# MAGENTO WEBSITE SECURITY REPORT


## CONTACT US

WWW.FOREGENIX.COM/WEBSCAN

TEL: +44 845 309 6232


22ND FEBRUARY 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

22ND FEBRUARY 2021

# OVERVIEW

## WHAT IS WEBSCAN?

We currently monitor nearly

**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.

FOREGENIX

22ND FEBRUARY 2021

# 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

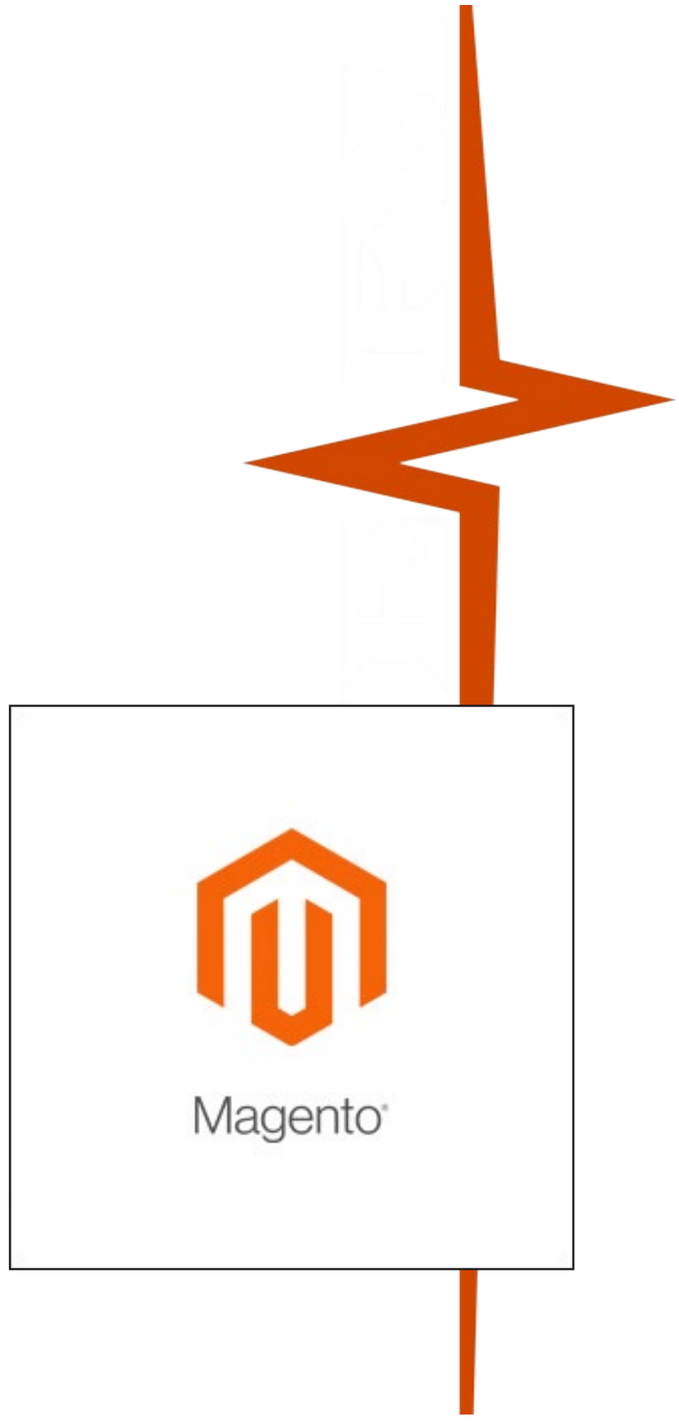
# OVERVIEW SUMMARY

Over **150,000** websites remain on the Magento 1 platform

The number of Magento 1 websites **DECREASED BY 2.4%**

Critical Magento 1 websites had a slight **DECREASE**

**26%** of Magento 2 websites are High/Critical Risk



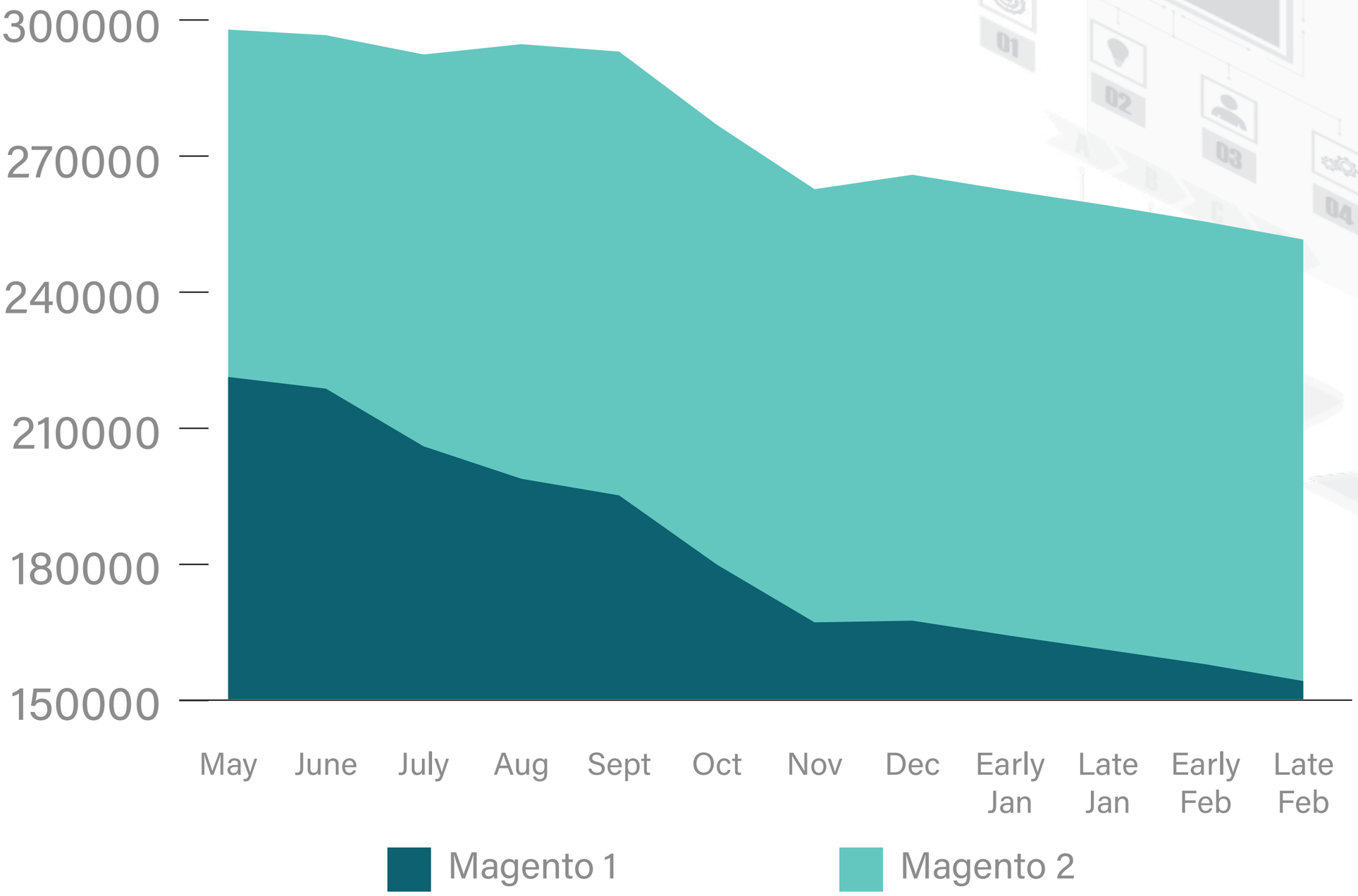

# MAGENTO 1 AND 2 REMAIN THE MOST TARGETED PLATFORMS BY CRIMINALS

FOREGENIX

22ND FEBRUARY 2021

# WEBSCAN RESULTS

## WEBSITE NUMBERS (ALL MAGENTO)



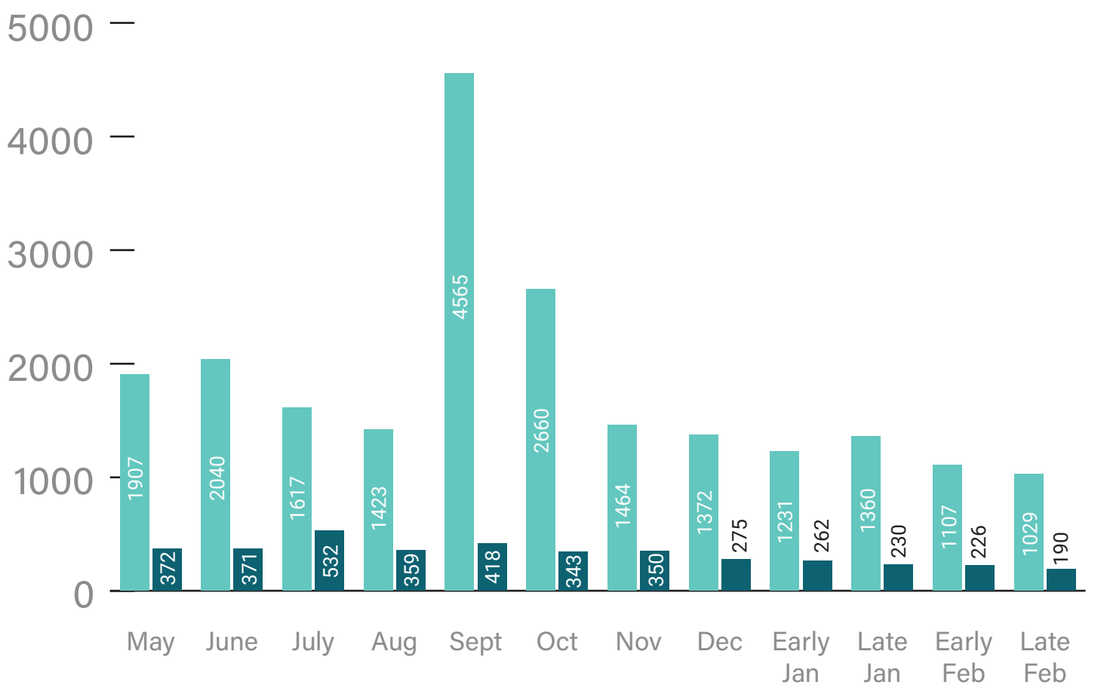

FOREGENIX

22ND FEBRUARY 2021

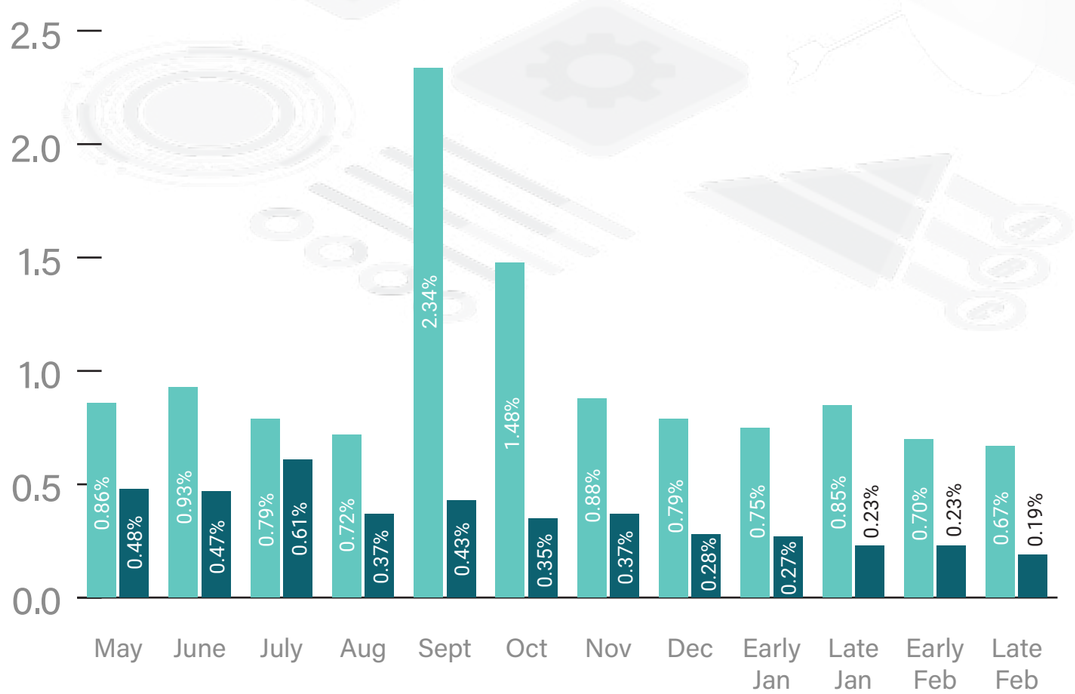
# WEBSCAN RESULTS CRITICAL RISK

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

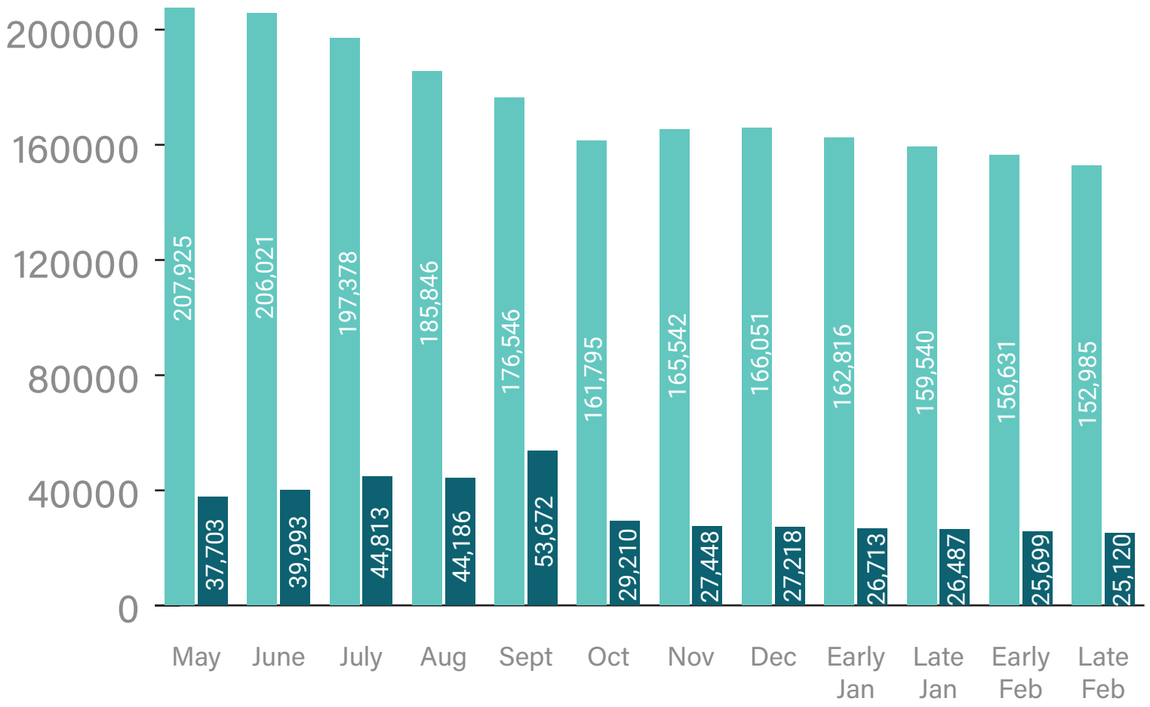
22ND FEBRUARY 2021

# WEBSCAN RESULTS HIGH RISK

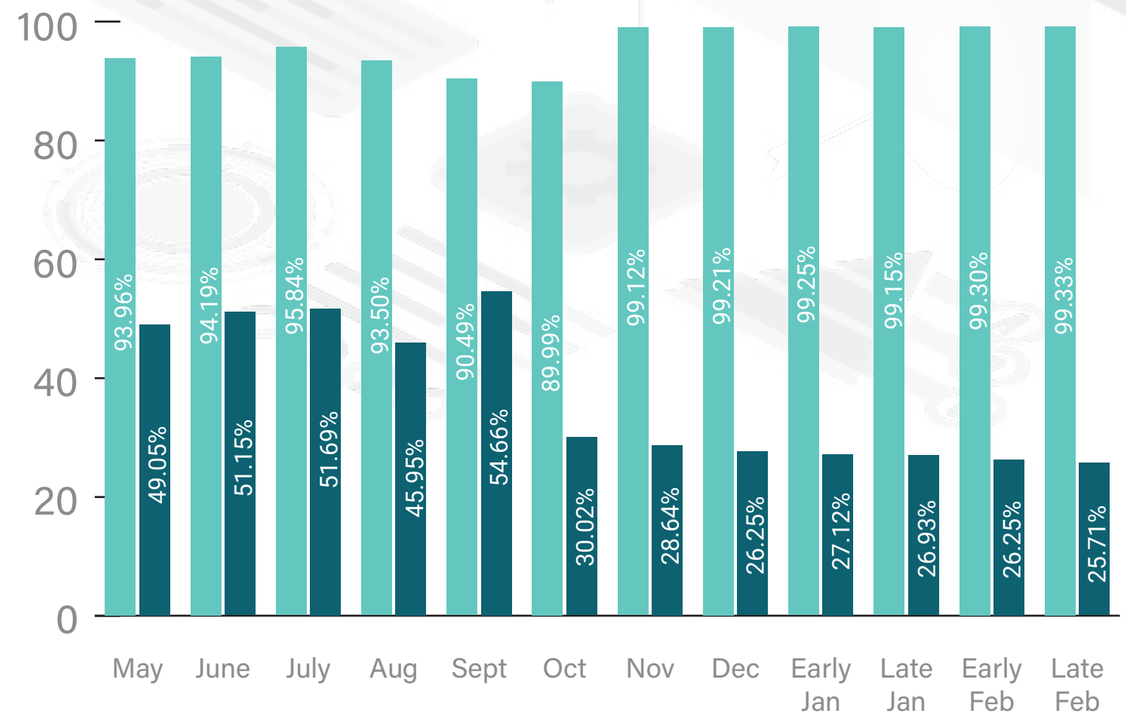
Websites identified as High Risk have significant security issues that make them very vulnerable to criminals. The sites have one or more of the following:

- 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



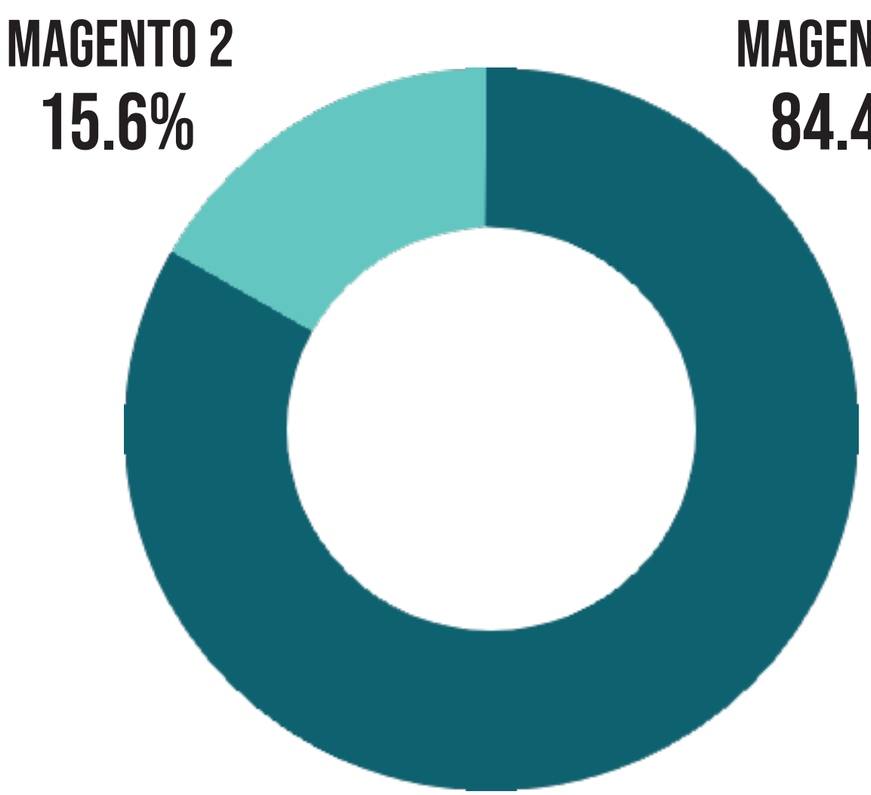

Magento 2

FOREGENIX

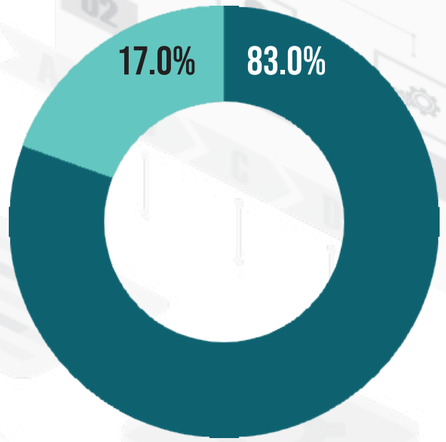
22ND FEBRUARY 2021

# WEBSCAN RESULTS

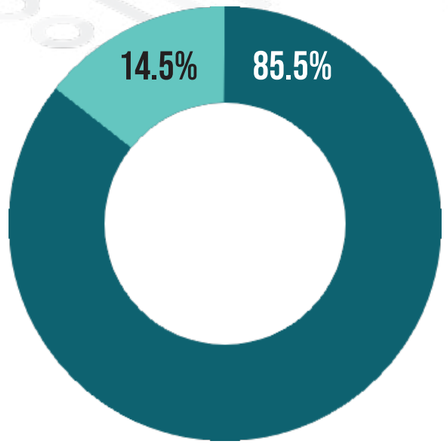
## CARD HARVESTING MALWARE DISTRIBUTION




TWO WEEKS AGO




ONE MONTH AGO




FOREGENIX

22ND FEBRUARY 2021

# WEBSCAN RESULTS

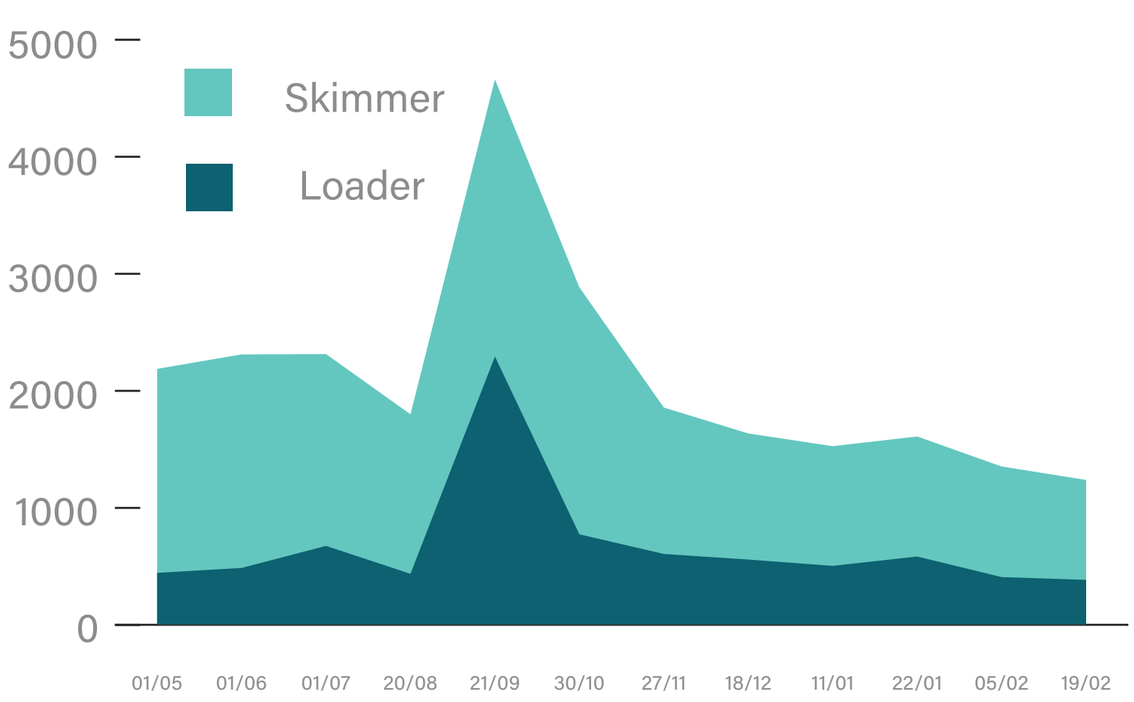
## MAGENTO 1 & 2 - LOADERS & SKIMMERS

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.

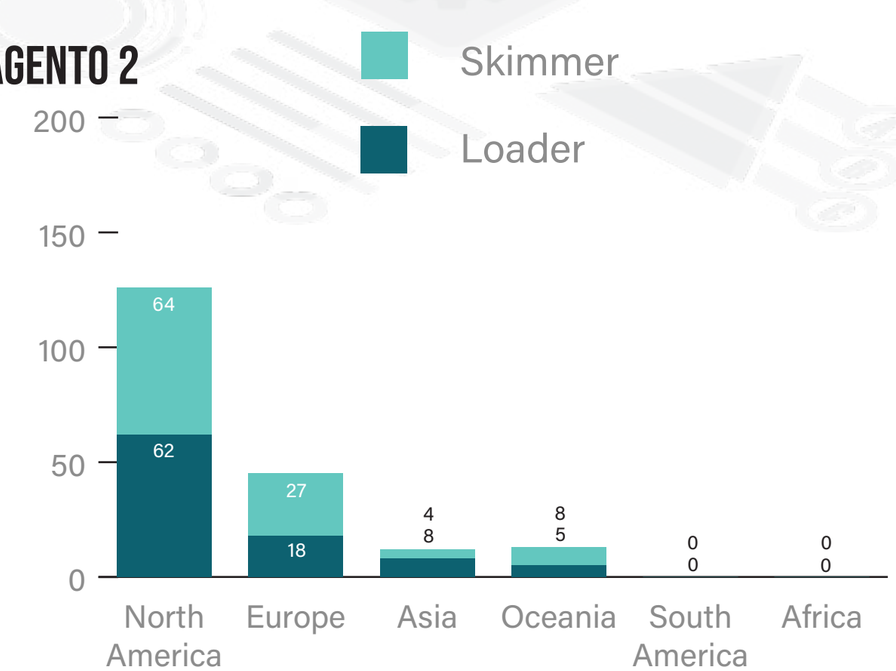
The charts to the right show which regions in the world have the highest infection rate, and below shows change over time.




### MAGENTO 1




### MAGENTO 2




FOREGENIX

22ND FEBRUARY 2021

# WEBSCAN RESULTS MAGENTO 1 & 2 - FRAMEWORK ISSUES

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

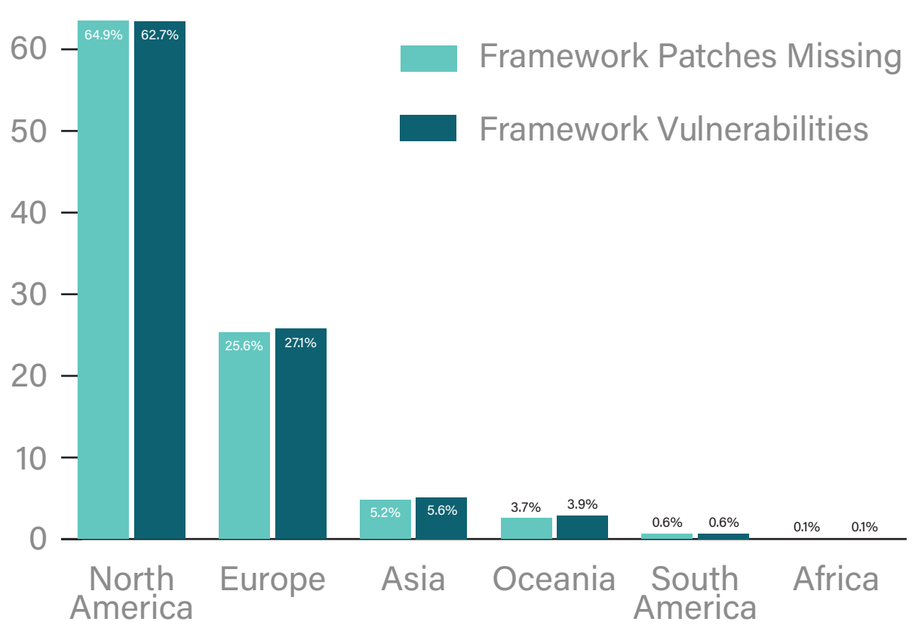
"**Framework Patches Missing**" means a website is missing security patches or updates that are already available.

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

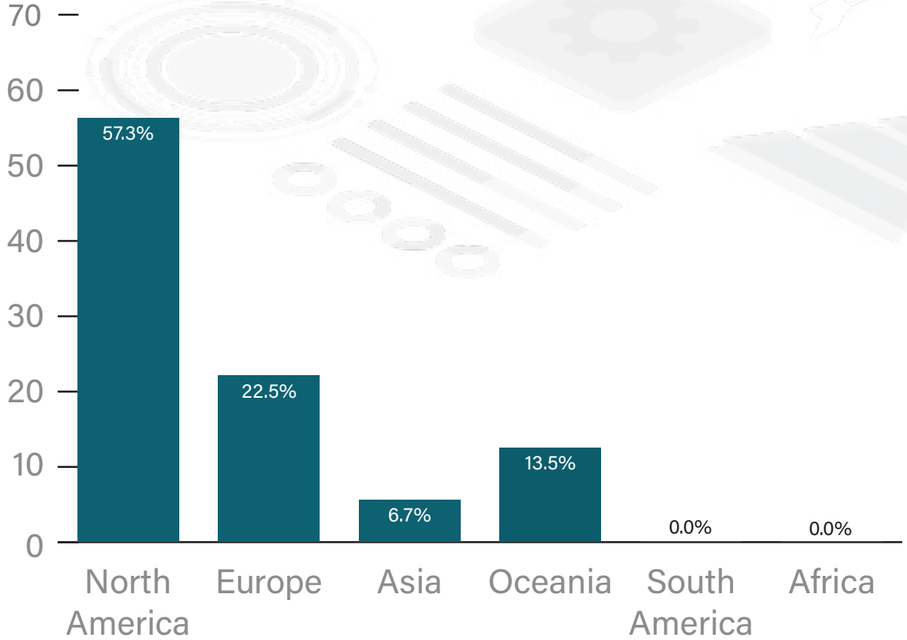
It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having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

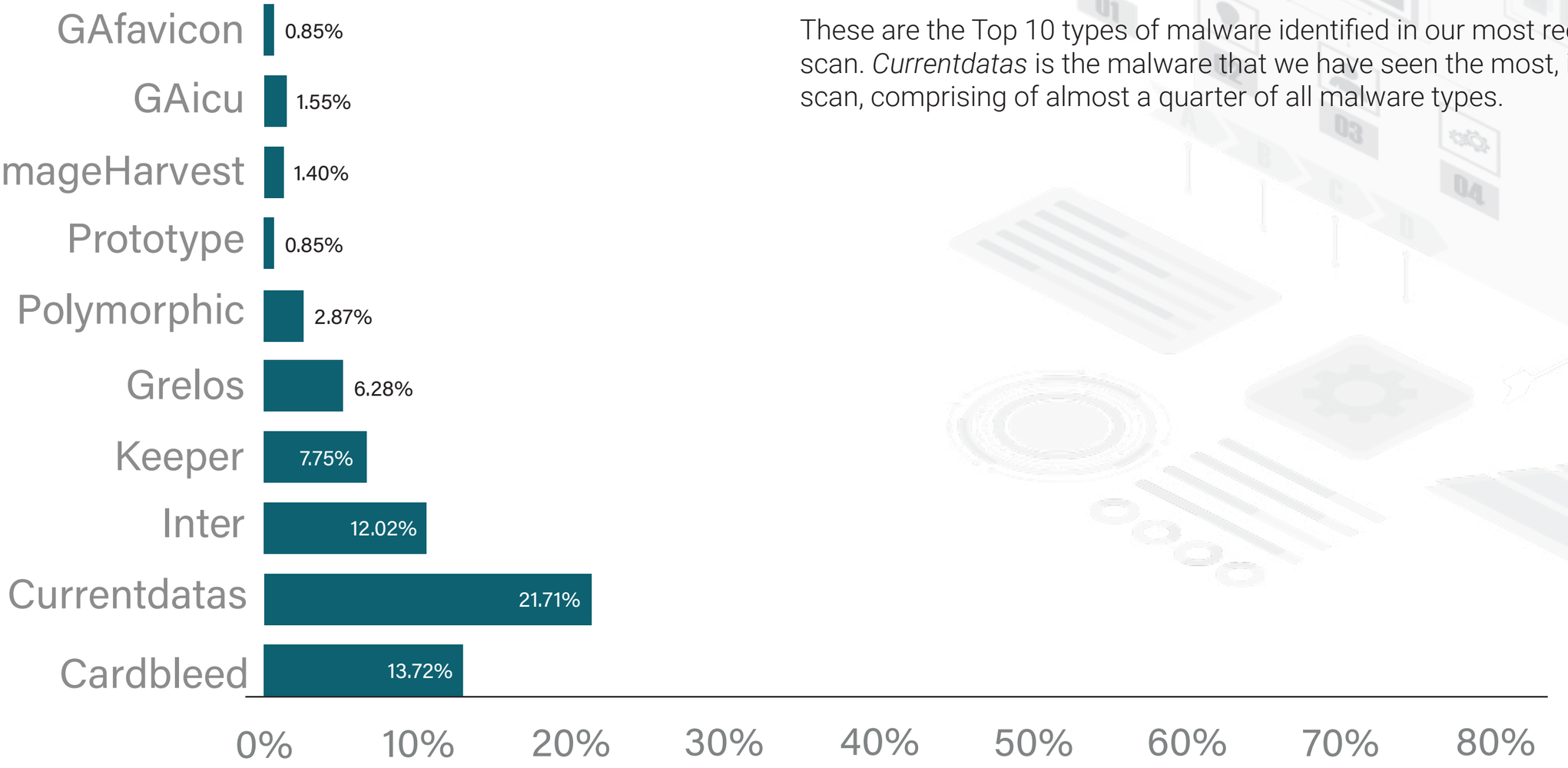



FOREGENIX

22ND FEBRUARY 2021

# WEBSCAN RESULTS

## MALWARE CAMPAIGNS



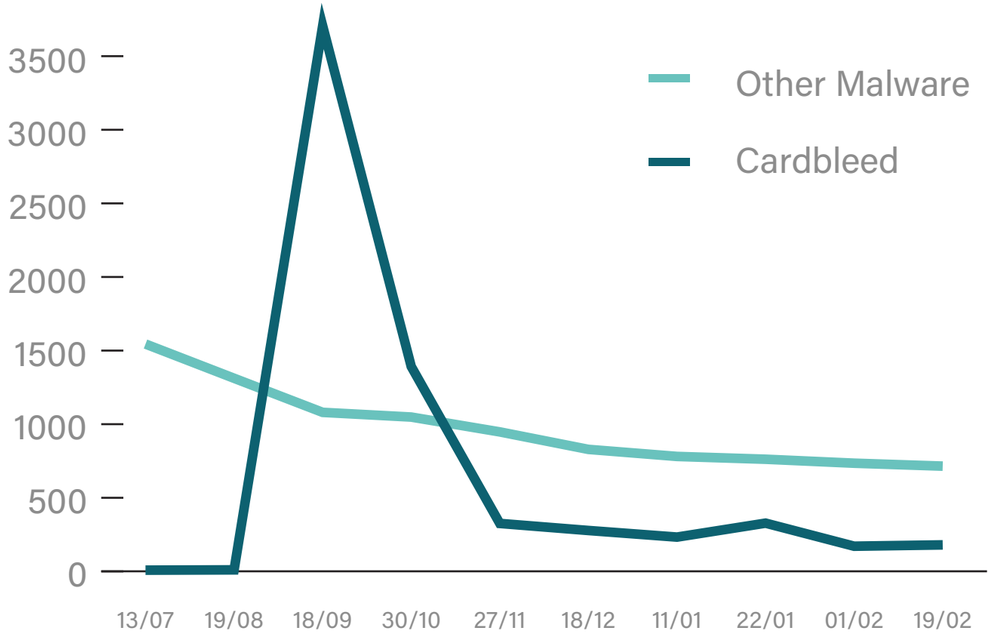

These are the Top 10 types of malware identified in our most recent Magento scan. *Currentdatas* is the malware that we have seen the most, in our latest scan, comprising of almost a quarter of all malware types.

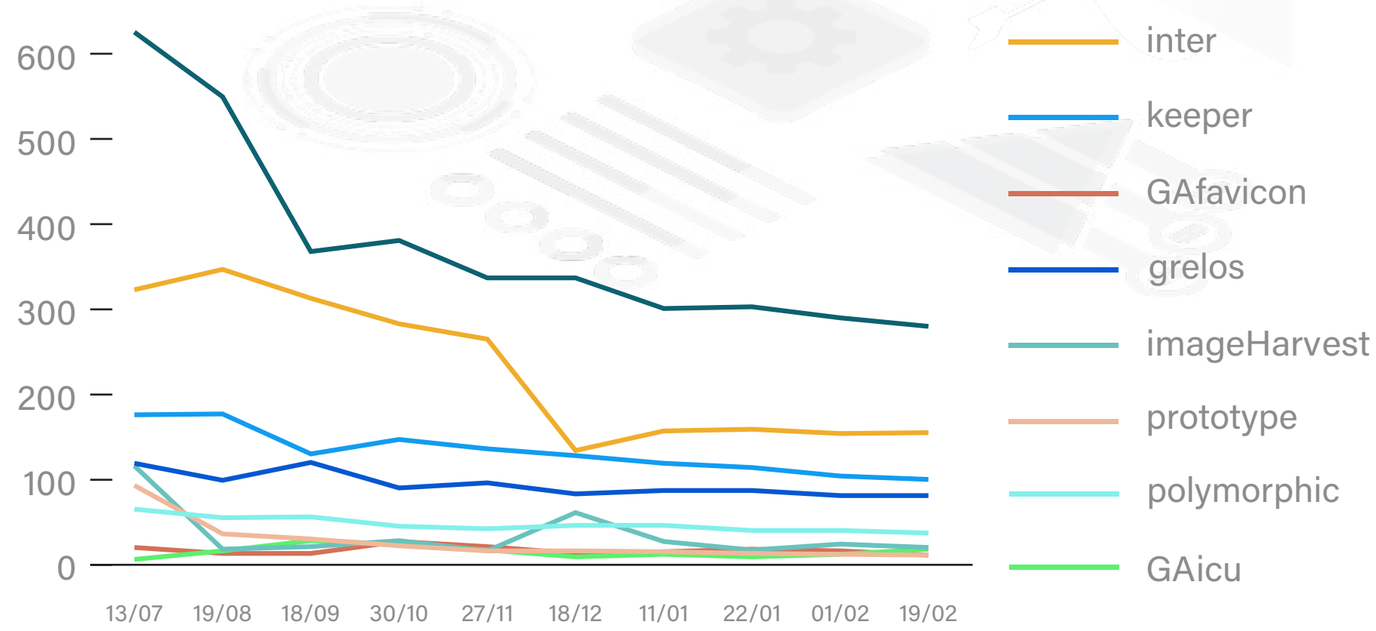
FOREGENIX

22ND FEBRUARY 2021

# WEBSCAN RESULTS MAGENTO 1 & 2 - MALWARE TRENDS

We are tracking the malware campaigns that are infecting Magento websites.
Due to the *Cardbleed* attack in September 2020, 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

22ND FEBRUARY 2021

# OUR INSIGHTS

The number of Magento websites continues to decline. In the last 14 days we saw a drop of 3,725 Magento websites; in which Magento 1 (M1) sees a decrease of 2.36%, and Magento 2 (M2) by 0.23%.

At the moment, 0.48% of all Magento websites are infected with card harvesting malware.

M1 websites have reached their end of life, meaning they are in constant danger of being breached. If your eCommerce website is still on M1, consider migrating to M2 as soon as possible. Remember, new automated attack campaigns, such as *Cardbleed*, can happen at any time.

Check out our Magento Security Insights page for free guidance. For that extra peace of mind, start 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

FOREGENIX

22ND FEBRUARY 2021