RISKIQ®

Magecart: The State of a Growing Threat

Research by
Jordan Herman and
Yonathan Klijnsma

Table of Contents

Introduction

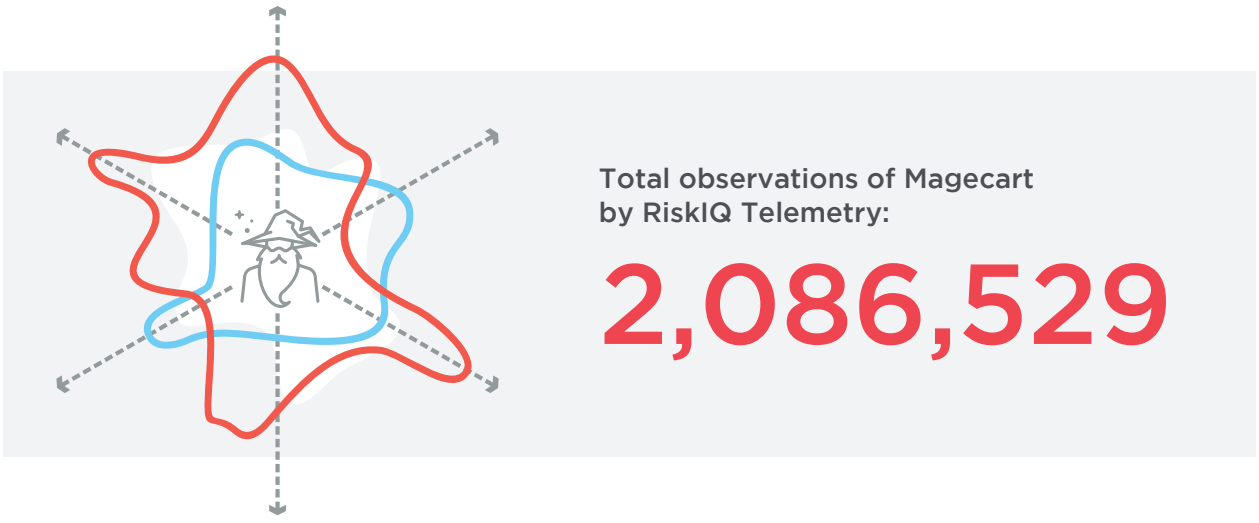
Magecart, a rapidly growing cybercrime syndicate comprised of dozens of subgroups that specialize in cyberattacks involving digital credit card theft by skimming online payment forms, is fundamentally changing the way we view browser security. A global phenomenon, Magecart is threatening the ability of consumers worldwide to shop online safely by stealthily intercepting their credit card data without the consumer or website owner's knowledge.

Although it's just now getting attention, Magecart has been active for nearly ten years—RiskIQ's earliest Magecart observation occurred on August 8th, 2010. Magecart works by operatives gaining access to websites either directly or via third-party services in supply-chain attacks and injecting malicious JavaScript that steals the data shoppers enter into online payment forms, typically on checkout pages.

RiskIQ's earliest observed Magecart incident: August 8th, 2010

RiskIQ's global discovery platform gathers internet-wide telemetry that enables us to view websites as Magecart actors do; a unique perspective that provides unmatched visibility into this surging threat. In this valuable report, we share this telemetry data, which yields critical insight into the state of Magecart, whose skimmers have appeared over two million times, and directly breached over 18,000 hosts.

Total observations of Magecart by RiskIQ Telemetry: 2,086,529



Supply-Chain Attacks

Supply chain attacks target third-parties that supply code to websites. Suppliers can include vendors that integrate with sites to add or improve site functionality or cloud resources from which websites pull code, such as Amazon S3 Buckets. These third-parties integrate with thousands of websites, so when one supplier is compromised, Magecart has effectively breached thousands of sites at once.

Supply chain attacks are responsible for the largest spikes in RiskIQ Magecart detections

The most substantial spike in Magecart instances occurred on June 27th, 2018, when Ticketmaster made public they had been compromised by actors stealing payment information from the company's various websites. RiskIQ discovered the breach was a result of Magecart operatives placing skimmers on Ticketmaster checkout pages through the compromise of third-party functionality suppliers.

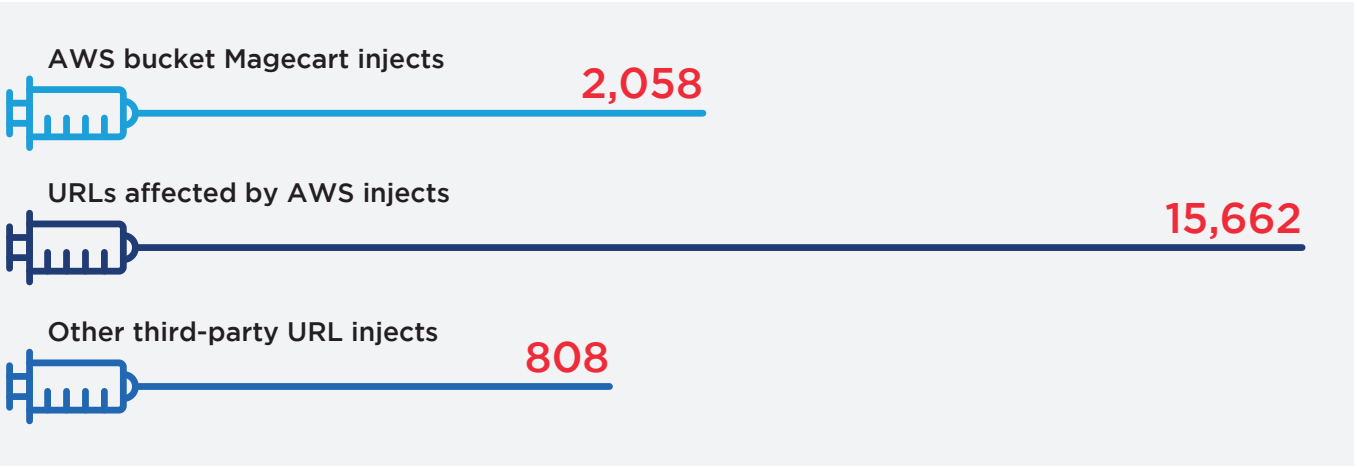
The Magecart group responsible, identified by RiskIQ as Group 5, attacked a large swath of third-parties, such as website analytics providers SociaPlus and Inbenta, getting access to over 800 e-commerce sites in the process and accessing an enormous victim pool.

S3 Mayhem

The second-largest spike in Magecart detections occurred in July when RiskIQ announced that the scale of a mass compromise of third-party web suppliers by a Magecart group was much larger than previously reported. The actors behind these compromises automated the process of compromising websites with skimmers by actively scanning for misconfigured Amazon S3 buckets, managing to compromise a vast collection of S3 buckets to impact well over 17,000 domains. This list includes websites in the top 2,000 of Alexa rankings.

RiskIQ has been monitoring the compromise of S3 buckets since the beginning of the campaign, which started in early April 2019.

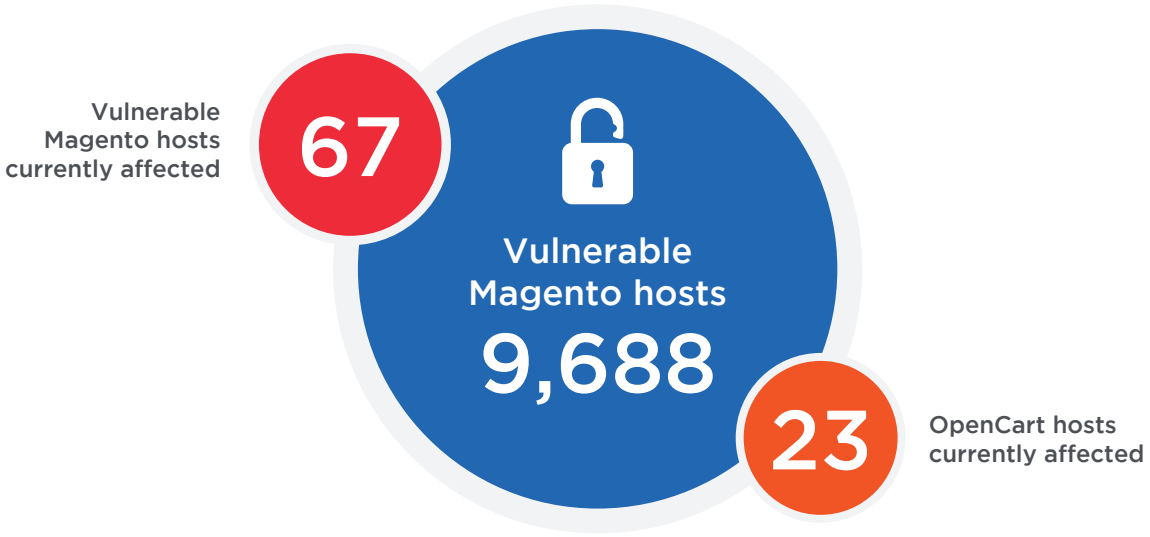
A Snapshot of Current Magecart AWS Injects



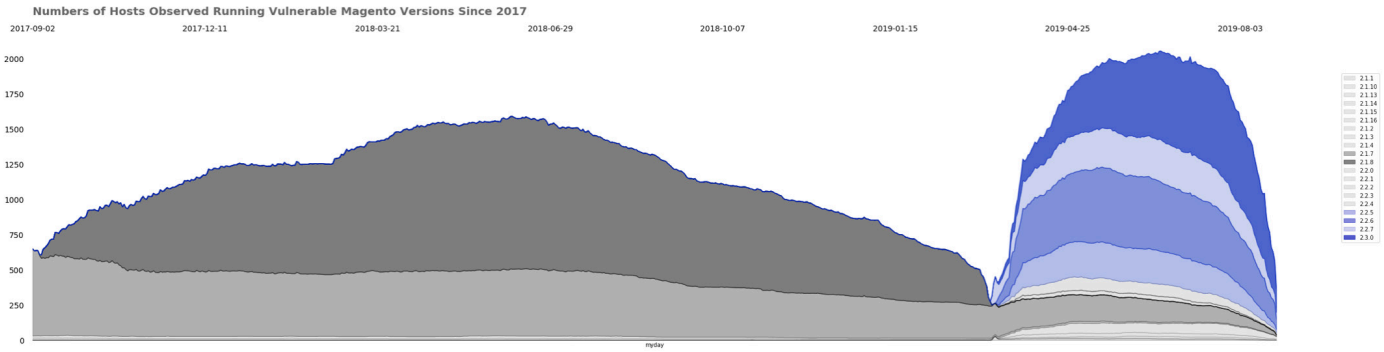
Magento Madness

Magecart will always be intrinsically connected to one program in particular: Magento. When we first wrote about Magecart back in 2016, Magento was the primary third-party shopping software targeted, inspiring the now-infamous name, which is a combination of “Magento" and "shopping cart."

To this day, third-party shopping platforms such as Magento and OpenCart, which fuel an enormous portion of e-commerce, are the lifeblood of many Magecart groups.



As you can see in the graph below, when a vulnerable version of Magento is released, the victim pool for Magecart grows exponentially. When a patch is released, that pool shrinks starkly.



Magecart Meets Malvertising

RiskIQ researchers recently discovered that Magecart groups are also compromising creative ad script tags to leverage digital ad networks to generate traffic to their skimmers on thousands of sites at once. Recent RiskIQ research shows that Magecart now makes up 17% of all malicious advertisements seen by RiskIQ.

Magecart Overstays its Welcome

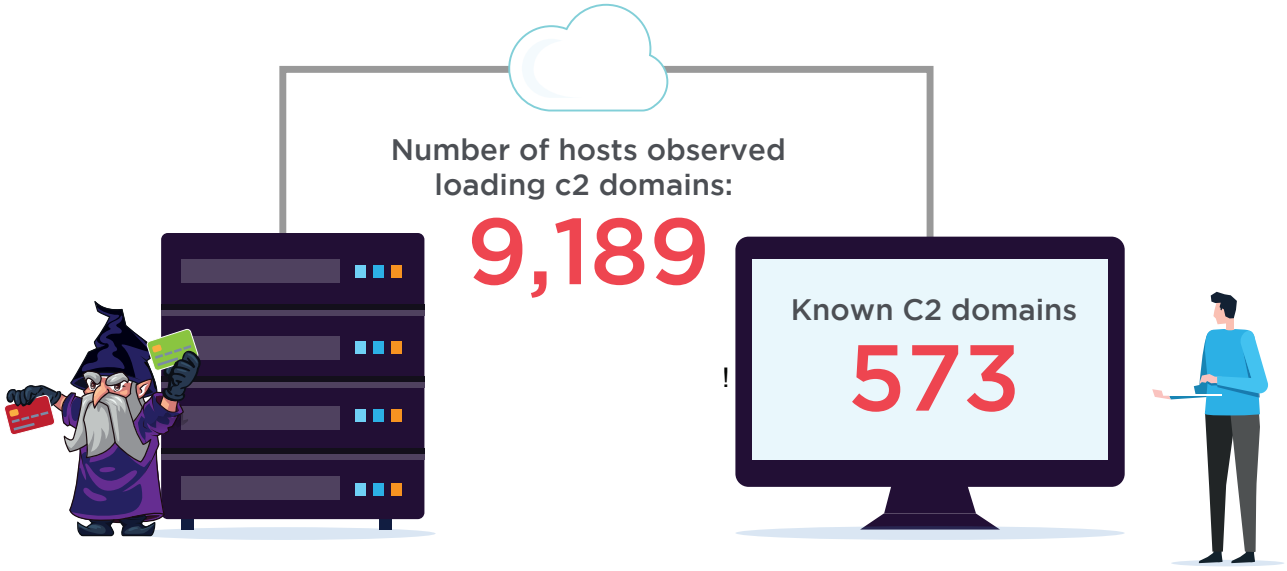
Magecart takes advantage of online businesses' general lack of visibility into their web-facing attack surfaces. In many cases, the victims have no idea the JavaScript on their site has been changed, allowing the malicious code to exist there indefinitely. In the case of supply-chain attacks, it's common a victim does not know that the compromised third-party JavaScript on their site is dangerous — or that they're even running the code from the breached supplier.

While a magecart skimmer is on a website, any visitor is susceptible to having their data intercepted. The total traffic to a compromised website over the course of the breach can be a proxy for the number of victims.

22 Days
Average length of a Magecart breach

Magecart Infrastructure

Magecart is now so ubiquitous that its infrastructure is flooding the internet. RiskIQ has identified dozens of known groups, and markets for skimmers and pre-breached websites are making the barriers to entry extremely low for new Magecart actors.



Magecart Trash is another Threat Actor's Treasure

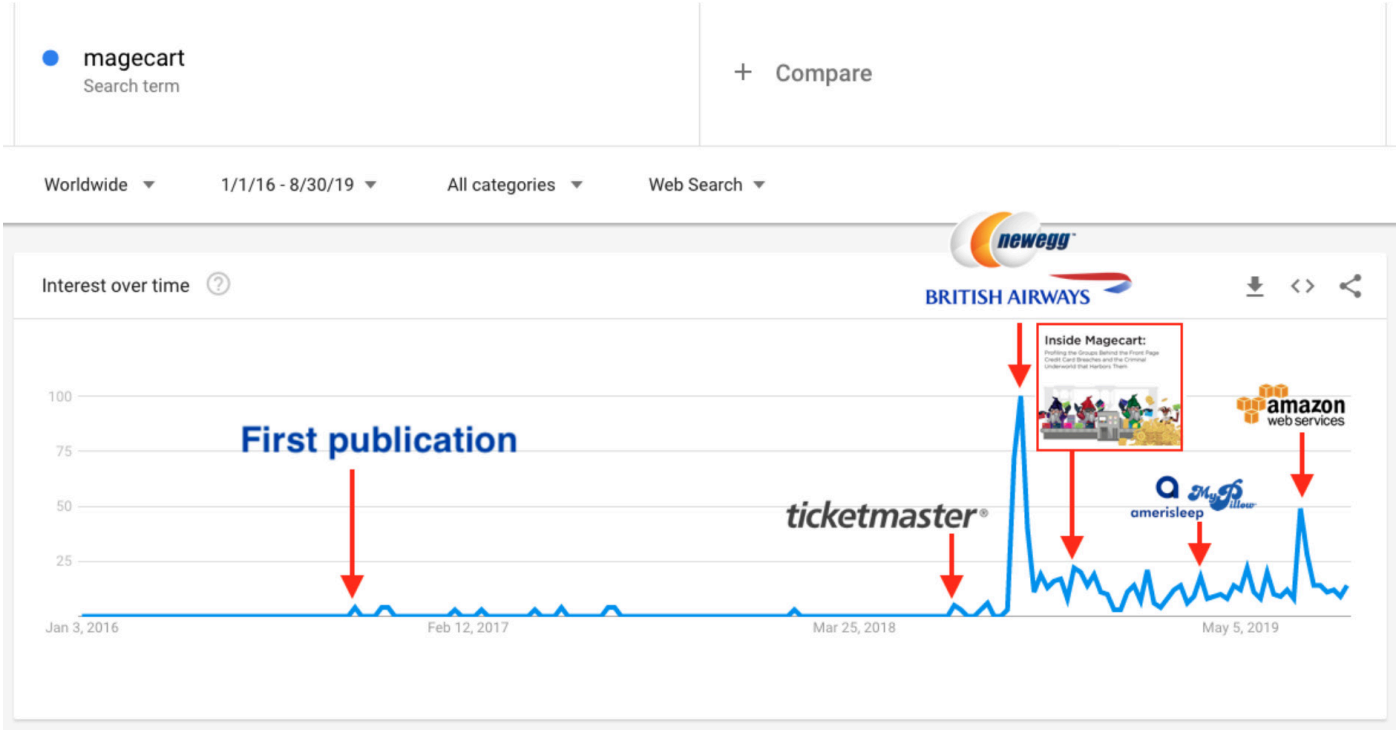
Because Magecart skimmers stay on websites for so long, often indefinitely, they can be beneficial to threat actors even when used second-hand.

Large portions of malicious Magecart domains have been taken up for sinkholing by various parties. However, some of them are kicked offline by the registrar, put on hold and eventually released back into a pool of available domains. RiskIQ researchers have noticed bad guys taking advantage of these domains coming back up for sale and buying them to continue skimming, or for other purposes, such as monetizing traffic through advertising or even serving malware.

Magecart is a Business Problem

Businesses need a continued focus on visibility into their internet-facing attack surfaces, as well as increased scrutiny of the third-party services used in their web applications. Magecart's recent ravages have shown that current investments in securing corporate infrastructure are ineffective in dealing with browser-based attacks. Companies will continue to be overwhelmed by the scale and tenacity of these kinds of groups, especially as attacks launch from outside the firewall and the data theft occurs in the user's browser. This is well outside the scope of modern network monitoring tools, requiring a new kind of monitoring that looks that things from the perspective of the end-user

A Magecart Timeline



RISKIQ

RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. RiskIQ's platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

Learn how RiskIQ PassiveTotal could help protect your digital presence by scheduling a demo today.

22 Battery Street, 10th Floor
San Francisco, CA. 94011

sales@riskiq.net RiskIQ.com

1 888.415.4447 @RiskIQ