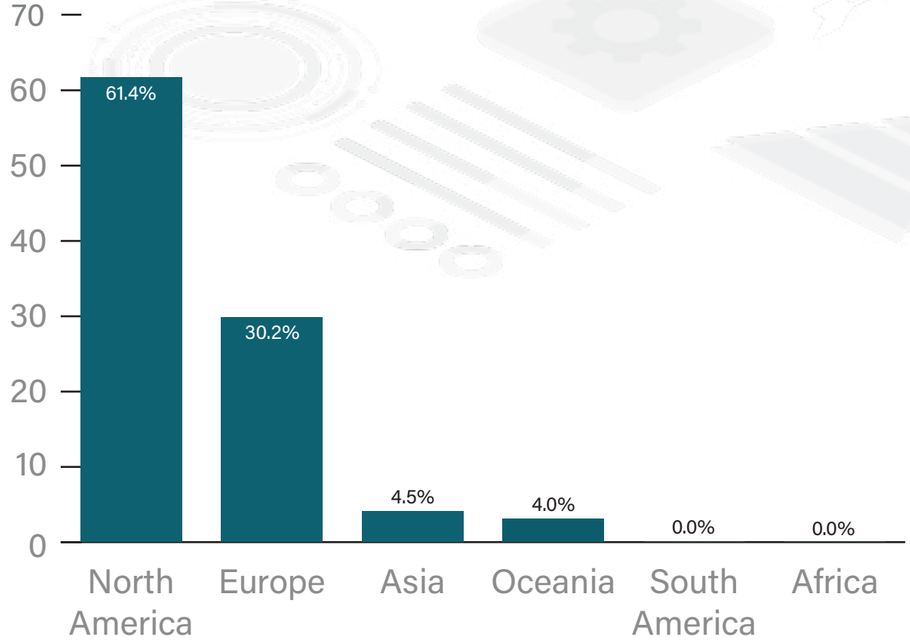
It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having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

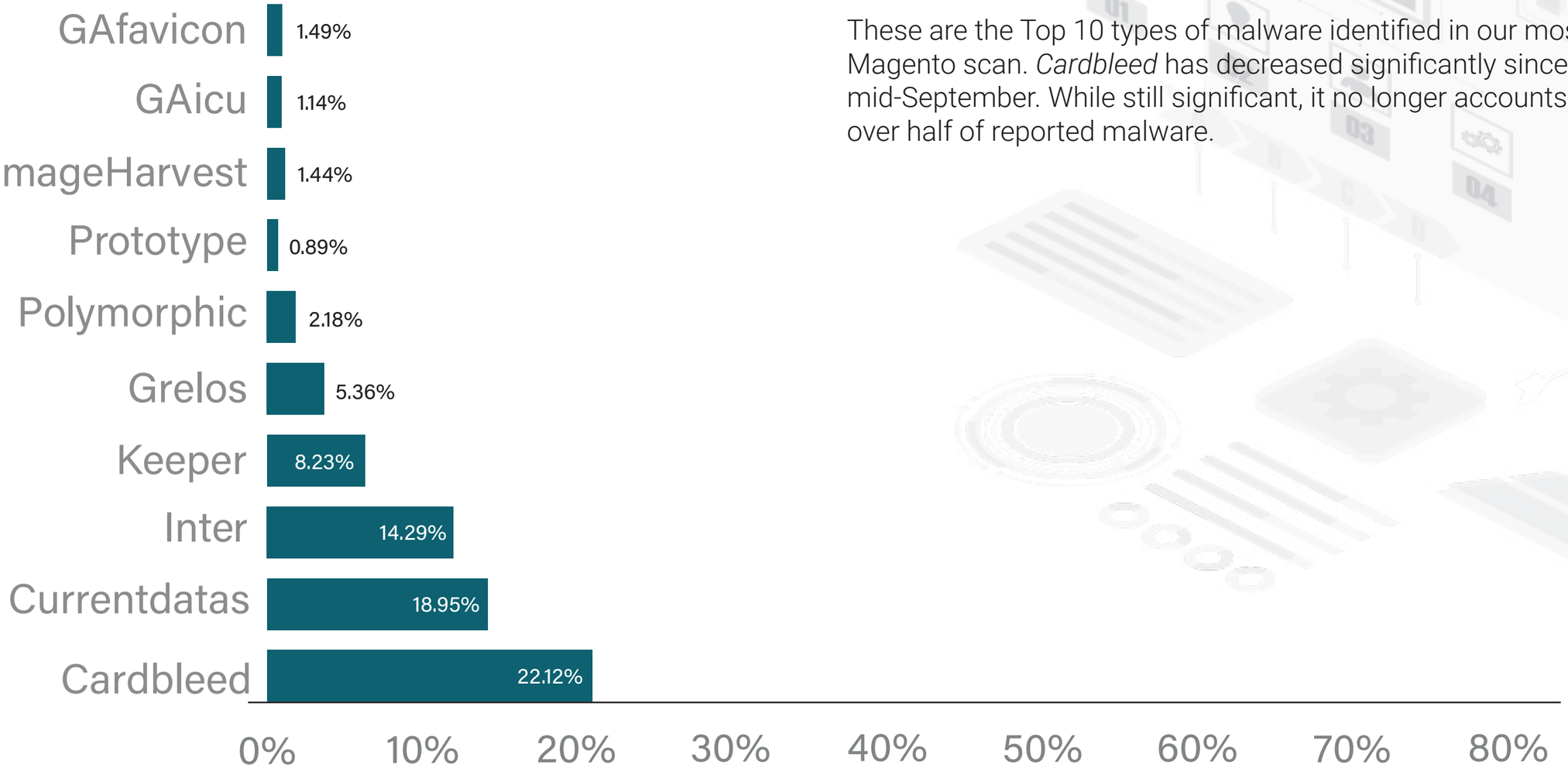
MAGENTO 1 PERCENTAGES



MAGENTO 2 PERCENTAGES



WEBSCAN RESULTS MALWARE TYPES



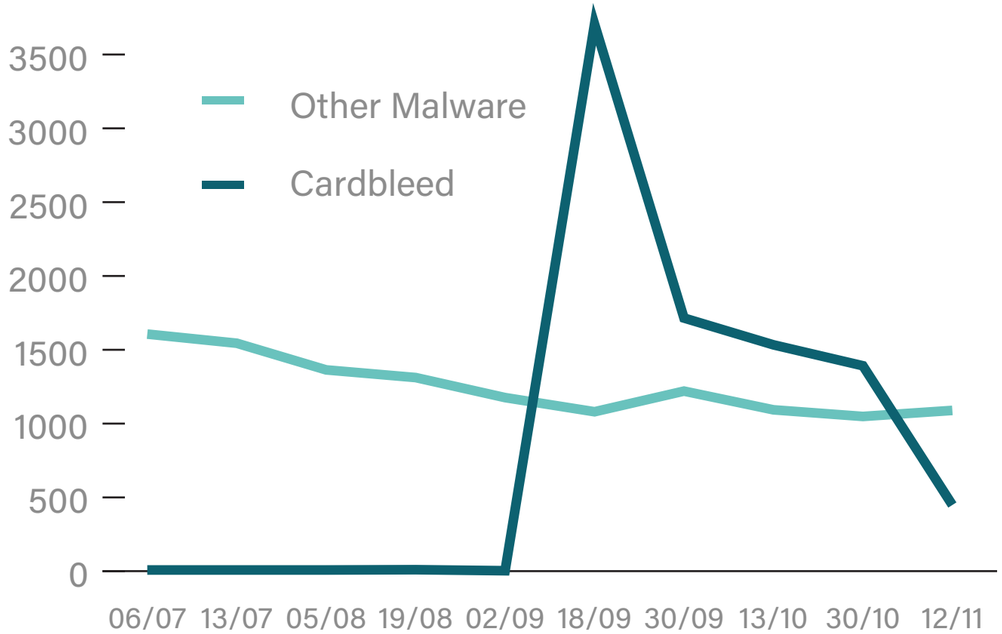
These are the Top 10 types of malware identified in our most recent Magento scan. *Cardbleed* has decreased significantly since its release in mid-September. While still significant, it no longer accounts for over half of reported malware.

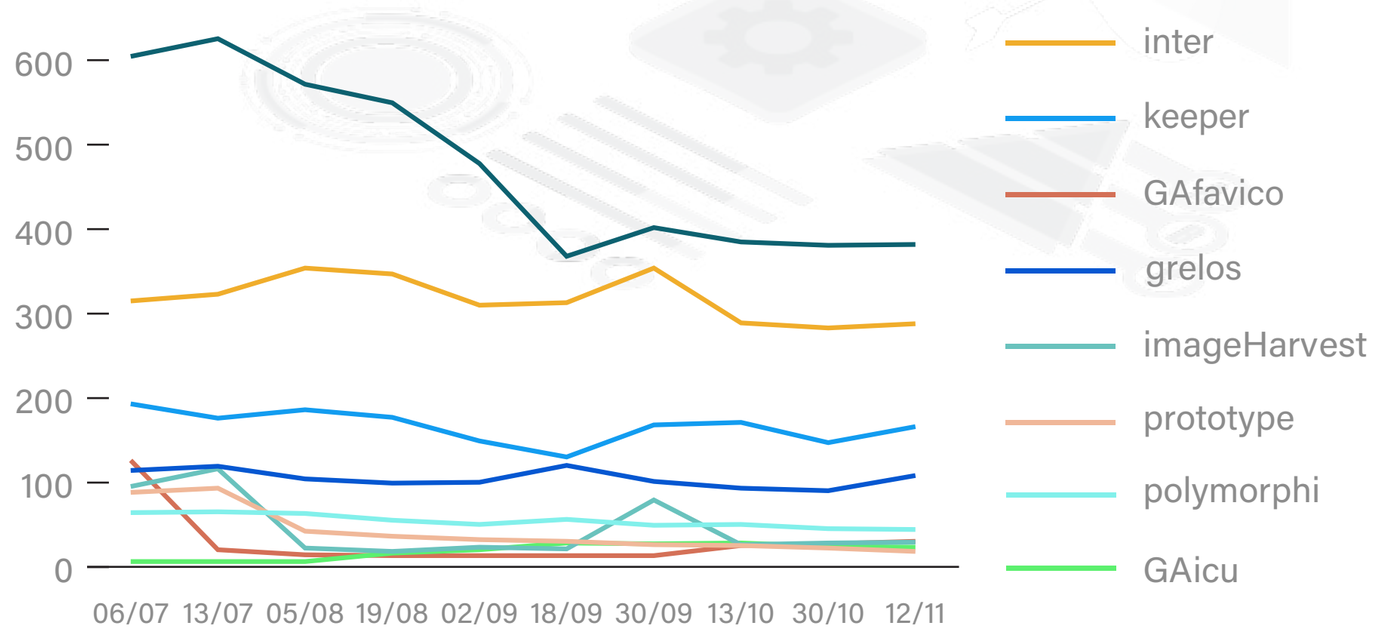
FOREGENIX

16TH NOVEMBER 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

16TH NOVEMBER 2020

OUR INSIGHTS

From this report onwards, we will classify any Magento 1 website as High risk. This is because Magento 1 has reached its End of Life, and will not have any more security updates. Therefore staying on this platform can be a real threat.

The number of Magento 1 websites continues to decrease. Which is good news, however, we believe that, unfortunately, some eCommerce websites on Magento 1, did not migrate to other platforms, but have indeed closed business. We believe this is due to the number of High and Critical Magento 1 websites, which were significant throughout 2020.

Some bad news, as well, is the fact that Magento 2 websites are increasingly getting hacked, as we can see that 24 sites have been hacked since our last report. This seems to be the trend at the end of the year.

We are not happy to see so many eCommerce sites closing their doors, nor the increasing number of hacked Magento 2 websites. Therefore, we remind website owners/administrators using Magento to check their configuration/set-ups and make sure it's secure. To protect your business we recommend using a website security solution, as well as cyber insurance.

For free guidance, check out our Magento Security Insights.

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

16TH NOVEMBER 2020