New JavaScript Malware Issue? Ensure You Have Deployed All Magento Security Patches

A new type of malware issue called JavaScript Malware issue has been affecting Magento based stores. This malware issue exploits vulnerability in Magento & forwards credit card information externally from your site's checkout pages. The malware infects the Magento store through Admin or database access (weak passwords, phishing, and other un-patched vulnerabilities). It seems that there is no new attack vector, and the impacted sites are facing this issue only due to lack of Shoplift Patch (February 2015) or the security patch was deployed after they were compromised. Thus, it is recommended to all unpatched Magento shops that they should deploy all security patches in a timely manner.

However, if you have not deployed previous security patches and find indication in the server logs or otherwise that credit card details may have been sent externally from your site, you should review your files, configurations, and backend accounts.

How to Determine You have Been Affected by New JavaScript Malware Issue?

As a Magento merchant, you should open the main page and view the page source. Look for the strings mentioned below. If you found any of below strings, it means that your site has been compromised.

- eval (atob (

regexp (“ checkout

Regexp (‘checkout

Regexp (“onepage

Regexp (‘onepage

Regexp (“onestep

Regexp (‘onestep

- the case of those strings can be dissimilar (For e.g, regexp, RegExp, etc.)
- However, if it is the case where you don’t find any of the above strings, you should carefully review your Admin configuration, taking account of your Admin accounts, follow best security practices, and deploy all security patches.

How to Remove Malicious Code if Your Site is Affected?

Begin by scanning your Magento site with a tool such as magereport.com. Deploy all security patches. Make sure that there are no any unknown files in the system. If you find unknown admin accounts while reviewing, it is recommended you to remove all such accounts. After removing such accounts, change the current passwords of the rest admin accounts to strong ones. As a Magento merchant, you should always follow best security practices summarized in the Magento User Guide. And, also review some parts (mentioned below) of your Admin configuration and remove any malicious code found.

- Configuration->General->Design->HTML Head->Miscellaneous Scripts
- Configuration->General->Design->Footer->Miscellaneous HTML

After removing such malicious code from your Magento based site, it is recommended you to review some server log files mentioned below. If you found such files or URLs, it means that your Magento site is totally compromised.

/downloader/Maged/Maged.php

/downloader/cache.php
/jquery.php
/jquery.pl
/css.php
/opp.php
/xrc.php
/order.php
/jquerys.php
/var/extendware/system/licenses/encoder/mage_ajax.php
/js/index.php

If you suspect your site has been compromised and you haven’t applied previous Shoplift security patch, implement such security patches immediately to stop this new JavaScript Malware issue attack.

Recommended product to solve this issue successfully.