NATIONAL CAPITAL REGION
THREAT INTELLIGENCE CONSORTIUM

Cyber Center

Cyber Advisory

7 May 2019 | Product No. 2019-05-013
NTIC SIN No. 2.5 | HSEC SIN No.1.8.2

Magecart: A Rapidly Growing Threat to Ecommerce Websites

The NTIC Cyber Center assesses with high confidence that profit-motivated cyber threat actors will increasingly leverage Magecart attacks against vulnerable ecommerce sites to steal payment card data and sell it through online black markets or use it to conduct fraudulent financial transactions. Chip-enabled payment cards and modern card-present payment processing systems have significantly deterred financial fraud and payment card data theft at physical retail locations.[i] As a result, cyber threat actors are increasingly turning to ecommerce platforms to skim customer payment data. Magecart attacks have historically targeted organizations across multiple sectors and industries; thus, any organization that facilitates online payments using ecommerce platforms is at risk of compromise and potential financial liability resulting from associated data breaches.

Magecart is an umbrella term that encompasses prevalent profit-motivated hacking campaigns targeting vulnerable ecommerce websites, the malicious code used in these campaigns, and the criminal groups conducting this activity. First perpetrated in 2014[ii], Magecart attacks targeted ecommerce websites built using Magento, an open-source ecommerce platform written in the PHP programming language. The first Magecart campaigns compromised Magento sites by employing brute-force attacks or using stolen login credentials to gain initial access to targeted websites. Over time, Magecart tactics, techniques, and procedures (TTPs) evolved to include targeting third-party plugins and conducting scans to identify vulnerable websites. Magecart threat groups have also expanded their range of targets to include ecommerce sites built on other platforms including OpenCart, OSCommerce[iii], and PrismWeb.[iv] The number of groups conducting these attacks has also increased, with some experts estimating that there are at least seven currently active groups that have collectively compromised the ecommerce platforms of more than 110,000 merchants to date.[v] Magecart attacks facilitate the exfiltration of data such as names, addresses, payment card numbers, card verification value (CVV) codes, expiration dates, and other information from forms on compromised websites.

Magecart attacks present an ever-increasing challenge to businesses, website administrators, and customers. The attack methods are difficult to detect, making them an attractive choice for cyber threat actors seeking to target payment card information on ecommerce platforms. Additionally, Magecart threat groups are often quick to identify and exploit unpatched zero-day vulnerabilities. The demand for stolen payment card data appears to be growing as well, as security researchers note a reduction in supply of payment card data and an increase in the average price per card on underground marketplaces, likely a result of merchants' adoption of more secure chip-enabled payment technology to reduce fraud associated with card-present transactions.[vi]

Recent Magecart Incidents

- In June 2018, cyber actors targeted TicketMaster via a website plugin provided by the third-party vendor Inbenta. After gaining access to Inbenta's JavaScript code, the cyber actors completely replaced the script with data-skimming code and used it to steal the personal and payment data of over 40,000 customers.[vii]

- From August to September 2018, cyber actors compromised British Airways customer information by altering the Modernizr JavaScript library hosted on the company's baggage claim information webpage. The modified code directed browsers to capture form data and send it to a server hosted at baways[.]com, a fraudulent website registered by the actors to appear legitimate. This attack resulted in the theft of the payment and personal information of approximately 380,000 customers.[viii]

- In August 2018, online electronics retailer Newegg suffered a Magecart breach after cyber threat actors injected malicious code into the website's payment processing page. The cyber threat actors registered and used the malicious site neweggstats[.]com as a drop server to seamlessly blend into Newegg's checkout infrastructure. This attack may have facilitated the theft of personal and payment card information belonging to millions of customers.[ix]

- In April 2019, cyber threat actors used obfuscated JavaScript code to skim customer payment and personal information from the ecommerce website of the Atlanta Hawks NBA basketball team.[x] The code logged keystrokes and exfiltrated data to a drop server, allowing attackers to pilfer an unknown number of victim names, addresses, and payment card numbers.

- In April 2019, cyber actors breached the Australian ecommerce website of clothing company Puma through either an unpatched vulnerability or a breached third-party component.[xi] Cyber actors perpetrated the attack using an advanced skimming technique involving polymorphic code compatible with numerous local currency payment systems.[xii]

- In April 2019, cybersecurity firm Trend Micro began observing Magecart attacks employed against multiple campus store websites and determined the attackers had compromised PrismWeb, an ecommerce platform designed for college stores. The attackers had injected a malicious script into PrismWeb's shared JavaScript libraries which, in turn, impacted 201 online campus stores. [xiii] The amount of stolen information is currently unknown.

How Magecart Attacks Work

1. Cyber actors use stolen or weak credentials or compromise known or zero-day vulnerabilities to obtain write access to a web application's source code. Recent TTPs have evolved to target Content Delivery Networks (CDNs) and compromise servers that host plugin or extension JavaScript code, enabling attackers to target all websites enabled with the same vulnerable third-party resources at once.

2. Cyber actors may leverage techniques such as PHP Object Injection (POI), SQL Injection (SQLi), Cross-Site Scripting (XSS), Remote Code Execution (RCE), Local File Extension (LFE), or Remote File Execution (RFE), or other vulnerabilities for this purpose.

3. Cyber actors are known to "crawl" target sites in advance to profile checkout processes, probe for vulnerable extensions, or examine third-party plugins.

4. Once write access is obtained, the cyber threat actor modifies application source code by inserting a data-skimming script. This script is often difficult to identify as it is frequently obfuscated, written to mimic Google Analytics code, or comprised of polymorphic code containing innumerable decoy keywords or commands that change each time the code is run.

5. The code directs the victim's browser to scrape and send data from checkout forms to a website or remote drop server accessible to attackers. To reduce suspicion, cyber threat actors frequently register and use a drop server domain that looks similar to a legitimate domain, allowing any anomalies in the code to go undetected upon a cursory review. Cyber threat actors may even obtain an SSL certificate for the drop server domain to give the appearance of legitimacy.[xiv]

6. Attackers collect stolen credentials from the drop server and use them to perpetrate fraudulent activity or sell through online black markets and forums.

Recommendations to Mitigate the Risk of a Magecart Attack

The NTIC Cyber Center strongly recommends all organizations using ecommerce platforms implement a robust and layered security strategy to identify and manage risk posed by Magecart attacks. Administrators of ecommerce websites are encouraged to review the following list of recommendations to help reduce the risk of compromise:

- Ensure that all administrator accounts associated with ecommerce websites, including cPanels, website analytics platforms, and ecommerce platforms, are secured with lengthy, complex, and unique passwords and multifactor authentication, if possible.

- Configure Content Security Policy (CSP) Headers to only execute scripts loaded in source files from whitelisted domains. This allows browsers to reject any JavaScript not delivered from pre-defined servers, restricts external domain communication to authorized interactions only, and helps mitigate risks of attacks such as XSS or data injections.

- Implement Subresource Integrity (SRI) configurations to instruct browsers to only fetch resources with a predetermined cryptographic hash value. This acts as a checksum for browsers to verify that libraries loaded from third-party sources have not been modified.

- Simplify checkout pages and avoid using third-party scripts on any page that records sensitive data to isolate payment forms from possible abuse by external plugins or scripts.

- Scrutinize all third-party scripts and investigate any unexpected presence of obfuscated scripts.

- Perform quality controls to confirm legitimacy of all external domains referenced in the website's source code.

- Consider implementing a reputable web application firewall (WAF) to protect websites against XSS, SQLi, path traversal, and other types of external attacks. Some WAFs advertise the ability to detect when dynamic analysis is performed on – or unauthorized changes are made to – a web application.

- Employ code obfuscation tools and techniques to protect front-end code and make analyzing and modifying web applications difficult.

- Maintain awareness of current and emerging threats and vulnerabilities by subscribing to associated security bulletins and implement patches for plugins and extensions as soon as possible.

- Work with third party vendors to ensure vulnerable or unprotected plugins and extensions are patched and kept up-to-date.

[i] https://usa.visa.com/visa-everywhere/security/visa-chip-card-stats.html
[ii] https://www.riskiq.com/blog/external-threat-management/inside-magecart/
[iii] https://www.bleepingcomputer.com/news/security/magecart-group-12-targets-opencart-websites/
[iv] https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/
[v] https://www.zdnet.com/article/how-magecart-groups-are-stealing-your-card-details-from-online-stores/
[vi] https://krebsonsecurity.com/2019/04/data-e-retail-hacks-more-lucrative-than-ever/
[vii] https://nakedsecurity.sophos.com/2018/06/28/ticketmaster-breach-what-happened-and-what-to-do/
[viii] https://www.riskiq.com/blog/labs/magecart-british-airways-breach/
[ix] https://thehackernews.com/2018/09/newegg-credit-card-hack.html
[x] https://labs.sansec.io/2019/04/24/atlanta-hawks-magecart/
[xi] https://labs.sansec.io/2019/04/29/puma-magecart/
[xii] https://labs.sansec.io/2019/04/29/polymorphic-skimmer-57-payment-gateways/
[xiii] https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/
[xiv] https://www.riskiq.com/blog/labs/magecart-adverline/