Following the tracks of MageCart 12

maxkersten.nl/2020/02/17/following-the-tracks-of-magecart-12/

17/02/2020

This research is a follow up on the two previous articles about MageCart 12. At first, two infected ticket resellers were found, after which multiple other infected websites were caught by Jacob and me. RiskIQ also followed up on our findings with additional research where they found two popular websites to be infected with a credit card skimmer that has been attributed by MageCart 12.

This article provides new websites that have been infected, but also websites that were infected once more. Before going into the websites, a small note about the skimmer's modus operandi is made.

The modus operandi

Similar to the *opendoorcdn.com* campaign, there is no legitimate JavaScript code within the file. The skimmer is (similar to the *opendoorcdn.com*) hosted on an external site, *toplevelstatic.com*, which resolves to different IP addresses. The location of these IP addresses are mostly (if not all) located in Russia.

The used obfuscation is similar to the previous skimmer script, where the first stage functions as a loader, whereas the second stage contains the original script with added garbage code and string obfuscation. Note that the second stage script is only loaded if it is not tempered with, based on the hash check that is included in the second stage.

When removing the dead code and string obfuscation from the second stage, the script is identical to the original input, aside from the function names. This skimmer script is identical to the one that was found on *opendoorcdn.com*, aside from the exfiltration gate's address.

The victims

All infected sites have been contacted prior to the publication of this blog, although there was no response back to us. Information about each victim is given below.

Suplementos Gym

The first sighting of a skimmer on Suplementos Gym was on he 31st of January 2020. This specific skimmer still connected back to opendoorcdn.com, which was taken down by the combined efforts of Jacob and myself. The first recorded sighting of the toplevelstatic.com

skimmer was on the 7th of February 2020. The latest recorded date that the skimmer was active, was on the 10th of February 2020, as can be seen here. Contact was established via e-mail, but there was no response back.

Bahimi

The Bahimi web shop, which was also infected with the opendoorcdn.com skimmer in November 2019, has also been infected with the toplevelstatic.com skimmer on the 7th of February 2020. It is unknown for how long the skimmer remained active on the website. Albeit our best efforts, there was no response to our e-mail and Tweet.

TitansSports

TitansSport is the last entry in the list of victims that was also infected with the opendoorcdn.com skimmer in early January 2020. The toplevelstatic.com infection was present on the 7th of February 2020, although the exact time span is not yet known. Contact was made via e-mail and WhatsApp, but no response was received.

BVC

BVC got infected on the 3rd of February 2020, as can be seen here. A snapshot of the 7th of February 2020 shows that the skimmer was still active, continuing on the 16th of February. The skimmer is still active at the time of writing, which is the 19th of February 2020. An e-mail was sent to inform BVC, but no response was received.

MyMetroGear

The infection on MyMetroGear was first sighted on the 4th of February 2020. The infection continued through the 7th of February, until the 16th of February 2020. The skimmer is still live at the time of writing, which is the 19th of February 2020. No answer was given based on the e-mail we sent to MyMetroGear.

True Precision

True Precision's web shop was infected on the 4th of February 2020. The infection is ongoing at the time of writing (which is the 19th of February 2020). The infection was also stored in snapshots on the 7th of February 2020 and the 19th of February 2020. There was no response to our e-mail nor Tweet.

Fashion Window Treatments

Fashion Window Treatments got infected on the 6th of February, and is still infected at the time of writing (the 19th of February 2020). There was no response back based on our e-mail or Tweet.

Skin Trends

Skin Trends's web shop was infected on the 6th of February 2020. After the 7th of February 2020, there is no record of an infection. Since our data collection is not exhaustive, the exact end date of the infection is unknown, but at least prior to the 16th of February 2020. No response was received towards our e-mail nor Tweet.

Natonic

Natonic got infected on the 10th of February 2020. On the 17th of February 2020, the entire skimmer was put on the website as a piece of JavaScript, instead of being loaded externally. Shortly after that, the skimmer was not present anymore. No response was received based on the e-mail that we sent out.

Conclusion

If you have shopped at one of the mentioned sites around the infected period, it is suggested to contact your bank and request a new credit card. Also note that all information that was entered on the site's payment form was stolen by the credit card skimmer and should be considered compromised.

Additionally, I'd like to thank Jacob for the clear communication and cooperation when conducting this research.