NETACEA / WHITEPAPER

Securing your Magento Website Against Malicious Bots

NETACEA

INTRODUCTION TO MAGENTO

Magento is the open commerce platform used by more than 250,000 merchants around the world. As a key player in the eCommerce industry, Magento is the second most popular eCommerce platform globally after Shopify, accounting for 12% of the eCommerce market.[1]

Throughout 2020, Covid-19 created a surge of eCommerce activity, resulting in more than 130 days that exceeded $2 billion in digital retail sales, compared to just two days in 2019.[2] As a result, the global eCommerce market is predicted to reach $5.4 trillion in 2022.[3]

While the pandemic drove a huge increase in retailers moving to digital platforms, this surge was equally attractive to hackers as to businesses. Around two-thirds of Magento merchants operate on an outdated version of the Magento platform, which reached end of life in June 2020, opening themselves up to security vulnerabilities as cybercriminals capitalised on the increase in online activity and broadened attack landscape.

Sources:
1. Hosting Tribunal: 25 Magento Statistics You Need in 2021 to Boost Your Online Business
2. Magento: Looking back to get ahead in the new year
3. Statista: Retail e-commerce sales worldwide from 2014 to 2024

ECOMMERCE SITES AND CYBERSECURITY

Growing online activity leads to greater potential for cyber-attacks. As customers create more online accounts, more data becomes available, and cybercriminals use more sophisticated methods to harvest data and make fraudulent purchases. 2020 saw more and more attacks on eCommerce websites, including Italian liquor vendor Campari, Claire's Accessories and global hotel chain Marriott – which suffered a cyber-attack that impacted 5.2 million guests when email accounts were illegitimately accessed.[4]

As cybercriminals seek new vulnerabilities to exploit, cybersecurity must become a priority investment for eCommerce organizations in 2021 and beyond.

Sources:
4. ZDNet: The biggest hacks, data breaches of 2020

Best practice Magento security

Magento offers both Magento Commerce and an open-source solution, the latter of which makes for an attractive target for hackers by providing them with insights into vulnerabilities. Cybercriminals are familiar with the open-source coding and can tailor it to attack types. There are plenty of questions around Magento site breaches and whether the platform is secure. The answer is that your Magento site is as secure as you make it. No eCommerce platform offers 100% protection against cyber-attacks; it takes one insecure password to break down security defenses. Platforms like Magento 2 offer out-of-the-box security features which are there to bolster the website's security, but it is up to the company whether and to what extent they adhere to these steps.

While any business still operating on Magento 1 should move over to Magento 2 immediately, there are some out-of-the-box security features which come packaged with the latest version. Before you take further steps with a security provider, here are some Magento security quick wins:

- Ensure you are complying with PCI DSS (Payment Card Industry Data Security Standard).
- Change the default admin username.
- Change or obfuscate the admin URL to deter cybercriminals from accessing your system.
- Use two-step verification for Magento admin login.
- Restrict access to the Magento admin login page to only approved IP addresses.
- Set a strong password policy for your admin account that rotates regularly.
- Rate limit login attempts for Magento admin.
- Enable CAPTCHA for login, account register and contact forms.
- Set recommended file and directory permissions.
- Set recommended admin user roles and permissions.
- Update security patches as soon as they are released.
- Only install extensions from a trusted source such as the Adobe marketplace. The vast range of plugins available for Magento increases the attack surface and the chance of there being vulnerabilities that an attacker can exploit.
- Secure your webstore with a web application firewall (WAF).

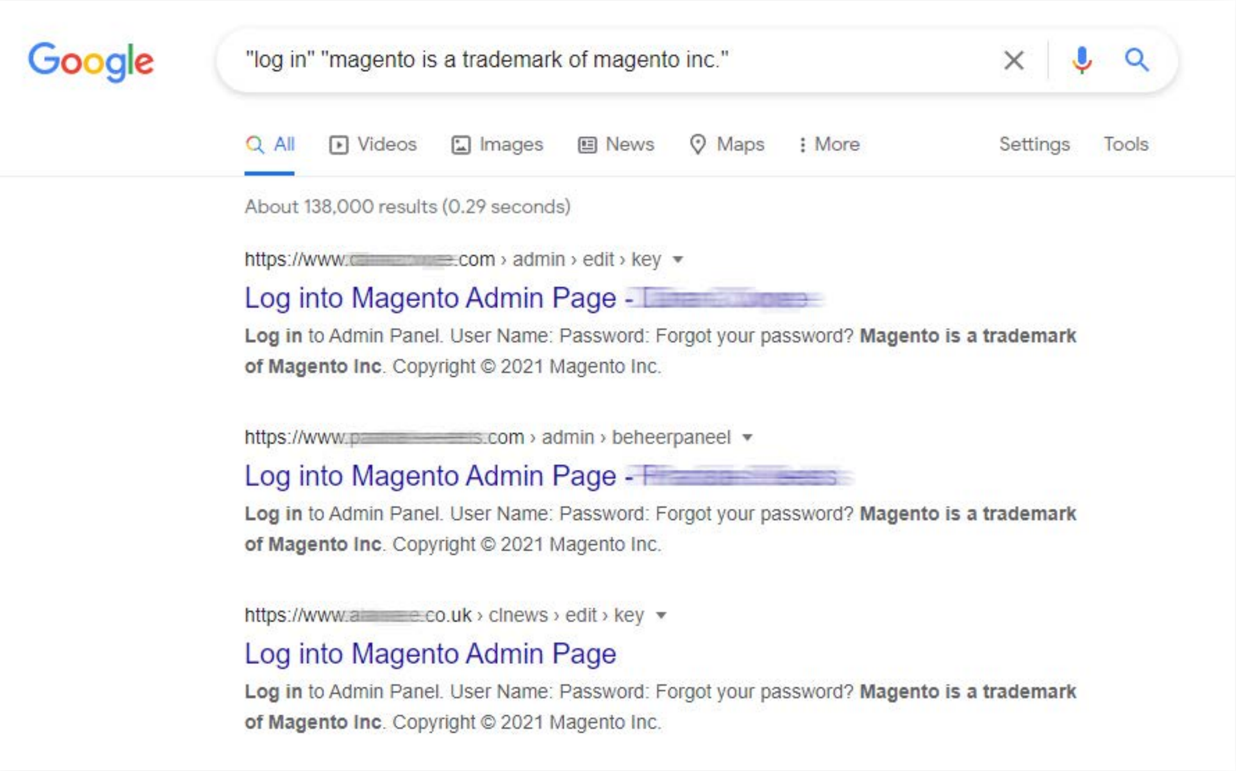
> *"It's always surprising how little has been implemented by new merchants with security at their fingertips on Magento – unlike other platforms where security is an add on."*
>
> *Matt Parkinson, Managing Director, Gene Commerce*

SECURITY CHALLENGES FACING MAGENTO SITE OWNERS

Although these security quick wins come available out of the box with Magento 2 to protect the front and back end of your site, Magento merchants face a range of security challenges from cybercriminals that aim to gain access to admin logins, customer data and valuable goods.

Google dorking

A technique widely used by adversaries and threat research teams, Google dorking utilizes Google's advanced search capabilities to find vulnerabilities on websites. Fig. 1 shows a basic Google search for a Magento 1 admin login. The search returns 138,000 sites in less than one second, and without multi-factor authentication (MFA) in place, the adversary can use bots to bombard the login page with username and password combinations until they eventually gain entry.



"log in" "magento is a trademark of magento inc."

About 138,000 results (0.29 seconds)

https://www.[redacted].com › admin › edit › key

Log into Magento Admin Page - [redacted]

Log in to Admin Panel. User Name: Password: Forgot your password? **Magento is a trademark of Magento Inc**. Copyright © 2021 Magento Inc.

https://www.[redacted].com › admin › beheerpaneel

Log into Magento Admin Page - [redacted]

Log in to Admin Panel. User Name: Password: Forgot your password? **Magento is a trademark of Magento Inc**. Copyright © 2021 Magento Inc.

https://www.[redacted].co.uk › clnews › edit › key

Log into Magento Admin Page

Log in to Admin Panel. User Name: Password: Forgot your password? **Magento is a trademark of Magento Inc**. Copyright © 2021 Magento Inc.

Fig. 1

Credential stuffing and account takeover

Following techniques like Google dorking being used to find a login page, credential stuffing is used to inject username and password combinations, obtained from the dark web, until entry is granted. Credential stuffing is a popular attack type on eCommerce customer accounts and is a signal that a site is under threat from a larger account takeover attack.

Fig. 2 shows the stages a typical credential stuffing attack goes through. A credential stuffing attack begins with purchasing thousands of username and password combinations from the web and identifying a target, using bots to bypass traditional security defenses such as CAPTCHA, and injecting credentials until they successfully gain entry to the account.

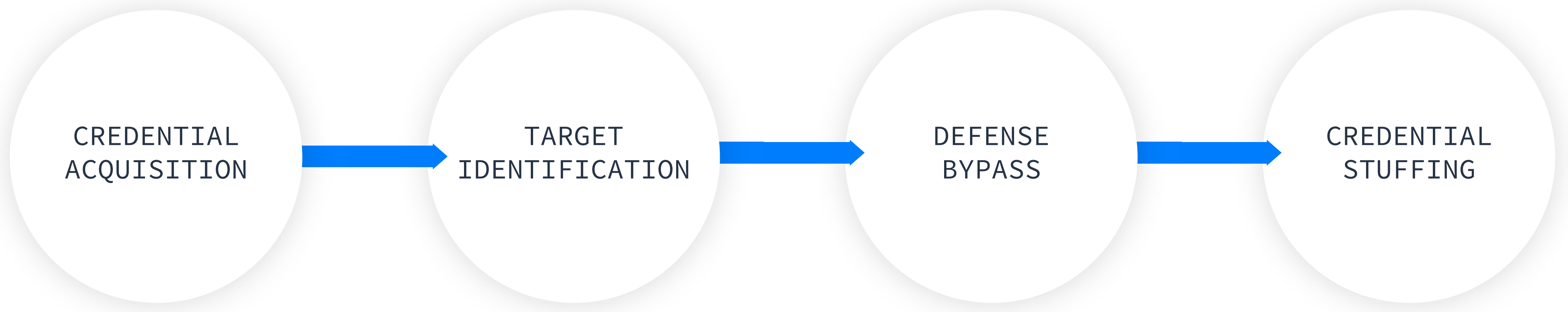


Fig. 2

According to Hootsuite, the average user now has around 190 accounts across hundreds of sites.[5] With this in mind, it's unsurprising that users reuse password combinations, making it easy for cybercriminals to infiltrate multiple accounts once they have access to the first.

Credential stuffing configs tell the bot how to target a particular site. Hackers can upload password combinations they wish to try and come back several hours later to see how many accounts they have taken over; these accounts are then stripped of personally identifiable information (PII). Some bots automatically strip PII out as soon as they gain access, giving no time for anyone to respond. This subsequently puts the targeted company at risk of breaching data privacy legislation, which leads to financial repercussions and brand damage.

Managing the risk of a credential stuffing attack for a Magento merchant depends on how high they are willing to build their security wall.

Basic steps to take to avoid credential stuffing attacks include:

- Implementing IP restrictions on admin URLs
- Enforcing a strong password policy
- Being vigilant when performing data migration or importing from legacy systems
- Use of CAPTCHA
- Implementing MFA
- Separating username and password fields with a two-step process
- Device fingerprinting to flag unusual login activity to the customer
- Real-time monitoring of passwords
- Rate limiting via WAF on login screens

Sources:
[5] Datareportal: Digital 2021: Global Overview Report

Card skimming

In 2020, 96% of eCommerce enterprises stated that card fraud posed the greatest online threat to their organization.[6] Card skimming is one of the most damaging threats to eCommerce websites, and Magento merchants are a common target of a specific type of card skimming known as Magecart. Many eCommerce sites fail to vet the code used with third-party pieces of software on checkout pages.

Magecart has been known to be active since 2016, notably targeting Ticketmaster, British Airways and Forbes magazine subscribers since then.[7] It is defined as a process whereby hackers inject malicious code into a website, typically on checkout pages, enabling them to harvest customer PII and credit card details. There are two ways attackers can gain access to your website and place skimming code; they can either break into your infrastructure on your server and place the skimmer there, or go after third-party vendors which may be an easier target and inject a third-party tag that runs malicious script on your site.

The skimming code is some form of JavaScript that 'listens' out for PII and collects it. Attackers can hide the malicious code inside other code on checkout pages to avoid detection. Once access has been gained and the adversary has harvested payment information input by customers, they can choose to hide it in the server or transmit it out to any location on the internet.

Often the customer is unaware of the attack, which can go on for months, and the level of sophistication is surprising to the merchant. Cybercriminals are incentivized to stay ahead of defense measures, and like any business they must adapt to stay ahead of the competition. Their primary opponent is security providers – and as they adapt to bypass security features, security vendors must adapt to stay ahead of sophisticated bots.

Common defense methods against card skimming on Magento include:

- Patching Magento to the latest version
- Employing decent malware scanning software on the server that can keep up to date with specific eCommerce vulnerabilities and offer real-time alerts
- Regularly reviewing admin users and permissions
- Applying IP restrictions on admin URLs
- Implementing MFA
- Setting permissions for files and folders to read only
- Employing a data integrity tool to receive alerts of potential infections
- Only using approved Magento extensions and ensuring they are kept up to date
- Limit access to the server's root account to only those who need it to perform their duties (generally this should only be sysadmins)
- Denying the ability to run scripts from certain folders e.g. /media/ where CMS users upload images. Run conditions to restrict ability to run scripts from this folder.
- Regularly carrying out maintenance and monthly checks

Sources:
[6] Netacea: The Bot Management Review 2020
[7] CSO: What is Magecart? How this hacker group steals payment card data

Attacks on payment details

Two main areas of concern for eCommerce sites are attackers stealing payment details and attackers using stolen payment details. Payment detail acquisition can be split into three methods:

- Malware (any malicious software designed to cause damage to a device)
- Phishing (a social engineering technique used by adversaries to steal sensitive information from individuals)
- Man-in-the-middle attack (when an adversary intercepts communications between two other parties, allowing them to eavesdrop on those communications or tamper with the messages being sent)

Acquiring card details comes first in the typical stages of making fraudulent purchases on an eCommerce site. Once the adversary has acquired payment details via one of the three methods listed above, they identify a target and use bots to bypass traditional security defenses such as CAPTCHA, before validating payment details in order to sell the data or make illegal purchases on the website.

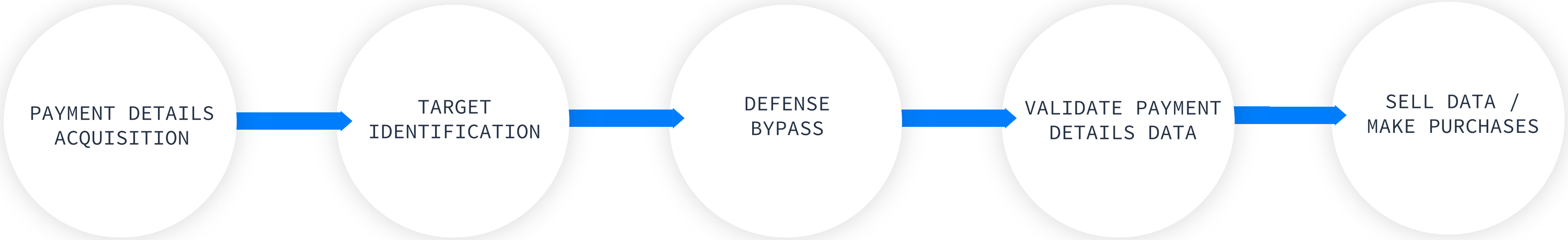
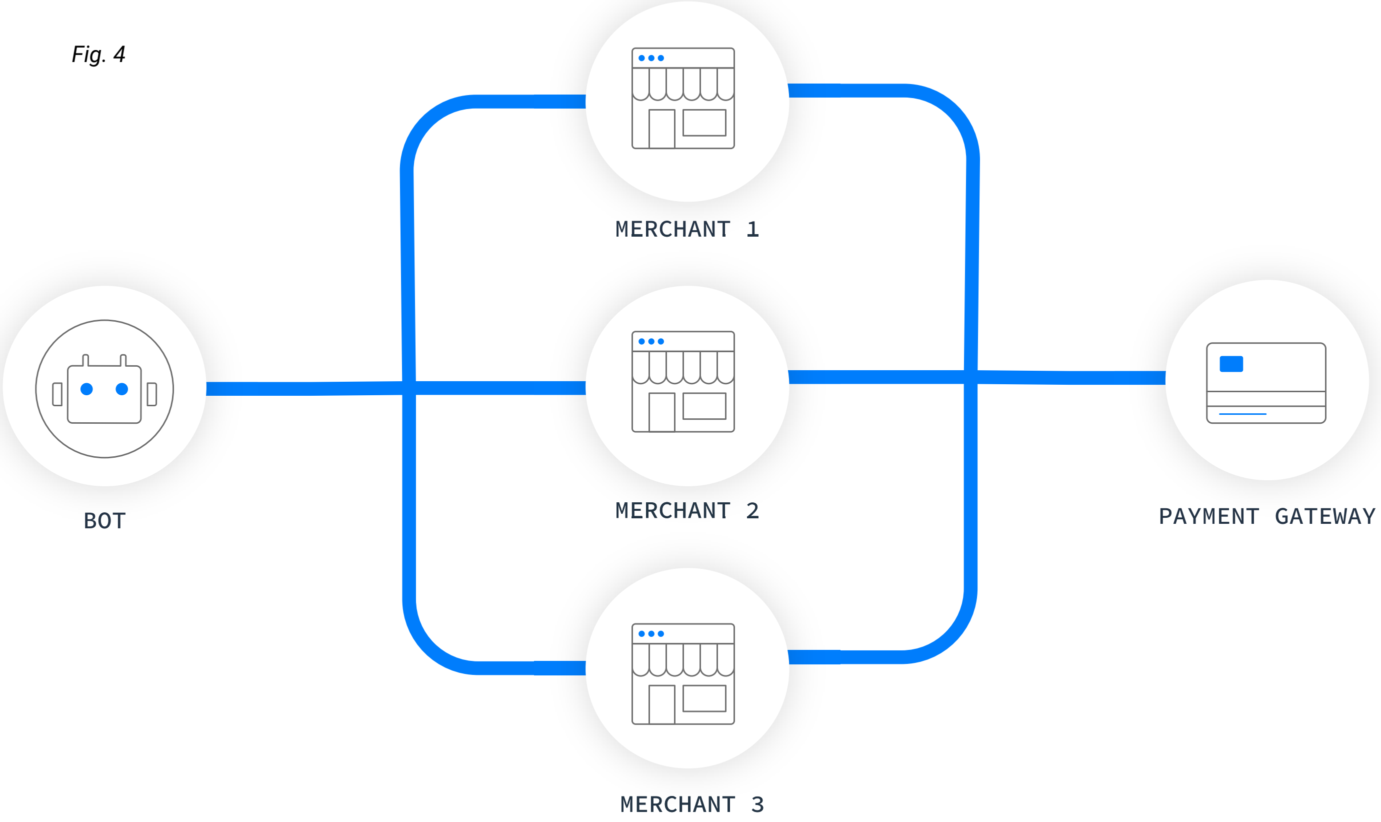

PAYMENT DETAILS ACQUISITION
TARGET IDENTIFICATION
DEFENSE BYPASS
VALIDATE PAYMENT DETAILS DATA
SELL DATA / MAKE PURCHASES

Fig. 3

Some banks are better than others at detecting this kind of activity, but Magento sites are more likely to be able to protect customers if they are aware of this kind of attack. Customers will quickly lose trust in a business that allows a third party to make purchases using stolen payment details. Alongside this brand damage, repatriating customers uses up valuable time and money.

More advanced adversaries split their activity across multiple merchants but target one gateway, making it much harder for any individual merchant to detect, as shown in Fig.4. Sophisticated bot management intercepts and can alert multiple merchants of malicious activity.

Fig. 4



HOW TO PROTECT YOUR MAGENTO WEBSITE

The top three threats Netacea sees affecting eCommerce, specifically Magento, sites are:

- Credential stuffing
- Card skimming
- Use of stolen payment details

While migrating to Magento 2 is the first and most important security step any merchant still operating on Magento 1 can take (verson 1 reached end of life in June 2020), the top security precautions from Netacea's Threat Research team are:

- IP restrict your admin area
- Implement MFA
- Invest in malware monitoring software and bot management

Sophisticated bot management for Magento websites

Card skimming, credential stuffing and attacks on payment details pose a significant risk to Magento sites. While security measures including MFA, IP restrictions and malware monitoring software act as a starting point, it is crucial for Magento merchants to implement a sophisticated bot management solution to combat new and emerging threats.

Netacea's revolutionary bot management technology is helping Magento merchants to detect and protect against malicious bot threats. At Netacea we take a consultative approach, working closely with you to understand not only the threats bots pose to your organization, but how our solution fits into your wider security strategy and business objectives. This partnership, paired with our server-side approach and innovative Intent Analytics™ technology, allows us to seamlessly integrate with your business and deliver accurate, intelligent and effective bot mitigation.

To find out how much bots could be costing your Magento site, try out Netacea's new bot calculator at www.netacea.com/impact-of-bots-calculator/

Or talk to our team today at hello@netacea.com.