UNITED STATES

FEATURE

What is Magecart? How this hacker group steals payment card data

Hacking groups that make up Magecart are effective and persistent at stealing customer and payment card data through skimmers. Here's how they work and what you can do to mitigate the risk.

By David Strom

CSO |

DEC 23, 2021 2:00 AM PST

Magecart definition

Magecart is a consortium of malicious hacker groups who target online shopping cart systems, usually the Magento system, to steal customer payment card information. This is known as a supply chain attack. The idea behind these attacks is to compromise a third-party piece of software from a VAR or systems integrator or infect an industrial process unbeknownst to IT.

[How much does a data breach cost? Here's where the money goes. | Get the latest from CSO by signing up for our newsletters.]

Shopping carts are attractive targets because they collect payment information from customers: if your malware can tap into this data stream, you have a ready-made card collection tool. Almost all ecommerce sites that use shopping carts don't properly vet the code that is used with these third-party pieces — a recipe for a ready-made hack.

Magecart is known to have been active since 2016 and is quite prolific. In its analysis of a Magecart breach in 2018, RiskIQ said it was seeing hourly alerts for websites being compromised by its skimmer code. That earned Magecart a spot on Wired magazine's list of Most Dangerous People On The Internet In 2018.

Most recently, Magecart was blamed for planting payment card skimming scripts at MyPillow.com and AmeriSleep.com. Other Magecart attacks include:

- Ticketmaster's UK operations (January 2018)
- British Airways (August 2018)
- NewEgg electronics retailer (September 2018)
- Shopper Approved (September 2018)
- Topps sports collectable website (November 2018)
- Atlanta Hawks fan merchandise online store (April 2019)
- Hundreds of college campus bookstores (April 2019)
- Forbes magazine subscribers (May 2019)
- NutriBullet (February 2020)
- Wordpress/WooCommerce attacks (May 2020)
- Favicon code injection attack (May 2021)
- Targeting reCAPTCHA (August 2021)

How Magecart works

Typically, the Magecart hacker substitutes a piece of Javascript code, either by altering the Magento source or by redirecting the shopping cart using an injection to a website that hosts the malware. Researchers have identified nearly 40 different code-injection exploits. The only way to detect this is to compare the entire ecommerce code stack line-by-line and see what has changed.

One clever way for attackers to host their malware (and not sadly limited to just Magecart attacks) is to upload their code to an unused GitHub project. The criminals try to take ownership of the project and then publish a "new" version of the code that contains the malware. This has a direct benefit of quickly getting malware in active use across thousands of websites. Security tools might not scan code from GitHub, so criminals can hide in plain sight and get away with the compromised project.

In at least the British Airways hack, Magecart tailored the attack to the specific system, according to the RiskIQ report. “This particular skimmer is very much attuned to how British Airways’ payment page is set up, which tells us that the attackers carefully considered how to target this site instead of blindly injecting the regular Magecart skimmer,” the report’s authors wrote.

Magecart showed that it is willing to evolve further with its MyPillow website attack. MyPillow discovered and removed their original malware quickly, but Magecart retained access to the site according to another report from RiskIQ. A second attack changed tactics. "The attackers played a brilliant game the second time they placed a skimmer on the MyPillow website, adding a new script tag for LiveChat that matched a script tag usually inserted by the LiveChat scripts," the RiskIQ researchers said. "The Magecart attackers went even further by proxying the standard script returned from the real LiveChat service and appended the skimmer code below it."

Three of the most recent Magecart skimmers target the open-source WooCommerce plugin for Wordpress, which is popular among online retailers. According to RiskIQ, the skimmers are:

- WooTheme: This skimmer is simple and easy to use. Its code is typically obfuscated to avoid detection.
- Slect: This skimmer gets its name from a misspelling of the word "select" that helped researchers discover it. It's another simple skimmer and believed to be a variation of the Grelos skimmer.
- Gateway: This skimmer uses multiple layers and steps to obfuscate its processes and avoid detection.

How Magecart has evolved

Analysts from RiskIQ and Flashpoint combined forces last year and published a report that dissects Magecart’s code and its methods of compromise. They continue to track at least six different hacking groups that are actively developing versions of the malware, adding various enhancements and trickery. Each group has its own distinctive code signature and methods so that researchers can classify them. That research has found a

series of improvements in this malware family.

- **Movement beyond Magento with new plug-ins.** The attack on the Shopper Approved website was significant. Most of the Magecart efforts have involved compromises to the Magento shopping cart. This one leveraged the vendor's customer scoring plug-in to rate various websites, which then displays a badge of honor. Researchers found that the malware was eventually deployed across more than 7,000 ecommerce sites. Once researchers identified the source of the infection, Shopper Approved moved quickly to remove the malware.

- **Using ad servers**. A second direction is still attacking shopping carts, but using a new method to infect advertising banners, so that ad servers will place Magecart code into a webserver. Once a user views the ad in a browser, the code is downloaded to their computer. The malware code can also be hosted by a compromised server.

- **Using more targeted and more elaborate attacks.** This shows a movement away from spraying malware widely and spending time with potential victims to study their coding and infrastructure. This is what happened with British Airways, when hackers were able to take advantage of the logic flow of their internal applications. Researchers were able to track 22 lines of code of an infected script that dealt with the British Airways baggage claim information page and came to the conclusion that they were seeing a XSS attack that compromised the British Airways' own servers. Magecart was able to steal data that wasn't stored on the British Airways-owned servers. They found the modifications because of an odd circumstance: The last time any of the baggage scripts had been modified prior to the breach was in December 2012.

- **Dual exfiltration and payment form injection.** In a September 2021 report, security firm RiskIQ documented the past and current activities of a Magecart group it calls Group 7 that has been operating since 2018. The group started out with a skimmer dubbed MakeFrame skimmer that they tested and constantly improved using victims' websites. This skimmer stood out because it used dual data exfiltration paths to both compromised sites and actor-controlled servers.
  The researchers have managed to link more recent attacks with a skimmer dubbed

Bom to Magecart Group 7. The new skimmer, which has been in use since last year and has been documented by other security firms as well, seems to be a predecessor to MakeFrame and shares similarities with it. Like MakeFrame, Bom uses dual exfiltration paths and even injects its own rogue payment forms into the compromised sites.

Supply chain attack mitigation and prevention methods

While hackers can use sophisticated techniques to plant and hide skimmers, website owners with limited resources should not despair. There are free website scanners online that can help spot suspicious connections opened by scripts like Magecart and browser developer tools that can help analyze their contents.

Researchers from Trustwave SpiderLabs published a guide with detailed information on how such investigations can be performed as well as a list of useful tools specifically designed for detecting and fixing Magecart infections. Web technologies like Content Security Policy (CSP) and Sub Resource Integrity (SRI) can also be used to protect website visitors, as they can be used to restrict where scripts are loaded from and to protect their integrity.

These best practices will help harden your networks and try to stop Magecart and other supply chain attacks.

- Think about first identifying all your third-party ecommerce and online advertising vendors. You could require them to do self-assessments of their code or other audits.
- Implement subresource integrity so that modified scripts are not loaded without your permission. This will require a concerted education of your devops teams and a thorough code review to track down these scripts.
- Host as many of your third-party scripts on your own servers as you can rather than on any of your suppliers' servers. That is more easily said than done, given that the average ecommerce webpage has dozens of third-party sources.

- Vet your endpoint protection provider and determine if they can stop Magecart and other third-party compromise attacks.
- Make sure your cyber insurance covers this type of compromise.
- Review and revise your security policies to include the same treatment of your contractors and suppliers, as if they are full-time employees working directly for your corporation. This is one reason why the supply chain attacks work, because the hackers are counting on less-than-stellar security applying to these workers.
- If you are using WordPress, make sure you update to v.5.2, which specifically screens and tries to prevent supply chain attacks being used across their plug-in library.

Editor's note: This article, originally published on June 6, 2019, has been updated with new information on data exfiltration and payment form injection capabilities.Information on new Magecart skimmers has also been added.

More on hacks and breaches:

- **The 16 biggest data breaches of the 21st century**
- **The Target data breach settlement sets a low bar for industry security standards**
- **Two years after the OPM data breach: What government agencies must do now**
- **Anthem: How does a breach like this happen?**
- **Lessons from the Heartland Payment Systems data breach, redux**

Next read this

- *The 10 most powerful cybersecurity companies*
- *7 hot cybersecurity trends (and 2 going cold)*
- *The Apache Log4j vulnerabilities: A timeline*
- *Using the NIST Cybersecurity Framework to address organizational risk*
- *11 penetration testing tools the pros use*