MAGENTO WEBSITE SECURITY REPORT

CONTACT US

WWW.FOREGENIX.COM/WEBSCAN

TEL: +44 845 309 6232

30TH 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

30TH 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.

FOREGENIX

30TH NOVEMBER 2020

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

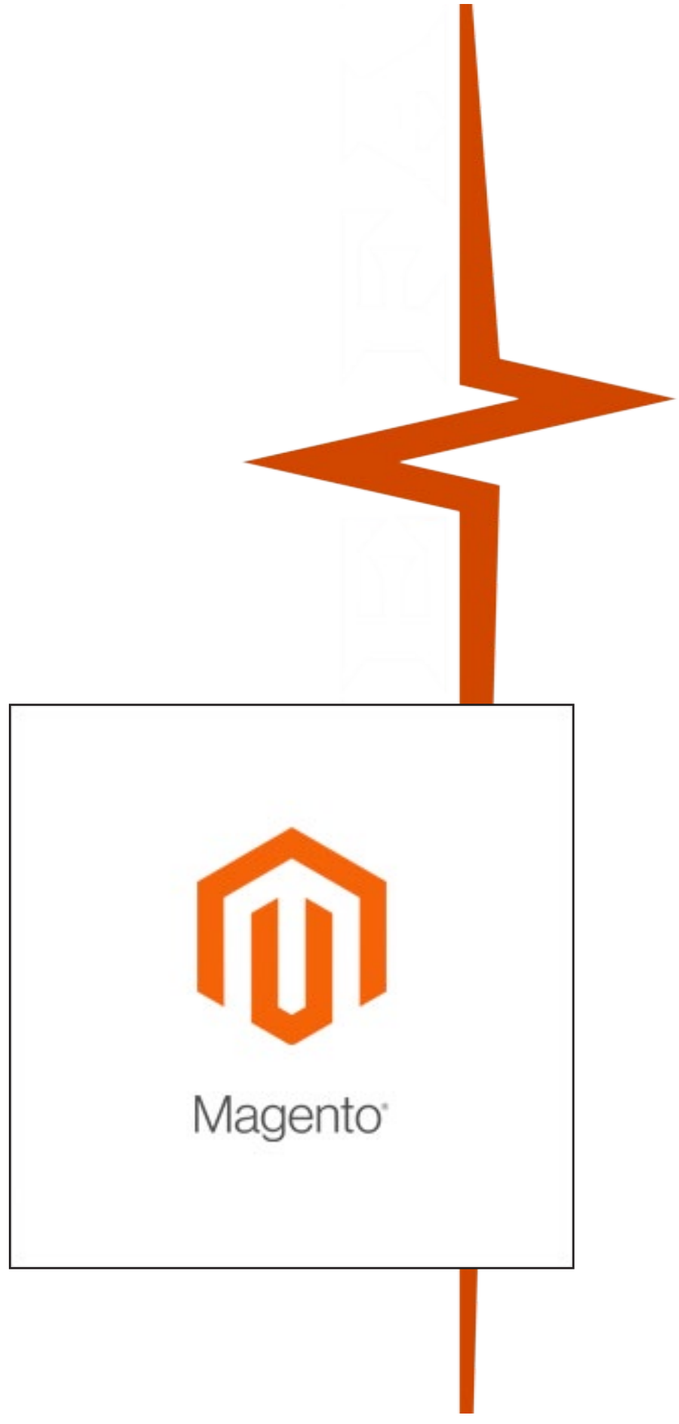
OVERVIEW SUMMARY

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

Magento 1 websites continue to slowly **DECLINE**

1,814 Magento websites are hacked, with card-harvesting malware.

29% of Magento 2 websites are High/Critical Risk



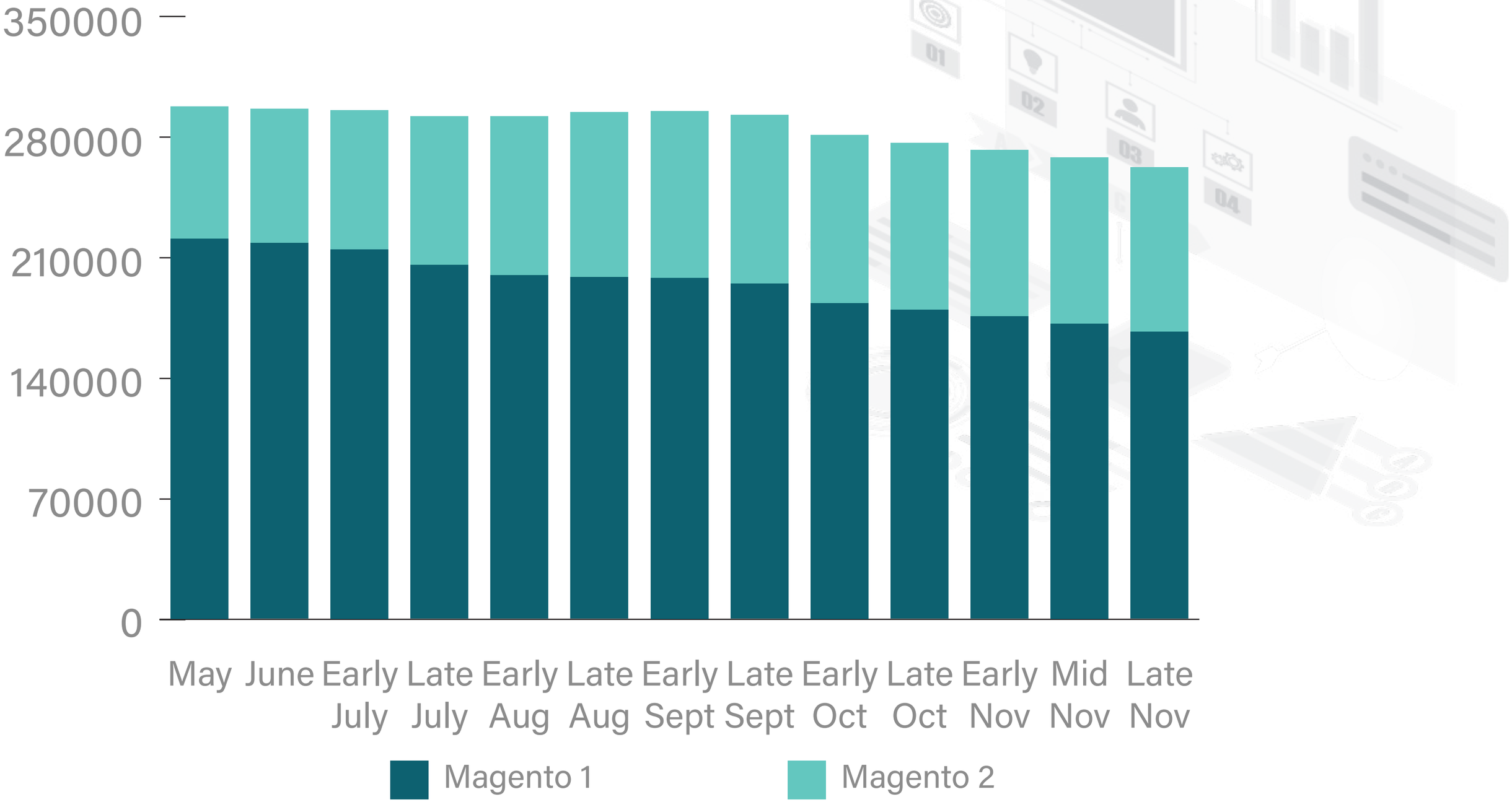
MAGENTO 1 REMAINS THE MOST TARGETED PLATFORM BY CRIMINALS, FOLLOWED BY MAGENTO 2

FOREGENIX

30TH NOVEMBER 2020

WEBSCAN RESULTS

WEBSITE NUMBERS (ALL MAGENTO)



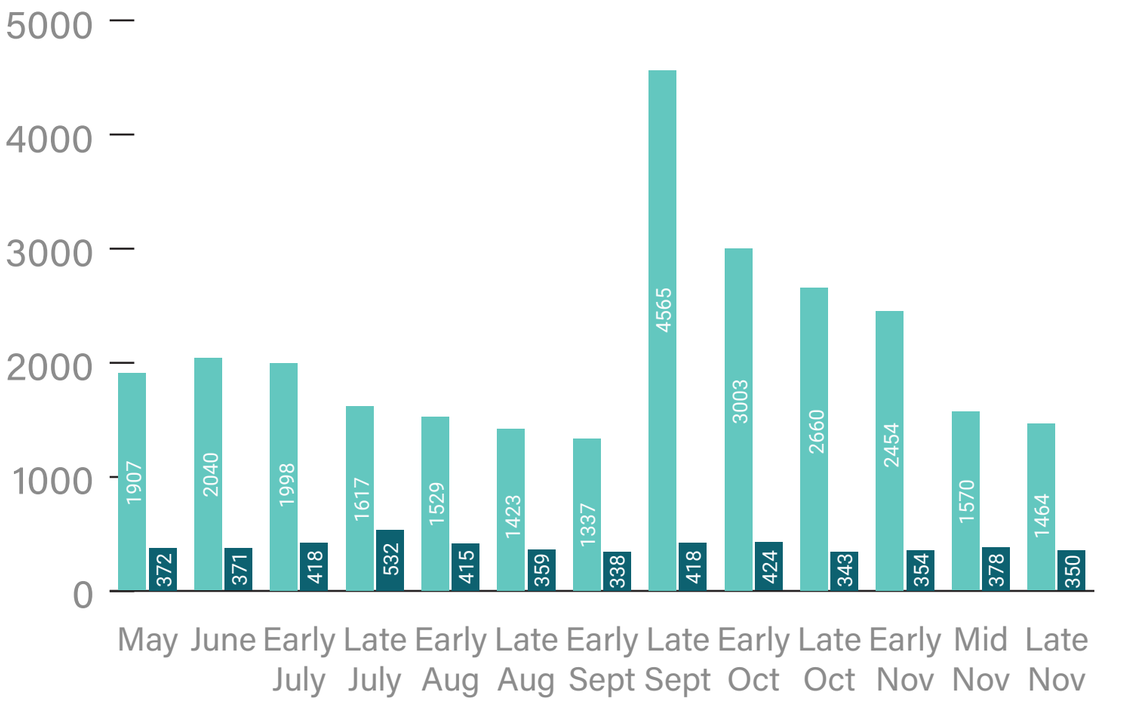
FOREGENIX

30TH NOVEMBER 2020

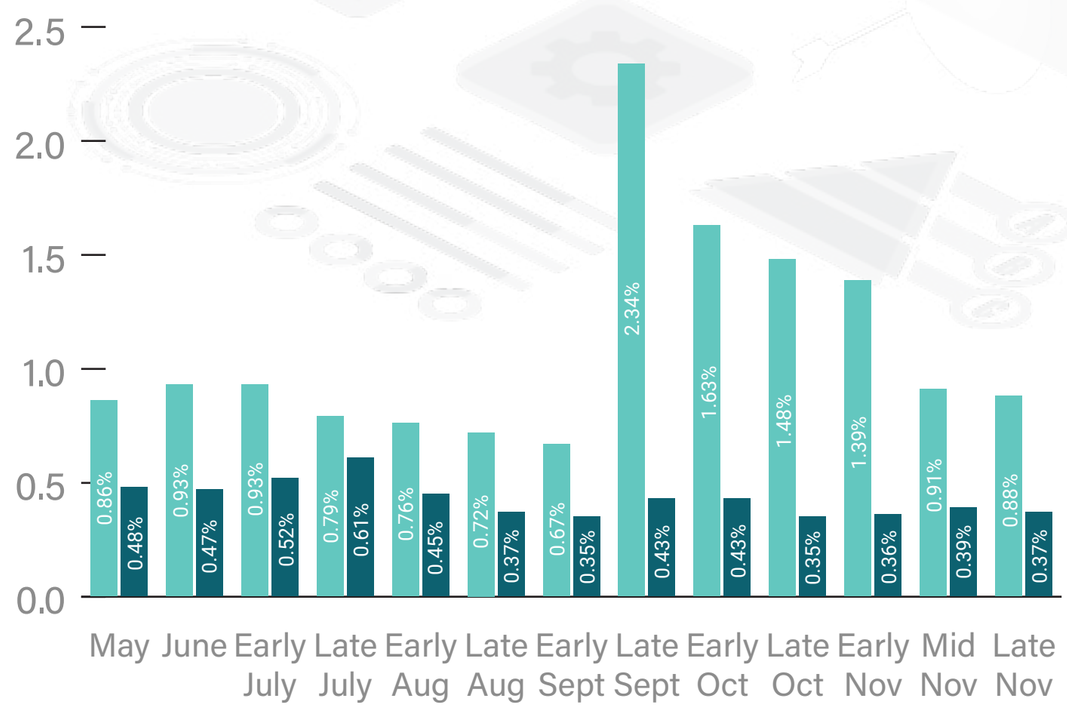
WEBSCAN RESULTS CRITICAL RISK

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

ACTUAL NUMBERS



PERCENTAGE OF TOTAL SITES



FOREGENIX

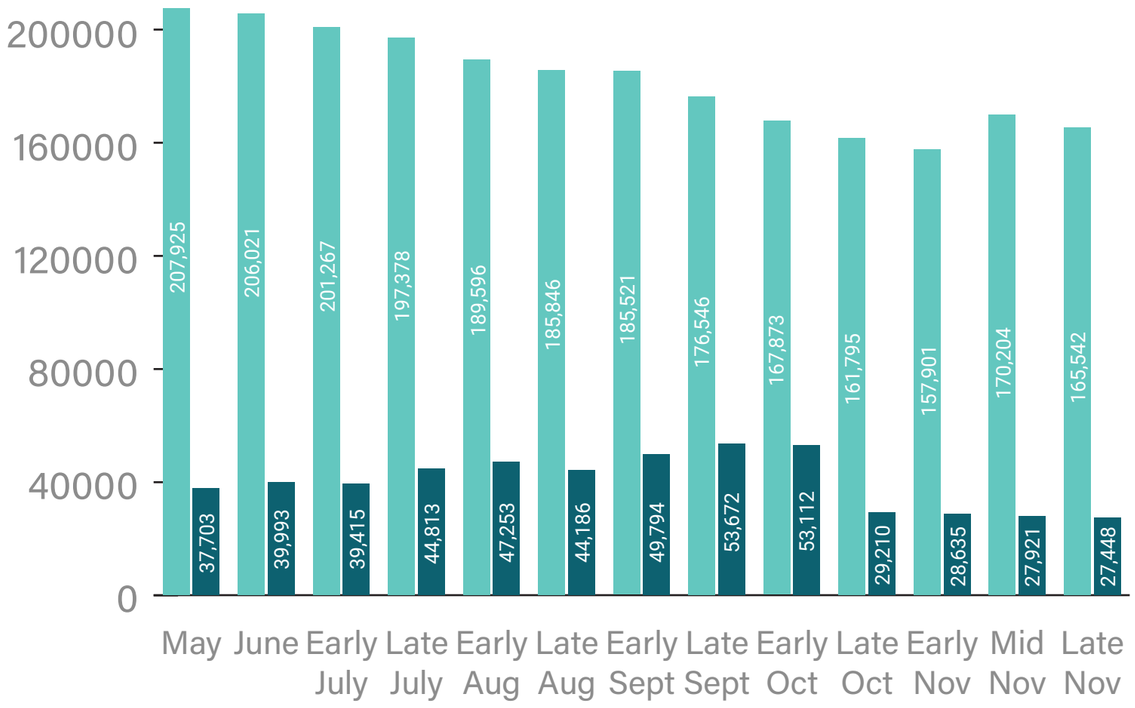
30TH NOVEMBER 2020

WEBSCAN RESULTS HIGH RISK

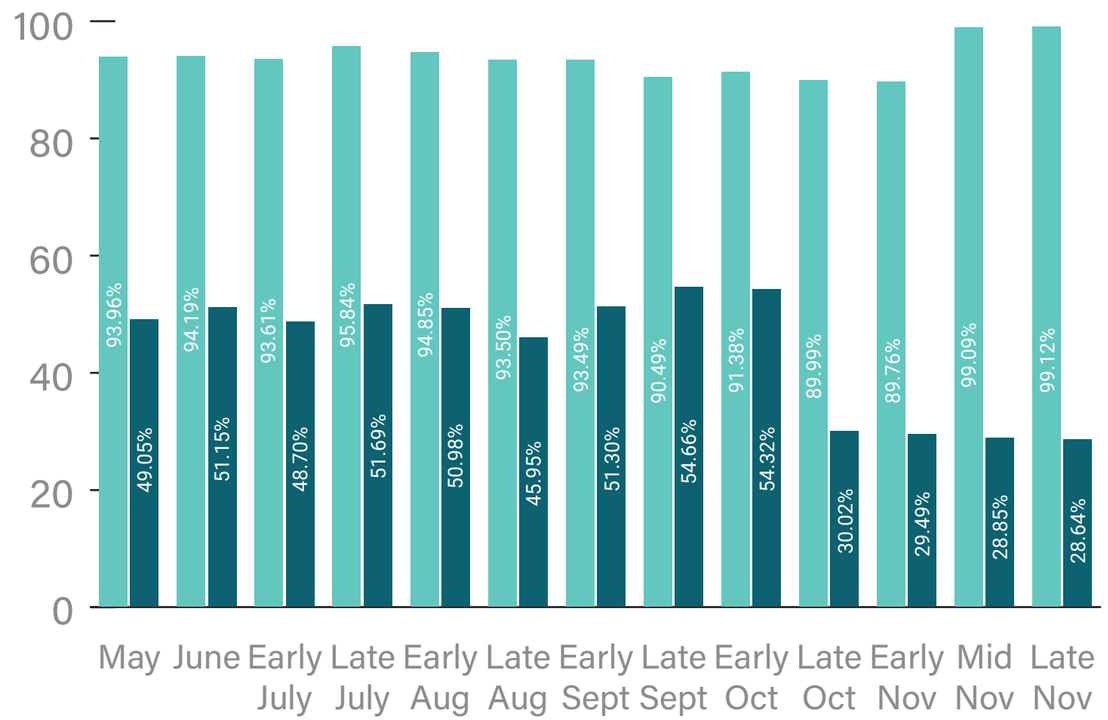
Websites with High Risk have significant security issues that make them very vulnerable to criminals.
The sites have one or more of the following:

- 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



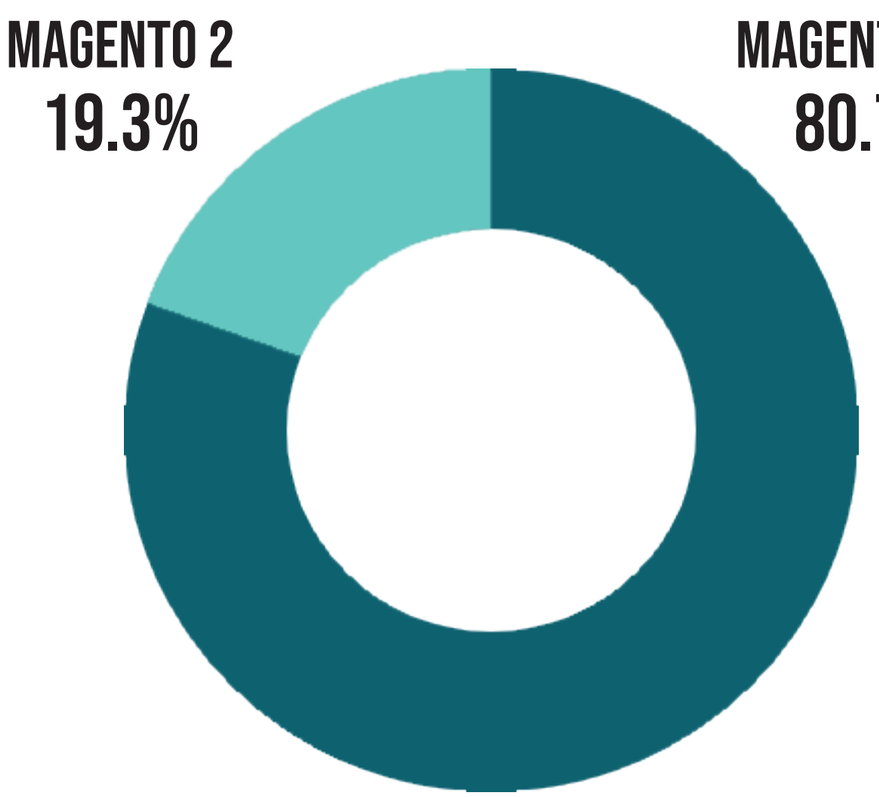
Magento 1 Magento 2

FOREGENIX

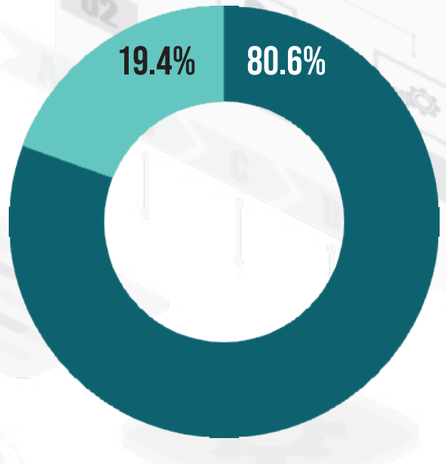
30TH NOVEMBER 2020

WEBSCAN RESULTS

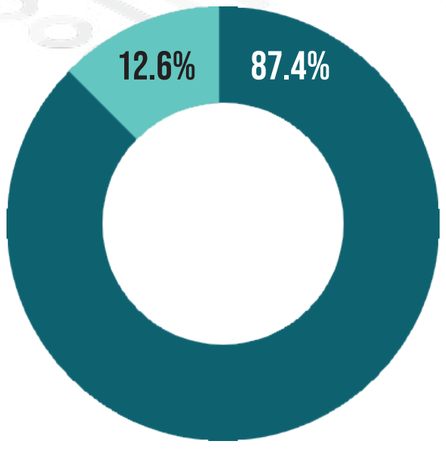
CARD-HARVESTING MALWARE DISTRIBUTION



TWO WEEKS AGO



ONE MONTH AGO



FOREGENIX

30TH NOVEMBER 2020

WEBSCAN RESULTS

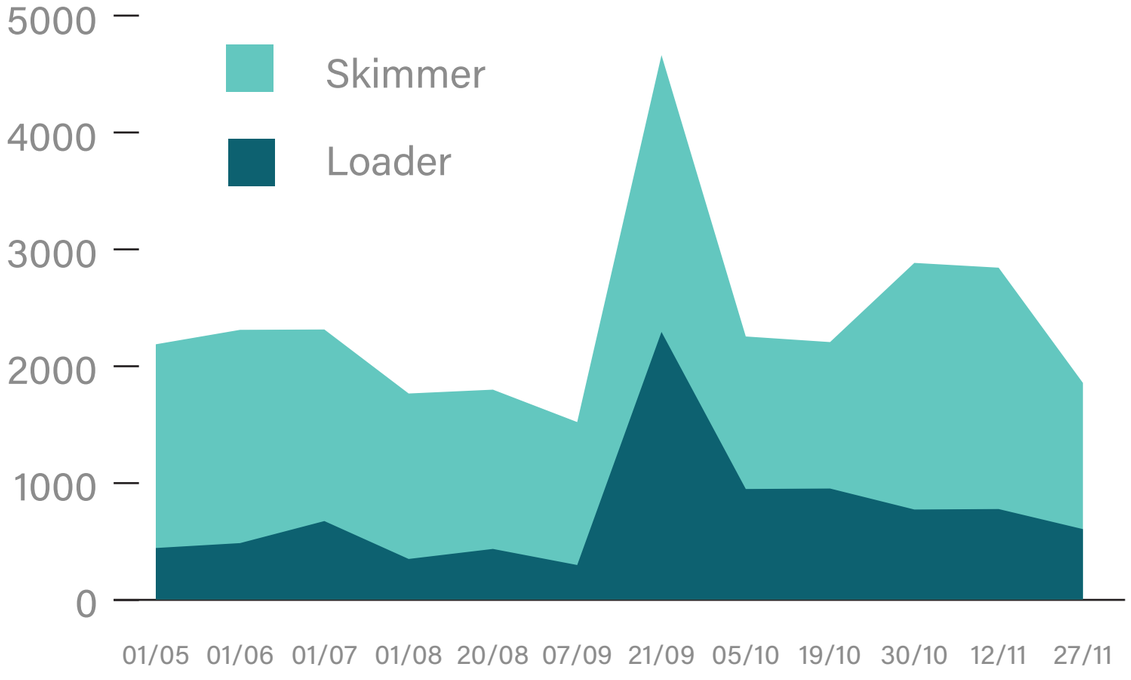
MAGENTO 1 & 2 - LOADERS & SKIMMERS

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

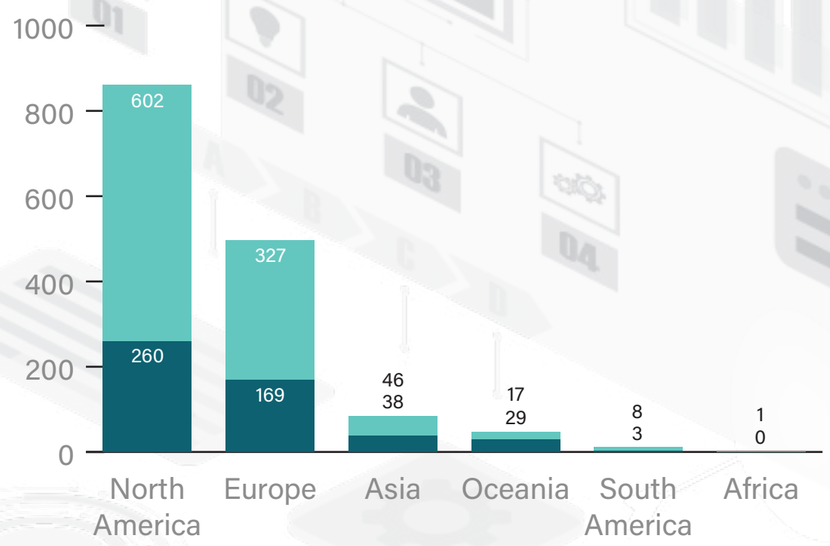
Loaders - are small pieces of code designed to load in additional malicious code onto a website.

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.

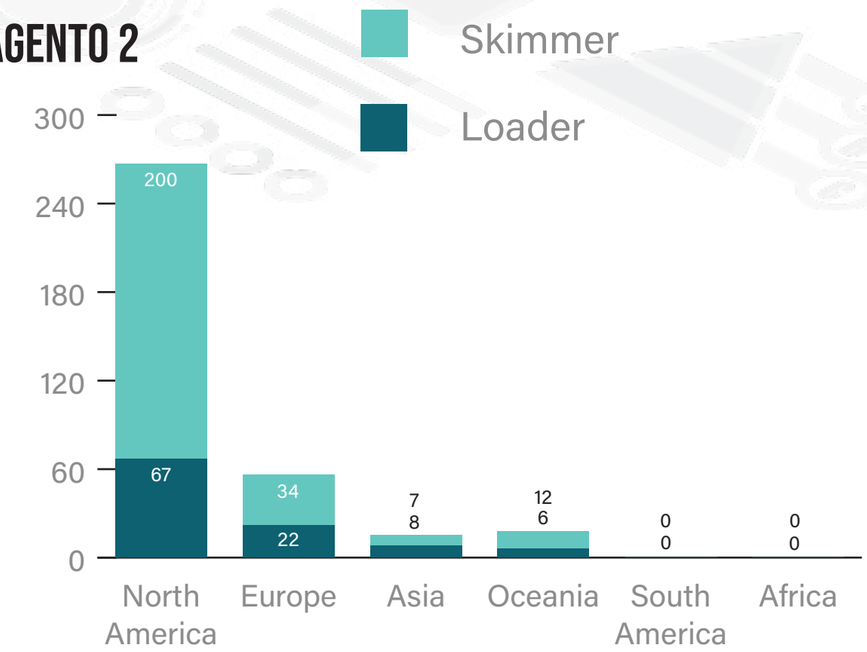
The charts to the right show which regions in the world have the highest infection rate, and below shows change over time.



MAGENTO 1



MAGENTO 2



FOREGENIX

30TH NOVEMBER 2020

WEBSCAN RESULTS MAGENTO 1 & 2 - FRAMEWORK ISSUES

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

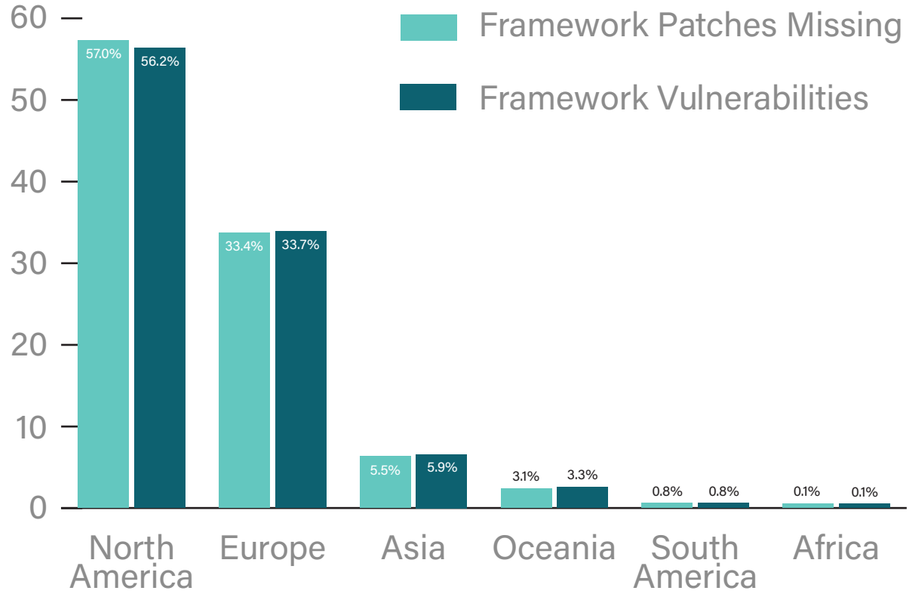
"**Framework security patches missing**" means a website is missing security patches/updates that are already available.

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

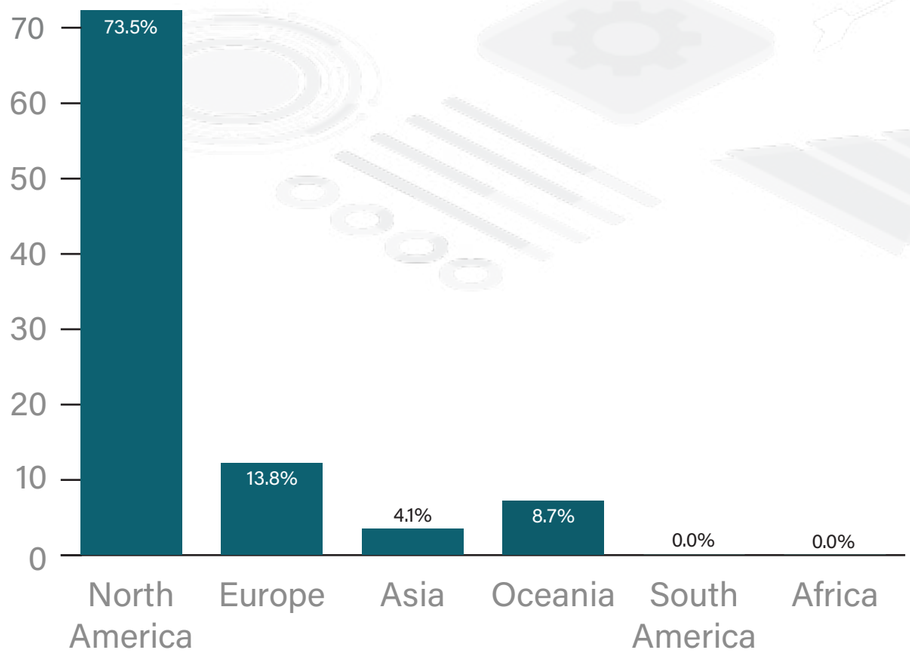
It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having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



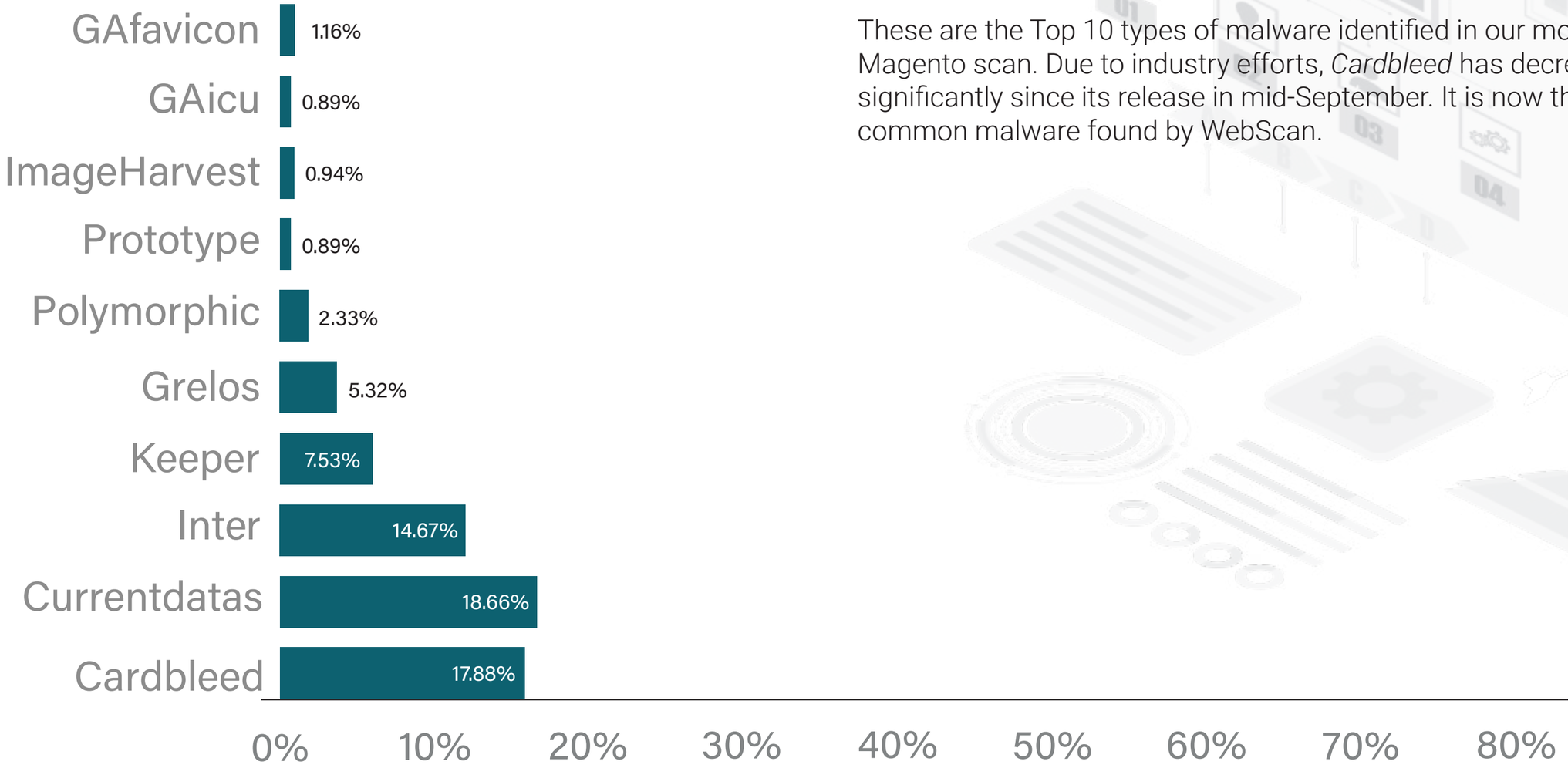
MAGENTO 2 PERCENTAGES



FOREGENIX

30TH NOVEMBER 2020

WEBSCAN RESULTS MALWARE TYPES



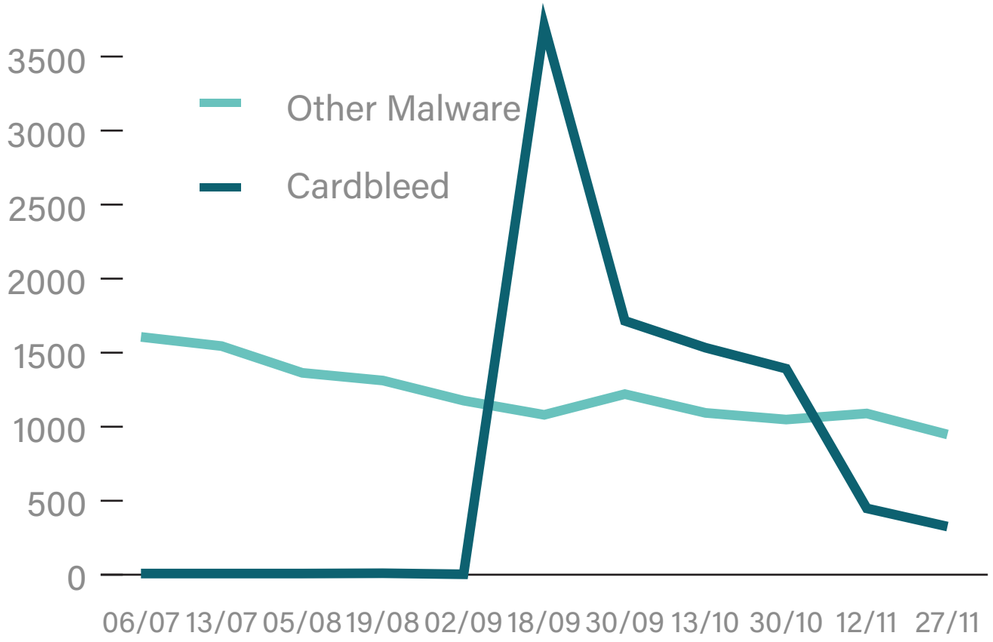
These are the Top 10 types of malware identified in our most recent Magento scan. Due to industry efforts, *Cardbleed* has decreased significantly since its release in mid-September. It is now the second most common malware found by WebScan.

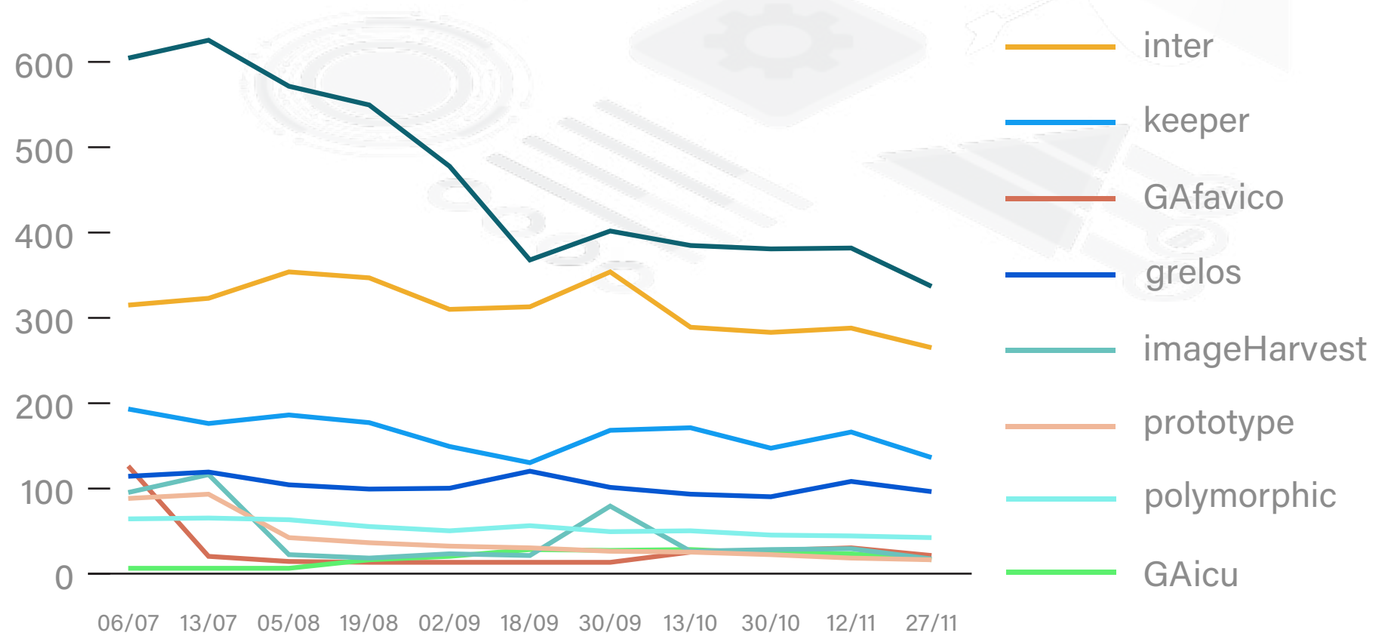
FOREGENIX

30TH 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

30TH NOVEMBER 2020

MALWARE ANATOMY CARDBLEED

In September 2020, thousands of Magento sites were hacked by an automated campaign that would later be dubbed "*Cardbleed*". This campaign appeared to exploit a zero-day vulnerability, taking advantage of Magento 1's End of Life, within the Magento Connect Manager, which is used to install Magento extensions and can be accessed via the `/downloader/` endpoint.

A webshell was uploaded to vulnerable sites, which was then used to inject malicious code into a core Magento file. The file `/js/prototype/prototype.js` was chosen as the target, as this file is loaded on every page (including the checkout page).

The injected code was a loader for the main skimming script. If the user was on the checkout page then a second script would be loaded from the URL `mcdnn[.]net/122002/assets/js/widget.js`. This is the script that performs the skimming itself. It scrapes the page for billing information and posts it to the URL `https://imags[.]pw/502.jsp`.

Shortly after the attack had been publicised, and the attacker's infrastructure started to get taken down, the attacker switched to injecting links to `www.facelook[.]no/en_US/pixel.js` in an attempt to disguise it as Facebook Pixel code. This script contained a loader which would load the skimming code from `ajaxcloudflare[.]com/cdn-cgi/scripts/10349f55d/cloudflare-static/widget.js`, which would, in turn, post the data to `https://consoler[.]in/502.jsp`.

Recently, WebScan and our team have found that the attackers are using a new URL to host the malware: `facedook[.]host/121034/assets/js/jet.js`. This script loads the main skimming code from `facedook[.]host/121034/assets/js/widget.php`, which continues to use `https://consoler[.]in/405.jsp` as a repository for the stolen data.

Some of the domains used by the attacker to host the malware and receive the exfiltrated card data appear to have been taken down now. However our scans show a large number of sites that have still not been cleaned since the initial attack took place. Given that Magento 1 has not received any further security patches since June, any site using Magento 1 is still vulnerable. This particular attack seemed to use the `/downloader/` endpoint, which can be restricted in order to help protect your site. However there could be other vulnerabilities found in the future that may be harder to protect against. It's recommended that sites still using Magento 1 migrate to Magento 2, or another platform that receives regular security updates.

MALWARE ANATOMY CURRENTDATAS

In October 2019, hundreds of Magento sites were infected with card skimming malware. The malware was most likely injected into the database in the *core_config_data* or *cms_block* table. This would ensure the malware is loaded on every page a customer visits, including the checkout page.

The malware searches through the input and select form elements on the page, and stores the names and values of these elements inside a cookie called *currentdatas*. If it detects that *cc_number* has been saved, it will attempt to send off the contents of this cookie to the exfiltration URL.

The following exfiltration URLs were observed:
halloweenhallway[.]com/js/mage/adminhtml/product/composite/validate.php
sharp-planet[.]eu/js/mage/adminhtml/product/composite/validate.php
103.139.113[.]34/validate.php

Both *halloweenhallway.com* and *sharp-planet.eu* were compromised Magento sites being used to receive the stolen card data. The attacker planted a file, *validate.php*, as a way to either relay the stolen data to the attacker's server or to store it somewhere for the attacker to retrieve at a later date. Another version of the skimmer was encoded with hexadecimal and posted to *103.139.113[.]34*.

Many sites that were infected by this campaign also appear to have been infected by a slightly earlier campaign that can be traced back to July 2019, one that would post the stolen data to the compromised store *tarrianalee.co.uk* and a server with the IP address *89.32.251[.]136*.
Both campaigns bear a number of similarities:

They appear to have targeted many of the same sites
They both involved compromising Magento stores and planting a file called *validate.php*
They both appear to have injected the skimming code into the database

So there's a good chance the two attacks were carried out by the same group.

It's worth noting that the compromised sites involved in these campaigns appear to have removed the *validate.php* files from their sites, so any card data that gets posted to those compromised websites may not end up in the hands of the attacker. However the exfiltration point at *103.139.113[.]34* still appears to be active and we're still seeing a large number of sites that have not cleaned up since the original infection. Given that these sites had been infected in the first place, the chances are they're still vulnerable to a similar, large-scale attack in the future.

OUR INSIGHTS

The number of Magento websites continues to decrease. Due to the current situation in the world, we're sad to say some eCommerce businesses closed their doors. We believe this is due to the number of High and Critical Magento websites found throughout 2020.

Cardbleed, which seemed to have its infrastructure shut down, has moved its operation to a different URL. We believe this malware campaign is still a threat to Magento 1 website owners.

Website owners/administrators using Magento should check their configuration/set-ups, and make sure it's secure. For extra peace of mind we recommend using a website security solution and getting cyber insurance.

For free guidance, check out our Magento Security Insights.

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

30TH NOVEMBER 2020