

Hackers Use Google Tag Manager to Steal Credit Card Numbers via @sejournal, @martinibuster



Hackers are actively exploiting a vulnerability to inject an obfuscated script into Magento-based eCommerce websites. The malware is loaded via Google Tag Manager, allowing them to steal credit card numbers when customers check out. A hidden PHP backdoor is used to keep the code on the site and steal user data.

The credit card skimmer was discovered by security researchers at Sucuri who advise that the malware was loaded from a database table, `cms_block.content`. The Google Tag Manager (GTM) script on a website looks normal because the malicious script is coded to evade detection.

Once the malware was active it would record credit card information from a Magento ecommerce checkout page and send it to an external server controlled by a hacker.

Sucuri security researchers also discovered a backdoor PHP file. PHP files are the 'building blocks' of many dynamic websites built on platforms like Magento, WordPress, Drupal, and Joomla. Thus, a malware PHP file, once injected, can operate within the content management system.

This is the PHP file that researchers identified:

`./media/index.php.`

According to the advisory published on the Sucuri website:

"At the time of writing this article, we found that at least 6 websites were currently infected with this particular Google Tag Manager ID, indicating that this threat is actively affecting multiple sites.

eurowebmonitortool[.]com is used in this malicious campaign and is currently blocklisted by 15 security vendors at VirusTotal."

VirusTotal.com is a crowdsourced security service that provides free file scanning and acts as an aggregator of information.

Sucuri advises the following steps for cleaning an infected website:

- *"Remove any suspicious GTM tags. Log into GTM, identify, and delete any suspicious tags.*
- *Perform a full website scan to detect any other malware or backdoors.*
- *Remove any malicious scripts or backdoor files.*
- *Ensure Magento and all extensions are up-to-date with security patches.*
- *Regularly monitor site traffic and GTM for any unusual activity."*

Read the Sucuri advisory:

Google Tag Manager Skimmer Steals Credit Card Info From
Magento Site

Featured Image by Shutterstock/sdx15

<https://www.searchenginejournal.com/hackers-use-google-tag-manager-to-steal-credit-card-numbers/539691/>