Closing in on MageCart 12

maxkersten.nl/2020/02/24/closing-in-on-magecart-12/

24/02/2020

This is the fourth blog with details on the activities of MageCart 12. In this article, yet another part of their ongoing campaign is uncovered. The amount of infected sites for this campaign is higher than in the previous cases.

Before diving into the infected sites, and the rough duration of the infections, information regarding the skimmer itself will be given.

Modus operandi

The modus operandi for this campaign is slightly different when comparing it to the other research that has been published so far. The skimmer, hosted on *jquerycdn.su*, changed four times during the campaign. The earliest recorded date of a hacked site linking to the skimmer domain is on the 30th of September 2019, whereas the latest new infection date is the 19th of February 2020.

In the four versions of the skimmer that were used in this campaign, the used obfuscation method is the same as in the other reported campaigns. The first stage loads the actual skimmer script, which is polluted with garbage code. The skimmer itself is different, compared to the first versions. The skimmer grabs all fields from the page, rather than all forms. Although the approach and script are different, the general concept remains the same: obtaining credit card credentials.

The exfiltration domains are linked to other skimming campaigns from MageCart 12, like the one Marco Ramilli wrote about, as well as Jacob's blog.

Infected web shops

All but three affected web shops have been contacted via e-mail or their web form on the 21st of February 2020. For each of the three uninformed web shops, there is a note in the list with the reason why. Similar to previous cases, I did not receive any response back at the time of writing (which is the 25th of February 2020).

The given dates are based upon the data set I created. This set is, by definition, not 100% accurate. As such, the actual dates might slightly differ. Additionally, it is possible that a website was not infected for the complete time between the begin and the end date, but this information is not present in my data set.

The mentioned dates are based upon the most accurate information from the data set and limited to this skimmer domain. Some sites are infected with another domain that is operated by the same group. To avoid confusion and keep things clear, this has not been included in this post.

Note that the skimmer domain (*jquerycdn.su*) has been down for a few days at least. This means that several sites that are still infected, are currently not actively sharing credit cards with the criminal actors, but this is subject to change at any given moment.

The list below is ordered from the past until the present, meaning the oldest infections are listed first. The end date is not taken into account at the sorting.

- BioPets was infected from the 30th of September 2019 and the infection is ongoing until now. The location where the skimmer is hosted right after that is different compared to the initial skimmer.
- Wellspring Wholesale was infected from the 30th of September 2019 until the 9th of February 2020.
- Wellspring Customer was infected from the 30th of September 2019 until the 9th of Feburary 2020.
- D2D Organics was infected from the 30th of September 2019 until the first of November 2019. At some point in time after that, the site went down. As such, there was no method to contact the owners of the website.
- Loud Shirts USA was infected from the first of October 2019 until somewhere prior to the 9th of Feburary 2020.
- Nilima Home was infected from the first of October 2019 until the 9th of February 2020.
- Silk Naturals was infected from the first of October 2019 until the 16th of February 2020.
- JD's Sound & Lighting was infected from the second of October 2019 until the 9th of February 2020.
- Nilima Rugs was infected from the second of October 2019 until the 10th of February 2020.
- Martin Services was infected from the second of October 2019 until an unknown point in the future.
- The Cheshire Horse was infected from the 6th of October 2019 until the 11th of December 2019.
- Kl&in More was infected on the 7th of October 2019. No more information is available.
- Schlaf Team was infected on the 17th of October 2019. No more information is available.
- The Top Collection was infected from the 19th of October 2019 until at least the 25th of February 2020.
- Selaria Dias was infected from the 5th of November 2019 until the 21st of February 2020.
- Tile was infected from the 13th of November 2019 until the 28th of January 2020.

- Liquorish Online was infected from the 13th of November 2019 until the 24th of November.
- Starting Line Products was infected on the 19th of November 2019. No more information is available.
- Sport Everest was infected from the 20th of November 2019 until at least the 25th of February 2020.
- ABC School Supplies was infected on the 26th of November 2019 until the 10th of February 2020.
- Motor Book World was infected on the 26th of November 2019 until the 22nd of February 2020.
- Contadores Digital was infected on the second of December 2019. No more information is available.
- Giocattoli Negozio was infected on the 12th of December 2019 until at least the 25th of February 2020.
- Academic Bag was infected on the 6th of January 2020. No more information is available.
- SoleStar was infected from the 11th of January 2020 until at least the 25th of February 2020.
- Surf Bussen Travel was infected from 17th of January 2020 until the 10th of January 2020.
- Surf Bussen Nu was infected on the 18th of January 2020. No more information is available.
- Haight Ashbury Music Center was infected on the 24th of January 2020 until the 18th of February 2020. Alas, the form on the website did not allow me to submit a message. Aside from that, there were no other contact methods available. As such, I was not able to inform them.
- MyCluboots was infected from the 25th of January 2020 until at least the 25th of February 2020.
- Sol's Italia was infected on the 30th of January 2020. No more information is available.
- Parkwood Middle School Bears was infected from the 31st of January 2020 until at least the 25th of February 2020.
- Voltacon was infected from the 12th of February 2020 until the 25th of February 2020.
- Pitcher's Sports was infected on the 13th of February 2020 until at least the 25th of February 2020. Alas, the only possible contact method was via a phone call. Since this was not an option for me, I could not contact them.
- Powerhouse Marina was infected on the 13th of February 2020 until the 25th of February 2020.
- Sukhi Rugs was infected on the 13th of February 2020. No more information is available.
- ZooRoot was infected from the 14th of February 2020 until at least the 25th of February 2020.
- Sukhi was infected on the 17th of February 2020. No more information is available.

- Integral Yoga Distribution was infected on the 18th of February 2020 until at least the 25th of February 2020.
- Kitchen And Couch was infected on the 19th of February 2020 until the 25th of February 2020.

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.