reflectiz

Who are we?
We're a cyber-security company that helps organizations mitigate security and privacy risks resulting from third-party components installed in their websites

Visit our website:
www.reflectiz.com

The Magecart Hacking Groups - How They Are Expanding Their Limits Beyond the "Regular" E-Commerce Websites

Magecart, the notorious e-commerce hacking group, has lately started targeting many other forms of online services and businesses.

The adversaries have developed sophisticated tools and techniques, and are constantly evolving new and innovative ways to target business enterprises.

Magecart – The Notorious Skimming Groups

Magecart today is a well-known name in the Cybersecurity community, and most of the web security professionals, security analysts must have heard of this cybercrime gang. Magecart's main methodology is to steal sensitive information from customers that commonly use e-commerce websites by exploiting third-party applications vulnerabilities on these websites.

Magecart has been active since 2015 and has attacked tens of thousands of e-commerce and B2C websites since then, started mostly with Magento, an open-source e-commerce platform, hence their name.

reflectiz

Who are we?

We're a cyber-security company that helps organizations mitigate security and privacy risks resulting from third-party components installed in their websites

Visit our website:
www.reflectiz.com

Who's Behind Magecart?

Magecart figures among the 'Most Dangerous People on the Internet in 2018' listed out by WIRED. And for "good" reasons.

Over the past couple of years, the Magecart threat, as a whole, have become more common in many aspects. The attacking groups behind it, present more sophisticated hacking techniques and the boundaries of Magento targets are expanded into new platforms. As a result, websites are more exposed, not only in terms of severity, but also in terms of the rising number Magecart groups potential targets. The fact that Magecart attacks are escalating dramatically, is also related to the increasing popularity amongst hackers and to its tool's availability on the Darknet.

Today there are at least 12 known Magecart groups. But who are the Magecart people? And what makes them dangerous? Magecart is not an individual or a single group of people. In a broader sense, Magecart refers to the form of supply-chain attacks in which hackers infiltrate e-commerce and other websites by exploiting third-party apps that are stored local or remotely, to steal sensitive information from unsuspecting users at the transactions and checkouts stages.

These groups are known to have attacked tens of thousands of e-commerce websites to date. Some of the most famous examples are Ticketmaster, British Airways, and Newegg, but they are not alone. All these organizations have one thing in common, and that is they were all hit by Magecart. These attacks create financial losses, reputational damage and legal and regulatory issues. The latest $230 Million fine which was issued to British Airways by the UK privacy watchdog, the ICO, shows that Magecart breaches are under the direct accountability of the breached organization.

How the Typical Magecart Attack Works

There are two stages which are most evident in Magecart hacking attack sequence:

Infiltration of your website - Generally, using two methods to place the malicious code on your website. One is to forcibly break into your website and place the code on your server. A better way is to target your third-party vendors. By infecting a third-party tag, it makes a malicious script run on your website when it is called on the browser. Additional information about third-party risks on websites can be found on one of our August 2019 blog post.

reflectiz

Who are we?

We're a cyber-security company that helps organizations mitigate security and privacy risks resulting from third-party components installed in their websites

Skim vital information from a form - There are many ways to capture data, but skimming is the most prevalent method. The skimming code is a JavaScript code that searches for and collects personal information, commonly known as hooking or keylogging. One way is to monitor all keyboard presses on a sensitive page. The other way to do it is to pick up information from specific parts of a form such as credit card number and CVV number fields, also known as form-jacking.

Usually, the cybercriminals conceal their malicious code behind other innocuous-looking codes to avoid identification, undetected by a regular static code testing. Once obtaining the requisite information, it is not hard to relay it to their server. The attackers can send the data wherever they want, without any real detection tools in their way.

Form-jacking is one of the most common techniques used by online skimming groups such as Magecart.

Who Does Magecart Target?

For the Magecart attacking groups, e-commerce websites are the most convenient targets, mainly because of their vulnerabilities and comparatively inefficient security controls in place. But if you think that these groups only targets "regular" e-commerce retailers, you are sadly mistaken. Magecart attackers have gone forward to target all sorts of service providers wherewith people use credit cards for making payments and transactions.

Visit our website:
www.reflectiz.com

reflectiz

Who are we?

We're a cyber-security company that helps organizations mitigate security and privacy risks resulting from third-party components installed in their websites

Visit our website:
www.reflectiz.com

The French advertising network - Adverline case, demonstrates how Magecart "crossed the line" of traditional e-commerce websites. It's not just an example, but also a frightening reminder, of how creative these skimming groups can be.

A quick overview: Two recent attacks that show how varied the Magecart cyber-threat is

National Baseball Hall of Fame

In this instance the Magecart attackers used a fake Google Analytics script to hack into the website of National Baseball Hall of Fame. The attackers included a malicious Magecart script to steal credit card information from people who purchased items on the site. This malicious script affected the website between November 15, 2018, and May 14, 2019. The breach was detected on June 18, 2019, but the damage had been done already. The breach affected only those customers who purchased merchandise from the website and not in the museum.

A crucial point to note here is that the breach was undetected for seven months! Now, that is quite an extended period. On investigation, it became evident that the associated script looked like a Google Analytics script. The domain indicated that it belonged to Google, but it was traced to an IP address in Lithuania.

Poker Tracker

Gambling websites are also prime targets. One such hack involved the compromising of the Poker Tracker website to steal payment information from customers. Poker Tracker is software that helps gamblers to improve their chances of winning by analyzing statistics compiled from the opponent's moves.

On August 8, 2019, Anti-malware blocked Poker Tracker from connecting to domains renowned for hosting credit card skimmers. Investigations revealed a Magecart type attack due to the injecting of a malicious code that caused the software to load it at every launch. Therefore, every payment made through the application would be compromised.

Tough Competition Among Magecart Groups

With more companies adopting the online route, there is intense competition among cyber-criminals like Magecart. According to ZDNet, There have been instances of one Magecart group attacking and sabotaging the efforts of a rival Magecart gang.

In one example, Group 9, a relatively recent entrant to the Magecart gang attacked another Magecart group, Group 3, primarily active in South America. Group 9 added a unique code to their card skimmer that sought information from domains associated with Group 3's operations. On identifying these domains, it came to be known that Group 9 was not only stealing data from Group 3, but also altering the data collected by Group 3, thereby rendering them useless. Therefore, the buyers of such spurious credit cards will find that the card does not work. Consequently, it affects the credibility of the seller. This is one of the best examples of a thief stealing information from the other.

What the Future Holds for Magecart?

With people preferring online payments more to cash, Magecart attacks will keep on increasing, that too in new ways. They already hide their malicious codes behind innocuous-looking codes to escape detection. We have seen how dangerous Magecart can get. Therefore, it is no surprise Magecart ranks amongst the eight 'Most Dangerous People' on the Internet today.

From a more technical perspective, we see growing number of security experts and researchers that point out how difficult it is to stop Magecart threats. A recent Security Boulevard blog post demonstrates it, naming Magecart as one of the most sophisticated cyber-attacks that are growing in 2019 and are difficult to stop.

The bottom line is clear and simple: the Magecart threat is escalating, it is becoming more sophisticated and challenging for security teams. These risks are extremely dangerous because they become harder to detect, as they are indirect and part of your supply-chain.

As someone rightly said "There are two types of companies, those that have been hacked, and those who don't know they have been hacked."

reflectiz

Who are we?

We're a cyber-security company that helps organizations mitigate security and privacy risks resulting from third-party components installed in their websites

Visit our website:
www.reflectiz.com