# MAGENTO WEBSITE SECURITY REPORT


## CONTACT US

WWW.FOREGENIX.COM/WEBSCAN

TEL: +44 845 309 6232


8TH 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

8TH 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

8TH 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

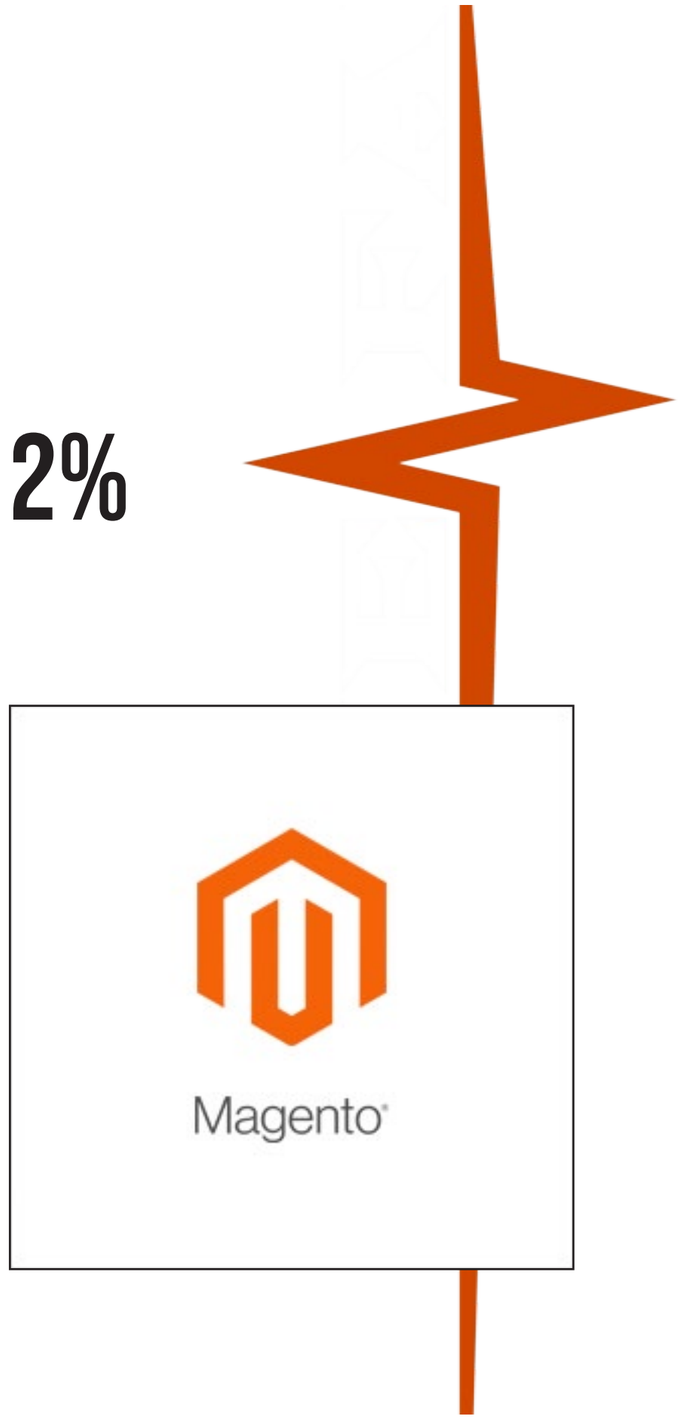
# OVERVIEW SUMMARY

Nearly **160,000** websites remain on the Magento 1 platform

The number of Magento 1 websites **DECREASED BY ALMOST 2%**

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

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



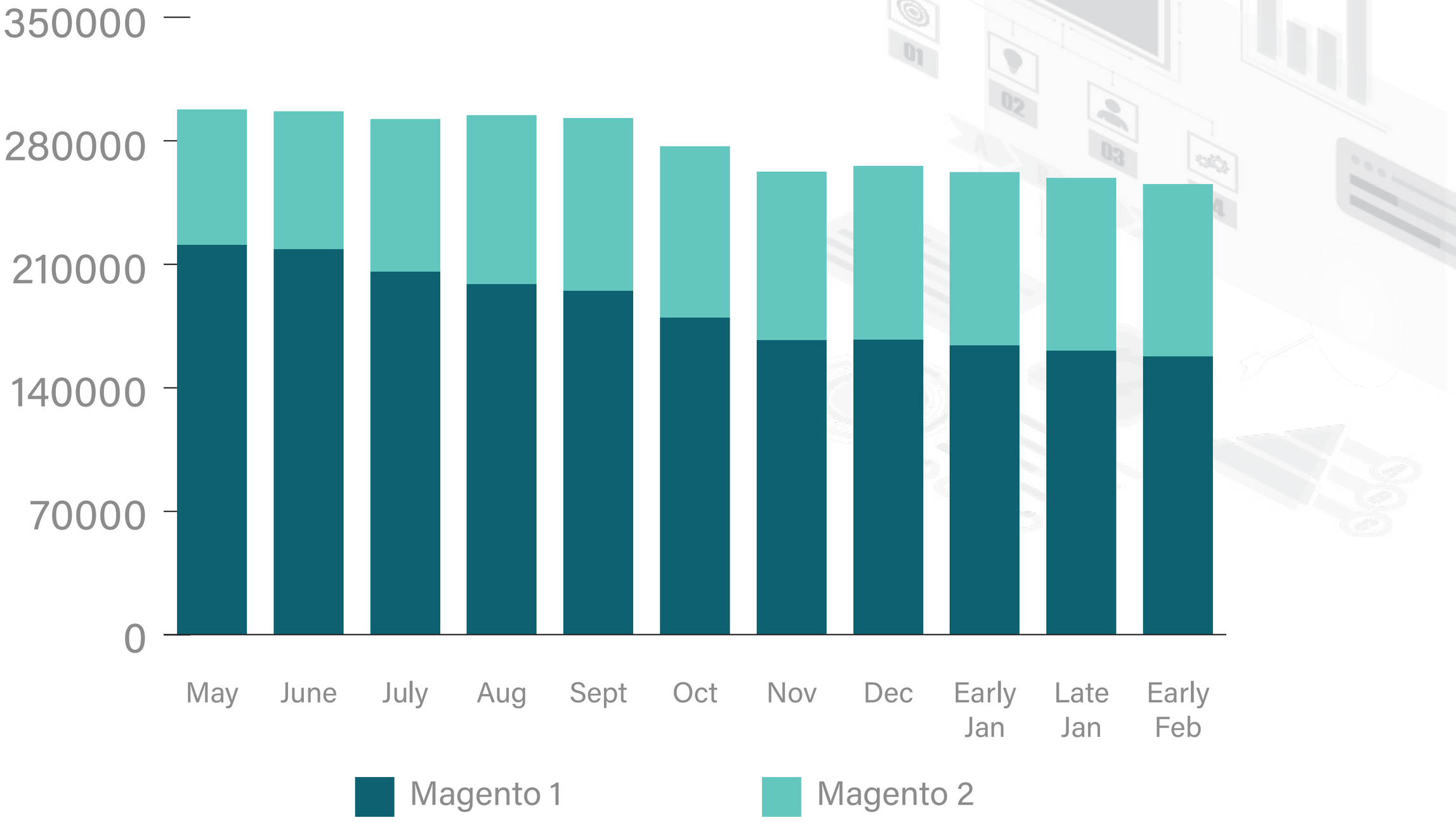

## MAGENTO 1 AND 2 REMAIN THE MOST TARGETED PLATFORMS BY CRIMINALS

FOREGENIX

8TH FEBRUARY 2021

# WEBSCAN RESULTS

## WEBSITE NUMBERS (ALL MAGENTO)



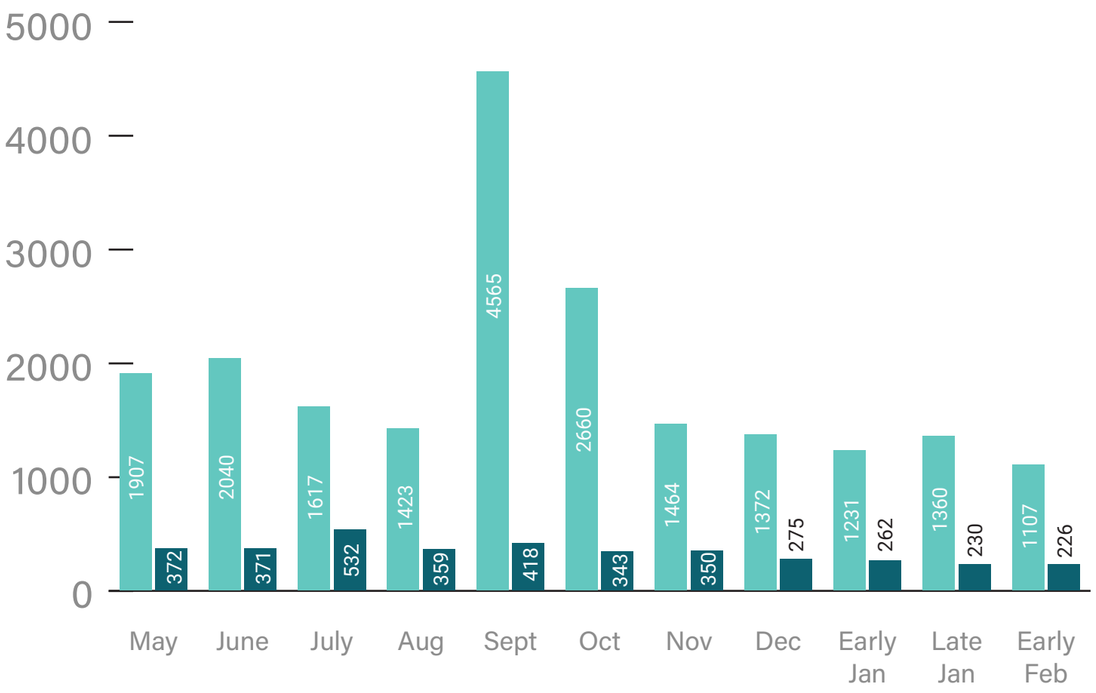

FOREGENIX

8TH FEBRUARY 2021

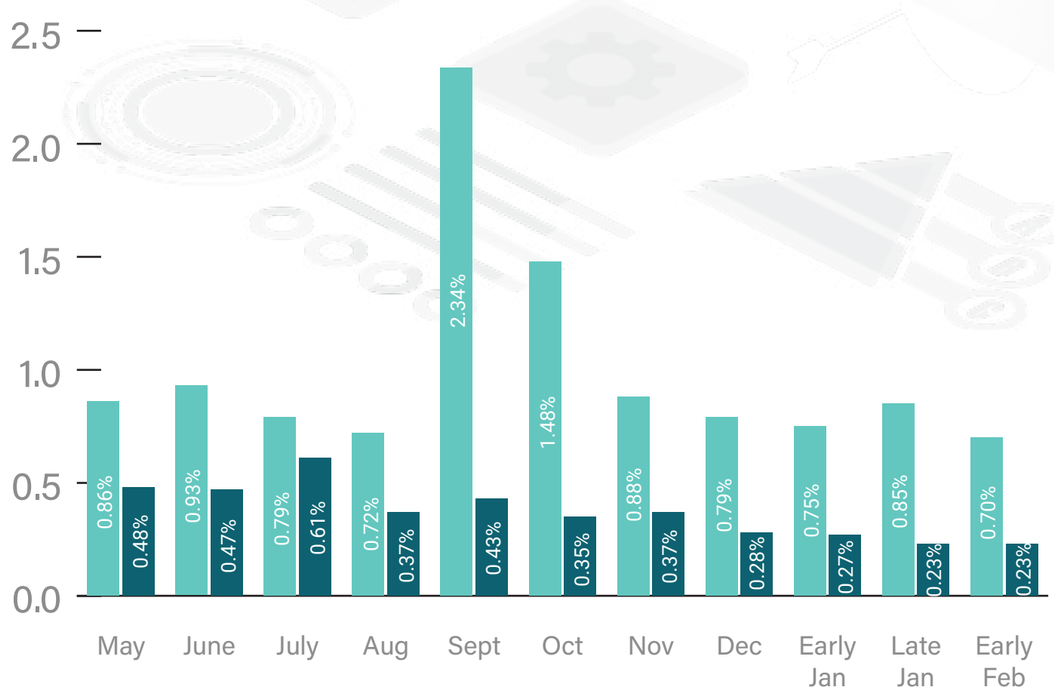
# WEBSCAN RESULTS CRITICAL RISK

Websites identified as Critical Risk have already been hacked
(with card data being actively stolen).

## ACTUAL NUMBERS




## PERCENTAGE OF TOTAL SITES




FOREGENIX

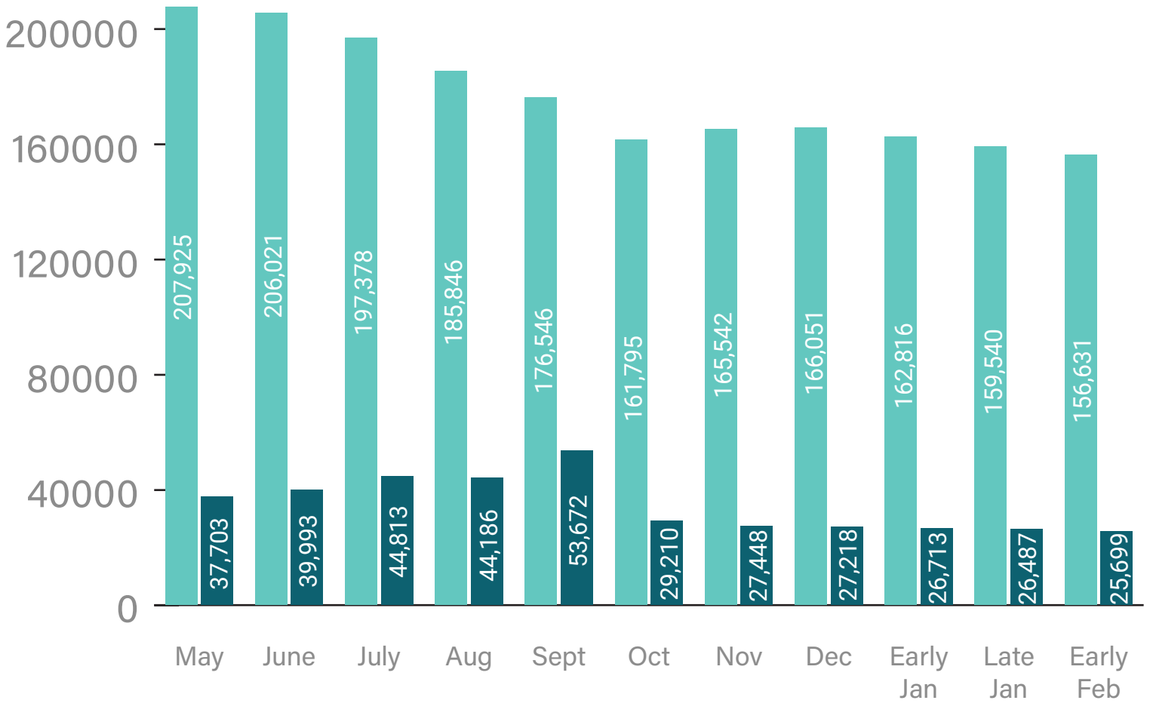
8TH FEBRUARY 2021

# WEBSCAN RESULTS HIGH RISK

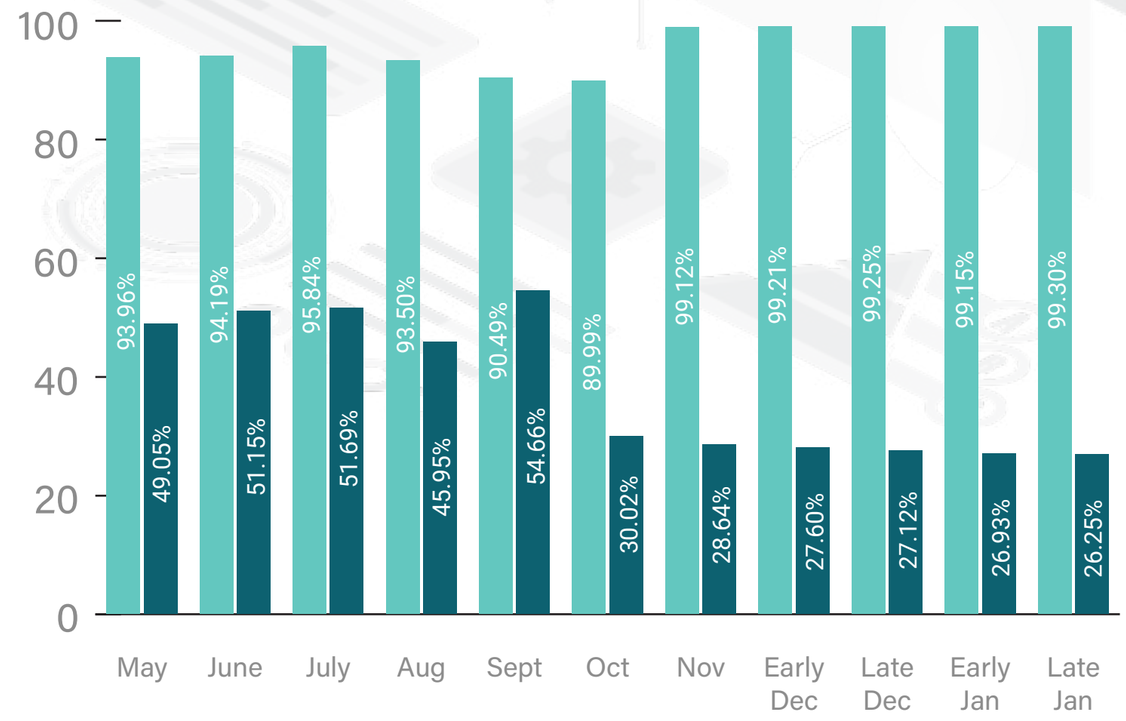
Websites identified as High Risk have significant security issues that make them very vulnerable to criminals. The sites have one or more of the following:

- 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



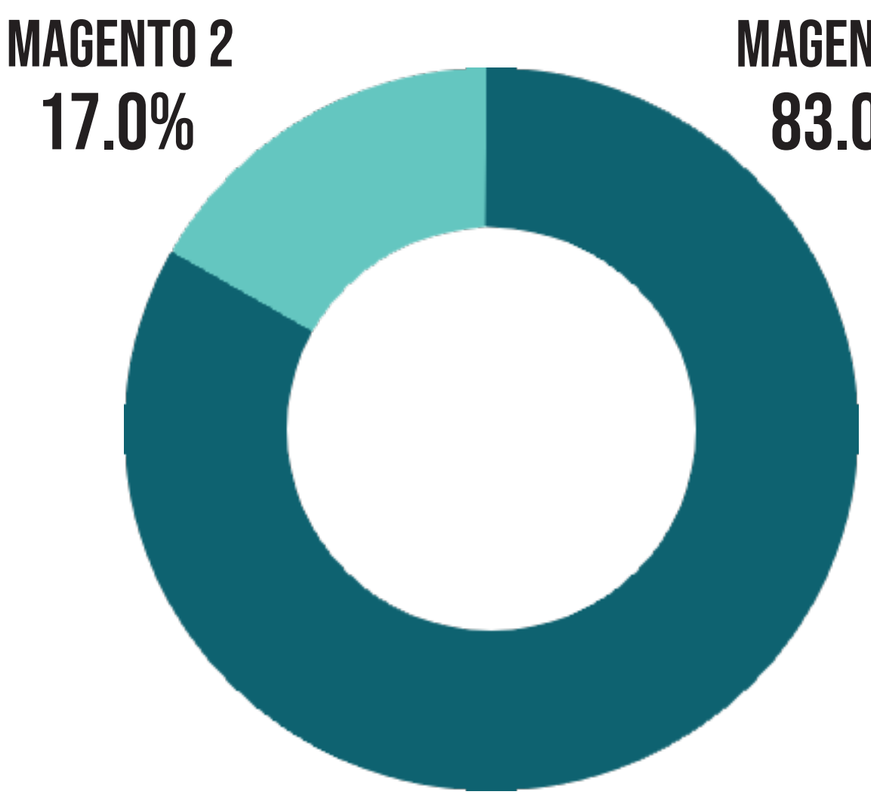

Magento 1 Magento 2

FOREGENIX

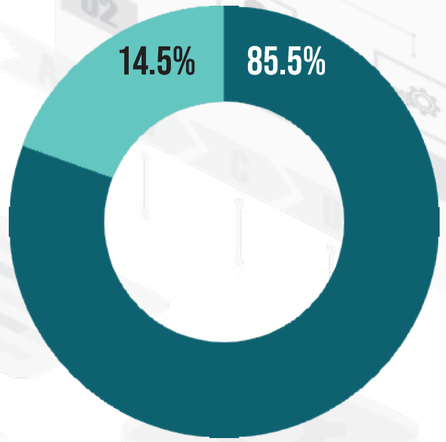
8TH FEBRUARY 2021

# WEBSCAN RESULTS

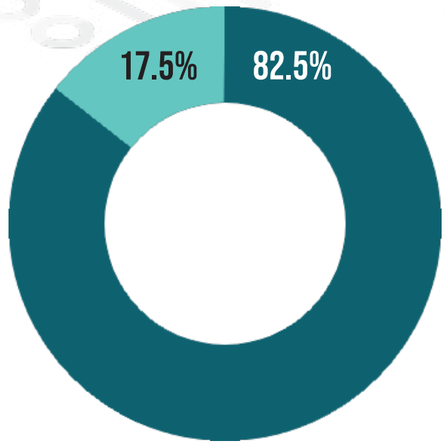
## CARD HARVESTING MALWARE DISTRIBUTION




TWO WEEKS AGO




ONE MONTH AGO




FOREGENIX

8TH FEBRUARY 2021

# WEBSCAN RESULTS

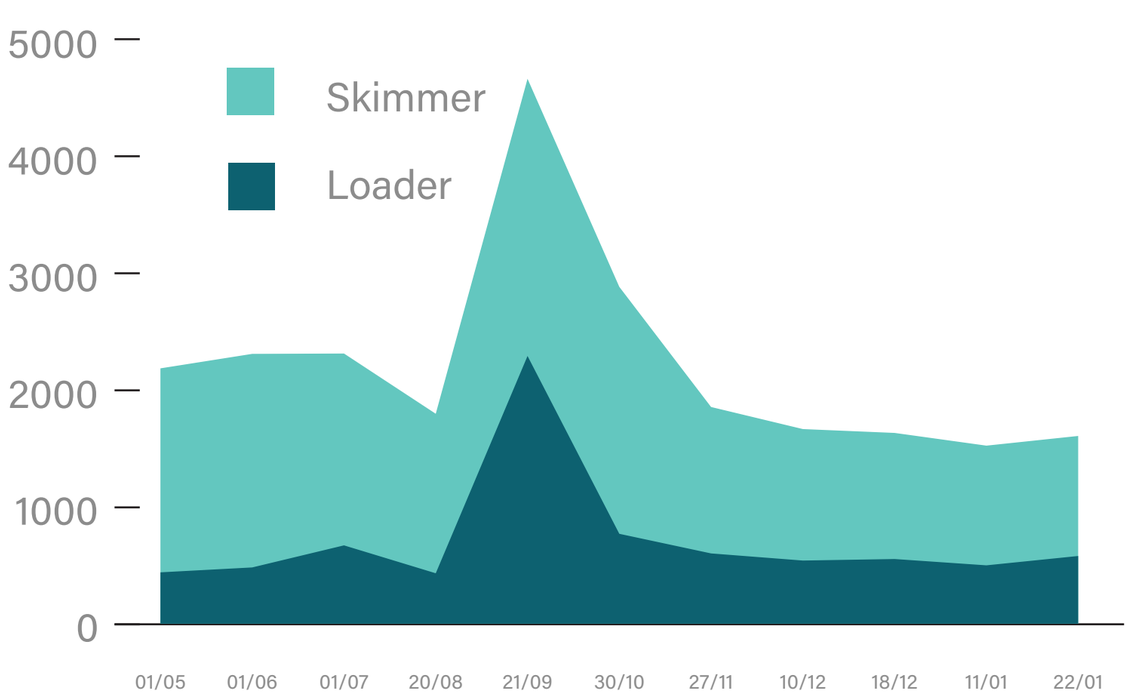
## MAGENTO 1 & 2 - LOADERS & SKIMMERS

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.

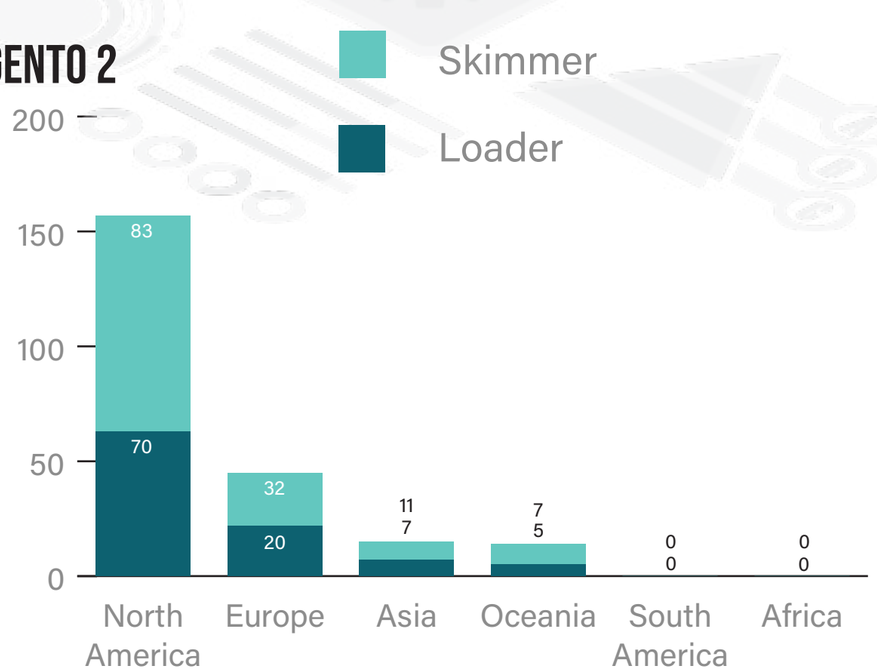
The charts to the right show which regions in the world have the highest infection rate, and below shows change over time.




### MAGENTO 1




### MAGENTO 2




FOREGENIX

8TH FEBRUARY 2021

# WEBSCAN RESULTS MAGENTO 1 & 2 - FRAMEWORK ISSUES

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

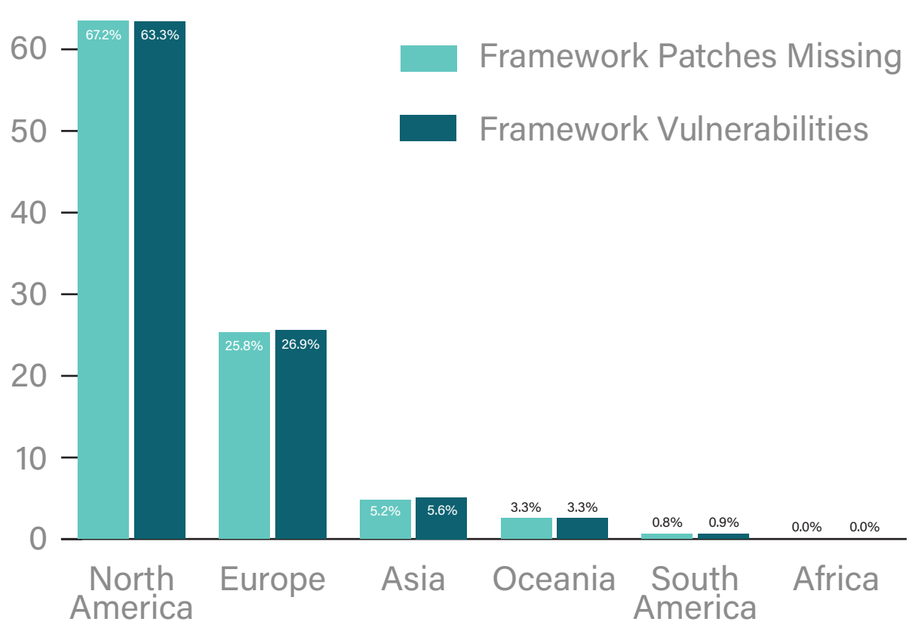
"**Framework Patches Missing**" means a website is missing security patches or updates that are already available.

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

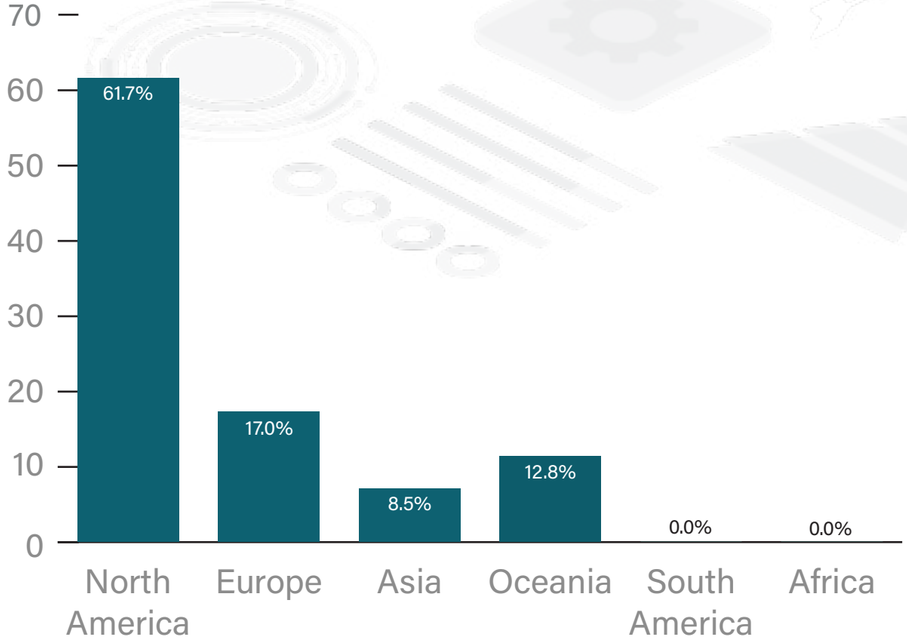
It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having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

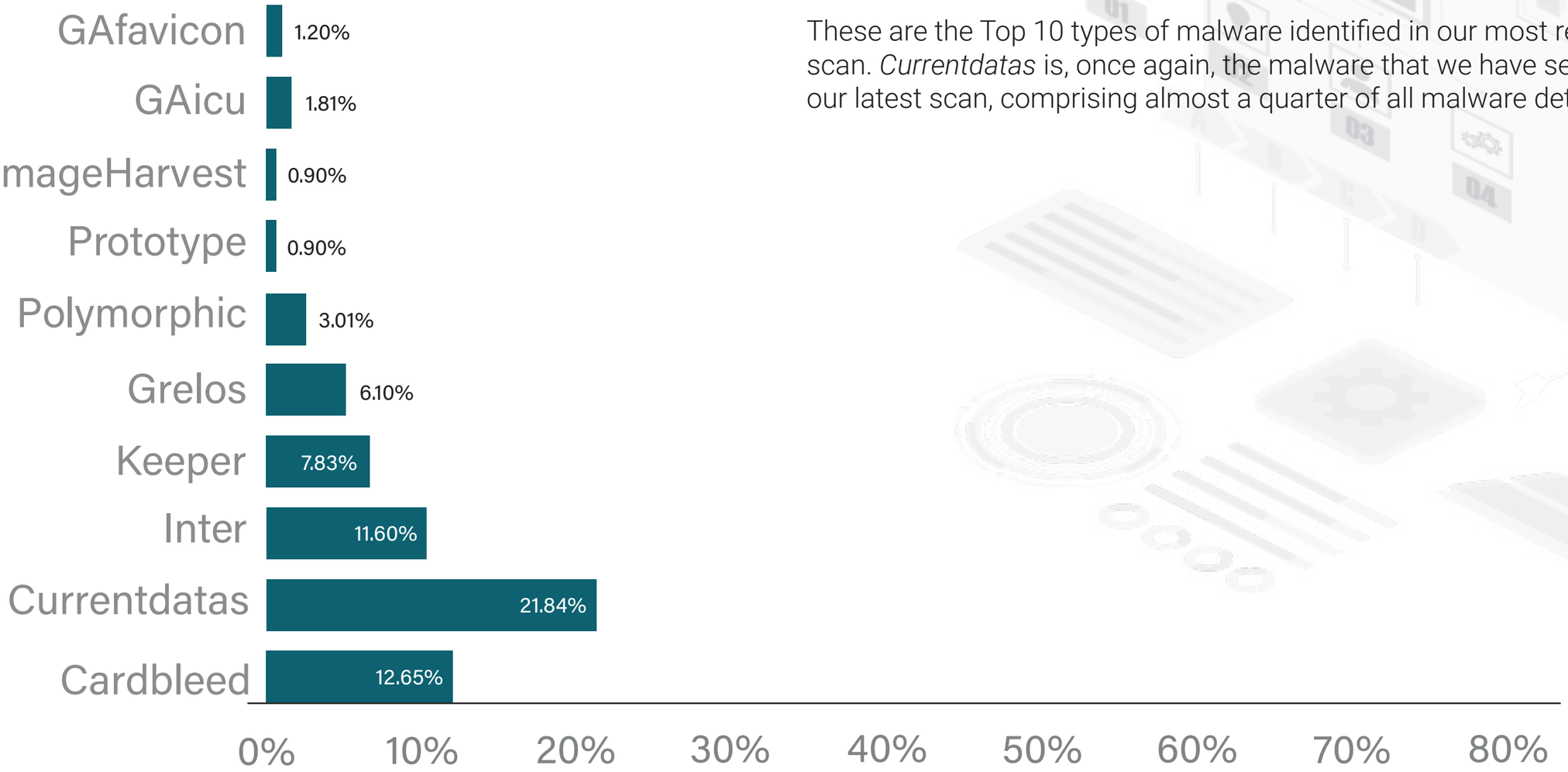



FOREGENIX

8TH FEBRUARY 2021

# WEBSCAN RESULTS

## MALWARE CAMPAIGNS



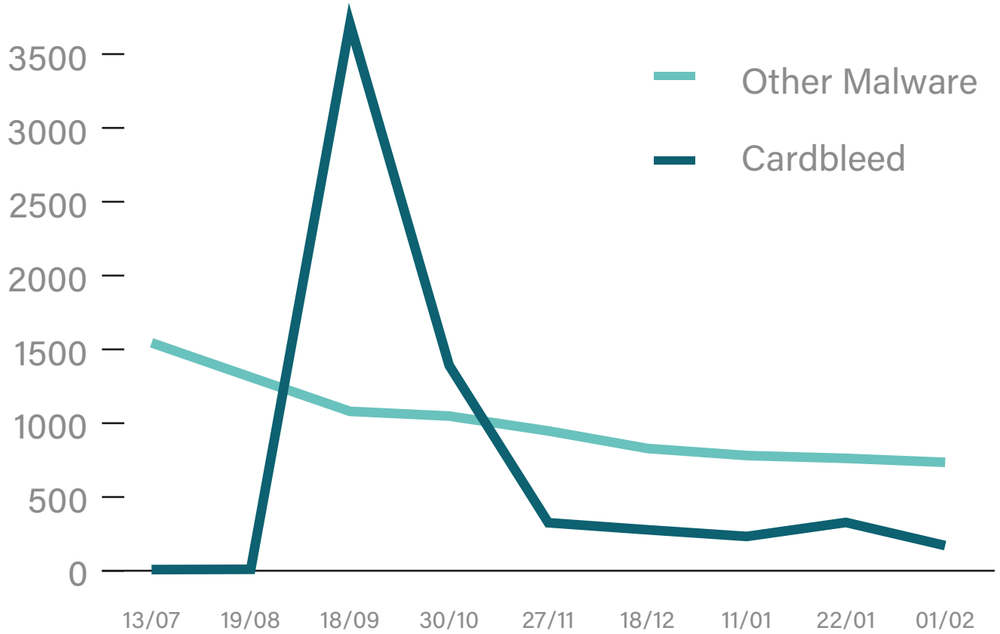

These are the Top 10 types of malware identified in our most recent Magento scan. *Currentdatas* is, once again, the malware that we have seen the most on our latest scan, comprising almost a quarter of all malware detections.

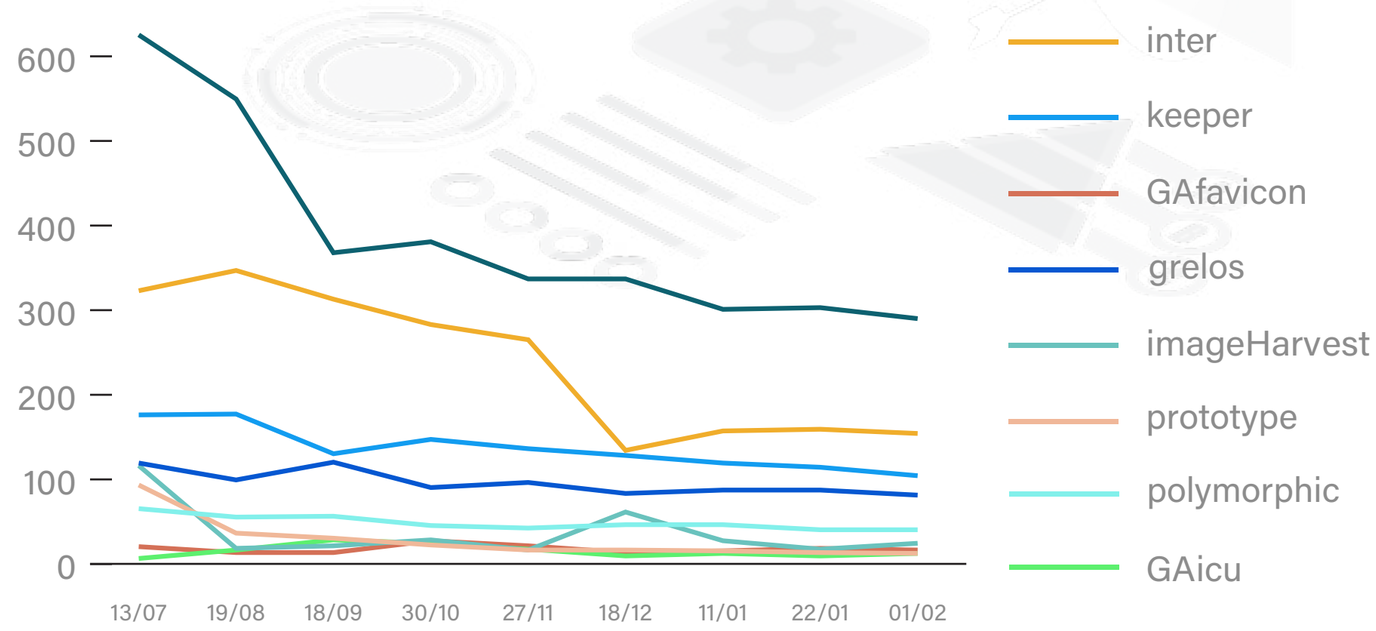
FOREGENIX

8TH 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

8TH FEBRUARY 2021

# MALWARE ANATOMY POLYMORPHIC

Back in April 2019, several eCommerce sites were hacked by a campaign that used a polymorphic loader. This meant that, while the injected code looked different on each victim site, the underlying functionality of the code would be the same across all of them.

In order to evade detection, the loader would contain variable names that looked like valid words you might see in a benign script. Examples include `keyProc`, `pickFooter`, `fromFrame`, `modelDescription`, etc. These variable names were most likely generated randomly by combining two words together. Using different variable names on different sites would help the malware avoid detection from malware scanners that just look for certain keywords.

While the variable names may have been random, the general algorithm used by the code was identical across all infected sites. A decoding function was defined that would take two arguments, an encoded string and a key, and perform an XOR operation on them. An array of encoded strings was also defined, these decoded to various checkout-related words like `checkout` and `onepage`. If the current URL contained one of these words, an additional skimming script would be loaded from an external URL. Typically this attack used domains that masqueraded as JQuery-related sites, e.g. `jqueres[.]com`.

Most of the infrastructure used in this attack has since been taken down. However we still see the loader on sites today, suggesting that they have not been cleaned since the original attack and they could be vulnerable to similar attacks in the future.

# MALWARE ANATOMY PROTOTYPE

This is a type of loader first seen in January 2020. It's notable for modifying the `Array` and `String` object prototypes in order to execute its malicious code and shows how attackers are taking advantage of more complex JavaScript features to write their malware.

The code defines some new functions for the `String` prototype. For example, it may define `String.prototype.xn` to be a custom decoding function. The code will contain several other encoded strings which can be decoded by executing `'encoded string'.xn()`. This allows the attacker to hide their URL from plain sight, as well as hiding other words that might reveal the functionality of the code (such as `script` and `checkout`). Another function is defined that checks whether the current page is the checkout page, another is used to retrieve the main skimming script from the attacker's URL and another is used to inject the newly loaded script into the current page.

Like the polymorphic campaign, most of the attacker's infrastructure for this campaign seems to have been taken down. But should the attacker's sites come back online, these infected sites would have their customers' card data stolen again. Given that they have already been infected once before without removing the malware, the chances are they can be targeted again in the future by a similar attack.

# OUR INSIGHTS

We have noted that the number of Magento websites continues to decline. In this report, we see a drop of 3,697 Magento websites; in which Magento 1 (M1) sees a decrease of 1.97%, and Magento 2 (M2) by 0.44%.

On the positive side, the number of M1 websites with card harvesting malware has decreased, while M2 remains at 0.23% of websites infected with this type of malware. Remember, M1 websites have reached their end of life, therefore you should migrate to M2 as soon as possible. New automated attack campaigns, such as Cardbleed, can happen at any time.

For free guidance on how to improve your website's security, check out our Magento Security Insights page. And, for that extra peace of mind, start using a website security solution, as well as investing in cyber insurance.

## 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

8TH FEBRUARY 2021