MAGENTO WEBSITE SECURITY REPORT

CONTACT US

WWW.FOREGENIX.COM/WEBSCAN

TEL: +44 845 309 6232

25TH JANUARY 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

25TH JANUARY 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

25TH JANUARY 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

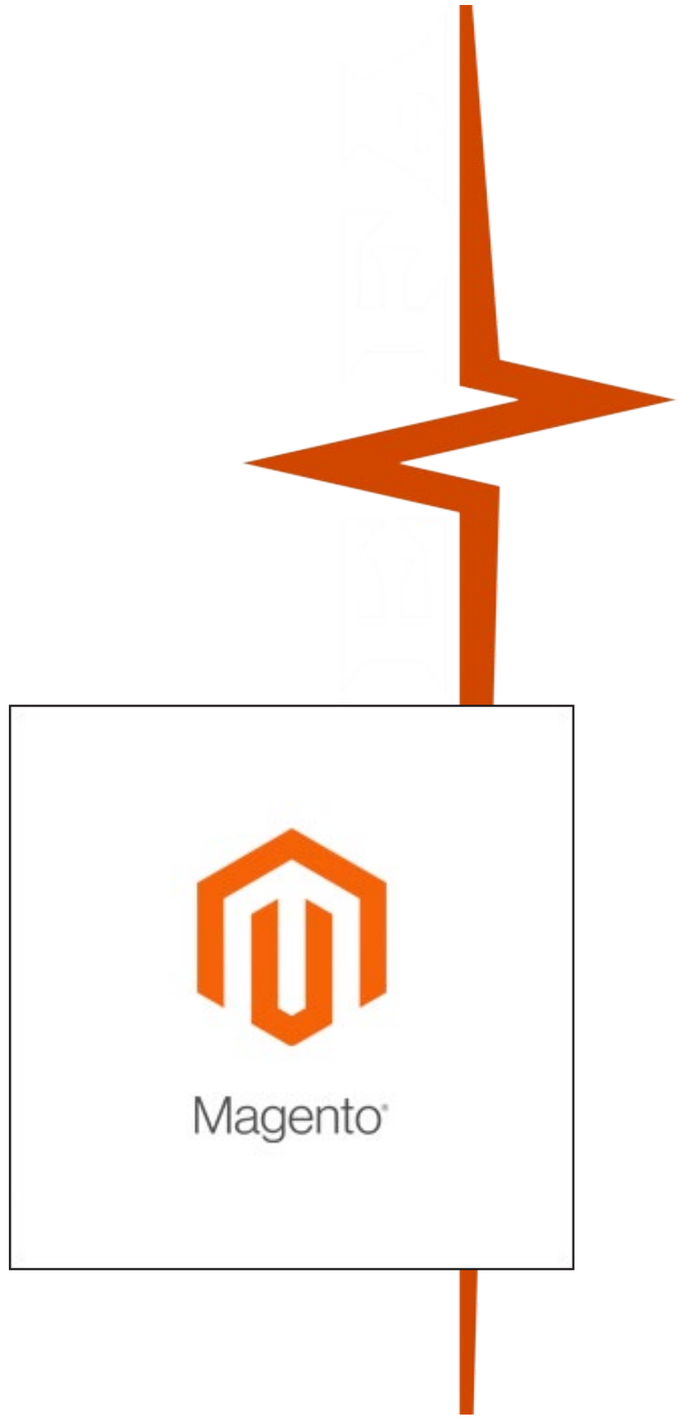
OVERVIEW SUMMARY

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

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

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

27% of Magento 2 websites are High/Critical Risk



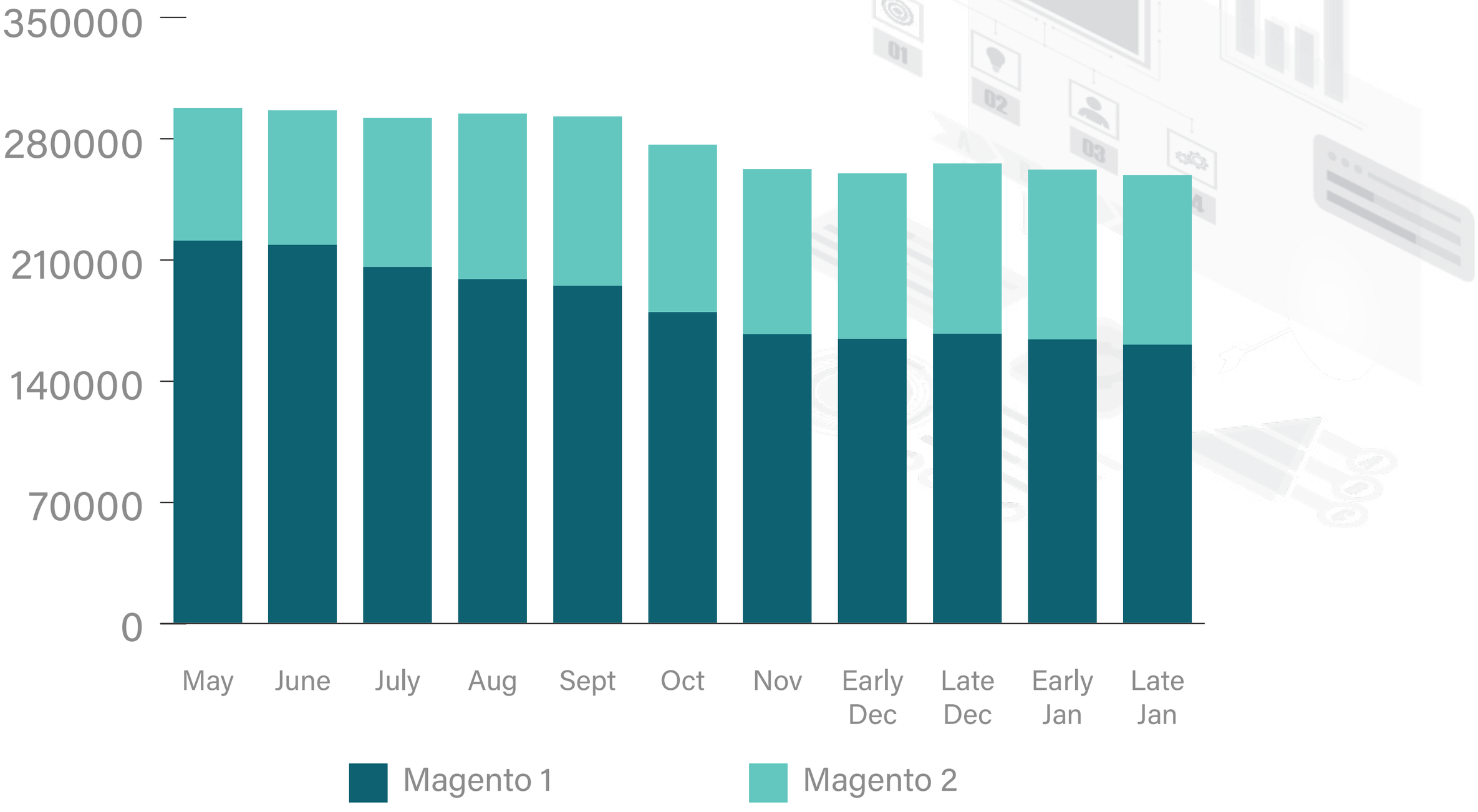
MAGENTO 1 AND 2 REMAIN THE MOST TARGETED PLATFORMS BY CRIMINALS

FOREGENIX

25TH JANUARY 2021

WEBSCAN RESULTS

WEBSITE NUMBERS (ALL MAGENTO)



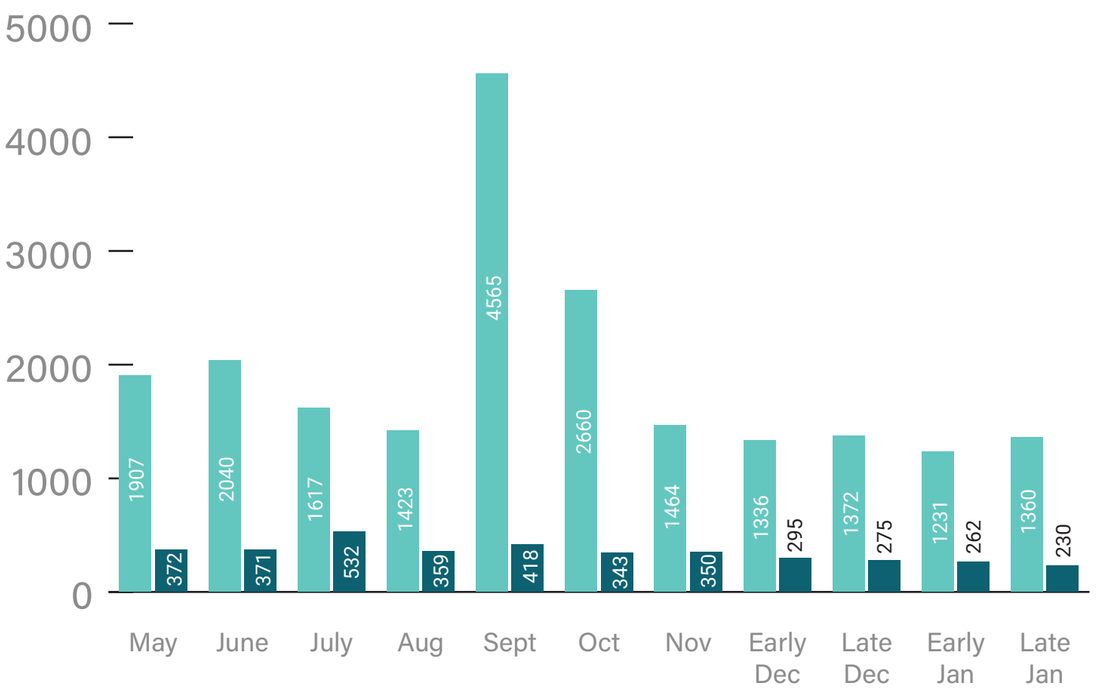
FOREGENIX

25TH JANUARY 2021

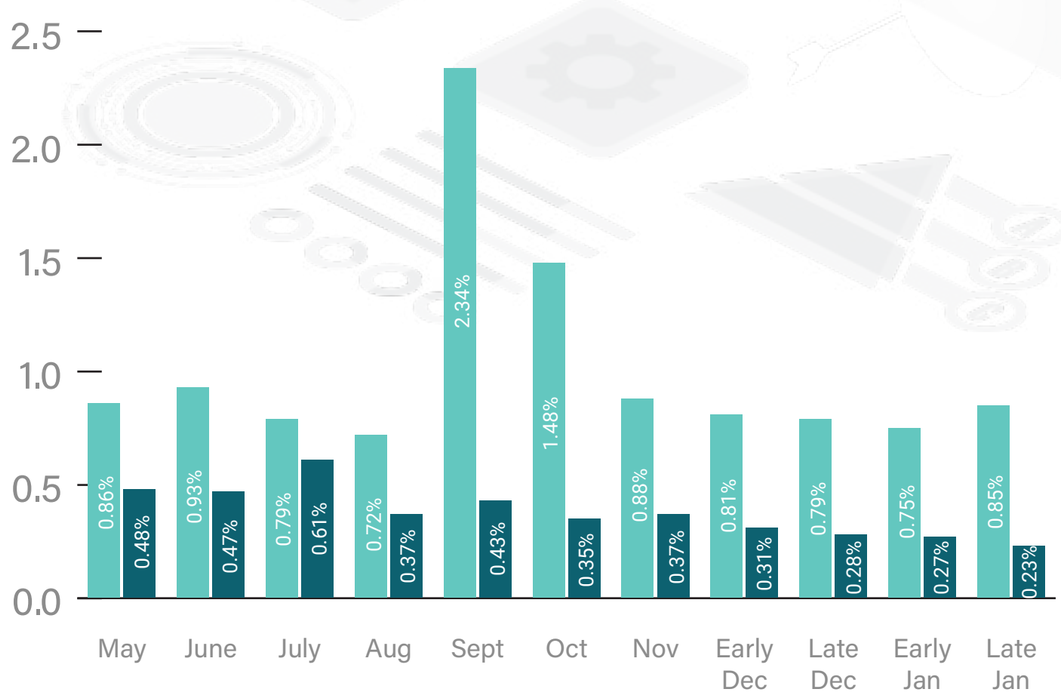
WEBSCAN RESULTS CRITICAL RISK

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

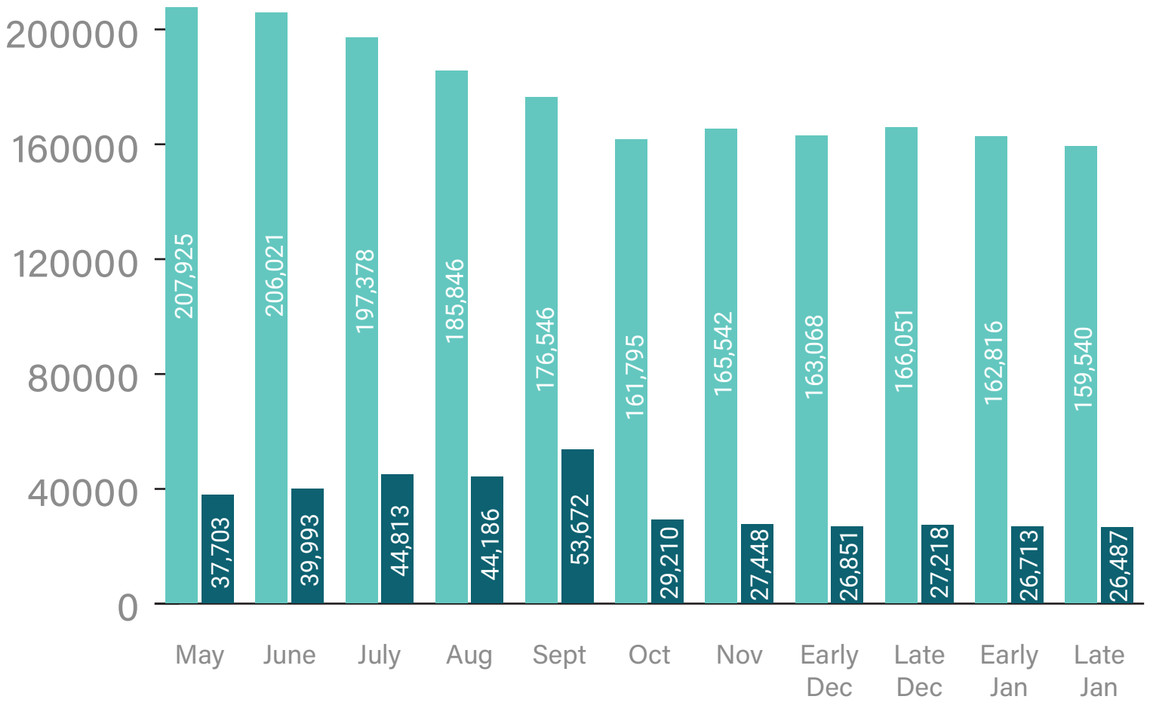
25TH JANUARY 2021

WEBSCAN RESULTS HIGH RISK

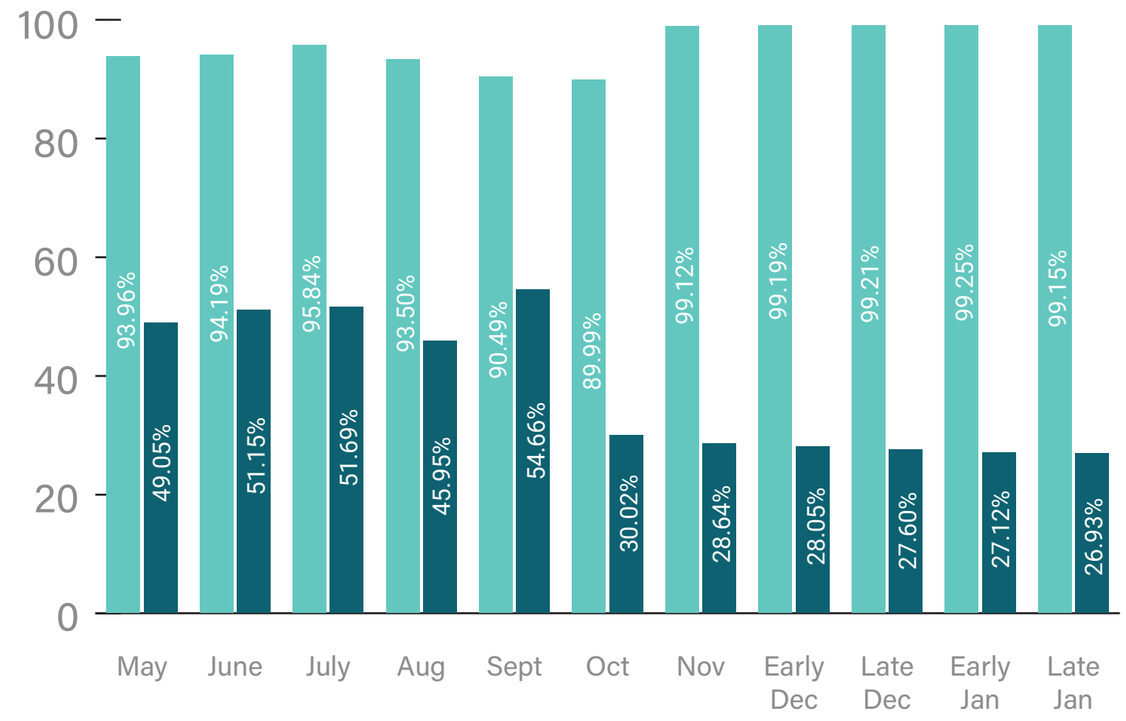
Websites identified as High Risk have significant security issues that make them very vulnerable to criminals. The sites have one or more of the following:

- 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



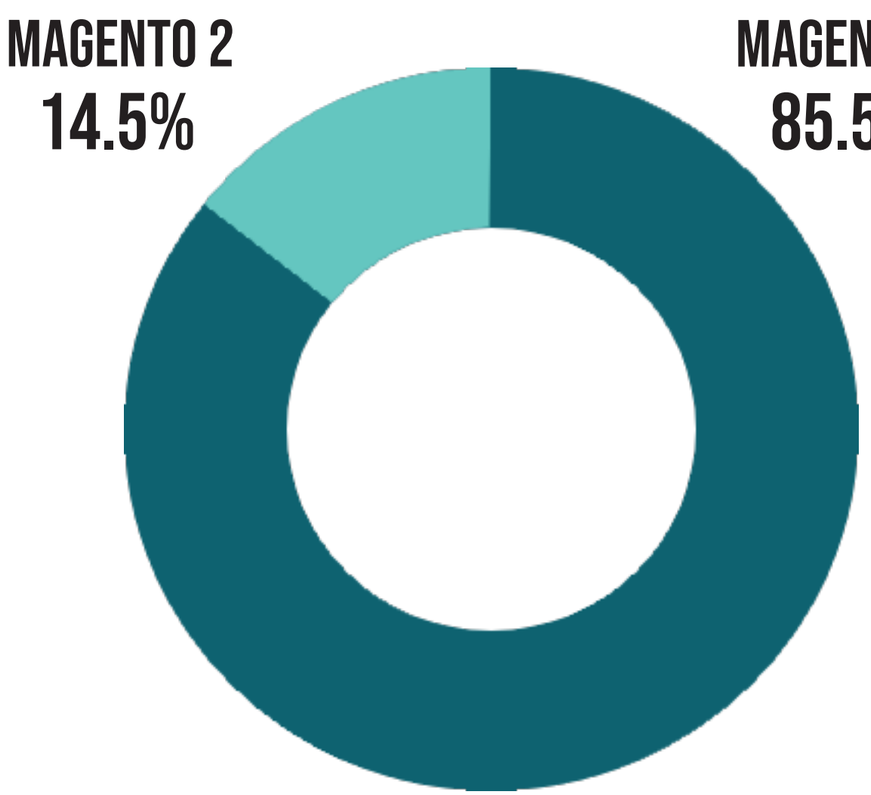
Magento 1 Magento 2

FOREGENIX

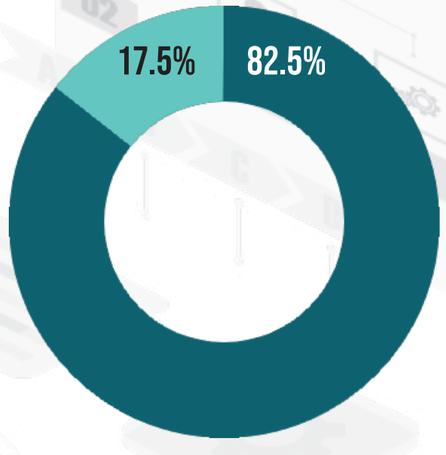
25TH JANUARY 2021

WEBSCAN RESULTS

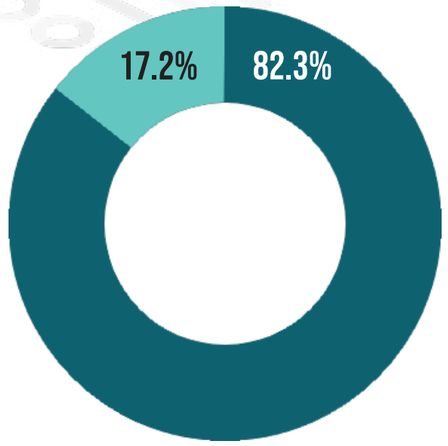
CARD-HARVESTING MALWARE DISTRIBUTION



TWO WEEKS AGO



ONE MONTH AGO



FOREGENIX

25TH JANUARY 2021

WEBSCAN RESULTS

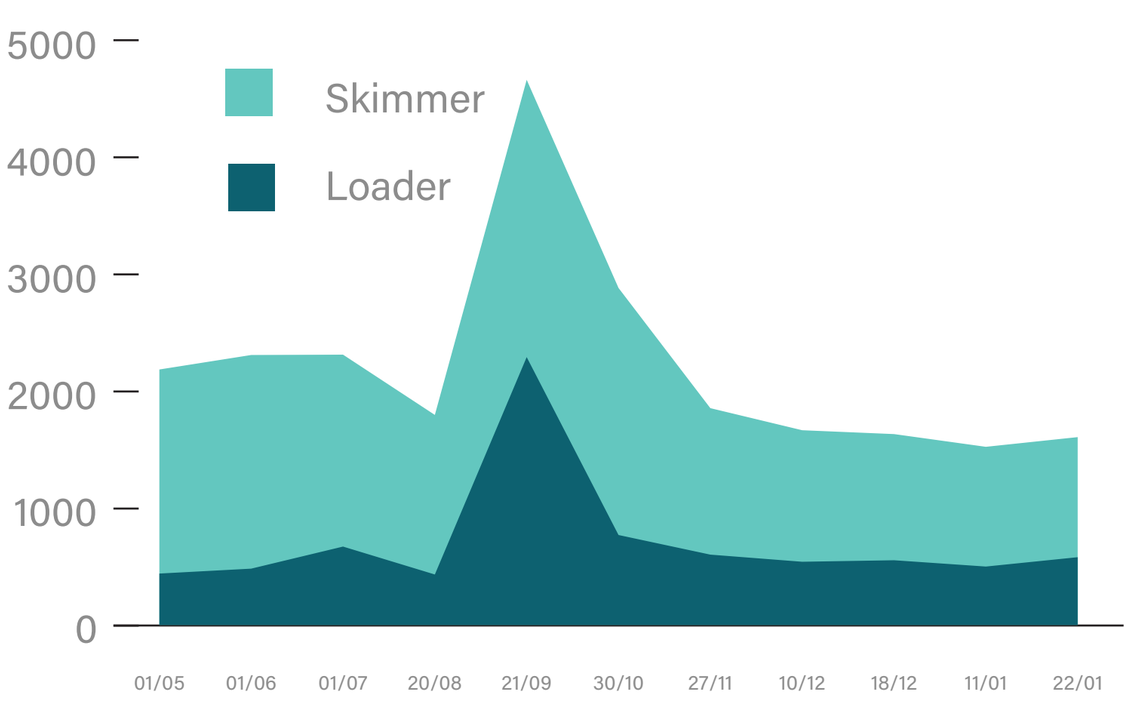
MAGENTO 1 & 2 - LOADERS & SKIMMERS

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

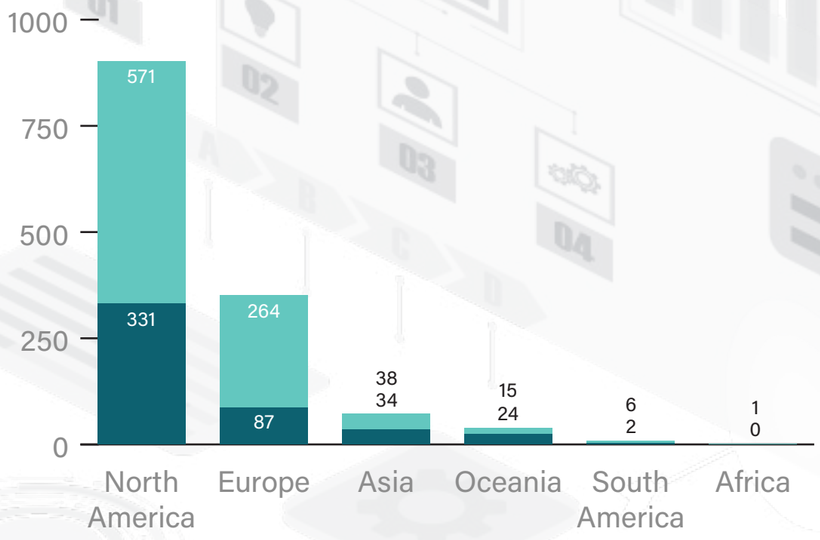
Loaders - are small pieces of code designed to load in additional malicious code onto a website.

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.

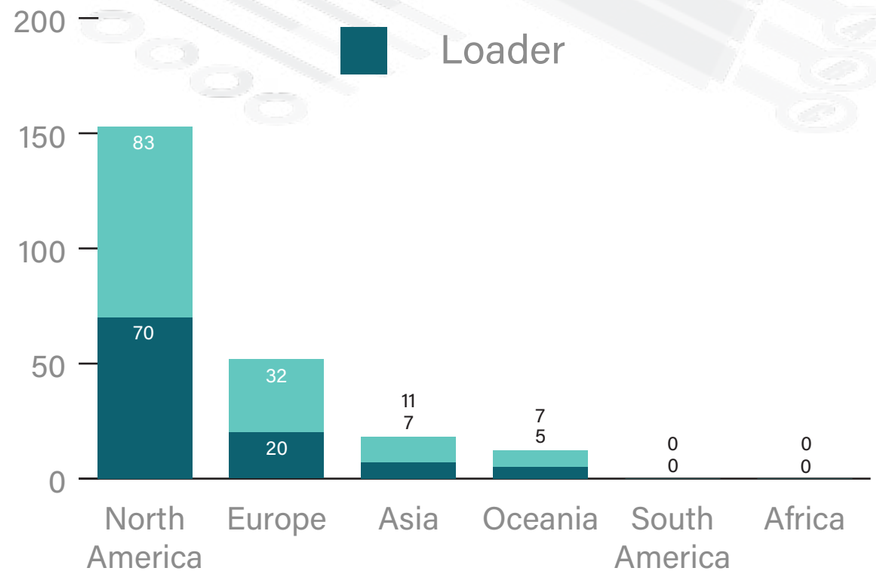
The charts to the right show which regions in the world have the highest infection rate, and below shows change over time.



MAGENTO 1



MAGENTO 2



FOREGENIX

25TH JANUARY 2021

WEBSCAN RESULTS MAGENTO 1 & 2 - FRAMEWORK ISSUES

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

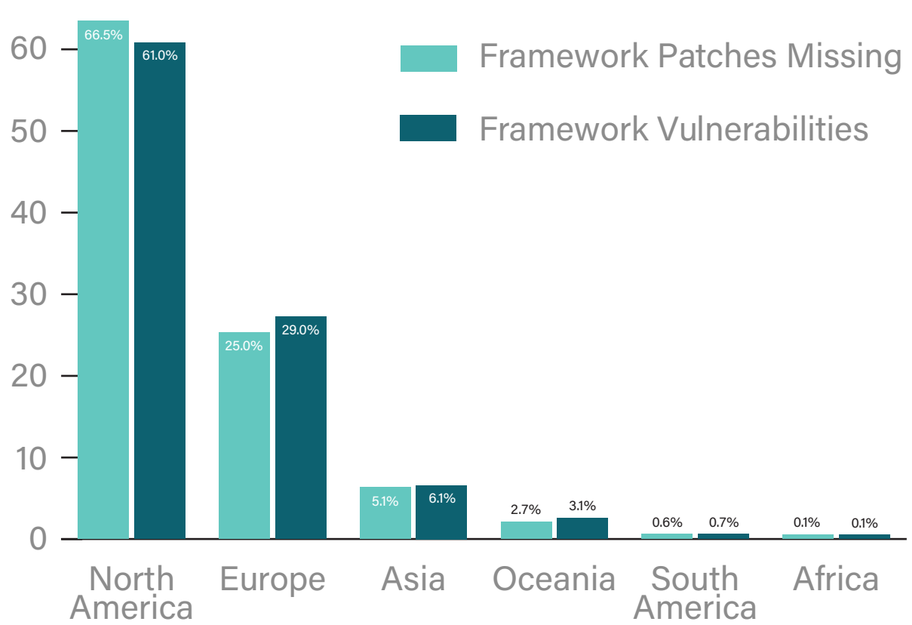
"**Framework Patches Missing**" means a website is missing security patches or updates that are already available.

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

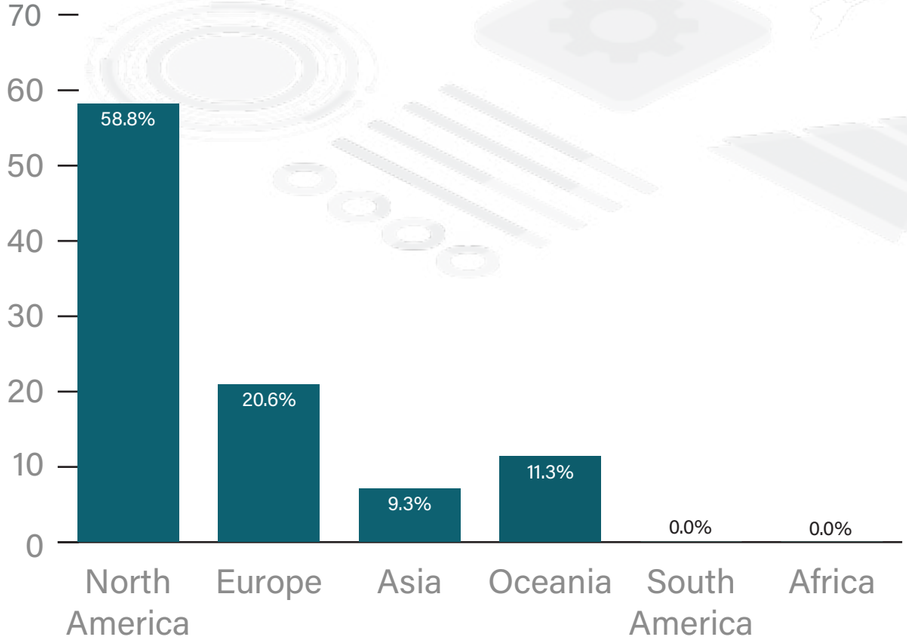
It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having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



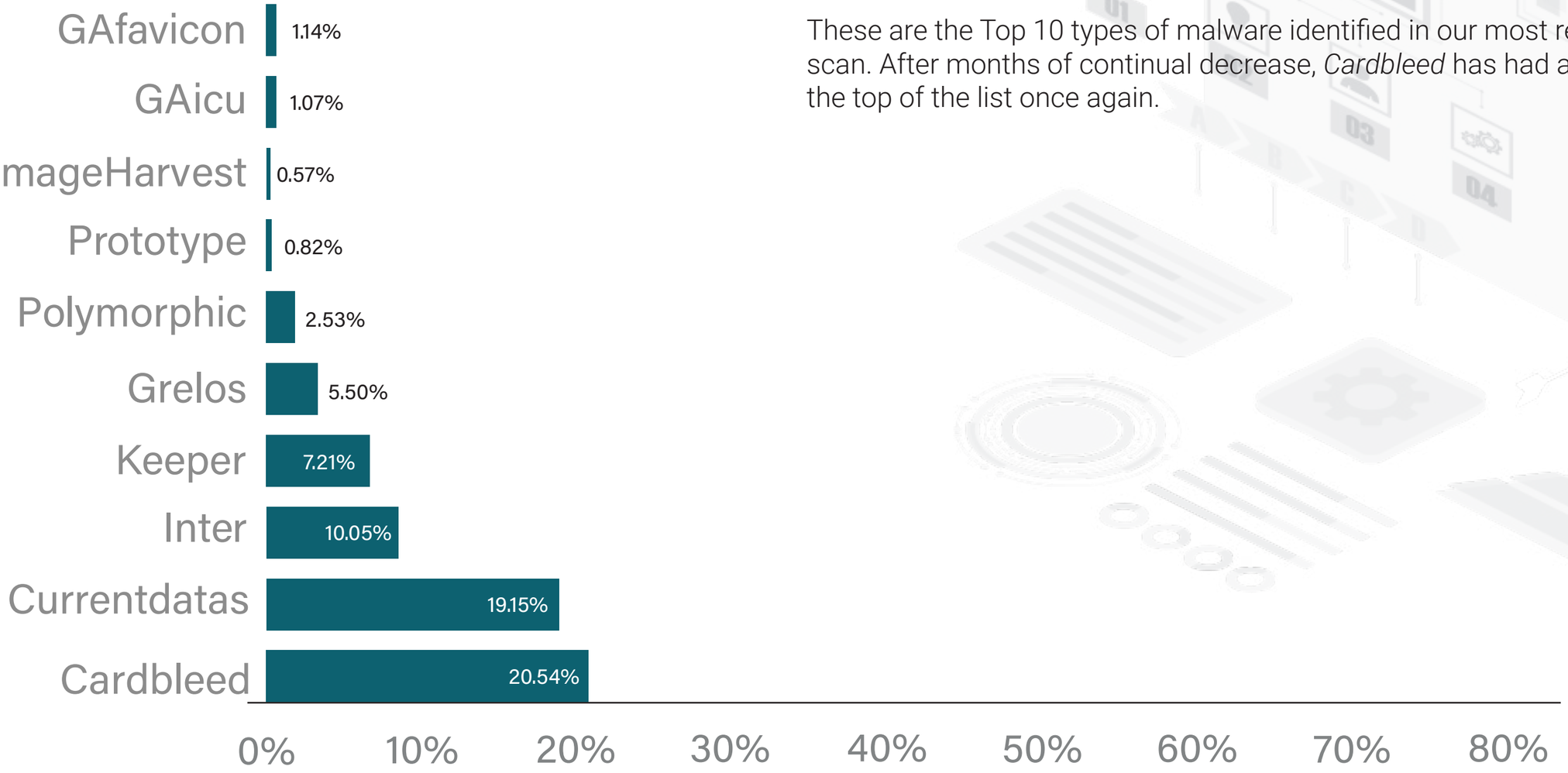
MAGENTO 2 PERCENTAGES



FOREGENIX

25TH JANUARY 2021

WEBSCAN RESULTS MALWARE TYPES



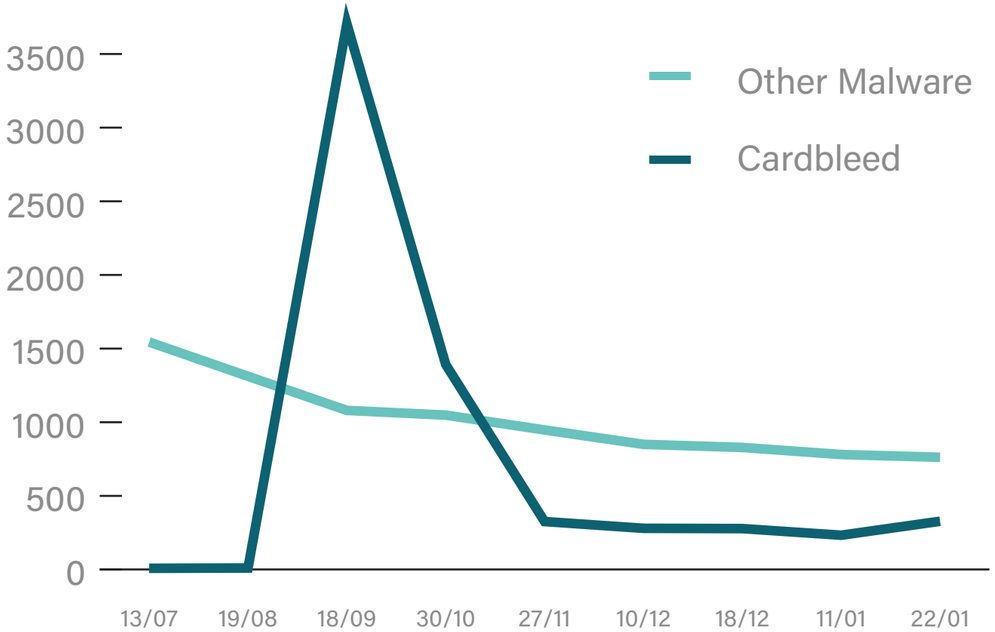
These are the Top 10 types of malware identified in our most recent Magento scan. After months of continual decrease, *Cardbleed* has had a jump, rising to the top of the list once again.

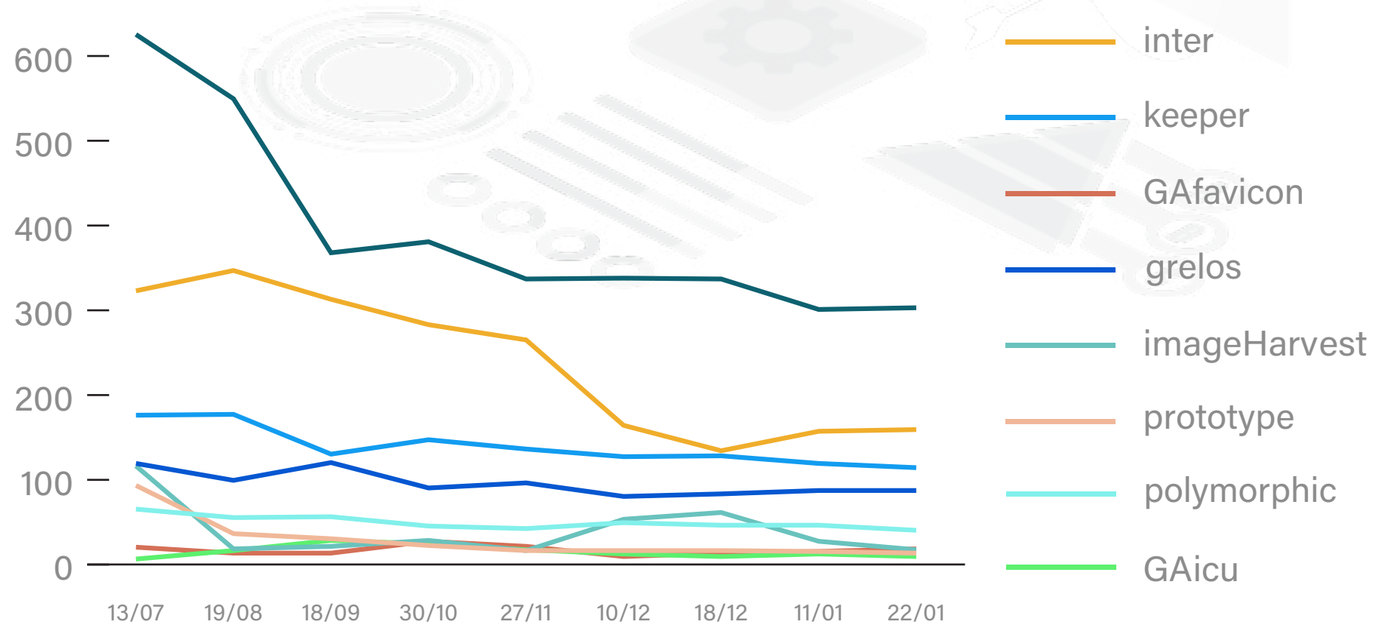
FOREGENIX

25TH JANUARY 2021

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 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

25TH JANUARY 2021

MALWARE ANATOMY GAICU

Similar to GAfavicon, this campaign attempts to masquerade their malware as Google Analytics code.

The attacker will inject a small script tag to the bottom of the infected site that appears to have a similar structure to the minified version of a legitimate Google Analytics tag. The script starts with the code `function(i,s,o,g,r,a,m)` and contains a reference to the legitimate Google Analytics URL. However, the malicious code will also contain a couple of Base64 strings: one decodes to “checkout”, “onepage”, or a similar word, while the other decodes to a URL. The malicious code checks whether the user is currently on the checkout page, if they are then additional malware will be loaded from the URL. This URL typically has the following structure: `//[attacker’s domain]/www.google-analytics.com/[victim site].js`. The attacker’s domain often ends in `.icu`, although other top-level domains have been observed recently. The URL contains the legitimate Google Analytics domain as part of the path, another way of trying to trick developers or analysts into thinking the code is benign.

The newly-loaded malware has been obfuscated with the Dean Edwards JavaScript packer, unpacking it will reveal it to be skimming code. Typically this skimmer will exfiltrate the card data to two different URLs, both ending in `g.php`.

MALWARE ANATOMY GRELOS

Despite being one of the older skimmers out there, we still see some variations of it to this day. The name comes from the variable name `grelos_v` that is used in the code. There have been variants that omit this word, however the rest of the code is still very similar.

The campaign predominantly targets Magento sites, with the attacker often adding the skimming code to the file `/js/lib/ccard.js`. This is a core part of any Magento installation and it used to validate card numbers, which makes it the perfect place to add skimming code since it will always be loaded when a customer enters their card data onto the checkout page. In some variants, the code will be injected into every page and a condition will be added to make sure the code only runs on the checkout page.

The code will scrape the checkout page and send it off to the exfiltration address. In some cases, the code will just post back to the same site at `/js/index.php`, the attacker would have placed additional malware here that will either forward it onto the attacker or store it somewhere on the infected site for them to retrieve later. In other cases, we see the code posting off to a remote location directly, stored in a variable called `Glink`.

OUR INSIGHTS

The number of Magento websites continue to decline. In our latest scan, we can see a drop of 3,147 Magento websites; in which Magento 1 (M1) sees a decrease of 1.92%, and Magento 2 (M2) 0.14%.

The number of M1 websites with card harvesting malware has increased. Fortunately, most websites infected with *Cardbleed* are trying to load malware from inactive domains. Additionally, M2 had a slight decrease in the overall number of websites with card harvesting malware.

We continue to remind the industry that M1 websites have reached their end of life. By failing to migrate to M2, eCommerce websites on M1 are putting their customers' data at risk. New automated attack campaigns, such as *Cardbleed*, can happen at any time.

Take action today and improve your website security with free guidance on our Magento Security Insights page. For extra peace of mind, we recommend 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

25TH JANUARY 2021