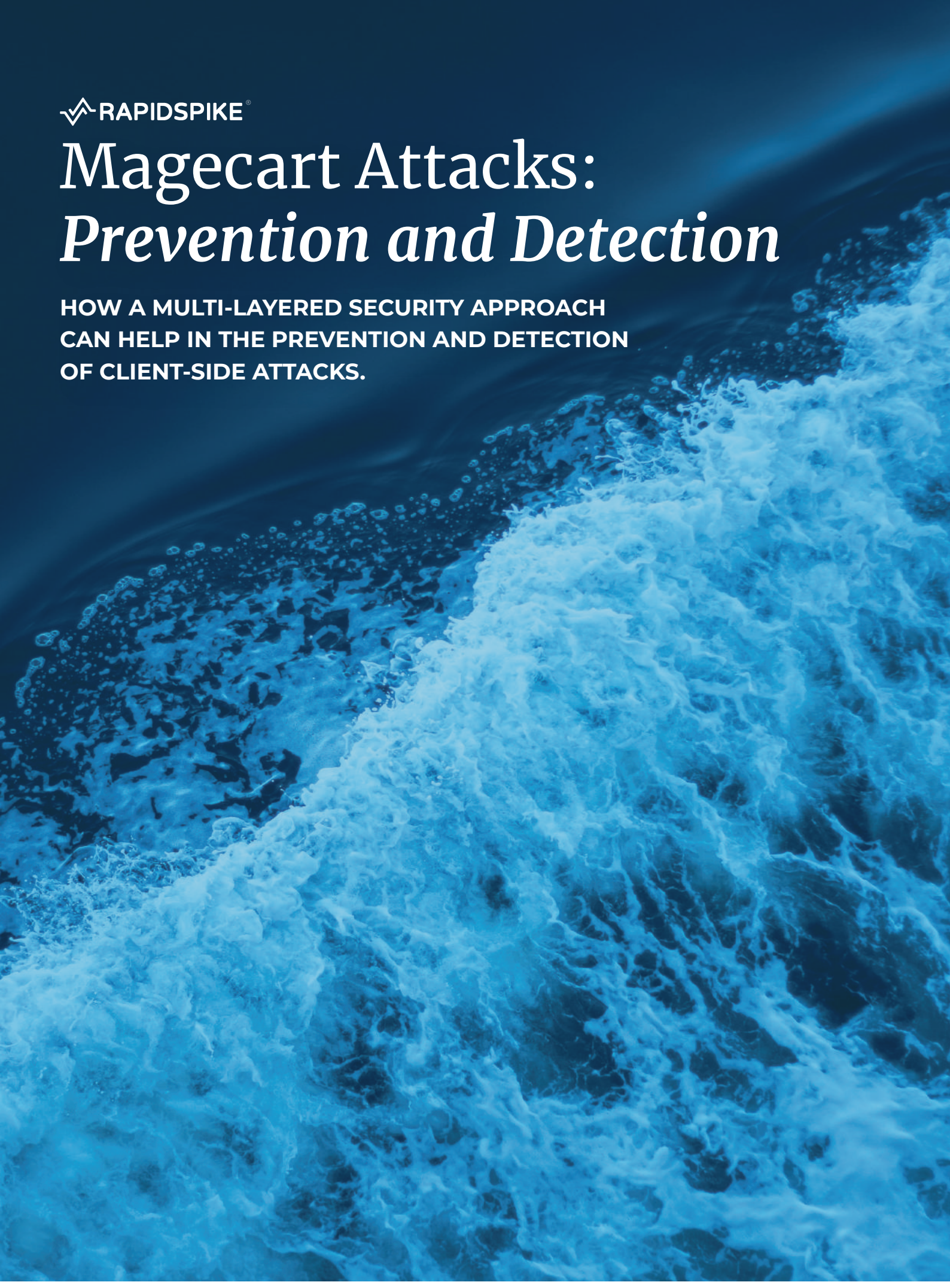
RAPIDSPIKE®

Magecart Attacks: *Prevention and Detection*

HOW A MULTI-LAYERED SECURITY APPROACH CAN HELP IN THE PREVENTION AND DETECTION OF CLIENT-SIDE ATTACKS.



WHAT ARE MAGECART ATTACKS?

Magecart attacks, also known as web-skimming, formjacking or supply chain attacks, are a client-side attack method used to steal customers' payment data from websites. They are currently the number one threat to ecommerce sites today. These types of attacks were first observed in 2015 and dubbed 'Magecart' after the hacking group originally targeting Magento website checkout pages. These days Magecart attacks occur across all website platforms and are undertaken by multiple cybercriminal groups.

These attacks occur by exploiting a vulnerability on the webserver to gain access to the website to either inject malicious JavaScript code into an existing file or edit the HTML of the website to call a new third-party JavaScript file that includes the malicious code. Third-party services include; advertising tools, customer analytics, live chat, and more. The average website uses 85 third-parties and therefore monitoring for changes can be challenging. Here is an example of a third-party attack:

1

Whilst your customers browse and purchase on your website, scripts are loaded from third parties.

2

If a third party is compromised, hackers then have a way to write scripts affecting your website.

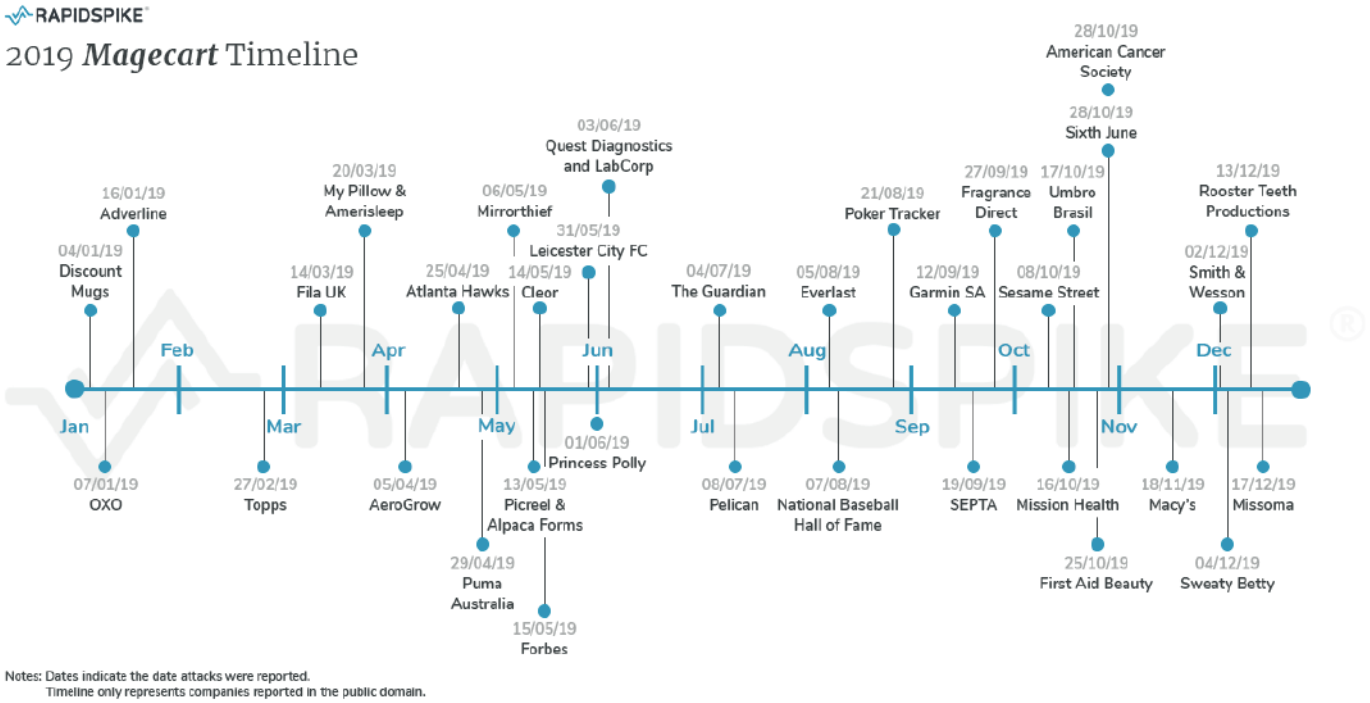
3

Hackers can then intercept customer card details without you even noticing, ciphoning them off to an external server to sell on the black market.

2019 CASE STUDIES - HIGH PROFILE

In 2019, there was an increase in companies impacted by Magecart attacks compared to the previous year. Companies are now more aware of web-skimming attacks, however, it is almost impossible for companies to keep up with web-skimming techniques, and to properly monitor their website to protect against attacks alone. In 2018, RapidSpike launched Attack Detection to monitor for data breaches. The monitor now consists of Client-Side Security Scanner, Synthetic Attack Detection, and Real User Attack Detection, giving data control back to companies. High-profile attacks in 2018 and 2019 prompted updates to the General Data Protection Regulation (GDPR) in 2018, and the California Consumer Privacy Act (CCPA) in 2020, meaning companies now need to take precautions to protect customers' data or face fines.

The 2019 Magecart Timeline includes all significant attacks reported in 2019:



BRITISH AIRWAYS

380,000 customers' details affected.
£500 million cost.
16 days of attack before detection.
Details were taken via a script designed to steal financial information by skimming the payment page before it was submitted.

ticketmaster

40,000 customers impacted.
4 months before detection.
Malicious software on third-party customer support product caused the hack. Stolen details included; names, addresses, email addresses, telephone numbers, and payment details.

volusion

6,589 websites affected.
239,000 payment details sold for $1.6 million.
Infected for 26 days before detection.
Volusion are an ecommerce shopping cart provider. The malicious file and domain were both disguised to look legitimate.

VisionDirect

6,600 customers' details stolen.
5 days before detection.
JavaScript file was injected into the Vision Direct website posing to be a legitimate Google plugin.
Vision Direct have provided all affected customers with an Identity Monitoring Service.

macy's

1 week before detection.
The breach occurred from October 7th-15th, 2019.
An unauthorised third-party added malicious code to two pages on macys.com, including the checkout page and the wallet page.

AMCA

20 million US citizens affected.
Website compromised for 8 months.
$3.8 million spent on mailing individuals.
AMCA have filed for Chapter 11 protection and listed assets of $10 million. Multiple lawsuits against AMCA and the companies this breach affected have been filed.

Q1 2020 CLIENT-SIDE SECURITY OVERVIEW

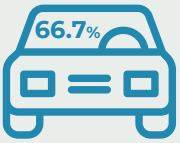
To understand how to prevent and detect Magecart and other client-side security attacks, first it is important to understand how these attacks occur. Hackers are continuously changing techniques to evade detection. Using the latest Q1 2020 data from both primary RapidSpike security research, as well as extensive industry research we can uncover key methods used by hackers in most recent times and understand how multi-layered security can prevent and detect these attacks.

Q1 2020 KEY FIGURES:

hacked websites in Q1 2020 were technology sites.

hacked websites in Q1 2020 were fashion websites.

rise in web-skimming attacks after COVID-19 outbreak.



of hacked websites in the transport industry were automotive websites.

of websites hacked in Q1 2020 were based in the US.

Q1 2020 HIGH PROFILE ATTACK TIMELINE:

JAN

Active Network
Reported: 4th January
Attack on school management platform that handles school accounting and online stores. Infected for 6 weeks from October 1st, 2019, and November 13th, 2019.

Focus Camera
Reported: 7th January
Infected from late December 2019 until January 6th, 2020. Malicious domain registered on November 11th, 2019 in the Netherlands. The attacker modified a JavaScript file to inject an obfuscated payload, encoded using base64.

Perricone MD
Reported: 9th January
Infected on and off for over 1 year from November 2018. Malicious code injected through a vulnerability in the Magento Platform. The server hosting the malicious domain is located in Japan and has been linked to multiple data breaches.

Australian Bushfire Donation Sites
Reported: 10th January
A malicious credit-card skimmer script named ATMZOW was loaded into the checkout pages of the donation sites. The malicious script stole submitted payment information and sent it to the vamberlo[.]com domain. The same script was active on 39 other websites.

Hanna Andersson
Reported: 20th January
Infected for at least 2 months from 15th September 2019 until 11th November 2019. The attack took place by a third-party ecommerce platform. Salesforce Commerce Cloud was infected with malware that may have scraped information entered by customers into the platform during the purchase process.

FEB

Khaddi
Reported: 28th February
The RapidSpike Security Team discovered a web-skimmer on uae.khaadi.com and uk.khaadi.com. The attack was discovered on 23rd January and was active for at least 5 weeks. The malicious code has been injected into the source of the website and only loads the skimmer on the /checkout/ page to help avoid detection. The malicious code loads a heavily obfuscated JavaScript file from hotjar[.]us. The malicious domain was registered on 21 January.

MAR

TrueFire
Reported: 17th March
Hacked for over 5 months from August 3rd, 2019 until January 14th, 2020. The attack occurred due to a website vulnerability, which the company have confirmed they have now patched.

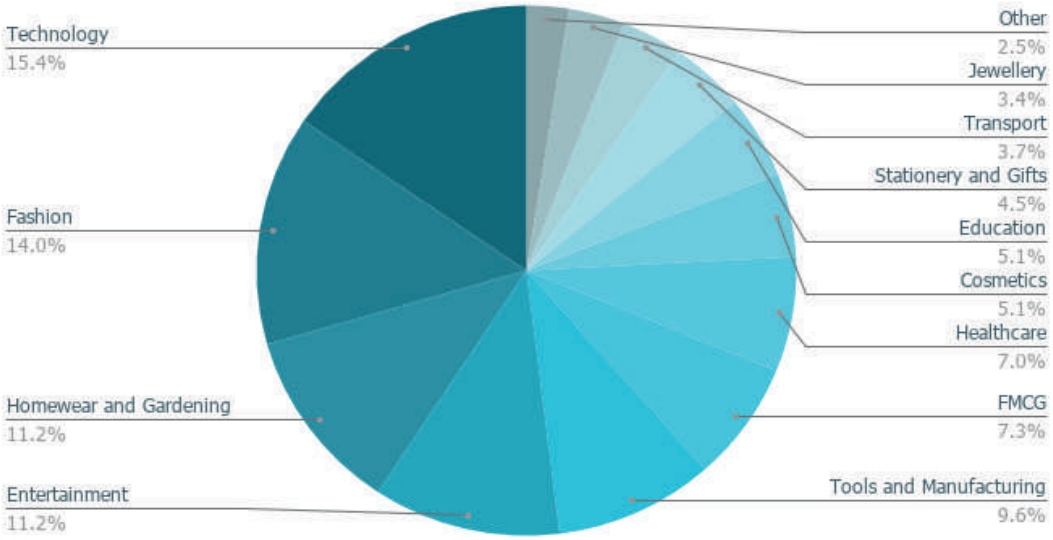
NutriBullet
Reported: 18th March
Malicious code was present on nutribullet.com for 26 days from February 20th, 2020. Researchers were able to take down the hacker's exfiltration domain, however, multiple more skimmers were injected into the website until March 17th, when NutriBullet removed the code.

Tupperware
Reported: 25th March
The attack was discovered on March 20th on tupperware[.]com site and some local sites. The hacker hid malicious code within an image file that activated a fraudulent payment form during the checkout process. Researchers discovered a suspicious iframe loaded from deskofhelp[.]com when visiting the Tupperware's checkout page, which displays the payment form fields used by shoppers. The domain was registered on March 9th and links to a Russian email address provider. The attack lastest at least 6 days. 1 million people visit the Tupperware website per month.

Q1 2020 RAPIDSPIKE CLIENT-SIDE SECURITY SCANNER RESULTS

RapidSpike's Client-Side Security Scanner works by scanning over 1 million websites each day and pattern-matching those websites against known malicious JavaScript code. In Q1, RapidSpike monitored the websites hacked with a web-skimmer, observing the industry, location, malicious code, and vulnerabilities of each website and compiled the results from this data. Our research indicated 12 prominent industries sectors along with 13 significant locations.

Q1 2020 HACKED WEBSITES INDUSTRY



TECHNOLOGY - 15.4%

Technology sites were the number one most hacked websites in Q1 making up 15.4%. Within the technology sector, websites included both hardware sites and software sites. The two technology streams made up 50% of the affected websites in this industry.

There are several reasons as to why technology sites are targeted so heavily by hackers, firstly hackers attack technology sites for bragging rights, with a potential reward. Additionally, it could be expected that as technology products are often expensive, customers purchasing the products are likely to have excessive income. Finally, technology sites had some of the poorest cybersecurity out of the industry sectors monitored. Ironically, websites advertising Magento services made up a portion of the websites hacked in this sector. In the past, we have witnessed technology website attacks including Garmin (SA) and Focus Camera.

FASHION - 14.0%

The fashion sector came in second and made up 14.0% of all hacked websites in Q1. The most hacked websites were located in the US, France, and the UK. Multiple popular brands were spotted by the scanner.

Hacked fashion websites observed in Q1 also had the most high-profile websites. Pakistani fashion brand - Khaadi made up one of the high-profile cases. Khaadi has over 5.4 million social followers, ranks in the Alexa Top 50,000, and has approximately 1.5 million monthly site visitors. RapidSpike reached out to the company twice across two weeks without any response, one month later and the skimmer was still active on the site. Other fashion companies who have suffered Magecart attacks include Macy's, Sweaty Betty, Fila UK, Sixth June, and Princess Polly.

HOMEWARE AND GARDENING - 11.2%

Making up 11.2% of hacked websites, homeware and gardening websites were matched by the scanner multiple times in Q1. The homeware & gardening sector is made up of websites that consist of homeware goods and furnishings, and others which had a mixture of homeware and gardening. 35.7% of sites featured in the sector were from the US, 22.6% were from the UK, followed by Germany and Spain making up 7.1% each. Previous high-profile homeware site attacks include OXO, and Mypillow & Amerisleep.

ENTERTAINMENT - 11.2%

Hacked websites in the entertainment industry sector included a variety of sites including; gaming sites, television sites, news & blogs, and art-focused websites. Making up 11.2% of Q1 hacked websites, these sites can often have complex processes that can be challenging to monitor. Betting & gaming websites are at risk of hacks more than other websites in this category as there are multiple ways a hacker could financially gain from these sites and their customers.

Various entertainment sites have suffered attacks in recent years including PokerTracker, Rooster Teeth Productions, Forbes, The Guardian, and Sesame Street.

TOOLS & MANUFACTURING - 9.6%

Tools & Manufacturing websites were the 4th largest industry in terms of hacked websites in Q1 (9.6%). Upon investigating, it is clear many of these websites were made with weak infrastructures and cybersecurity measures. Often these sites did not have HTTPS in place and basic security scans returned various vulnerabilities. Many of these sites were victim to a 'spray and pray' web-skimming technique and therefore the malicious code was present on pages that did not have payment forms on.

FMCG - 7.3%

The FMCG market was the 5th largest industry hacked and made up 7.3% of Q1 hacked websites. US websites made up 25% of hacked FMCG websites, followed by; Germany (16.7%), India (16.7%), and Australia (8.3%). Hacked websites observed included supermarket chains and food and drink suppliers. After the hacked websites in the fashion sector, the hacked FMCG websites included the most high-profile brands of all of the Q1 hacked websites.

High-profile websites in this sector included a US-based chocolate brand with over 945,000 social followers, which was hacked for more than a week. Due to the website being outside of Europe and therefore not under GDPR law, the company have less responsibility in reporting the data breach.

HEALTHCARE - 7.0%

The healthcare sector made up 7.0% of hacked websites in Q1. Previous attacks included American Medical Collection Agency which affected more than 20 million US citizens and the American Cancer Society. Continuing this trend into Q1 2020, American sites made up 35% of this sector, followed by Brazil (20%), UK (15%), and India (10%). Healthcare websites included medical research sites, doctors' practices, gyms & alternative treatment centres, healthcare equipment, and drug manufacturers. One of the more high-profile websites in this sector included a supplement website based in Mexico with over 85,000 social followers.

COSMETICS - 5.1%

In 2019, the cosmetic industry had multiple attacks on companies including; Fragrance Direct and Procter & Gamble's First Aid Beauty. In Q1 2020, RapidSpike Security Researcher discovered multiple web-skimming attacks on cosmetic site, Perricone MD.

Overall, there has been an increase in the number of attacks on cosmetic-based websites in 2019. Cosmetic websites make up 5.1% of hacked websites in Q1, popular brands were spotted including products sold in high street stores including Waitrose, Selfridges, and Harvey Nichols. Some attacks observed were highly advanced with a dedicated customised skimmer for the website as well as multiple layers of encoding to disguise the skimmer. The majority of hacked cosmetics sites were based in the US (31.6%), followed by France (15.8%), and India (10.5%).

EDUCATION - 5.1%

Education-based websites were prominent in 2019 when the 'Mirrorthief' attack affected 201 online college stores in the US and Canada. The very first high-profile attack of 2020 was on school management software provider Active Network. Parents who paid school fees or bought via the online stores had their credit card details stolen. The attack was active over 6 weeks from October 1st, 2019 to November 13th, 2019.

Other hacked education sites in Q1 included guitar tutorial website - TrueFire who were recently hacked for over 5 months from August 3rd, 2019 until January 14th, 2020. It is unknown how many customers have been affected, however, the site had approximately 470,000 website visitors in the month when the attack took place.

STATIONERY & GIFTS - 4.5%

4.5% of hacked websites in Q1 fell into the stationery & gifts sector. Websites included boutique gifting sites, school supply sites, office and stationery supply sites, and more.

This was a fairly large sector of hacked websites and attacks occurred due to the poor cybersecurity on the sites. Few sites had HTTPS and were built very poorly. It appears sites within this sector also fell victim to the 'spray and pray' technique as multiple pages had malicious code injected rather than just the checkout pages.

TRANSPORT - 3.7%

The transport industry has become notorious with Magecart due to the British Airways data breach. Additionally, in September 2019, public transport company SEPTA also suffered a data breach lasting 25 days affecting 761 customers. This attack trend has continued into Q1 of 2020 with 3.7% of all attacks being on the transport sector.

Websites included; automotive sites (66.7%), bike & scooter shops (26.7%), and public transport (6.7%). 50% of transport websites hacked were located in the US, followed by 14.3% in both the UK and Spain.

JEWELLERY - 3.4%

3.4% of hacked websites were within the jewellery sector. Within this group, a mixture of sites were hacked in Q1. Inexpensive goods sites hacked were mainly based in China and India. More expensive goods websites hacked were based in the US, UK, and France.

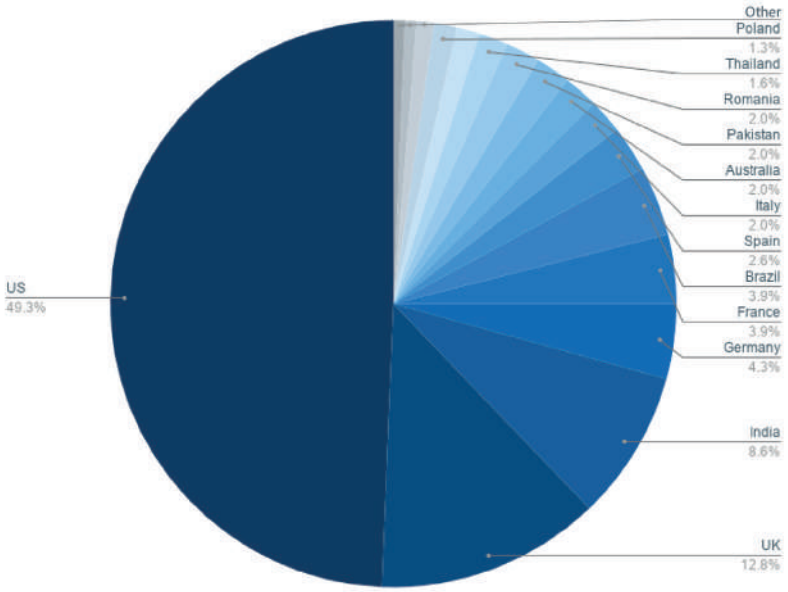
The most high-profile website attack in the sector in Q1 was a US brand with over 200 stores worldwide. The website was only hacked for one day but with an estimated 660,000 visitors to the site during the month it was hacked, this is still a potentially large data breach. In the past, attacks have occurred on jewellery websites including; Missoma and Cleor.

OTHER - 2.5%

Other industries hacked with malicious code included; sports, charities, pet supplies, finance, property markets, and more. The sports industry has had several attacks in the past including; Puma Australia, Atlanta Hawks, Fila UK, Leicester City FC, National Baseball Hall of Fame, and Everlast to name a few. Sports websites could be a prime target for attacks due to the number of loyal sports fans remaining high throughout the year.

Magecart are opportunistic and take advantage of sites with vulnerabilities regardless of their cause. In Q1, charity websites for children with disabilities were hacked as well as the Australian Bushfire Donation sites. Often charities have small budgets for technology and cybersecurity, many sites have vulnerabilities that leave them open to attacks.

Q1 2020 HACKED WEBSITES LOCATION



LOCATION

Almost half of all hacked websites in Q1 2020 (49.3%) were based in the US. This is unsurprising as over the 5 years Magecart have been active, the US has consistently had the most hacked websites. Additionally, across all 12 prominent industries established in Q1, the US websites were also the most hacked websites in every industry sector.

The UK was in second place - although only 12.8% of all hacked websites in Q1, this figure is high compared to other countries. In third place, India made up 8.6%, followed by Germany with 4.3%, and joint 5th were France and Brazil making up 3.9% each. The location results from the Client-Side Security Scanner indicate a need for higher cyber-security, in particular, in the US, UK, and India, to protect customers from data theft.

Overview

Khaadi is a global Pakistani fashion brand including seven stores in the UK and the company boasts over 5.4 million followers on social media. On January 23rd, 2020, RapidSpike's Security Team discovered a skimmer on uae.khaadi.com and uk.khaadi.com which was active for at least five weeks. The skimmer is designed to steal payment details from customers purchasing from the site.

Malicious Code

The malicious code was injected into the source of the website and only loads the skimmer on the /checkout/ page to help avoid detection. Although there is code in place to stop the skimmer from loading if the browsers developer toolbar is open (a popular and effective way for hackers to further avoid detection), it wasn't working.

Skimmer

Once a customer is on the checkout page the malicious code loads a heavily obfuscated JavaScript file from hotjar[.]us. This domain was registered on 21 January 2020, just two days before the hack appeared on Khaadi. It was likely chosen to look like a plugin from Hotjar, a behavior analytics tool installed on "over 350,000 organizations across 184 countries". Although Hotjar's website is hosted on the "hotjar.com", their official plugin is loaded from "hotjar.io". This just goes to show how tricky it can be to determine when a third party is loading from a legitimate domain and when it is not.

Another domain spotted in similar hacks that belongs to the same hacking group is jquery[.]us. jQuery is an extremely popular JavaScript library installed on 74.4% of all websites. Anyone looking at the resources loaded on websites with these skimmers on would be forgiven for missing the fact that these have nothing to do with the official organisations.

Exfiltration

Once a customer has entered their card details on the checkout page and they have hit the "Place Order" button, all card details – including the three-digit CVC / CVV – are encoded and sent to the same malicious host.

According to Similar Web, Khaadi has had an average of nearly 1.5 million monthly visits in the last six months. Although this does not tell us the exact number of victims, the site was infected for at least five weeks which implies this attack may have affected a huge number of customers.

Khaadi

Q1 2020 WEB-SKIMMING TECHNIQUES

Analysing web-skimming attacks observed in Q1 2020, there are some key trends, techniques, and attack approaches that have been seen across multiple attacks. Highlighting these issues can help to understand what to look out for and how to improve security:

Malware Under Images

In early January 2020, one of the new hacking methods observed was steganography-based skimmers. The technique involves hiding code within imagery to avoid detection. Hackers hide the image's background JavaScript code to scrape the data needed. The Tupperware website was one victim of this style of attack, with malicious code hidden within a PNG file that activated a fraudulent payment form during the checkout process.

Fake Checkouts

A key web-skimming attack method is loading a fake checkout form before the legitimate checkout page or before a PayPal page. Customers have a good indication of if an attack has occurred if a second payment form is presented, unfortunately, at that point, the customer's payment details have already been stolen. Checkout pages carry the most valuable information on the website and should be monitored carefully. A Synthetic User monitor can continuously walk through the checkout page and alert to any new hosts found, potentially before a data breach occurs.

Targeted Customers

Skimmers are continuously advancing to evade detection including performing a search before loading a skimmer, to target a specific type of customer. In Q1, RapidSpike's Security Researcher discovered a hyper-targeted skimmer that only loaded after some prerequisites were met. The skimmer required the user to be on a mobile phone and in landscape mode. Additionally, a check was undertaken to ensure the user was on the checkout page, and did not have a developer toolbar present. Once the targeted customer had passed all the requirements, the skimmer would then load.

It is therefore important that companies test their website from multiple browsers to ensure all customers receive the same experience.

Plugins

In early March, WordPress announced that their Threat Intelligence team had discovered several vulnerabilities in 'Popup Builder', a WordPress plugin installed on over 100,000 sites. They explained how one vulnerability allowed an unauthenticated attacker to inject malicious JavaScript into any published popup, which would then be executed whenever the popup loaded.

Plugins can be useful tools in delivering great customer experience, making design changes, and helping with workflow, however, they can also leave a website vulnerable to attacks. WordPress plugins have had multiple vulnerabilities over the years, they should be minimised to a manageable level and continuously updated to patch any vulnerabilities.

Regional Sites

Regional websites can be beneficial for brands as they can allow more people to access products and companies can create specific marketing campaigns for regional holidays and events. This being said, regional websites also increase the workload for a company's developers to keep up with. The increase in workload could let vulnerabilities slip through the net.

RapidSpike discovered a regional attack on one of Belgium's most popular chocolate brands on their Hong Kong website. Hackers can often make mistakes on regional sites including language errors. One thing customers can be observant about is making sure the checkout form is displayed in the website's native language. For companies, it is important not to neglect regional sites and to have the same security measures in place across websites.

Domain Spoofing

Web-skimming attacks often include domain spoofing to assist in going undetected, this can be seen in some of the most high-profile client-side security attacks. British Airways malicious skimmer exfiltrated card details to a spoof domain, 'baways.com'. To an untrained eye, many of these domains could be seen as legitimate.

Another popular spoof with hackers are third-parties, such as Hotjar, jQuery, and Google Analytics. In the past, the legitimate domain 'google-analytics.com' has been impersonated by 'google-anaiytic.com' and 'g-analytics.com'. In Q1, a skimmer was observed spoofing HTTPS, the malicious domain 'http.ps' was customised to specific websites and could easily be hidden in the website source code. On grandwesternsteaks.com website, the malicious code appeared in the source code as '//http.ps//grandwesternsteaks.com', which could easily go undetected.

A good indicator of the legitimacy of the domain is to check the WHOIS record and view when and where the domain was registered, and who to. Often attackers only register the domain a few days or weeks before an attack takes place.

MULTI-LAYERED SECURITY

The best approach to ecommerce security is defence in depth. We advocate a layered approach using multiple tools to ensure coverage across a variety of potential security issues. Companies need to have security measures in place to both prevent and detect client-side attacks. Attackers are coming up with new ways to disguise their attack techniques, therefore companies need to continuously analyse their site for vulnerabilities as well as monitor for attacks present.

PREVENT ATTACKS:

Security Procedures

A Security Analysis should be completed regularly to check on the general health of a website. Penetration tests can be performed to find key security flaws hackers take advantage of. In addition, vulnerability scans should be performed to check for known vulnerabilities that leave websites open to be attacked. Patching security issues quickly can stop attacks occurring in the first place.

Third-party Vetting

Third-parties are commonly used by ecommerce sites, with the average site loading 85 third-parties, companies can easily mistake malicious domains for genuine ones.

Tactics include: imitating domains or domain squatting, where the domain is a commonly misspelt version of the domain. Both of these tactics can easily be mistaken or overlooked. We recommend companies vet all 3rd parties before putting them live.

Content Security Policy (CSP)

A Content Security Policy (CSP) is a security option website owners can undertake to increase baseline security. CSP requires website owners to manually check what code can be loaded by the browser. Content not outlined within the CSP will not be loaded, therefore malicious code injected by attackers will not be loaded.

Although a CSP appears to give control back to website owners, a CSP is both time and resource-consuming if a website owner does it themselves, and can be expensive with a tool, making it ineffective for a lot of businesses.

A CSP also leaves large gaps in security measures and as client-side attacks become more sophisticated, it is important to know not only what content is loaded, but also how the content interacts with a website visitor. Additionally, if your website is hacked, a CSP is useless. Therefore a CSP should be used as an added layer of security and not as an end-all solution.

Stay Aware of Emerging Attack Techniques

New client-side attack techniques are being discovered on an ever-increasing basis. To protect your site it is important to be knowledgable on new vulnerabilities, techniques, and hacked third-parties reported in the news to then make sufficient changes to your site.

DETECT ATTACKS:

Data Breach Monitoring

If the prevention approach to security fails or human error occurs, companies still need to monitor for an actual breach. This is key to reducing the size of data exposure. Monitoring can greatly reduce reputational damage as well as fines associated with data breaches. RapidSpike Attack Detection is powdered by three monitoring tools to give you additional layers to your security.

Data Breach Response Plan

When a breach occurs a plan is necessary to be able to quickly and effectively respond. The basic steps will include the following:

1. Investigate

Put the website into maintenance mode as soon as possible to investigate. Discover the source of the infection, remove the skimmer, and patch the vulnerability.

2. Inform the ICO

A company has a duty by law to inform the ICO as soon as they discover a data breach but no later 24 hours of becoming aware. Depending on your country, you may also have to inform other authorities including the Police.

3. Inform Customers

GDPR states companies have 48 hours to inform affected customers of a data breach. However, it is important to use this time efficiently and not to rush a response to make sure you give correct and clear information to all customers affected.

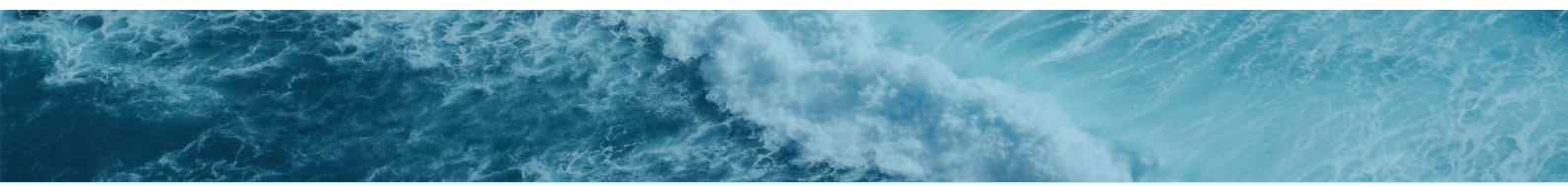
4. Monitor for Reinfection

The average time for reinfection is only 10 days. Companies who make active changes to continuously monitor their security will be able to stay in control and could re-gain trust from customers.

5. Offer Protection for Customers

Companies are not obliged to pay for credit report monitoring services for customers after a breach, however, it is an additional service you could offer customers and could save brand reputation or prevent lawsuits.

ico.
Information Commissioner's Office



RAPIDSPIKE ATTACK DETECTION

In today's online world, hackers are constantly evolving their tactics, growing stronger, and attacking more frequently than ever. Platforms that could not be hacked today will be hacked tomorrow, so vigilance is key. By accepting nothing is perfect, then adopting a security-first approach from development practices to client-side monitoring is the only way to ultimately be safe and protect your customers. RapidSpike reduces average detection time from weeks to minutes and the beauty is, even if you do have other security flaws, RapidSpike can act as your last line of defence against this particular issue.

RapidSpike Client-Side Security: Attack Detection is made up of three layers of protection: Client-Side Security Scanner, Synthetic Attack Detection, and Real User Attack Detection.

CLIENT-SIDE SECURITY: **ATTACK DETECTION**

When configuring the Attack Detection monitor, you can either protect everything or choose the areas of your site which are the most vulnerable. Attack Detection works in two phases: 01 - The Scanning Phase, and 02 - The Detection Phase.

01 - CLIENT-SIDE SECURITY SCANNER

Actively scans the code on your website looking for commonly used patterns that have been used in historic client-side attacks.

02 - SYNTHETIC ATTACK DETECTION

Continuously walks through the critical areas of your website. It will see any data sent to untrusted hosts as it browses.

02 - REAL USER ATTACK DETECTION

Collects where real website visitor's data is being sent. If a malicious destination is added to your website, RapidSpike will alert you.

PHASE 1 - SCANNING

The scanning method of operation is similar to the way AntiVirus applications function. The Client-Side Security Scanner actively scans the code of your website looking for pattern matches against the propriety database of known issues. This scanning service provides you with a level of protection against client-side security attacks such as Magecart by notifying you as soon as the scanner identifies a potential issue. This allows you to fully investigate the issue and remediate the issue before it causes significant risk to your brand and customers' data. If an issue is found, you can decide who is notified using a method of your choice including email, text message, webhook alert, Pager Duty alert, or Slack notification.

KEY BENEFITS:

- Actively scan your website at frequent intervals for potential malicious code.
- Gain trust from your users that you are taking action against credit card skimming.
- Receive a timely notification if your website does suffer an issue so you can take immediate action.
- Protect brand revenue suffered after a breach.
- Avoid heavy fines for data loss and payment card loss.
- Utilise the knowledge of the RapidSpike Security Research team to help protect your website.

PHASE 2 - DETECTION

Phase 2 involves continuous detection by RapidSpike's two detection methods; Synthetic Attack Detection and Real User Attack Detection. The two tools work in synergy to provide cover from a wider number of sources.

Synthetic Attack Detection

This machine-driven method uses critical User Journeys that run on a continuous cycle, looking for new hosts and scanning for telltale signs of a potential Magecart attack. If it spots anything suspicious, you'll be alerted as soon as it happens, meaning it could potentially alert you even before a data breach occurs.

Real User Attack Detection

As an additional layer of protection, real website users are used to detect attacks as they visit your site. There are millions of potential hosts that your users are sending data to so we've included a filtered view allowing you to fine-tune sensitivity to reduce any unwanted noise and false positives. This helps you gain a thorough understanding of hosts affecting customers without picking up on hacks that are on the individual client machine and are not in your jurisdiction or your responsibility.

DEFENCE IN DEPTH

This multi-layered approach means we can examine more data points than ever before - helping us to understand exactly where customers' information is being sent to, allowing companies to both proactively and reactively detect data breaches on the client-side faster than ever.

These three services work as a blended service to offer a best-in-breed defence in depth solution to client-side security issues. The services aims to cover a plethora of attacks scenarios over its three services. Focussing on the scanning of your website looking for known patterns, looking for the appearance of new JavaScript files, and also looking at where your clients are sending data to. This is a comprehensive suite of protection tools that when combined, is the market-leading tool of choice for anybody serious about protecting their brand revenue and client data from client side security issues.

BENEFITS OF ATTACK DETECTION:

- Reduces the average time to detection from weeks to minutes.
- Turns every user into a data guardian for your organisation.
- Ensures no malicious destinations get added to your website without your prior knowledge.
- Detects website skimming, formjacking, and supply chain attacks.
- Clear evidence for the ICO that you have taken steps to defend yourself.
- Insurance against your third-party security failures.
- Continuously monitor for attacks 24 hours a day 7 days a week.
- Last line of defence in case of issues, errors, misconfiguration which allow an attack.
- Receive alerts of any issues in the format of your choice (Email, SMS, Slack, etc.).

ADDITIONAL PLATFORM FEATURES:

In addition to Attack Detection, the RapidSpike platform offers advanced features in monitoring, performance, and security.

RapidSpike interacts with your online platforms exactly as your customers do, creating key insights to increase website performance & detect client-side attacks. We help make your digital experience better, faster & more secure to convert more revenue.

Security

Scheduled scans that detect security vulnerabilities across all digital assets. Coupling industry-standard platforms with bespoke scanners which build a comprehensive picture of the threat landscape whilst also running standard client-facing security checks, perimeter port scanning, cipher scans, security headers & more.

Reliability

Keeps digital platforms live at all times with uptime, availability monitoring & SEO stats, from global locations every minute, 24/7. Be alerted to issues on any communication platform (Slack, Email, SMS, etc.), includes retesting to reduce false positives.

Performance

Track & measure individual page performance and user journeys from global locations, grab screenshots & video, perform google audits, technical SEO, best practices, test accessibility, understand 3rd parties, track elements, collect cookie data & debug issues.

Real Users

Records live real user interactions to deliver insight on vital performance & security metrics. Collect data on platforms, browsers, countries, and devices on every page, interrogate every page, in collections, or view as a whole viewing overall speed as a percentile.