INSTART

Attack guide: How Magecart skimming attacks work

SOLUTION BRIEF

Contents

3 Introduction

4 Step 1: Gain access to your website

4 Step 2: Skim sensitive information from a form

5 Step 3: Send information back to their server

6 The best defense against Magecart skimming attacks

Introduction

Online data and credit card skimming attacks, like the Magecart British Airways breach, have become a serious concern for ecommerce websites and web applications around the world, especially as the market continues to shift towards online purchasing. Magecart and other card skimming attacks have increased in scale and scope over the last decade, proving that these types of attacks continue to be a persistent problem for online retailers.

The client-side browser is the front-door for consumer interactions—it's where customer data is displayed, entered, and then received by vendors. "Skimming" is a method used by attackers to capture sensitive information from online payment forms, such as name, passwords, and credit card numbers.

Data skimming attacks like Magecart typically follow a well-established pattern. They must achieve three things to be successful:

Step 1: Gain access to your website

There are typically two ways that attackers gain access to your website and place skimming code. They can either break into your infrastructure or your server and place the skimmer there. Or, they will go after one of your third-party vendors (especially if they are an easier target) and infect a third-party tag that will run a malicious script on your site when it is called in the browser.

The latter mode of attack has become increasingly common since most of today's websites often leverage third-party services and their code for data-capture and processing. Third-party scripts have the same access to resources and content that your own first-party code has and browsers provide only limited control of what third-party tags can access. So, any time third-party code loads on your website—your customers' data could be at risk.

It's also easier for cybercriminals to go undetected because third-party code does not run through internal infrastructure or security controls. That's why Magecart attackers were able to insert 22 lines of code on the British Airways website and steal 385,000 passengers' transaction, credit card, and personal details. It took 15 days before the breach was detected.

Step 2: Skim sensitive information from a form

So, what happens once attackers gain access to your website? There are lots of different ways that groups can capture data, but skimming code is always some sort of JavaScript that is listening for personal information and collecting it.

Here are three common ways skimming occurs on a website:

- **Keylogging**: Listening for all possible keydown events and then filters out everything except the keystrokes they want to capture (i.e. a 12-digit number followed by a date code).

- **Sniffing form submissions**: Listening for a click on a submit button or form submission event and then requesting all of the fields on the form.
- **Form jacking**: Swapping out a field in a real form with an infected field that sends the information to a bad source, or rendering a fake version of a form on top of the real form.

All three of these skimming scripts do the same thing, whether it's infecting first-party or third-party code. They basically ask the browser to share what consumers are typing into a page or a form. And once that JavaScript is loaded, it has access to all the same resources and all the same information as your first-party JavaScript.

Step 3: Send information back to their server

This is the simplest part of the whole process. Once hackers have gained access to your website and scraped the data they want—it's game over.

Attackers can send information to themselves in a variety of ways: POST, GET, or image requests that are being sent to proxied domains that are disguised as legitimate sounding domains. For example, when Newegg suffered a Magecart attack, the stolen information was being sent to a registered domain www.neweggstats.com, which blended in with the primary domain of the site.

The best defense against Magecart skimming attacks

In an ideal world, third-party services would use the same security protocols that you use (or better) in their infrastructure, but the unfortunate reality is that many third-parties do not. And even more concerning, Magecart attacks are not only common—they can happen again and again. In fact, one in five online stores that have been infected get reinfected again within 10 days.

So, what can you do to protect your customers?

The best defense against Magecart attacks is preventing access. Instart Tag Control intercepts all of the API calls your website makes to the browser and blocks access to sensitive data you have not previously authorized. This prevents any malicious script, or any non-critical third-party script, from gaining access to any information your customers enter on your website. website.

You can allow scripts on a page without fully understanding how they work as long as you ensure that the browser won't provide sensitive information. The point is that a skimmer can't steal what it can't see, and preventing access is the best way to protect your website and your customers from data skimming attacks.

Learn more about how to prevent Magecart skimming attacks and minimize the risk of browser attacks.

REQUEST A DEMO