MageCart Group Sabotages Rival to Ruin Data and Reputation

bleepingcomputer.com/news/security/magecart-group-sabotages-rival-to-ruin-data-and-reputation/

Ionut Ilascu

By
Ionut Ilascu

- November 21, 2018
- 03:09 AM
- 0

Cybercriminals in the web-skimming business are sabotaging their competition by poisoning the payment data they exfiltrate from online stores. This cause the losing party to end up with a big fat nothing and a ruined reputation on underground forums.

The groups colliding on the real victim's server are from the MageCart line of cybercriminals, identified by the Yonathan Kliknsma of RiskIQ in order of their appearance, as group 3 and group 9. Obviously, one of them is better at this game and that is the latter.

> Say hello to Magecart group 3 being bullied by Magecart group 9. https://t.co/omO9D1Co3h
>
> — Yonathan Klijnsma (@ydklijnsma) November 20, 2018

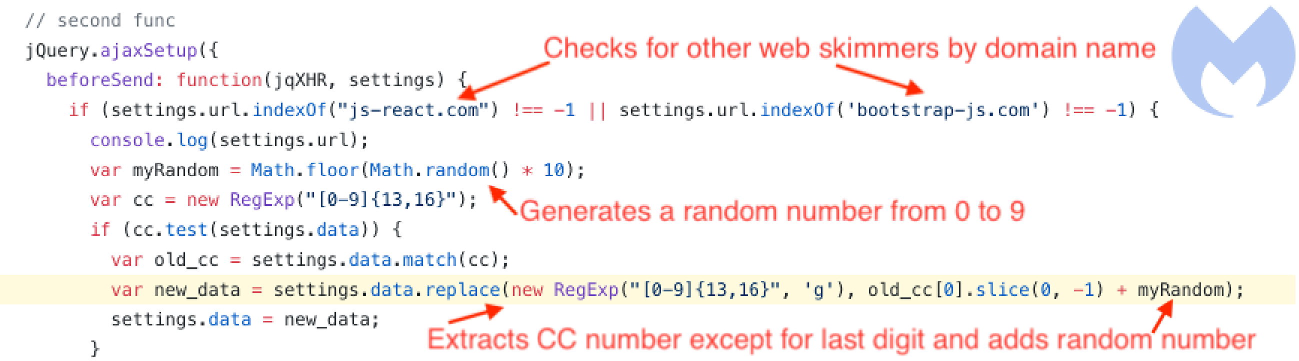
Independent security researcher Willem de Groot and Jérôme Segura of Malwarebytes published two reports about the web-skimming code from Magecart group 9 wrecking their competition's operation.

The 'playground' was the website of Umbro Brazil and the B.Liv online cosmetics shop.

Hunting for rival's exfiltration domains

According to the researchers, the code used by group 9 is heavily obfuscated and it can detect the presence of other web-skimmers on the server. If a competing skimmer is detected, it intercepts the card data captured by the competition and changes the last card number so that the data becomes worthless.

To trigger the data-poisoning mechanism, the code checks for domain names used by the competitor to exfiltrate the payment details. If detected, it generates a random number from 0-9 and replaces the last card number with it.



```
// second func
jQuery.ajaxSetup({
  beforeSend: function(jqXHR, settings) {
    if (settings.url.indexOf("js-react.com") !== -1 || settings.url.indexOf('bootstrap-js.com') !== -1) {
      console.log(settings.url);
      var myRandom = Math.floor(Math.random() * 10);
      var cc = new RegExp("[0-9]{13,16}");
      if (cc.test(settings.data)) {
        var old_cc = settings.data.match(cc);
        var new_data = settings.data.replace(new RegExp("[0-9]{13,16}", 'g'), old_cc[0].slice(0, -1) + myRandom);
        settings.data = new_data;
      }
```

Checks for other web skimmers by domain name

Generates a random number from 0 to 9

Extracts CC number except for last digit and adds random number

Detecting competitor's exfiltration domain and changing card number (credit: Malwarebytes)

Segura says that the slight modification of the card number may be sufficient to pass validation, but the payment information is useless.

Selling non-working card data on the black market is a serious hit to the seller's reputation, de Groot explains.

"Why the subtle sabotage, instead of just killing the inferior skimmer? On the dark web markets, reputation is everything," stated de Groot in a blog post about the competing skimmers. "If one sells non-working cards, angry customers will publicly complain and it will destroy the competing “brand”."

Sabotaging competition is a strategy seen in the past in cryptomining operations. GhostMiner, the first fileless cryptocurrency miner scans and stops other processes that may be mining on the host, a behavior later adopted by CroniX.

Magecart operations typically take advantage of third-party scripts that are loaded at checkout. To protect themselves, website owners should remove payment information pages any components that are not required to process the transaction or customer data. Risk of compromise is further reduced by keeping plugins updated to the latest version.

Related Articles:

Microsoft: Credit card stealers are getting much stealthier

Caramel credit card stealing service is growing in popularity

Refine your JavaScript knowledge with this training bundle deal

Ukraine targeted by DDoS attacks from compromised WordPress sites

Hacked WordPress sites force visitors to DDoS Ukrainian targets

- JavaScript
- MageCart
- Skimmer

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: