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

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

February 7, 2020



Labs Magecart

February 07, 2020

By Jordan Herman

A recent <u>blog post</u> by Jacob Pimental and <u>Max Kersten</u> highlighted Magecart activity targeting ticket re-selling websites for the 2020 Olympics and EUFA 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, "<u>New Year, Same Magecart: The Continuation of Web-based Supply Chain Attacks"</u> and "<u>Magento Attack: All Payment Platforms are Targets for Magecart Attacks</u>." 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:"



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'):

```
Document Object Model

<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
```

The variable loading the skimmer

Next Domain Up

On February 3rd, Pimental and Kersten published their followup <u>blog</u> detailing their efforts to identify further opendoorcdn.com victims and have the skimming domain taken down by the Chinese company through which it was registered. On February 2nd, RiskIQ observed that opendoorcdn.com was replaced on at least two of the victim sites named in the blog by a live skimmer domain, toplevelstatic.com:

Page https://www.titanssports.com.br/natacao



Page https://storefrontcdn.com/scripts/1.1/general.js

| Status | Messages (0) | Dependent Requests (0) | Cookies (0) | Links (0) | Headers | SSL Certs (1) |
|--|---|---|---|---|---|---|
| 😑 Res | oonse Body | | | | | |
| var DDT var mn5 ZtK="2w la2r2"+ d2="da lNQ="0w a2p360" jwB="38 nVE="33 NVE="33 OWS="40 n4B=[n4 nZd="1c hxB="0w SmB="14 | ="alg2b2k3c1k1h2 = document[""+(2p372w0w1p0w1c1r "%2p361v332s2t1t a7bqd8u67uk1d89a 0w0w0w0w0w0w0w0w +"w2q332s3d1p3b2 332b38362x322v14 41k142j2k3b2k2s2 "+"62r1a37392q37 y2s2p2p1j2q352s1 B,ZtK,1NQ,jwB,nV 1p141d111a1c170y 241d3e14372t302t 1g1a1c170y231e15 | 0a0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0w0 | <pre>eateEleme"+Str 70w0w0w0w0w2u"+ 70w0w0w0w";; w120w2w2p372w1 'j2m2p193e1"+"t a362t34302p2r2 7382w191d151n0a k0y172r362r180 :"\x65")+"oin" b1d252k3"+"c1k1 7342p362p31370w +"1161i15 1521</pre> | ing.fromChai "33360w143a2 n0a0w0w0w0w0w0 192i1c19112) t140y2s2p2p 0w0w"+"0w0wi y2s2p2p1j2g](".');; d3f1x2w3g2ki 1p0y0y2j141 | rCode(110)+" 2p360w2x0w1 0w0w0w0w0w0w k190y21171b2 1j2q3"+"52s1 0w0w0w0w092q 352s1k3"+"91 3c1k1f2e0y2j "+"d1e1a1c17 c2v27351u2d3 | t"]("div");; p0wlcln0w2x0wlo0w 0w0w0w0w0w3h0a0 v180y0y151n0a0w0w k391i1j392z1d2s2z 332s3d1p2w2w142q3 i1j392z1d2s2z112p 0y2r2w2p36"+"1v33 0y1q2k3c1k1e3a2i3 a0y180y0y151n3a2p |
| | | Now ekimme | r domoin | | | |

New skimmer domain

RiskIQ has observed the toplevelstatic.com domain on three victim sites so far, all of which were previously compromised by opendoorcdn.com, as seen through our host pairs data set in RiskIQ Community:

| kiq Q opend | loorcdn | .com | 9 | | | | | | | | | | | |
|--|---------|-------------------------------|--------------|--------------------|-----------------|-----------------------------|-----------------|-----------------|--------------|--------------|-----------------|---------------|-------------------|------|
| 2019-01-14 Registrar 2020-01-28 Registrar | Web Com | merce Co tection.cc | Categori | ze | | | | | | | | | | |
| | | 42 Resolution | 2 s Whois | 17 Certificates | 4 Subdomains | 0 Trackers | 2 Components | 8 Host Pairs | 10 OSINT | 80 Hashes | 9 DNS | 0 Projects | 0 Cookies | |
| | HOST P | AIRS © ⊴ 1-8 of 8 ▼ | Sort : | Last Seen Desce | nding 🔻 25 / P | age 🔻 | | | | | | | | |
| | | Parent Hostna | | | | Child Hostna opendoorcdr | | First 202 | t 0-01-11 | | Last 2020-02 | -02 | Cause script.s | rc |
| STNAME (8 | | natonic.com.a | | | | opendoorcdr | | | 0-01-23 | | 2020-01 | | script.s | |
| t.facebo 1 .com.au 1 | 0 | www.guimepa | | | | opendoorcdr | | | 9-11-27 | | 2020-01 | | script.s | |
| oorcdn.c 1 dnnsport 1 | | www.naturalg | igments.eu | | | opendoorcdr | .com | 201 | 9-11-28 | | 2019-11 | -28 | script.s | rc |
| uimepa.c 1 | 0 | connect.faceb | | | | opendoorcdr | | | 2019-11-28 | | 2019-11-28 | | script.s | |
| | | www.naturaij | agments.com | | | openadorcar | com | 201 | 2-11-20 | | 2013-11 | -20 | scripes | H %. |

Victims of original skimmer domain

| oplev | elstatic.c | om O | | | | | | | | | | | | | Tours | |
|-------|------------------|---------------------------|------------------------------|--------------------|-------------------------|--------------------|-----------------|------------|------------|----------------------|-------|-----------|---------|-----------|-------|--|
| | Eranet Interr | | Categori | ze | | | | | | | | | | | | |
| | Aug | | Sep | | Oct | | Nov | | | Dec | | Jan | | Fe | b | |
| | | 10 | 1 | 3 | , | 0 | , | 3 | 0 | 0 | 6 | 0 | 0 | | | |
| | | Resolutions | Whois | Certificates | Subdomains | Trackers | Components | Host Pairs | OSINT | Hashes | DNS | Projects | Cookies | | | |
| | HOST PAIL | RS () | | | | | | | | | | | | | | |
| | • | 1 - 3 of 3 🔻 | Sort : I | Last Seen Desce | nding 🔹 25 / Pa | age 🔻 | | | | | | | | | | |
| | | Parent Hostnam | e | | c | Child Hostname | | | First | | Last | | c | Cause | Tags | |
| | natonic.com.au | | | | te | topievelstatic.com | | | 2020-02-02 | | 2020- | 02-04 | 50 | cript.src | | |
| | • | www.titanssports.com.br b | | | toplevelstatic.com 2020 | | 2020-02-02 2020 | | 2020- | 2020-02-03 | | cript.src | Ма | licio | | |
| | www.tjvip.com.br | | | toplevelstatic.com | | | | | | 020-02-03 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.

| Q | topleve | elstat | ic.com O | | | | | | | | | | | |
|----------|---------|--------|-------------------------------|------------|-------------------|-----------------|---------------|---------|-------------|-----------------|------------|-------------|------------|-------------|
| 01 05 | | | International TED FOR PRIV | Categorize | | | | | | | | | | |
| | | | 10 Resolutions | 1 Whois | 3 Certificates | 1 Subdomains | 0 Trackers | | 1 onents | 3 Host Pairs | 0 OSINT | 0 Hashes | 6 DNS | 0 Projec |
| | | RESO | LUTIONS 🚱 | Sort : | Last Seen Desc | ending 🔻 25 / | Page 🔻 | | | | | | | |
| 10 | | | Resolve | Loca | tion N | etwork | | ASN | First | | Last | Sou | irce | |
| 2 | | | 46.29.164.54 | RU | 4 | 5.29.164.0/24 | 1 | 51659 | 2020-0 | 2-04 | 2020-02-05 | risk | iq, pingly | |
| 2 | | | 176.107.160.153 | RU | 1 | 76.107.160.0/24 | | 49063 | 2020-0 | 2-05 | 2020-02-05 | pin | gly | |
| | | | 45.143.138.40 | RU | 4 | 5.143.136.0/22 | | 47196 | 2020-0 | 2-04 | 2020-02-04 | risk | iq | |
| | | | 91.215.169.43 | RU | 9 | 1.215.168.0/22 | | 49693 | 2020-0 | 2-03 | 2020-02-04 | risk | iq, kaspe | sky |
| 2 | | | 45.140.168.169 | RU | 4 | 5.140.168.0/23 | 1 | 51659 | 2020-0 | 2-03 | 2020-02-04 | risk | iq, kaspe | rsky |
| 2 1 | | | 194.147.34.175 | RU | 1 | 94.147.34.0/24 | 1 | 51659 | 2020-0 | 2-02 | 2020-02-03 | risk | iq | |
| | | | 82.146.34.113 | RU | 8 | 2.146.34.0/23 | : | 29182 | 2020-0 | 2-02 | 2020-02-02 | risk | iq | |
| 2 | | | 45.143.138.14 | RU | 4 | 5.143.136.0/22 | | 47196 | 2020-0 | 2-02 | 2020-02-02 | risk | iq | |
| 2 2 | | | 176.107.160.87 | RU | 1 | 76.107.160.0/24 | | 49063 | 2020-0 | 2-01 | 2020-02-01 | risk | iq | |
| 1 | | | 91.215.170.252 | RU | 9 | 1.215.168.0/22 | | 49693 | 2020-0 | 2-01 | 2020-02-01 | risk | iq | |
| 1 | | 4 | 1 - 10 of 10 🔻 🕒 | R | esolutior | ns for tople | evelstat | tic.con | n | | | | | |

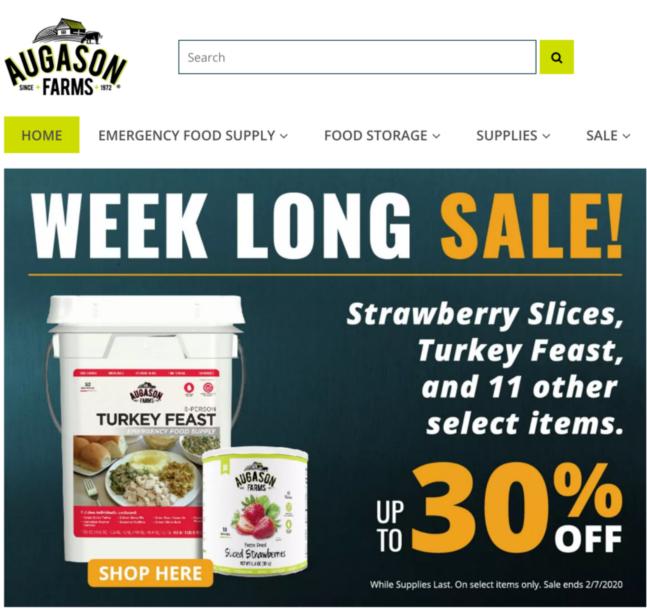
Resolutions for toplevelstatic.com

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.

| 0 | A https:/ | //comn | nunity. | r iskiq.com /sear | rch/opendo | oorcdn.com | | | | | | |
|--------------------|-------------------------|--------|---------|--------------------------|--------------|---------------|-----------|-----------|--------|------------|-----------|------------------|
| Q | opend | oorc | dn.co | om o | | | | | | | | |
| 9-01-14 9-01-28 | Registrar Registrant | | ommer | | • Categorize | 5 | | | | | | |
| | | | | 42 | 2 | 17 | 4 | | 0 | 2 | 8 | 10 |
| | | | | Resolutions | Whois | Certificates | Subdomai | ns Trac | kers: | Components | Host Pair | rs OSINT |
| | | RESC | DLUTIC | NS 🔁 | | | | | | | | |
| 84) | | - • | ~ | 1 - 25 of 42 🔻 | Sort : | Last Seen Des | cending 🔻 | 25 / Page | • | | | |
| 42 | | | Resol | /e | Location | Network | | ASN | First | Last | | Source |
| na 28 | | | 188.2 | 46.229.211 | RU | 188.246.22 | 9.0/24 | 49505 | 2020-0 | 01-15 2020 |)-01-28 | riskiq |
| enc 5 | | | 199.5 | 9.242.150 | US | 199.59.242 | .0/24 | 395082 | 2020-0 | 01-14 2020 |)-01-15 | riskiq |
| rk 3 3 | | | 161.1 | 17.189.60 | SG | 161.117.12 | 8.0/17 | 45102 | 2020-0 | 01-12 2020 |)-01-14 | riskiq |
| | | | 161.1 | 17.229.125 | SG | 161.117.12 | 8.0/17 | 45102 | 2020-0 | 01-10 2020 |)-01-11 | riskiq |
| | | | 124.1 | 56.216.20 | JP | 124.156.20 | 8.0/20 | 132203 | 2019- | 12-15 2020 |)-01-10 | riskiq |
| na 28 | | | 47.25 | 4.233.8 | MY | 47.254.224 | .0/19 | 45102 | 2019- | 12-08 2019 | -12-13 | riskiq |
| enc 5 | | | 34.77 | 160.68 | US | 34.76.0.0/1 | 4 | 15169 | 2019- | 10-21 2019 | 9-12-07 | riskiq |
| 3 ork 3 | | | 45.76 | 85.165 | DE | 45.76.80.0/ | /20 | 20473 | 2019-0 | 09-10 2019 | 9-10-22 | riskiq, kaspersl |
| 1 | | | 129.2 | 26.123.164 | SG | 129.226.11 | 2.0/20 | 132203 | 2019- | 10-19 2019 | 9-10-20 | riskiq |
| 42) | | | 8.208 | 24.221 | GB | 8.208.0.0/1 | 9 | 45102 | 2019- | 10-18 2019 | 9-10-19 | riskiq |
| 3 | | | 150.1 | 09.105.215 | нк | 150.109.10 | 4.0/23 | 132203 | 2019- | 10-11 2019 | 9-10-18 | riskiq, kaspersk |
| .0/17 3 1/19 2 | | | 47.25 | 2.15.2 | US | 47.252.0.0/ | /18 | 45102 | 2019-0 | 09-02 2019 | -09-09 | riskiq, kaspersk |
| 0 2 | | | 47.25 | 4.174.17 | DE | 47.254.160 | .0/19 | 45102 | 2019-0 | 08-25 2019 | 9-09-01 | riskiq, kaspersk |
| 1/19 2 | | | 35.23 | 4.128.225 | US | 35.232.0.0/ | /14 | 15169 | 2019-0 | 07-29 2019 | 9-08-24 | riskiq, kaspersk |
| | | | | Re | esolution | is for open | doorcdn. | 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.



FREE SHIPPING ON ORDERS OVER \$200

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.

MY ACCOUN

| ۹ | storefr | ontcdn.o | com 📀 | | | | | | | | | | | | | Tours |
|----------------|---------|-------------------------|--------------------|----------------------|-----------------|----------------|-----------|-------------------|------------|-------|------------|-----|----------|------------|--|------------|
| 01-12 02-05 | | NameCheap WhoisGuard | • • Ca | tegorize | | | | | | | | | | | | |
| | | | Resolutions | Whois | Certificates | Subdomains | Trackers | Components | Host Pairs | OSINT | Hashes | DNS | Projects | Cookies | | |
| | | HOST PAI | | Sort : L | ast Seen Descen | ding 🔻 25 / Pa | ge 🕶 | | | | | | | | | |
| | | | Parent Hostnam | e | | | Child Hos | Child Hostname | | | First | | | | | Cause |
| | | | www.beprepared.com | | | | | storefrontcdn.com | | | 2020-01-16 | | | 2020-01-29 | | script.src |
| ME (S | | 0 | www.augasonfa | www.augasonfarms.com | | | | storefrontcdn.com | | | 2020-01-27 | | | 2020-01-27 | | script.src |

Host pairs showing sites loading storefrontcdn.com

Page https://www.beprepared.com/year-supply-of-grains-le

| Status | Messages (26) | Dependent Requests (747) | Cookies (21) | Links (319) | Headers | SS |
|--------|----------------|--|--------------|-------------|---------|----|
| 😑 Doci | ument Object M | odel | | | | |
| | | <pre><script 2v<br="" src="https://</td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td>Magecart script on bepr</td><td>epared.com</td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Page</td><td>https://sto</td><td>orefrontcdn.com/s</td><td>scripts/1.1</td><td>/general.j</td><td>js</td><td></td></tr><tr><td>Status</td><td>Messages (0)</td><td>Dependent Requests (0) Co</td><td>ookies (0) Links</td><td>(0) Headers</td><td>SSL Certs</td><td>(1)</td></tr><tr><td></td><td></td><td></td><td></td><td>(-,</td><td></td><td></td></tr><tr><td>😑 Res</td><td>ponse Body</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>var DD var mn ZtK=">la2r2"- gd2="da lNQ="0v a2p360" jwB="38 nVE="z3</td><td>T="alg2b2k3clklh23 5 = document[""+(8 w2p372w0wlp0wlcln0 +"w2p361v332s2tlt3 aa7bqd8u67uk1dk9ak w0w0w0w0w0w0w0w0w0w "+"w2q332s3dlp3b2x 8332b38362x322v141 3alk142j2k3b2k2s2k</td><td>a0w0w0w0w0w0w0w0w0w0w0w0w0w0w0u2u39 302p2k3c1k1k1m2g2k3";; 22>34?"\x63":"\x5e")+"r"+"eate a0w00w0w0, w0w0w0w0w0w0w0w0w0w 8142x151n0a0w0w0w0w0w0w0w0w0w vw8-144";; w2p372w0w1p0w2w"+"2p372w0w120 322s33b1a2x3d2i1a";; 51a362t 343. 02p2r2t141b2j2m2 192117150y1b2v152j1, c211a362 836141c182r362r1a302t322v382w</td><td>Eleme"+String.fro 0w0w0w2u"+"33360w 0w0w";; w2w2p372w1n0a0w0w p193e1"+"t192i1c1 t34302p2r2t140y2s</td><td>mCharCode(110)+ 143a2p360w2x0w1 0w0w0w0w0w0w0w0w0 9112k190y21171b 2p2p1j2q3"+"52s 0w0w0w0w0w0w092</td><td>"t"]("div");; p0wlcln0w2x0 w0w0w0w0w0w0w0w 2v180y0y151n0 1k391i1j392z1</td><td>wlc 3h0 a0w</td></tr></tbody></table></script></pre> | | | | |

Magecart script on beprepared.com

It appears the injections have been removed from sites, and they are currently free of skimming code. Additional IOCs can be viewed in our Magecart Group 12 project here: <u>https://community.riskiq.com/projects/b959cb28-d99c-b27b-bfd8-ae15d60a7e1b</u>

Safety in the Age of Magecart

The activity seen here demonstrates that magecart is a persistent and resilient threat. Given the lucrative nature of card skimming, Magecart attacks will continue to evolve and surprise security researchers with new capabilities. They're learning from past cyberattacks to stay one step ahead, so it's on us to do the same. <u>Make sure you're staying up to date by reading</u> <u>all our findings on Magecart</u> and stay tuned as we continue to shine a light on new developments. Also, find out how RiskIQ protects customers <u>by reading up on our JavaScript</u> <u>Threats Module here</u>.

*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