Digital skimmers: Keeping card details safe online

By Trend Micro (words)

Published: 2019-08-07 · Archived: 2026-04-05 21:43:39 UTC

"A few weeks ago, British Airways was hit by the largest ever regulatory fine of its kind, after global customers visiting its website had their card data stolen. The $228m penalty levied by the UK's privacy watchdognews article reflects the seriousness of the attack and the carrier's failure to protect its customer's personal and financial information. However, this incident has repercussions way beyond the UK airline and its customers. It's part of a new wave of attacks designed to implant "digital skimming" code on e-commerce sites, in order to siphon off your card details as they are entered in to pay for goods.

Although tens of thousands of websites have been caught out in this way, there are things you can do to stay safe —most notably by running Trend Micro Security. But first, here's more on what you need to know.

The story so far

Data breaches are so often in the news headlines today, that you could be forgiven for becoming a little desensitized. From retailers like Target and Home Depot to government breaches at agencies including the Office of Personnel Management (OPM), and from financial organizations like Equifaxnews article to tech giants like Yahoonews article, billions of our personal records have been stolen by cyber-thieves over the past few years.

Yet in all of these cases, there has been little the customer could do about it. That's because the hackers target the organization directly. They find ways to bypass its security controls and sneak inside the company networks to find what they're looking for: usually databases full of customer data.

A new type of data breach

However, these new digital skimming attacks are different. In what way? They involve a hacker deploying malicious code known as Magecart to an organization's website. This code is typically designed to stay hidden, under the radar of the company. And it has a very specific purpose: to steal customer card details as they are entered into the site during payment. In short, it's the digital equivalent of those physical skimming devices that criminals insert into ATMs to steal card data as it's entered: it's highly effective and happens completely without the knowledge of the cardholder.

By using this method, the hackers get access to the full card details, which have a higher resale value on the cybercrime black market. The problem (for them) with the more traditional types of attack targeting back-end databases, is that these organizations may store card data encrypted, or else minus the crucial CVV/CV2 code. Magecart attacks get around that.

What sites are at risk?

Indeed, the Magecart attackers have proven over the past year that no website is safe from skimming attacks. Whether it's a big-name e-commerce brand like Newegg, a national airline, a global ticketing site (Ticketmaster), or even online campus stores serving nearly 200 universities in the US and Canada–as long as they accept online payments, they're at risk.

Magecart is so effective that multiple groups are said to be using the code, a piece of malicious JavaScript, to infect websites around the world. And they're developing new tools and tactics all the time to improve their monetization. These include:

- Infecting third-party companies which supply code to other sites (e.g., those that provide online ad services). Thus, with just one attack, the hackers can get their Magecart code onto potentially thousands of payment pages.
- Using automated tools to scan the internet for companies that may be running unsecured servers, which they can then infect with Magecart. Some 17,000 sites were recently compromised in this way. In a separate attack, 962 online stores were hit in just 24 hoursnews article.
- Developing new skimming code which is usable across as many different payment pages as possible. The record is 57 different payment gatewaysnews article, which makes the hackers' job much easier as they can launch attack campaigns across the globe with the same tools

All this is bad news for online shoppers. So how do you know that the site you're entering card data into is safe?

What can you do to stay safe?

Unfortunately, there's nothing obvious that differentiates a website infected with Magecart from any other site. It will look completely normal and will allow you to pay in the usual manner. The only difference is that, in the background, a tiny piece of code will be stealing your data and transferring it to the hackers. So what can you do to protect yourself?

- You could try to avoid smaller sites that may not have the same level of security as larger ones. However, as we've seen, Magecart has hit big-name brands as well as less well-known companies.
- Another option would be to use a browser plug-in like NoScript for Firefox that prevents JavaScript loading from other untrusted sites – although this won't prevent you getting potentially stung if the well-known and trusted site you're on is compromised
- Payment systems like Apple Pay and Google Pay can offer more protection. They use a one-time generated series of numbers for each transaction, so that if attackers get their hands on it, they won't be able to use it in the future.
- It goes without saying that you should keep a close eye on your card statements/bank account at all times – watching out even for small amounts that hackers may be making to test if your card is still active.
- However, the most effective way to stay safe is to use Trend Micro Security.

How Trend Micro can help

Trend Micro Security features two key mechanisms to help stop Magecart attacks:

- It can detect whether the website you want to visit has been injected with skimming code, and block you from visiting the URL (via web reputation), as well as from going to malicious domains the skimming code has access to.
- It uses a combination of techniques (via its Advanced Threat Scanning Engine and TrendX-File machine learning) to detect whether the malicious JavaScript code has landed on your local drive and is ready to run in your browser – and then blocks it. This can spot both Magecart and similar digital skimming code.

Read our Security Intelligence Blog for more technical details on Magecart. Then go to our Security Products Overviewproducts to get Trend Micro Security. "" "

Source: https://blog.trendmicro.com/trendlabs-security-intelligence/home-depot-breach-linked-to-blackpos-malware/