CASE STUDY

How a Major Airline is Mitigating Magecart Attacks With Jscrambler

*"This solution has met our requirements and **we're confident to deploy it in our live environment to help us prevent a Magecart breach**."*

As per the request of our clients, we have anonymized all company and personal names.

OVERVIEW

MAGECART: EVOLVED WEB SKIMMING

Magecart cybercriminal groups are known for injecting **web credit card skimmers** on e-commerce and payment websites. These groups have been very active since 2018.

In a Magecart attack, attackers inject a skimmer that can hijack the submission of a form containing credit card details. These details are then sent to attacker-controlled drop servers. During this whole process, neither the end-user nor the company have any awareness that the attack took place.

While we've seen both first-party and third-party Magecart attacks, third-party attacks are especially critical because they **don't require a first-party server breach** or direct access to the company's website. Attackers can exploit a third-party integration such as a live chat widget to inject the skimmer's code without being detected.

THE KEY BUSINESS THREATS OF MAGECART

Because many Magecart attacks occur without any awareness from the users and the affected company, **many Magecart attacks remain active for months** before being detected and taken down. From our own analysis of known attacks, skimmers remain active for **104 days** on average before being detected and taken down.

These attacks pose a significant threat to businesses. Looking back at known Magecart attacks, we see that they have originated over **$1.3 billion in direct business losses** - notably, the $230 million GDPR fine on British Airways.

Then, we still have to consider the potential deep impact of indirect business losses. Because of negative PR and loss of customer trust following a Magecart data breach, losses in revenue can have a long-lasting impact on the business.

BEHAVIOR-BASED MAGECART MITIGATION

New Magecart attacks are still emerging every week and getting more sophisticated. Companies are gradually understanding the need to think outside the firewall and looking to protect the client-side. But several security approaches commonly associated with Magecart prevention often fail to make the cut against this new wave of sophisticated Magecart skimmers. Some, like domain sinkholing or CSP, are often bypassable; others introduce unsustainable performance drops and cause malfunctions.

While these skimmers keep evolving their tactics, they always display specific types of malicious behavior. As such, a behavior-based approach to Magecart mitigation provides the best chances of detecting and blocking this malicious behavior in real-time and stopping this exfiltration of data

> *“After learning about the Magecart attack on British Airways, it became our* ***priority*** *to detect and prevent these attacks from happening to us.”*

SUMMARY

CHALLENGES

Prevent Magecart credit card skimmers from running on their web pages

Reduce exposure to data leaks

Integrate with their SIEM

Ensure easy configuration and maintenance

SOLUTION

Jscrambler Webpage Integrity:

Behavior-based detection

Fine-grained behavior control

Comprehensive Inventory, detection live feed, and explorer

Real-time Magecart mitigation

RESULTS

Passed all detection tests

Clear, accurate reporting of malicious client-side behavior

Much superior results compared to other tested solutions

Implementation passed strict requirements

Zero performance overhead

Smooth transition from PoC to production environment

Easy configuration and maintenance

CHALLENGES

The August 2018 Magecart attack on British Airways made headlines around the world because it managed to silently exfiltrate over 380,000 credit cards and remain active for **15 days** before being detected and taken down.

After it was disclosed that BA faced a **$230 million GDPR fine**, the threat of Magecart attacks became much more noteworthy.

And as companies started to look for solutions that could actually mitigate this type of sophisticated client-side attack, we were contacted by a **major airline** with this challenge: to prevent Magecart web skimmers from running undetected on their pages and exfiltrating data.

Just like several other enterprises, this company had web apps running scripts from third-parties. One key priority was being able to **know when one of these scripts changed behavior.** Such a change could potentially be linked to attackers exploiting vulnerabilities of these third-party providers and injecting malicious code that could lead to a Magecart attack.

> *“We had to be* ***alerted immediately*** *when a third-party script started doing things that it shouldn’t do.”*

Fast implementation was one of the biggest requirements of this project. **Each unmonitored user session could potentially be hiding a web skimmer** and the risk of a breach was tangible.

And with the company having such a complex web environment, several other requirements had to be met. For one, the company required a solution that could be easily integrated into the SIEM that it was currently using. Then, it had to guarantee minimal performance overhead, ensuring that the end-users’ experience wouldn’t be negatively affected.

The company also wanted to make sure that the solution would be able to work correctly even in scenarios where file names change frequently.

SOLUTION

Due to the urgency of implementing a solution that was capable of stopping potential Magecart attacks, the company was testing several different vendors.

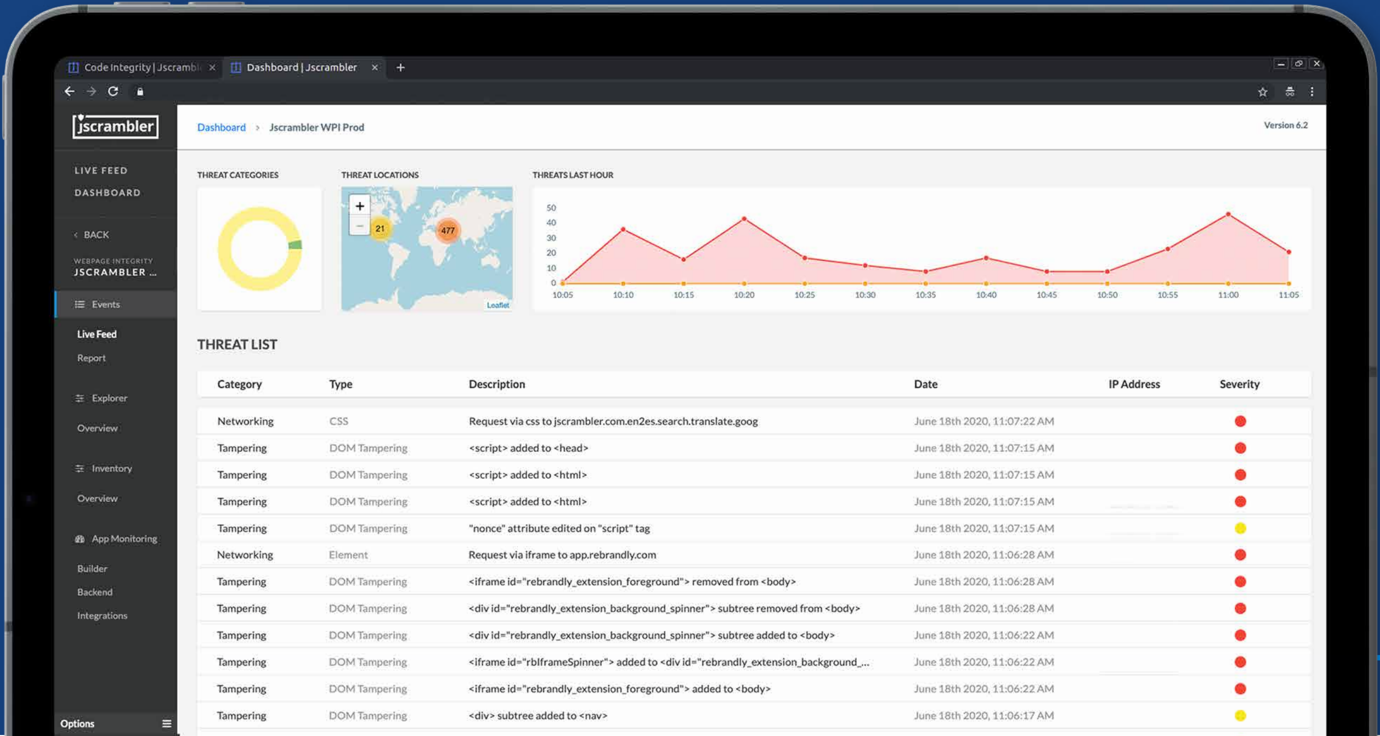
It is now widely known and reported that most "mainstream" security approaches that could be implemented to fight off Magecart often fail to mitigate today's more advanced web skimmers.

As such, the company put Jscrambler Webpage Integrity to the test in multiple different attack scenarios.

These dozens of tests included being able to detect the illegitimate addition/ modification/removal of content to the page (**DOM tampering**), the **poisoning of form events**, and the **exfiltration of data** to a drop server.

Jscrambler Webpage Integrity excelled at each and every one of these tests and provided the company with some of the best results of all the solutions that they tested.

> *"Jscrambler has merit in **passing every test** we threw at it with and being able to thwart the web skimming scenarios that we tested."*



THREAT LIST

Category	Type	Description	Date	IP Address	Severity
Networking	CSS	Request via css to jscrambler.com.en2es.search.translate.goog	June 18th 2020, 11:07:22 AM		●
Tampering	DOM Tampering	<script> added to <head>	June 18th 2020, 11:07:15 AM		●
Tampering	DOM Tampering	<script> added to <html>	June 18th 2020, 11:07:15 AM		●
Tampering	DOM Tampering	<script> added to <html>	June 18th 2020, 11:07:15 AM		●
Tampering	DOM Tampering	"nonce" attribute edited on "script" tag	June 18th 2020, 11:07:15 AM		●
Networking	Element	Request via iframe to app.rebrandly.com	June 18th 2020, 11:06:28 AM		●
Tampering	DOM Tampering	<iframe id="rebrandly_extension_foreground"> removed from <body>	June 18th 2020, 11:06:28 AM		●
Tampering	DOM Tampering	<div id="rebrandly_extension_background_spinner"> subtree removed from <body>	June 18th 2020, 11:06:28 AM		●
Tampering	DOM Tampering	<div id="rebrandly_extension_background_spinner"> subtree added to <body>	June 18th 2020, 11:06:22 AM		●
Tampering	DOM Tampering	<iframe id="rblframeSpinner"> added to <div id="rebrandly_extension_background_...	June 18th 2020, 11:06:22 AM		●
Tampering	DOM Tampering	<iframe id="rebrandly_extension_foreground"> added to <body>	June 18th 2020, 11:06:22 AM		●
Tampering	DOM Tampering	<div> subtree added to <nav>	June 18th 2020, 11:06:17 AM		●

Beyond testing the raw detection and mitigation capabilities of Jscrambler, the company also highlighted the **exceptional level of control** that the tool provides. Unlike most solutions out there, Jscrambler Webpage Integrity provides **fine-grained behavior control both based on high-level assumptions and user-defined rules.**

> *"The* ***level of control*** *and the ease of taking out the solution* ***with no impact*** *are added benefits."*

Performance was also tested to understand the potential impact that Jscrambler could have when added to the company's web pages. During these tests, our client found that **Jscrambler could easily be taken out with zero impact** and this flexibility was very valuable in their case.

After pondering all the factors, from the raw capabilities to the ease of integrating and maintaining the solution, the company concluded that **Jscrambler outperformed all other vendors.** As a result, they took the step forward of migrating from a PoC environment to a live production one.

*"This solution has met our requirements and **we're confident to deploy it in our live environment to help us prevent a Magecart breach**."*

RESULTS

Throughout every stage of the demanding testing process, **Jscrambler Webpage Integrity consistently received approval by several different teams and committees** within the company, from software development to architecture and legal.

By providing support from a dedicated engineering team, we were able to deliver in this very challenging timeframe.

We were successful in ensuring a **very smooth transition from PoC to a live environment**. During the 2-week learning process after the official kick-off, we were able to fine-tune Jscrambler and ensure it would be ready for the battlefield.

More than being able to deliver a timely, robust, and flexible solution to a major airline (and receiving additional confirmation that our solution is the best choice to mitigate Magecart attacks), we're thrilled to know that now **millions of travelers will benefit from protection against credit card skimmers** and enjoy a safer online experience.

jscrambler

CONTACT US

If you want to know more about how Jscrambler can help you mitigate Magecart attacks, don't hesitate to contact us

hello@jscrambler.com
+1 **650 999 0010**
jscrambler.com

Gartner®

Jscrambler is the leader in Client-Side Application Security
Recognized in Gartner's **Market Guide for Online Fraud Detection**
and in Gartner's **Market Guide for In-App Protection**

Trusted by the Fortune 500 and thousands of companies globally.