ENSIGHTEN

Ensighten eGuide

The Rise of Magecart: Detection and Prevention

Cybercrime groups such as Magecart are on the rise. Learn how you can protect your business from common methods used by Magecart, such as digital payment card skimming, to prevent website data leakage

July 2020

Introducing Magecart

With incidents of Magecart attacks exploding throughout 2019 and 2020, we look at how you can best protect your customers' data and your reputation. Last year saw an alarming increase in the frequency and complexity of cyberattacks being levelled at organizations, which resulted in several high-profile customer data breaches.

While businesses are increasingly aware of the dangers associated with cyberattacks – most notably around data theft – they often look to shore up their network or servers as a priority. This means that their website can get overlooked, despite it being a valuable source of personal customer data and home to a raft of third-party technologies. However, one method that Magecart employ to steal customer data specifically hijacks these website technologies – and attacks of this sort are on the rise.

2020 has already seen an alarming increase in the frequency and complexity of cyberattacks beign levelled at organizations

In Q1 2020, 7,836 websites were compromised with formjacking code – up from 7,663 in the previous quarter

Magecart are a syndicate of cybercriminals that targets ecommerce websites to steal customers' credit card information. The threat from Magecart is now so great that the FBI have issued a warning to the US private sector regarding the attacks.

Magecart operatives inject malicious JavaScript which steals the data from online payment forms, typically on checkout pages – a process known as formjacking. Magecart code has been inserted on millions of sites and compromised the payment information of millions of users. They gain access to websites either directly or via supply chain attacks that target the third parties who supply functionality to the sites. It is these supply chain attacks that are responsible for the largest spikes in Magecart detections

In Q1 2020, 7,836 websites were compromised with formjacking code – up from 7,663 in the previous quarter. 27% of the attacks targeted American websites, making U.S. the country with the highest percentage of detected formjacking attacks.

The 2020 Cost of a Data Breach Report by Ponemon Institute found that the average time to identify and contain a data breach is 280 days (270 days to identify and 73 days to contain). Moreover, they found the average total cost of a data breach to be a staggering $3.68 million.

Other research shows the most significant factor in Magecart's rise is that site owners lack visibility into the code running on their site. Moreover, research found that the average breach lasts over two weeks, with many lasting much longer than that.

Platforms

Shopping platforms such as Magento and OpenCart are the lifeblood of many Magecart groups

Infrastructure

Magecart infrastructure is vast, with 573 known C2 domains and 9,189 hosts observed loading C2 domains

Skimmers

Because Magecart skimmers stay on websites for so long, threat actors are purchasing Magecart infrastructure that's gone offline to assume access to these breached sites

Website owners beware

Some recent high-profile breaches were attributed to 'skimming code'– where Magecart installed suspect code designed to steal customers' financial details. This is also known as digital payment card skimming (DPCS) or web skimming, where criminals use malicious JavaScript code to steal credit card details and other information from payment forms on the checkout pages of ecommerce websites.

Worryingly, the method of attack is becoming more common. Research has shown 2,552 detected Magecart attacks in Q1 2020 alone, which amounts to an alarming average of 425 attacks each month.

2,552 Magecart attacks were detected in Q1 2020, which amounts to an alarming average of 425 attacks each month

The spike in attacks is particularly significant because we as consumers now make more purchases online than ever before

Online shopping puts pressure on businesses

This spike in attacks is particularly significant because we as consumers now make more purchases online than ever before – a trend that has only continued with the prevailing COVID-19 situation around the world. As of April 2020, there were a 129 percent year-on-year growth reported for the US and Canadian ecommerce.

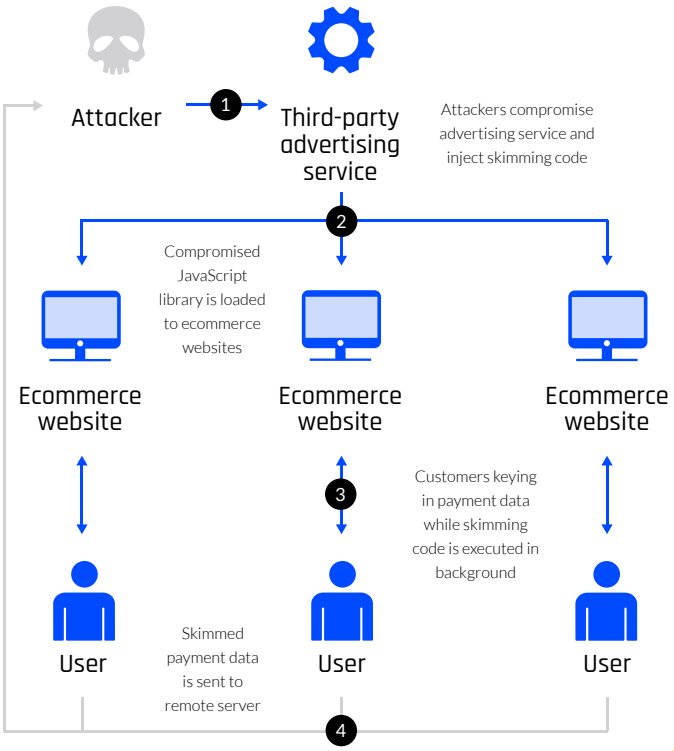
Consumers spent $347.26 billion online with U.S. retailers alone in the first six months of 2020 – up 30.1 percent from $266.84 billion for the same period in 2019.

But while it's great news for businesses that consumers are spending more online, the current regulatory environment means the pressure to safeguard customer data has never been greater. In Europe, companies can be subject to huge fines in the event of a data breach under the Global Data Protection Regulation (GDPR), while the US has followed suit with the California Consumer Privacy Act (CCPA).

The long-term effects of a data breach can be disastrous too. According to research, more than two-thirds of consumers would walk away from an organization if it suffered a data breach where their financial and sensitive information was stolen. 93 percent of those questioned believe the business would be at fault and would think about acting against them – with retailers, banks and social media sites considered the most at risk of losing customers.

Therefore, it is hugely important that any company that processes payments on its website ensures they take every possible precaution to prevent a website data breach.

How Magecart performs supply chain attacks



67% *of consumers would walk away from an organization if it suffered a data breach where their financial and sensitive information was stolen*

93% *of consumers believe a business would be a fault if it suffered a data breach and would think about acting against them*

What is web skimming?

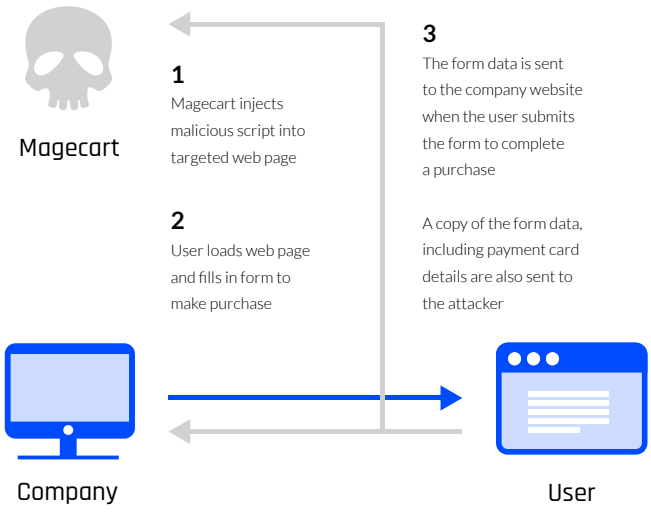
While not a new technique, web skimming or DPCS-based attacks are increasing in size and sophistication and are occurring more regularly than ever before.

Traditionally, criminals use devices known as card skimmers – gadgets hidden within credit card readers on ATMs, fuel pumps and other machines people use their credit cards – to steal customers' credit card data. This has now evolved to digital skimming where hackers can steal sensitive data that consumers enter via online payment forms directly on ecommerce platforms.

As consumers, we're used to entering our personal and financial details when paying for goods online. Formjacking works via malicious JavaScript code which collects all information – such as payment card details and the user's name and address – that visitors submit into a website's payment form when checking out. Attackers can then use this information to perform payment card fraud or sell the details to other criminals on the dark web.

While not a new technique, web skimming or DPCS-based attacks are increasing in size and sophistication and are occurring more regularly than ever before

How Magecart steals data via formjacking



The third-party problem

One tactic employed by Magecart is to use 'supply chain compromise' to steal payment card data. This method was used to steal customer data from Ticketmaster UK when they injected malicious JavaScript code into the firm's website after compromising a chatbot originating from a third-party customer support company.

While third-party scripts like ads, analytics, trackers and social media buttons provide great functionality, interaction and even revenue-generating opportunities to your website, they can also come with security risks if you do not have the correct website security measures in place.

Aside from the security implications, 'external' third-party technologies, tags and scripts can affect a website's performance. Even a change to a single line of code by a third-party vendor can increase page load times. Alongside this, third-party tags often call upon fourth-party tags for enhanced functionality and operational capabilities, adding further complexity and risks to your environment.

44% *of organizations say they have no controls in place for third-party suppliers*

59% *of companies have experienced a data breach caused by one of their third parties*

63% *of all cyberattacks could be traced either directly or indirectly to third-party technologies*

While third-party scripts like ads, analytics, trackers and social media buttons provide great functionality to your website, they can also come with security risks if you do not have the correct websit security measures in place

Steps for a more secure website

Software supply chain attacks can be difficult to guard against, but the key to managing third-party technologies and ensuring criminals don't slip through your security perimeters, is to have a holistic overview of your entire ecosystem and understand the dependencies and performance costs created by these services.

Your organization should be implementing security best practices such as a layered approach to protection, as well as proactively and regularly updating any out of date security devices.

The starting point is conducting an audit and seeking help to rectify any vulnerabilities. With a real-time marketing security strategy and enforcement tools such as Ensighten's, you can prevent website data leakage and unauthorized sharing of PII while complying with the CCPA, GDPR and other data privacy regulations.

Best practice should be based on a combination of observation, defense and protection. For example:

Regular site scan

Performaing a regular site scan to see just what's running on the site that includes testing any new updates to detect any suspicious behaviour

Observing site traffic

Monitoring site traffic, in real-time with real user activity to help identify any suspicious patterns so ou can act before any damage can be done

Allowing third parties

Allowing trusted third-party services - creating an allowlist and a blocklist allows you to only share data with trusted vendors

Magecart prevention: MarSec™

Magecart attacks can be difficult to detect as its malicious script resides on the client-facing side of the website, waiting to skim off any personal information when a customer is at the checkout. Once a website is infected, the payment card information is harvested without the merchant or consumer being aware that the information has been compromised.

Businesses therefore clearly need a continued focus on visibility into this expanded attack surface, as well as increased scrutiny of the third-party services used in their web applications. However, current investments in maintaining website security are falling short.

Ensighten research shows that 83 percent of US companies suspect they are at risk of a data breach, but two-thirds of them have not yet put proper protective measures in place. Respondents also claim a high level of awareness of client-side website security vulnerabilities and yet, they admit their organizations are not taking proactive measures and are effectively under-invested in protection. However, as we've seen in the wake of the Magecart attacks, it is essential to have full visibility of your third-party technologies.

83% *of US companies suspect they are at risk of a data breach*

67% *of US companies have not yet put proper protective measures against data leakage in place*

57% *of US companies cannot identify leakage of sensitive data from the browser*

The Ensighten MarSec™ solution will keep your website and customer PII secure from attack groups such as Magecart:

- Real-time website monitoring: Monitoring of all network requests coming into the website or out of the website to detect potential malicious threats
- Automated website privacy audit and alerts: Detect risks to your organization's data privacy rules – website scanning will check for unapproved technologies that may have access to your customer data
- Masking of sensitive data: Determine unique data patterns to prevent sensitive data being exposed within the URL and passed to unauthorized third-party technologies
- Allow and block third-party technologies: Define permissions for approved third-party vendors you choose to allow to access data – or block from receiving specific types of data
- Privacy gateways: Block unknown and unwanted website trackers, technologies and tags from firing on site and collecting sensitive customer data
- Blocking of unauthorized network calls: Block Magecart style attacks, CSS hacks, man in browser attacks to protect end-users and stop data leakage

Ensighten's MarSec™ solution protects your organization against malicious third-party vendor technologies and unauthorized data collection. The platform enables a real-time view of your digital data supply chain, where you can also view all technologies running on your digital properties and perform a full privacy risk assessment as web pages are loaded, along with unique whitelisting capabilities.

Ensighten mitigates against formjacking by allowing control over third-party JavaScript that is given permission to operate within the user's browser. This allows you to extend security protection to your website visitors, without impacting the customer experience. Get in contact to learn more about preventing Magecart data leakage and cyberattacks.

About Ensighten

Ensighten is a global cybersecurity leader, offering next generation client-side protection against data loss, ad injection and intrusion. Through the Ensighten solution, organizations can assess privacy risk and stop unauthorized leakage or theft of data, as well as comply with the CCPA, GDPR and other data privacy regulations. Ensighten's MarSec™ platform protects some of the largest brands in the world from data leakage whilst ensuring maximum web page performance.

Ensighten is headquartered in Menlo Park, US with the European HQ in London, UK. To learn more visit www.ensighten.com and join the conversation on LinkedIn and Twitter.