



Payment Card Skimmer Investigation

What did marketing do to get our corporate credit card compromised?

Scenario:

Your credit card company just called the head of the marketing department and told them that they saw fraudulent credit card transactions using the Marketing Corporate Credit Card. They asked what the recent transactions that were made with the card. After the fraud investigator verified the last real transaction, they determined that the fraud started after a purchase were made from the website called [www\[.\]almamaterstore\[.\]in](http://www.almamaterstore.in). They mention that his might be a credit card skimmer attack.

Goal: You work in the Incident response department in your organization. You want to use the payment card fraud as a learning experience to train your team.

Important Note: During your investigation you have informed your team not to directly visit the website in order to prevent any potential malware from entering the organization.

Objective 1: Was [www\[.\]almamaterstore\[.\]in](http://www.almamaterstore.in) compromised?

Objective 2: If the website was compromised, how do you know?

Objective 3: What evidence do you have for a compromise other than the word of the credit card company?

Objective 4: If you determine the site was compromise, how do you suspect the website was compromised?

Step 1: Check to see if the organizations website [www\[.\]almamaterstore\[.\]in](http://www.almamaterstore.in) is still on the google safe browsing list.

Open your web browser and search for “google safe browsing”

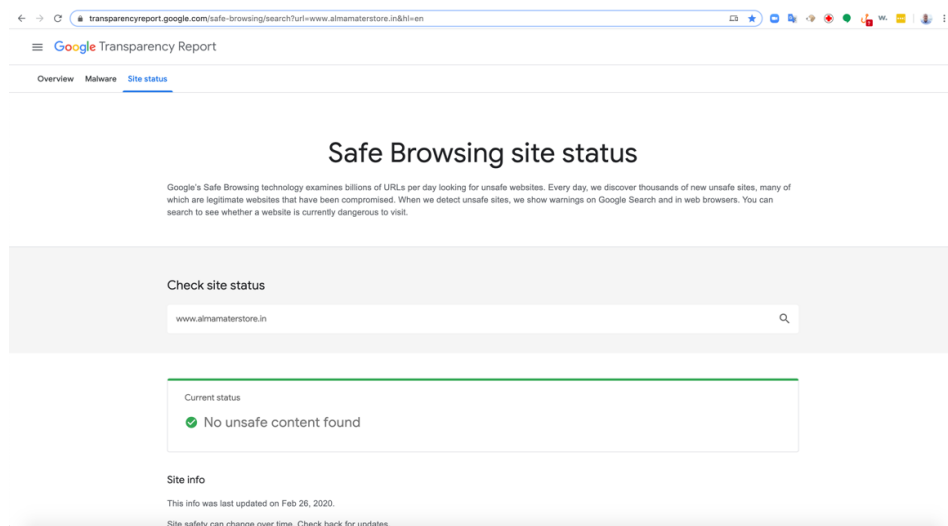
In the results click on the link for google transparency report:

<https://transparencyreport.google.com/safe-browsing/search?hl=en>

Enter the website `www[.]almamaterstore[.]in`

The URL should now be:

<https://transparencyreport.google.com/safe-browsing/search?url=www.almamaterstore.in&hl=en>



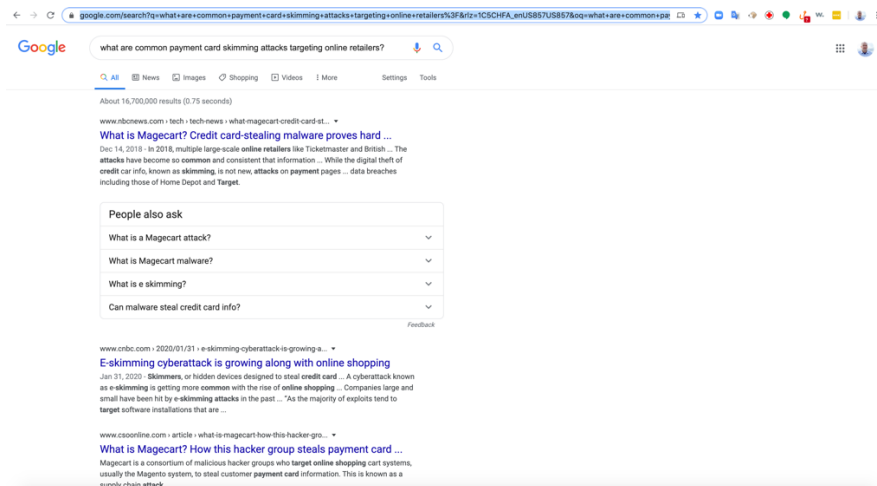
Google is not currently blocking this website. This is a good indicator, but this does not mean that the website is 100% safe.

Step 2: Open a new tab and go to <https://www.google.com>

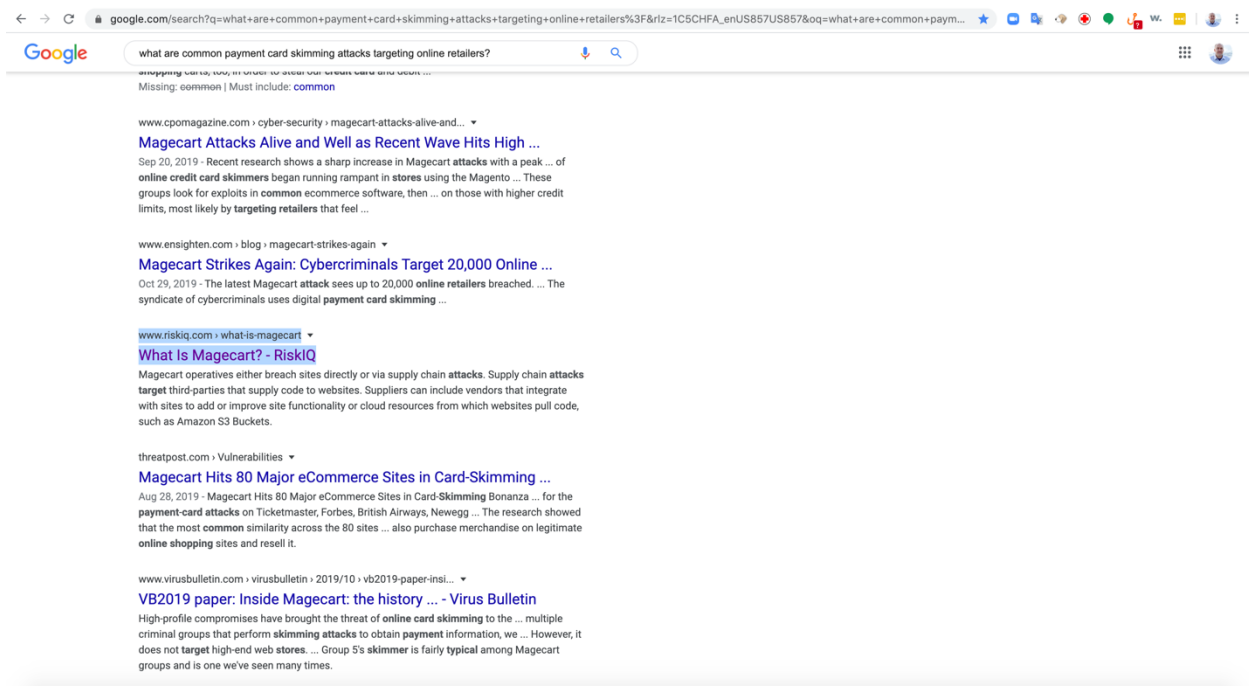
Search for the following question:

what are common payment card skimming attacks targeting online retailers?

https://www.google.com/search?q=what+are+common+payment+card+skimming+attacks+targeting+online+retailers%3F&rlz=1C5CHFA_enUS857US857&oq=what+are+common+payment+card+skimming+attacks+targeting+online+retailers%3F&aqs=chrome..69i57j69i65.1909j0j8&sourceid=chrome&ie=UTF-8



What is Magecart?



Click on the link for RiskIQ

<https://www.riskiq.com/what-is-magecart/>

Just from reading the results you can see that one of the popular payment card skimmers is Magecart a JavaScript attack that targets online merchants. If click on the links, you will get more information about Magecart.

What is Magecart?

Magecart injects a script designed to steal sensitive data that consumers enter into online payment forms on e-commerce websites directly or

through compromised third-party suppliers that websites might depend upon to make their sights function.

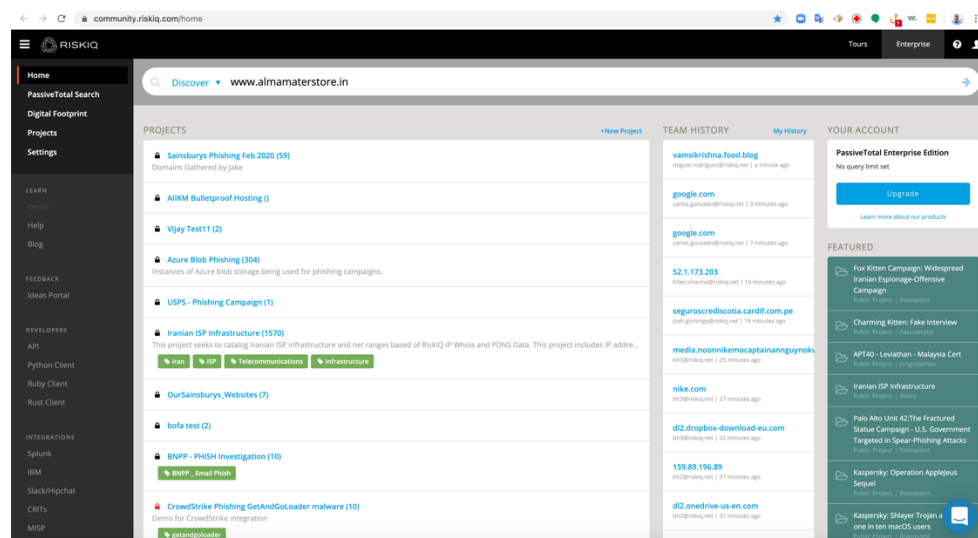
Now we are going to utilize RiskIQ's PassiveTotal threat hunting tool to further your investigation. PassiveTotal has over 10 years of rich internet from gathering information on the Open Internet (IPv4). This information allows threat hunters and researchers to understand information about a domain and the relationships the domain has had to other domains on the internet.

Step 3: Search for the domain `www[.]almamaterstore[.]in`

Open a new tab in your web browser go to <https://community.riskiq.com>

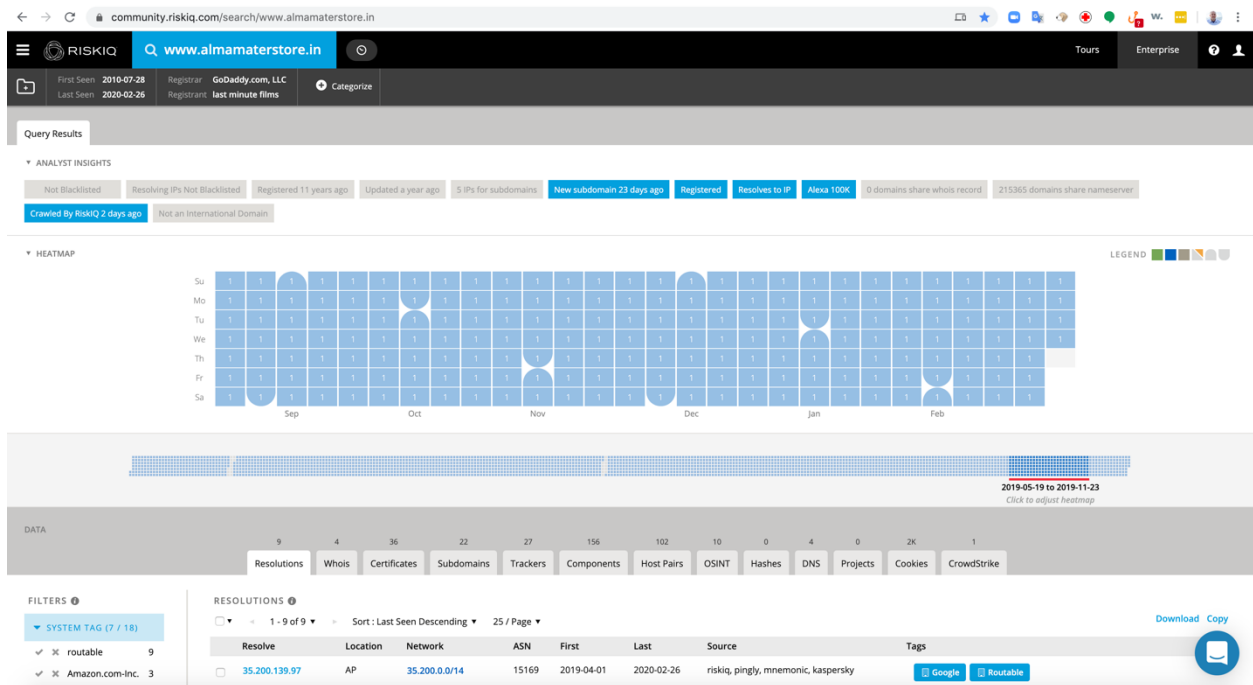
Login using your credentials and begin by searching for `www[.]almamaterstore[.]in`.

<https://community.riskiq.com/search/www.almamaterstore.in>



After your search the URL should be:

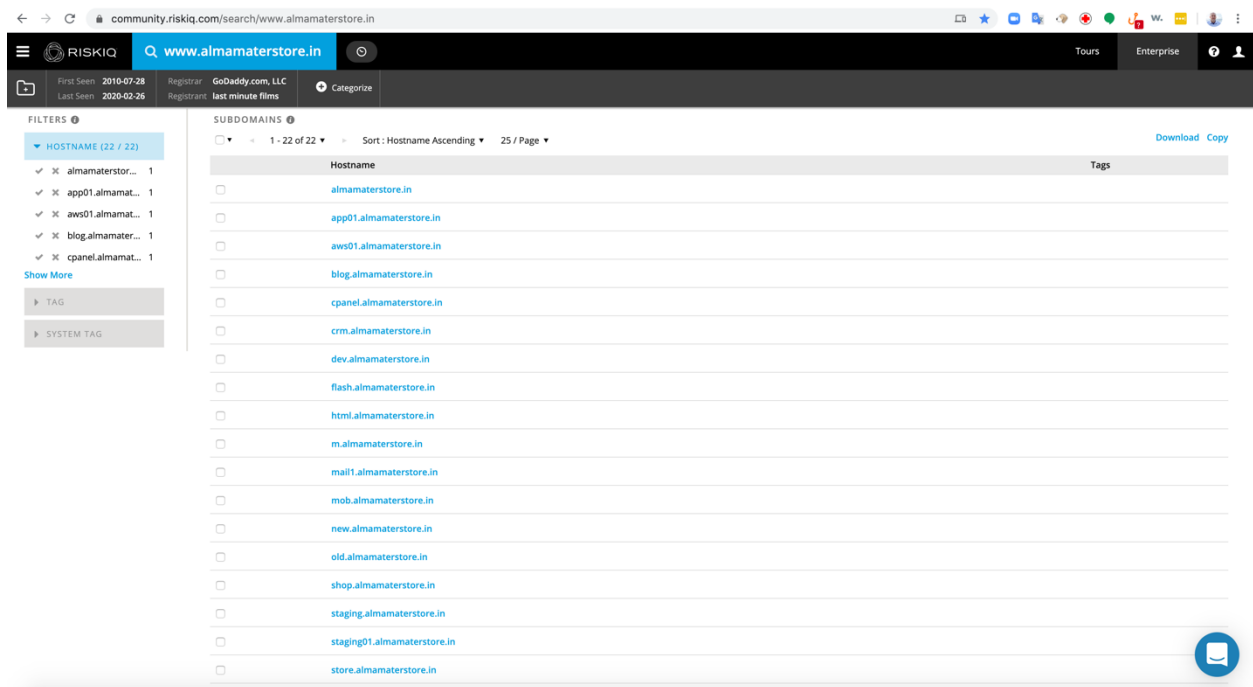
<https://community.riskiq.com/search/www.almamaterstore.in>



The Current IP address is hosted at google. Nothing strange

Step 4: Click on the subdomains tab.

<https://community.riskiq.com/search/www.almamaterstore.in/subdomains>



All of the domains are part of **www[.]almamaterstore[.]in** and do not seem to be unusual and nothing sticks out this point.

Step 5: Click on the Trackers tab.

<https://community.riskiq.com/search/www.almamaterstore.in/trackers>

Hostname	First	Last	Type	Value	Tags
www.almamaterstore.in	2019-06-25	2020-02-24	DocumentBaseHost	www.almamaterstore.in	
www.almamaterstore.in	2018-05-01	2020-02-24	InstagramId	almamaterstore	
www.almamaterstore.in	2012-03-07	2020-02-24	FacebookId	almamaterstore	
www.almamaterstore.in	2017-12-16	2020-02-24	FacebookPixelId	1538473942840080	
www.almamaterstore.in	2019-04-20	2020-02-24	GoogleTagManagerId	gtm-wsl637z	
www.almamaterstore.in	2019-06-25	2020-02-24	DocumentBaseUrl	https://www.almamaterstore.in/	
www.almamaterstore.in	2012-03-07	2020-02-24	GoogleAnalyticsAccountNumber	ua-25508277	
www.almamaterstore.in	2012-03-07	2020-02-24	GoogleAnalyticsTrackingId	ua-25508277-1	
www.almamaterstore.in	2019-04-05	2020-02-24	GoogleTagManagerId	gtm-5jqr5sz	
www.almamaterstore.in	2019-11-18	2020-02-24	YouTubeChannel	uc0mr-ijq	
www.almamaterstore.in	2020-01-13	2020-02-24	HotjarId	1579854	
www.almamaterstore.in	2017-11-14	2020-02-24	FacebookId	1538473942840080	
www.almamaterstore.in	2019-08-10	2020-02-15	DocumentBaseHost	www.googleadservices.com	
www.almamaterstore.in	2019-04-27	2020-01-15	AddThisPubId	ra-515eeaf54693130e	
www.almamaterstore.in	2012-03-07	2019-11-18	TwitterId	almamaterstore	
www.almamaterstore.in	2019-11-18	2019-11-18	LinkedInId	alma-mater-store	
www.almamaterstore.in	2019-04-05	2019-09-29	YouTubeChannel	ucjshifd0hrkhw5xtd_illcw	
www.almamaterstore.in	2019-04-09	2019-06-05	BitlyId	getsizebug1	

Look for trackers like MarkOfTheWeb or TorHiddenServiceAddress that are usually associated with threat actor activity. MarkOfTheWeb is created when someone duplicates your website using Internet Explorer. This is usually associated with phishing attacks. TorHiddenServiceAddress is associated with Tor exit nodes that bridge the open internet and the darkweb.

The trackers results listed do not show anything unusual.

Step 6: Click on the Components tab

<https://community.riskiq.com/search/www.almamaterstore.in/components>

Payment Card Skimmer Investigation

community.riskiq.com/search/www.almamaterstore.in

RISKIQ **www.almamaterstore.in** Tours Enterprise

First Seen 2010-07-28 Registrar GoDaddy.com, LLC
Last Seen 2020-02-26 Registrant last minute films

DATA

9 Resolutions 4 Whois 36 Certificates 22 Subdomains 27 Trackers 156 Components 102 Host Pairs 10 OSINT 4 Hashes 0 DNS 0 Projects 2K Cookies 1 CrowdStrike

FILTERS

TYPE (10 / 126)

- Tracking Pixel 53
- JavaScript Libr... 30
- Analytics Service 8
- CDN 7
- Ad Exchange 6

Show More

HOSTNAME (1 / 156)

- www.almam... 156

NAME (10 / 32)

- jQuery 7
- PHP 5
- Facebook 3
- Font Awesome 3
- Google 3

Show More

COMPONENTS

1 - 156 of 156 Sort: Last Seen Descending 250 / Page

Hostname	First	Last	Category	Value	Tags
www.almamaterstore.in	2019-04-04	2020-02-24	Operating System	Ubuntu	
www.almamaterstore.in	April 4th 2019, 2:09:08 am	2020-02-24	Server	nginx (v1.14.0)	
www.almamaterstore.in	2019-04-04	2020-02-24	Hosting Provider	Google Cloud	
www.almamaterstore.in	2019-04-05	2020-02-24	JavaScript Library	Bootstrap (v3.3.5)	
www.almamaterstore.in	2015-12-01	2020-02-24	Ad Network	Google	
www.almamaterstore.in	2013-11-27	2020-02-24	Ad Exchange	Google Ads - DoubleClick	
www.almamaterstore.in	2019-04-05	2020-02-24	JavaScript Library	Swiper (v3.4.2)	
www.almamaterstore.in	2015-11-20	2020-02-24	Tracking Pixel	Google Analytics	
www.almamaterstore.in	2020-01-13	2020-02-24	Tracking Pixel	q. quora.com	
www.almamaterstore.in	2013-11-27	2020-02-24	Ad Exchange	Facebook	
www.almamaterstore.in	2018-12-09	2020-02-24	JavaScript Library	mustache.js (v0.8.1)	
www.almamaterstore.in	2019-04-20	2020-02-24	Customer Engagement	ZenDesk Chat	
www.almamaterstore.in	2018-06-30	2020-02-24	Analytics Service	Google Tag Manager	
www.almamaterstore.in	2018-08-13	2020-02-24	Tag Mgmt	Google Tag Manager	
www.almamaterstore.in	2016-12-24	2020-02-24	Tracking Pixel	Facebook Pixel	
www.almamaterstore.in	2015-12-20	2020-02-24	Tracking Pixel	Facebook	

There are over 100 results, expand the number of results to 250 by clicking on Show: 25 and then clicking on 250.

community.riskiq.com/search/www.almamaterstore.in

RISKIQ **www.almamaterstore.in**

First Seen 2010-07-28 Registrar GoDaddy.com, LLC
Last Seen 2020-02-26 Registrant last minute films

DATA

9 Resolutions 4 Whois 36 Certificates 22 Subdomains 27 Trackers 156 Components

FILTERS

TYPE (10 / 126)

- Tracking Pixel 53
- JavaScript Libr... 30
- Analytics Service 8
- CDN 7
- Ad Exchange 6

Show More

HOSTNAME (1 / 156)

COMPONENTS

1 - 156 of 156 Sort: Last Seen Descending 250 / Page

Hostname	First	Last
www.almamaterstore.in	2019-04-04	2020-02-24
www.almamaterstore.in	2019-04-04	2020-02-24
www.almamaterstore.in	2019-04-05	2020-02-24
www.almamaterstore.in	2019-04-05	2020-02-24
www.almamaterstore.in	2015-12-01	2020-02-24

Hostname	First	Last	Category	Value	Tags
www.flowerexplosion.com	2019-09-10	2019-09-10	Online Videos	YouTube	
www.flowerexplosion.com	2019-09-10	2019-09-10	JavaScript Library	WordPress Emoji (v5.2.2)	
www.flowerexplosion.com	2019-09-10	2019-09-10	CMS	WordPress (v5.2.2)	
www.flowerexplosion.com	2019-09-10	2019-09-10	JavaScript Library	WordPress Embeds (v5.2.2)	
www.flowerexplosion.com	2019-07-05	2019-09-17	Server	Cloudflare	
www.flowerexplosion.com	2019-05-02	2019-09-17	Customer Engagement	ZenDesk Chat	
www.flowerexplosion.com	2019-02-07	2019-02-07	Tracking Pixel	www.google.es	
www.flowerexplosion.com	2018-12-31	2019-09-17	JavaScript Library	Bootstrap (v3.3.1)	
www.flowerexplosion.com	2018-11-10	2018-11-10	WordPress Plugin	Akismet Anti-Spam	
www.flowerexplosion.com	2018-11-10	2019-09-10	WordPress Plugin	Instagram Feed	
www.flowerexplosion.com	2018-11-10	2019-09-10	Development Tool	AddToAny	
www.flowerexplosion.com	2018-11-10	2019-09-10	WordPress Plugin	AddToAny Share Buttons	
www.flowerexplosion.com	2018-11-10	2019-09-10	Sharing	Lockers Share	
www.flowerexplosion.com	2018-11-10	2019-09-10	CDN	Bootstrap CDN	
www.flowerexplosion.com	2018-11-10	2019-09-10	Web Design	Font Awesome (v4.7.0)	
www.flowerexplosion.com	2018-11-10	2018-11-10	Publisher	Instagram	
www.flowerexplosion.com	2018-11-10	2018-11-10	CMS	WordPress (v4.9.8)	
www.flowerexplosion.com	2018-08-13	2019-08-29	Tracking Pixel	hi.hellobar.com	
www.flowerexplosion.com	2018-08-10	2019-09-17	JavaScript Library	Credit Card Validation JavaScript	
www.flowerexplosion.com	2018-06-23	2018-06-23	CDN	Google Hosted Libraries	
www.flowerexplosion.com	2018-06-23	2018-06-23	JavaScript Library	jQuery (v1.8.0)	

We can see that jQuery v2.1.1, ZenDesk Chat. Nothing unusual listed. But some of the entries might be contain vulnerabilities. We will come back to investigate if vulnerabilities exist a little later.

Step 7: Investigate the JavaScripts used on www[.]almamaterstore[.]in.

Now some information about payment card skimmers and identified one of the most popular skimmers as Magecart. We now have a potential avenue of attack via a malicious JavaScripts. We will now need to examine the JavaScripts used on your website to see if you can identify a potential JavaScript that needs to be further investigate. RiskIQ PassiveTotal will not display contents of the JavaScripts it has detected it will only identify the sources where the JavaScripts came from. RiskIQ has other modules and solutions that can monitor and alert organizations to changes in JavaScripts or Malicious code contained in JavaScripts.

To start our JavaScript investigation in PassiveTotal, you need to click on the Host Pairs tab.

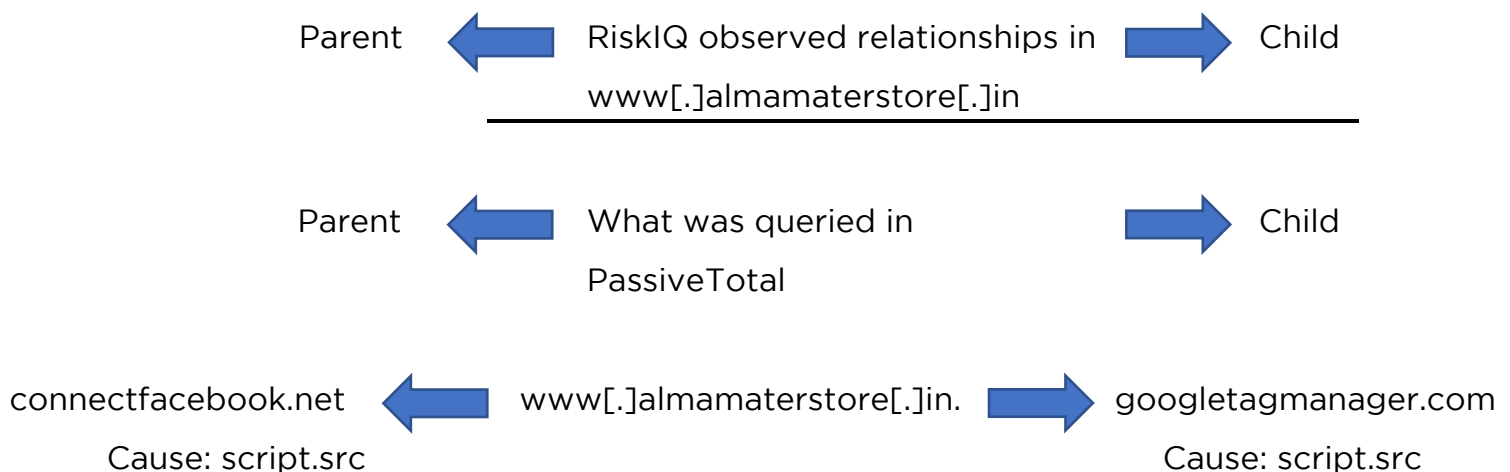
Note:

Host Pairs are the relationship between two websites that were observed during RiskIQ's crawl the website. For example, a website that you visit might be pulling in the logo from Amazon (Parent relationship) or the website might send analytic data to google to track user experience (child relationship).

The connection could range from a top-level redirect (HTTP 302) to something more complex like an iframe or script source reference.

Think of the relationship with regards to what you have searched. In our case we searched for `www[.]almamaterstore[.]in`.

Host Relationships



In our `www[.]almamaterstore[.]in` is going to `connect.facebook.net` and loading a JavaScript. It does not state which JavaScript was loaded, just where it was loaded from. `www[.]almamaterstore[.]in` is also sending information to `www.googtagmanager.com`.

community.riskiq.com/search/www.flowerexplosion.com

RISKIQ www.flowerexplosion.com

First Seen: 2010-07-27 Registrar: GoDaddy.com, LLC
Last Seen: 2019-09-16 Registrant: Domains By Proxy, LLC

Categorize

Resolutions: 14 WHOIS: 9 Certificate: 6 Subdomains: 8 Trackers: 21 Components: 137 Host Pairs: 128 OSINT: 10 Hashes: 1 DNS: 5 Projects: 0 Cookies: 769

FILTERS

DIRECTION

- ✓ parents
- ✓ children

PARENT HOSTNAME (10 / 121)

- ✓ X www.flower... 103
- ✓ X d1nfcmmipia... 5
- ✓ X media.florp... 4
- ✓ X cdn.optimizely... 2
- ✓ X static.addtoan... 2

Show More

CAUSE (10 / 124)

- ✓ X script.src 46
- ✓ X img.src 26
- ✓ X unknown 24
- ✓ X link.href 7
- ✓ X css.import 5

Show More

CHILD HOSTNAME (10 / 48)

- ✓ X www.flower... 26
- ✓ X d10psik18cd... 3
- ✓ X d1nfcmmipia... 3
- ✓ X media.florp... 3
- ✓ X www.google-a... 3

Show More

HOST PAIRS

□ Show: 25 1-25 of 128 Sort: Last Seen Descending

Parent Hostname	Child Hostname	First	Last	Cause	Tags
frame	www.flowerexplosion.com	2018-09-06	2019-09-17	unknown	
www.flowerexplosion.com	c683207.asl.cf2.rackcdn.com	2016-02-07	2019-09-17	img.src	
www.flowerexplosion.com	d1nfcmmipia.d.cloudflare.net	2016-10-30	2019-09-17	img.src	
www.flowerexplosion.com	fonts.gstatic.com	2016-06-30	2019-09-17	css.import	
www.flowerexplosion.com	my.hellobar.com	2017-05-01	2019-09-17	script.src	
www.flowerexplosion.com	www.googleadservices.com	2016-07-15	2019-09-17	script.src	
www.flowerexplosion.com	www.googlecommerce.com	2016-02-07	2019-09-17	script.src	
www.flowerexplosion.com	v2.zopim.com	2016-02-07	2019-09-17	script.src	
www.flowerexplosion.com	bat.bing.com	2016-02-07	2019-09-17	script.src	
www.flowerexplosion.com	114199.tctm.co	2017-10-06	2019-09-17	script.src	
www.flowerexplosion.com	bounceexchange.com	2016-02-07	2019-09-17	script.src	
www.flowerexplosion.com	d10psik18cd9.cloudflare.net	2016-10-29	2019-09-17	script.src	
www.flowerexplosion.com	www.gettagmanager.com	2017-05-29	2019-09-17	script.src	
www.flowerexplosion.com	connect.facebook.net	2016-02-07	2019-09-17	script.src	
www.flowerexplosion.com	cdn.optimizely.com	2016-02-07	2019-09-17	script.src	
www.flowerexplosion.com	d1nfcmmipia.d.cloudflare.net	2016-10-29	2019-09-17	script.src	
www.flowerexplosion.com	www.google-analytics.com	2016-02-07	2019-09-17	script.src	
flowerexplosion.com	www.flowerexplosion.com	2018-05-05	2019-09-17	redirect	
www.flowerexplosion.com	flowerexplosion.com	2018-05-05	2019-09-17	redirect	
www.flowerexplosion.com	fonts.gstatic.com	2019-09-07	2019-09-16	parentPage	
www.flowerexplosion.com	www.flowerexplosion.com	2019-09-07	2019-09-16	parentPage	

Since we are looking just for scripts in the CAUSE filter section on the left click on the check next to script.src. This will filter the results to only show causes in host pairs that were scripts.src.

Show More

CAUSE (10 / 100)			
✓	X	img.src	25
✓	X	script.src	25
✓	X	unknown	25
✓	X	link.href	6
✓	X	redirect	6

Show More

Now sort the results on the screen to First Seen Descending:

HOST PAIRS i

☐ ▼ 1 - 25 of 25 ▼ Sort : First Seen Ascending ▼ 25 / Page ▼

Parent Hostname	First Seen Descending	Child Hostname
<input type="checkbox"/> www.almamaterstore.com	First Seen Ascending	www.google-analyt
<input type="checkbox"/> www.almamaterstore.com	Last Seen Descending	connect.facebook.l
<input type="checkbox"/> www.almamaterstore.com	Last Seen Ascending	a.adroll.com

community.riskiq.com/search/www.flowerexplosion.com

RISKIQ [www.flowerexplosion.com](#) First Seen: 2019-07-27 Last Seen: 2019-09-18 Registrar: GoDaddy.com, LLC Registrant: Demand By Proxy, L...

Resolutions WHOIS Certificate Subdomains Trackers Components Host Pairs OSINT Hashes DNS Projects Cookies

FILTERS

DIRECTION

- ✓ parents
- ✓ children

PARENT HOSTNAME (10 / 121)

- ✓ x [www.flower...](#) 103
- ✓ x [d1nfcmmipia...](#) 5
- ✓ x [media.florp...](#) 4
- ✓ x [cdn.optimizely...](#) 2
- ✓ x [static.addoan...](#) 2

Show More

CAUSE (10 / 124)

- ✓ x [script.src](#) 46
- ✓ x [img.src](#) 26
- ✓ x [unknown](#) 24
- ✓ x [link.href](#) 7
- ✓ x [css.import](#) 5

Show More

CHILD HOSTNAME (10 / 48)

- ✓ x [www.flower...](#) 26
- ✓ x [d10psik18lc...](#) 3
- ✓ x [d1nfcmmipia...](#) 3
- ✓ x [media.florp...](#) 3
- ✓ x [www.google-a...](#) 3

Show More

HOST PAIRS

☐ Show: 25 1-25 of 46 Sort: First Seen Descending

Parent Hostname	Child Hostname	First	Last	Cause	Tags
<input type="checkbox"/> www.flowerexplosion.com	jquery.su	2019-05-23	2019-09-13	script.src	
<input type="checkbox"/> www.flowerexplosion.com	www.shopperapproved.com	2019-01-22	2019-02-13	script.src	
<input type="checkbox"/> www.flowerexplosion.com	kinfrighbetted.host	2018-11-24	2019-01-27	script.src	
<input type="checkbox"/> www.flowerexplosion.com	load.sumo.com	2018-11-10	2019-09-10	script.src	
<input type="checkbox"/> www.flowerexplosion.com	static.addtoany.com	2018-11-10	2019-09-10	script.src	
<input type="checkbox"/> 114109.tctm.co	www.flowerexplosion.com	2018-11-08	2018-11-08	script.src	
<input type="checkbox"/> www.flowerexplosion.com	www.g-static.com	2018-08-10	2019-01-27	script.src	
<input type="checkbox"/> www.flowerexplosion.com	ajax.googleapis.com	2018-06-23	2018-06-23	script.src	
<input type="checkbox"/> www.flowerexplosion.com	ajax.cloudflare.com	2018-05-13	2018-05-13	script.src	
<input type="checkbox"/> www.flowerexplosion.com	stats.wp.com	2018-04-28	2018-04-28	script.src	
<input type="checkbox"/> www.flowerexplosion.com	secure.gravatar.com	2018-04-28	2018-04-28	script.src	
<input type="checkbox"/> www.flowerexplosion.com	s0.wp.com	2018-04-28	2018-04-28	script.src	
<input type="checkbox"/> www.flowerexplosion.com	114109.tctm.co	2017-10-06	2019-09-17	script.src	
<input type="checkbox"/> www.flowerexplosion.com	www.googletagmanager.com	2017-05-29	2019-09-17	script.src	
<input type="checkbox"/> www.flowerexplosion.com	my.hellobar.com	2017-05-01	2019-09-17	script.src	
<input type="checkbox"/> www.flowerexplosion.com	assets.pfcl.co	2017-05-01	2017-11-15	script.src	
<input type="checkbox"/> www.flowerexplosion.com	load.sumome.com	2017-02-11	2018-04-28	script.src	
<input type="checkbox"/> www.flowerexplosion.com	html5shiv.googlecode.com	2017-02-11	2018-04-28	script.src	
<input type="checkbox"/> d1nfcmmipiaw0.cloudfront.net	www.flowerexplosion.com	2017-02-11	2019-09-10	script.src	
<input type="checkbox"/> www.flowerexplosion.com	cs.luckyorange.net	2017-01-28	2017-04-04	script.src	
<input type="checkbox"/> www.flowerexplosion.com	d10psik18lc9.cloudfront.net	2016-10-29	2019-09-17	script.src	

From the list you can see a typosquatted domain.

community.riskiq.com/search/www.almamaterstore.in

RISKIQ

manager.com 2/2

Tours Enterprise

First Seen: 2010-07-28 Last Seen: 2020-02-26 Registrar: GoDaddy.com, LLC last minute films Categorize

CAUSE (10 / 100)	CHILD HOSTNAME (10 / 58)
www.licareerm... 2	
img.src 25	
script.src 25	
unknown 25	
link.href 6	
redirect 6	
www.almamat... 34	
cdn.staticans.co... 4	
www.facebook... 4	
assets.pinterest... 3	
ik.imagekit.io 3	

Source	Target	First Seen	Last Seen	Type
www.almamaterstore.in	www.almamaterstore.in	2016-04-29	2016-11-19	script.src
www.almamaterstore.in	ajax.googleapis.com	2016-05-09	2016-07-18	script.src
www.almamaterstore.in	www.googleadservices.com	2016-12-24	2019-04-09	script.src
www.almamaterstore.in	code.jquery.com	2017-04-11	2018-07-29	script.src
www.almamaterstore.in	platform.twitter.com	2017-05-02	2018-07-26	script.src
www.almamaterstore.in	apis.google.com	2017-05-02	2018-07-15	script.src
www.almamaterstore.in	assets.pinterest.com	2017-05-02	2018-07-26	script.src
connect.facebook.net	www.almamaterstore.in	2017-11-09	2018-05-05	script.src
www.almamaterstore.in	cdn.izooto.com	2018-05-05	2019-04-01	script.src
www.almamaterstore.in	dev.almamaterstore.in	2018-05-08	2018-06-24	script.src
www.almamaterstore.in	www.googletagmanager.com	2018-06-30	2020-02-24	script.src
www.almamaterstore.in	ssl.google-analytics.com	2018-08-06	2019-04-01	script.src
www.almamaterstore.in	app.wigzo.com	2018-08-13	2018-08-20	script.src
www.almamaterstore.in	server.connecto.io	2018-09-04	2020-02-24	script.src
www.almamaterstore.in	ik.imagekit.io	2019-04-05	2020-02-24	script.src
www.almamaterstore.in	cdn.onesignal.com	2019-04-05	2020-02-24	script.src
www.almamaterstore.in	s7.addthis.com	2019-04-27	2020-01-15	script.src
www.almamaterstore.in	googletagmanager.com	2019-08-09	2020-02-24	script.src
www.almamaterstore.in	static.hotjar.com	2020-01-13	2020-02-24	script.src
www.almamaterstore.in	tag.cottonusa.org	2020-01-13	2020-01-15	script.src

1 - 25 of 25

www.googletagmanager.com and googletagmanager[.]com both are active and the typosquatted domain needs to be further investigated.

Now that we have the suspect script what can we do next?

RiskIQ has enterprise products and features that would automatically monitor your websites and alert you to changes in the website's JavaScripts that you directly control or a third-party website you rely upon. But since we are using the RiskIQ Threat Investigation tool PassiveTotal we will have to manually investigate the domain to further understand what it is and if it is associated with malicious activity.

The next steps need to be done cautiously. Since we might be dealing with an active attack could infect your computer by visiting the website directly. It is important to have a safe way to visit the website and to not get compromised during your investigation.

You could just visit the website and view the source and see what is happening but that is really not safe. I will show you a safer way to do the investigation. You can investigate the websites and scripts and to not tip them off.

Step 8: Pivot search on googletegmanager[.]com, right click on googletegmanger[.]com and open it in a new tab.

The screenshot shows a web browser window displaying search results on community.riskiq.com/search/www.almamaterstore.in. The search results are filtered by 'CAUSE (10 / 100)' and 'CHILD HOSTNAME (10 / 58)'. A right-click context menu is open over the link 'googletegmanager.com' in the search results. The menu options include 'Open Link in New Tab', 'Open Link in New Window', 'Open Link in Incognito Window', 'Send Link to Benjamin', 'Save Link As...', 'Copy Link Address', 'Copy', 'Go to googletegmanager.com', 'Print...', 'Blockade', 'FatBeagle', 'Google Translate', 'LastPass', 'Inspect', 'Speech', and 'Services'. The search results table shows various domains and their associated scripts.

Domain	Script	First Seen	Last Seen	Script Type
www.almamaterstore.in	www.googleadservices.com	2016-12-24	2019-04-09	script.src
www.almamaterstore.in	code.jquery.com	2017-04-11	2018-07-29	script.src
www.almamaterstore.in	platform.twitter.com	2017-05-02	2018-07-26	script.src
www.almamaterstore.in	apis.google.com	2017-05-02	2018-07-15	script.src
www.almamaterstore.in	assets.pinterest.com	2017-05-02	2018-07-26	script.src
connect.facebook.net	www.almamaterstore.in	2017-11-09	2018-05-05	script.src
www.almamaterstore.in	cdn.izooto.com	2018-05-05	2019-04-01	script.src
www.almamaterstore.in	dev.almamaterstore.in	2018-05-08	2018-06-24	script.src
www.almamaterstore.in	www.googletegmanager.com	2018-06-30	2020-02-24	script.src
www.almamaterstore.in	ssl.google-analytics.com	2018-08-06	2019-04-01	script.src
www.almamaterstore.in	app.wigrow.com	2018-08-13	2018-08-20	script.src
www.almamaterstore.in	server.com	2018-09-04	2020-02-24	script.src
www.almamaterstore.in	ik.imagekit.io	2019-04-05	2020-02-24	script.src
www.almamaterstore.in	cdn.onesig	2019-04-05	2020-02-24	script.src
www.almamaterstore.in	s7.addthis.com	2019-04-27	2020-01-15	script.src
www.almamaterstore.in	googletegmanager.com	2019-08-09	2020-02-24	script.src
www.almamaterstore.in	static.hotjar.com	2020-01-13	2020-02-24	script.src
www.almamaterstore.in	tag.cotton.com	2020-01-13	2020-01-15	script.src

<https://community.riskiq.com/search/googletegmanager.com>

The location information on the Resolutions tab shows IP addresses from the Russian Federation. This is a little bit of a warning that it might not be a legitimate google domain.

Step 9: Click on the WHOIS tab.

<https://community.riskiq.com/search/googletegmanager.com/whois>

The screenshot shows the RiskIQ community search interface. The search results for **googletegmanger.com** are displayed. The top navigation bar includes the RiskIQ logo, search bar, and user profile. Below the search bar, there are tabs for Records (4), Emails (3), Registrars (2), Name Servers (11), Phone Numbers (3), and Organization (2). The main content area is titled **WHOIS RECORDS** and shows a table of changes over time. The most recent record is from 2019-04-04, showing the domain was updated. The table lists attributes such as WHOIS Server, Registrar, Email, Name, Organization, Street, City, and State, along with their values and the registrant's role (registrant, admin, tech). To the right of the table, there is a detailed WHOIS record for **GOOGLETEGMANGER.COM**, including the domain name, ID, registrar, creation date, expiration date, and various status codes. A notice at the bottom of the WHOIS record states: "NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration."

We see that the domain is registered to **smrimur@yandex[.]ru** not to a google domain. This is a red flag as well.

<https://community.riskiq.com/search/whois/email/smrimur@yandex.ru>

Step 10: SSL Certificates tab for googletegmanger[.]com.

Click on the Certificate tab and expand the SHA-1 results to identify where the certificate came from.

<https://community.riskiq.com/search/googletegmanger.com/domaincertificates>

The screenshot shows the RiskIQ search interface for the domain **googletegmanger.com**. The search results are filtered by **CERTIFICATES**. The main table displays the following data:

SHA-1	First Seen	Last Seen	Infrastructure
3deca3b851e3ccb7d5004d7b903b16e91d7c386	2020-01-13	2020-02-24	
CERTIFICATE DETAILS: Issued: 2019-12-11 Expires: 2020-03-10 Serial Number: 271722178714016001851935662716344085795470 SSL Version: 3 Common Name: Let's Encrypt Authority X3 (issuer) googletegmanger.com (subject) Alternative Names: googletegmanger.com (subject), www.googletegmanger.com (subject) Organization Name: Let's Encrypt (issuer) Organization Unit: Street Address: Locality: State/Province: Country: US (issuer)			
82c47798690aa50b22d807b59544132c82f83586	2019-12-15	2020-01-19	91.134.122.252
cd5bc8565020aeb384d2c2e954eac9993cb96ae	2019-12-11	2019-12-13	-
60eeca54a268d166a3c8c39099bcb1ef3c877630	2019-12-10	2019-12-12	-
517eb808305490a9f7f3ca7b5271cea1d6e9229f	2019-12-11	2019-12-11	-

The results show that the domain **googletegmanger.com** is utilizing free let's Encrypt SSL certificates. This is common item we see with threat actors.

We see a free Let's Encrypt certificate. This is another indicator this is a malicious or fraudulent website. Google would not be using free SSL certificates for its infrastructure.

The screenshot shows the RiskIQ search interface for the domain **googletegmanger.com**. The search results are filtered by **SUBDOMAINS**. The main table displays the following data:

Subdomains	First Seen	Last Seen	Infrastructure
googletegmanger.com	2019-04-03	2020-03-30	
www.googletegmanger.com	2019-04-03	2020-03-30	

Below the table, there is a **HEATMAP** visualization showing the frequency of subdomain activity over time, with a legend indicating the color scale for activity levels.

Step 11: Googletegmanager[.]com subdomain tab

<https://community.riskiq.com/search/googletegmanager.com/subdomains>

Each of the subdomains could have completely different infrastructure associated with it. We will investigate this later in a different use case.

The screenshot shows the RiskIQ community search interface. The search query is "googletegmanager.com". The results are displayed under the "Subdomains" tab. The interface includes a header with the RiskIQ logo and search bar, a sidebar with filters, and a main content area showing the search results. The results table lists two subdomains: "googletegmanager.com" and "www.googletegmanager.com".

Hostname	Tags
googletegmanager.com	
www.googletegmanager.com	

One other subdomain is list `www[.]googletegmanager[.]com`.

Step 12: Click on the Components tab

<https://community.riskiq.com/search/googletegmanager.com/components>

community.riskiq.com/search/googletgmanager.com

First Seen: 2017-11-29, Last Seen: 2020-02-26, Registrar: URL Solutions, Inc., Registrant: Private Person, Categorize

2019-08-17 to 2020-02-26

DATA: Resolutions (4), Whois (4), Certificates (15), Subdomains (2), Trackers (0), Components (7), Host Pairs (14), OSINT (4), Hashes (1), DNS (13), Projects (3), Cookies (0), CrowdStrike (1)

FILTERS: TYPE (4 / 7): Server Module (3), Framework (2), Operating System (1), Server (1); HOSTNAME (1 / 7): googletgmanager.com (7); NAME (5 / 7): PHP (3), Apache (1), CentOS (1), OpenSSL (1), mod_fcgid (1)

COMPONENTS: 1 - 7 of 7, Sort: Last Seen Descending, 25 / Page

Hostname	First	Last	Category	Value	Tags
googletgmanager.com	2019-04-23	2020-02-24	Server Module	mod_fcgid (v2.3.9)	
googletgmanager.com	2019-04-23	2020-02-24	Server Module	OpenSSL (v1.0.2k-fips)	
googletgmanager.com	2019-04-23	2020-02-24	Operating System	CentOS	
googletgmanager.com	2019-04-23	2020-02-24	Server Module	PHP (v7.0.31)	
googletgmanager.com	2019-04-23	2020-02-24	Framework	PHP (v7.0.31)	
googletgmanager.com	2019-04-23	2020-02-24	Server	Apache (v2.4.6)	
googletgmanager.com	2019-06-05	2020-02-20	Framework	PHP	

5.475.0 © 2020 RiskIQ Inc. All Rights Reserved. Proprietary and confidential; do not distribute without prior approval. Privacy Policy Terms and Conditions

We see a very lean components list. Threat actors do not usually stand up components they do not utilize. We can see they this domain utilizes CentOS, PHP, and Apache.

Step 13: Click on the Host Pairs tab

<https://community.riskiq.com/search/googletgmanager.com/hostpairs>

community.riskiq.com/search/googletegmanager.com

First Seen: 2017-11-29, Last Seen: 2020-02-26, Registrant: URL Solutions, Inc., Private Person

2019-08-17 to 2020-02-26

DATA: 4 Resolutions, 4 Whois, 15 Certificates, 2 Subdomains, 0 Trackers, 7 Components, 14 Host Pairs, 4 OSINT, 1 Hashes, 13 DNS, 3 Projects, 0 Cookies, 1 CrowdStrike

FILTERS: TYPE (4 / 7), HOSTNAME (1 / 7), NAME (5 / 7)

COMPONENTS: 1-7 of 7, Sort: Last Seen Descending, 25 / Page

Hostname	First	Last	Category	Value	Tags
googletegmanager.com	2019-04-23	2020-02-24	Server Module	mod_fcgid (v2.3.9)	
googletegmanager.com	2019-04-23	2020-02-24	Server Module	OpenSSL (v1.0.2k-fips)	
googletegmanager.com	2019-04-23	2020-02-24	Operating System	CentOS	
googletegmanager.com	2019-04-23	2020-02-24	Server Module	PHP (v7.0.31)	
googletegmanager.com	2019-04-23	2020-02-24	Framework	PHP (v7.0.31)	
googletegmanager.com	2019-04-23	2020-02-24	Server	Apache (v2.4.6)	
googletegmanager.com	2019-06-05	2020-02-20	Framework	PHP	

5.475.0 © 2020, RiskIQ Inc. All Rights Reserved. Proprietary and confidential; do not distribute without prior approval. Privacy Policy Terms and Conditions

The results show us all of the domains that are going to googletegmanager[.]com and running JavaScripts. From the names listed most appear to be online retailers. If googletegmanager[.]com is determined to be malicious all of these domains might also be compromised.

Step 14: Click on the Resolutions tab

Right click on the IP address 92[.]63[.]192[.]191 and open it in a new tab.

<https://community.riskiq.com/search/92.63.192.191>

community.riskiq.com/search/92.63.192.191

First Seen: 2017-11-29, Last Seen: 2020-02-26, Registrant: URL Solutions, Inc., Private Person

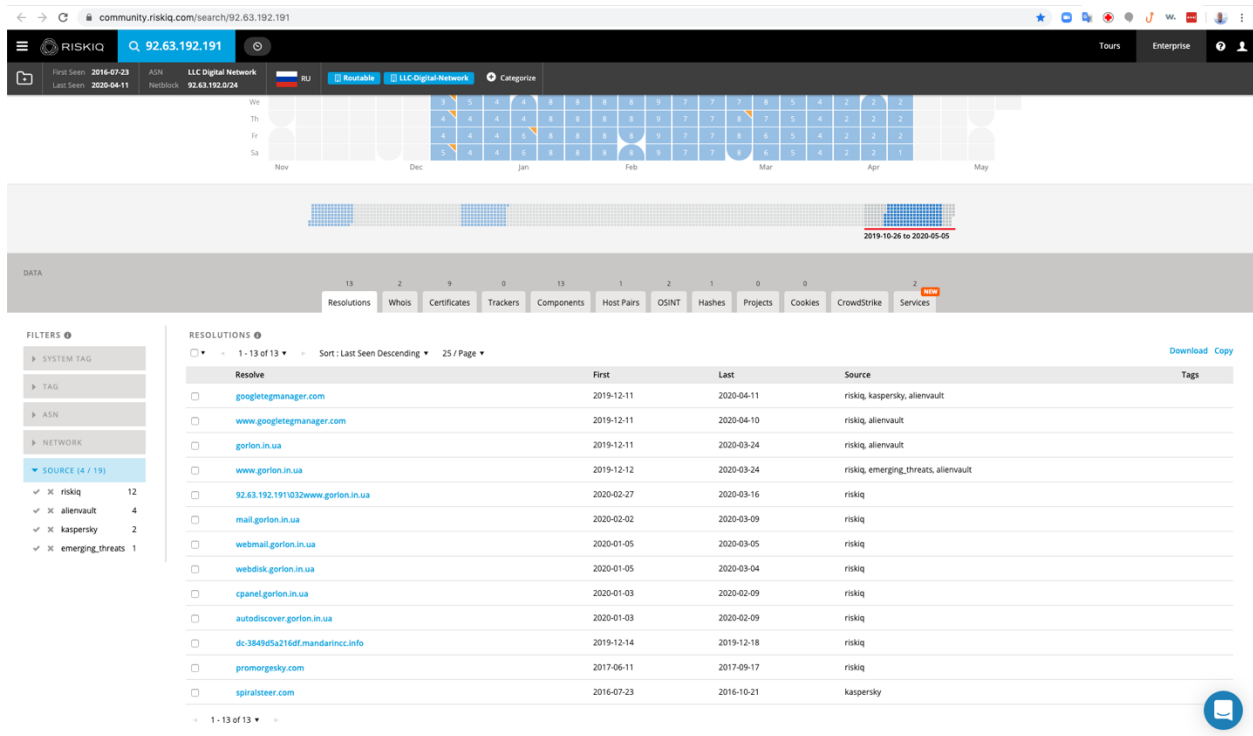
DATA: 4 Resolutions, 4 Whois, 15 Certificates, 2 Subdomains, 0 Trackers, 7 Components, 14 Host Pairs, 4 OSINT, 1 Hashes, 13 DNS, 3 Projects, 0 Cookies, 1 CrowdStrike

FILTERS: SYSTEM TAB (4 / 7), ASN (2 / 2), NETWORK (4 / 4), SOURCE (4 / 10)

RESOLUTIONS: 1-4 of 4, Sort: Last Seen Descending, 25 / Page

Resolve	Location	Network	ASN
92.63.192.191	Ch...	as-92-63-192-024	47081
92.63.192.191	Open Link in New Window	as-92-63-192-024	47081
92.63.192.191	Open Link in Incognito Window	as-92-63-192-024	47081
92.63.192.191	Send Link to Benjamin	as-92-63-192-024	47081
92.63.192.191	Copy Link Address	as-92-63-192-024	47081

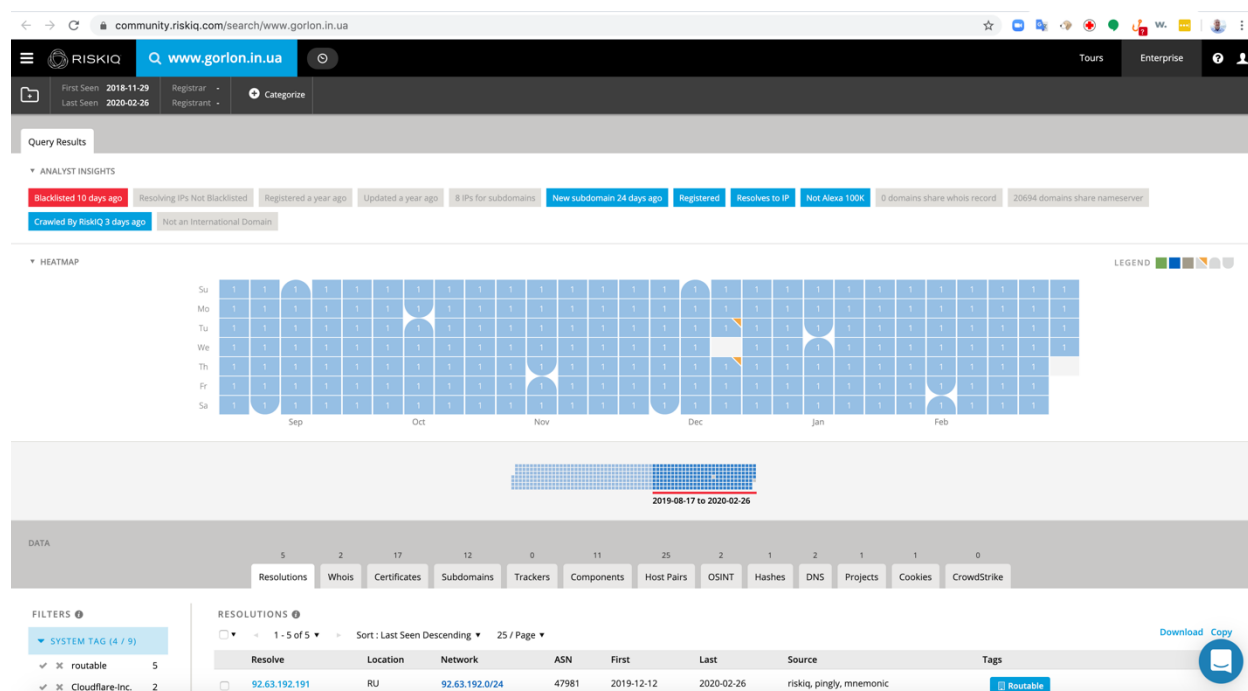
Right-click context menu options: Copy, Open Link in New Window, Open Link in Incognito Window, Send Link to Benjamin, Copy Link Address, Blockade, Pathhaggle, Google Translate, LastPass, Inspect, Speech, Services.



The results show 12 new domains that have used this IP address over time.

Step 15: Right click and open `www[.]golon[.]in[.]au` in a new tab.

<https://community.riskiq.com/search/gorlon.in.ua>



We can immediately see that the domain was blacklist 10 days ago. This related infrastructure is showing that the googletegmanager[.]com domain is associated with known malicious or fraudulent infrastructure.

Step 17: Crawl the website www[.]almamaterstore[.]in utilizing urlscan.io

We are now going to use a tool to visit and crawl the website www[.]almamaterstore[.]in.

This is a safe way to investigate a website's content without directly going to the website. You can just view the results from the web crawl and understand what is happening. This will prevent your computer from potentially getting compromised and potentially tipping off the threat actor that you are investigating them.

In a new tab open the website <https://urlscan.io>

Search for www[.]almamaterstore[.]in

The screenshot shows the urlscan.io homepage. At the top, there's a navigation bar with links for Home, Search, API, Live, About, and Login. A search bar contains the URL "www.almamaterstore.in". Below the search bar, there's a "Public Scan" button and an "Options" button. A "Recent scans" section displays a table of recent scans with columns for URL, Submitted time, Size, and IP addresses. The table lists various URLs, including "miaroba.com/", "info.x1.com/UnsubscribePage.html", "chouitar.nl/vw8Ym50lB81&subid2=wg100g8adcro71gm39ga4", "www.x1.com/error.html", "americancapitalone.com/", "chestyl.com/suntrust/login.online-banking.suntrust.com/SunTrust/1/1.html?%3C?ph...", "www.vakantievelingen.nl/producten.html?utm_source=selligent&utm_medium=email&...", "eu1-us1.cckdnassets.com/448/creatives/33077/hyrestore-start.jpg?platform=hoots...", "www.x1.com/error.html", and "ww1.walmarcapitalone.com/?sub1=2eb03d38-58f8-11ea-9614-bc2ca8556ef0".

URL	Submitted	Size	IPs
miaroba.com/	36 seconds ago	3 MB	139 37 7
info.x1.com/UnsubscribePage.html?mkt_tok=eyJpIjoiWkRnNU9XUTR...	37 seconds ago	66 KB	16 5 3
chouitar.nl/vw8Ym50lB81&subid2=wg100g8adcro71gm39ga4	38 seconds ago	244 KB	2 3 3
www.x1.com/error.html	38 seconds ago	720 KB	50 24 6
americancapitalone.com/	40 seconds ago	12 KB	2 1 1
chestyl.com/suntrust/login.online-banking.suntrust.com/SunTrust/1/1.html?%3C?ph...	41 seconds ago	1 MB	66 10 7
www.vakantievelingen.nl/producten.html?utm_source=selligent&utm_medium=email&...	41 seconds ago	1 MB	38 12 4
eu1-us1.cckdnassets.com/448/creatives/33077/hyrestore-start.jpg?platform=hoots...	44 seconds ago	65 KB	1 1 1
www.x1.com/error.html	45 seconds ago	719 KB	50 24 5
ww1.walmarcapitalone.com/?sub1=2eb03d38-58f8-11ea-9614-bc2ca8556ef0	45 seconds ago	104 KB	8 4 2

21982077 public scans - 45909605 in total

Thanks to our sponsors

SecurityTrails Tines

Step 18: Review the results

<https://urlscan.io/result/2b115d7c-95a8-422b-b00d-76aee0733ef1>

The screenshot shows the urlscan.io result page for the URL "www.almamaterstore.in". The page displays the submitted URL, effective URL, and submission details. A "Summary" section provides information about the website's IP addresses, domains, and transactions. A "Screenshot" section shows a live screenshot of the website. A "Detected technologies" section lists various technologies used on the website, including Ubuntu, Bootstrap, Nginx, Mustache, Zendesk Chat, Facebook, Font Awesome, Google Analytics, and Google Analytics Enhanced eCommerce.

Summary

This website contacted 23 IPs in 8 countries across 22 domains to perform 137 HTTP transactions. The main IP is 35.200.139.97, located in Ascension Island and belongs to GOOGLE, US. The main domain is www.almamaterstore.in. TLS certificate: Issued by Let's Encrypt Authority X3 on January 28th 2020. Valid for: 3 months.

The main domain was scanned 11 times on urlscan.io

1782 structurally similar pages on different IPs, domains and ASNs found

Verdict: No classification

Google Safe Browsing: Clean (Current Classification)

Additional live information

Current DNS A record: 35.200.139.97 (AS15169 - GOOGLE, US)

Domain & IP information

IP/ASNs	IP Detail	(Sub)Domains	Domain Tree	Links	Certificates
1 → 69	35.200.139.97	15169 (GOOGLE)	AS Autonomous System		
2	2a00:1450:4001:81a::200a	15169 (GOOGLE)			

Screenshot

THIS SUMMER! CUSTOMER TEES FOR YOUR TEAM. CUSTOM DESIGNED TEES. ORDER 10 AT ₹299/- EACH. SHOP NOW

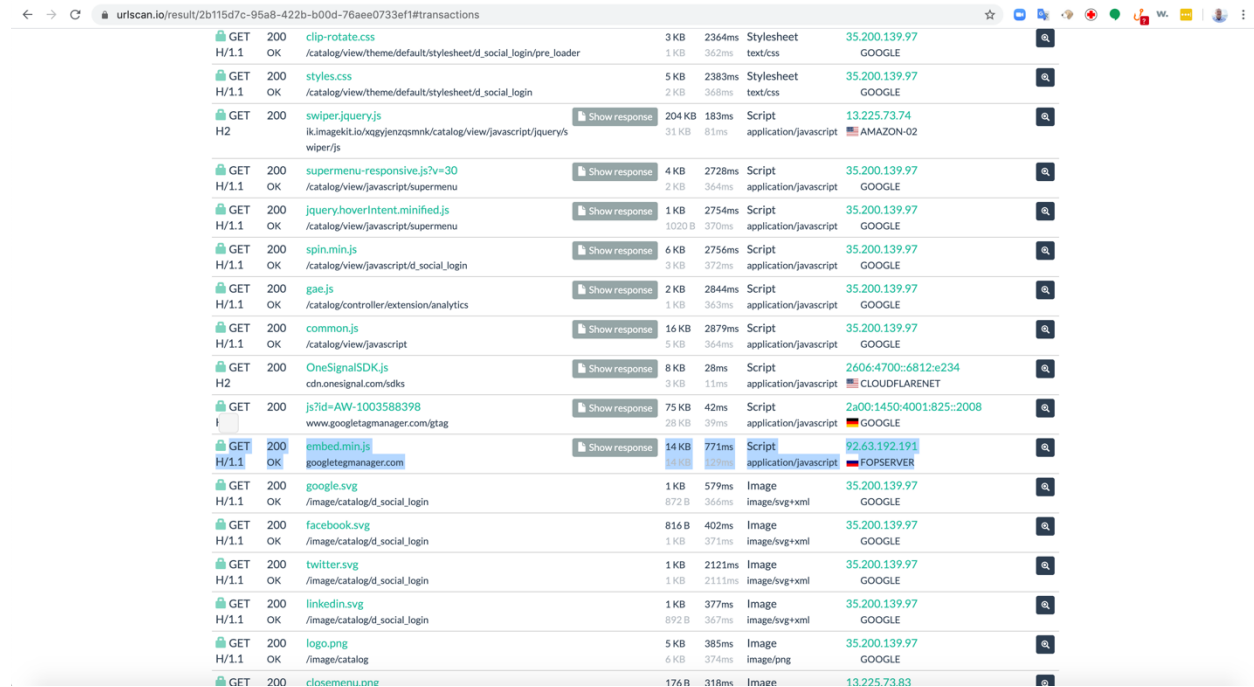
Detected technologies

- Ubuntu (Operating Systems) → Website
- Bootstrap (Web Frameworks) → Website
- Nginx (Web Servers) → Website
- Mustache (JavaScript Frameworks) → Website
- Zendesk Chat (Live Chat) → Website
- Facebook (Widgets) → Website
- Font Awesome (Font Scripts) → Website
- Google Analytics (Analytics) → Website
- Google Analytics Enhanced eCommerce (Analytics) → Website
- Google Font API (Font Scripts) → Website

We see an image of the website and all of the collected information.

Click on the HTTP tab.

Scroll down until you see the entry for googletagmanager[.]com



Method	Status	URL	Size	Time	Content Type	IP Address	Organization	Action
GET	200	clip-rotate.css	3 KB	2364ms	Stylesheet	35.200.139.97	GOOGLE	
H/1.1	OK	/catalog/view/theme/default/stylesheet/d_social_login/pre_loader	1 KB	362ms	text/css	35.200.139.97	GOOGLE	
GET	200	styles.css	5 KB	2383ms	Stylesheet	35.200.139.97	GOOGLE	
H/1.1	OK	/catalog/view/theme/default/stylesheet/d_social_login	2 KB	368ms	text/css	35.200.139.97	GOOGLE	
GET	200	swiper.jquery.js	204 KB	183ms	Script	13.225.73.74	AMAZON-02	
H2	OK	ik.imagekit.io/xggyjenzqmkn/catalog/view/javascript/jquery/swiper.js	31 KB	81ms	application/javascript	13.225.73.74	AMAZON-02	
GET	200	supermenu-responsive.js?v=30	4 KB	2728ms	Script	35.200.139.97	GOOGLE	
H/1.1	OK	/catalog/view/javascript/supermenu	2 KB	364ms	application/javascript	35.200.139.97	GOOGLE	
GET	200	jquery.hoverIntent.minified.js	1 KB	2754ms	Script	35.200.139.97	GOOGLE	
H/1.1	OK	/catalog/view/javascript/supermenu	1020 B	370ms	application/javascript	35.200.139.97	GOOGLE	
GET	200	spin.min.js	6 KB	2756ms	Script	35.200.139.97	GOOGLE	
H/1.1	OK	/catalog/view/javascript/d_social_login	3 KB	372ms	application/javascript	35.200.139.97	GOOGLE	
GET	200	gae.js	2 KB	2844ms	Script	35.200.139.97	GOOGLE	
H/1.1	OK	/catalog/controller/extension/analytics	1 KB	363ms	application/javascript	35.200.139.97	GOOGLE	
GET	200	common.js	16 KB	2879ms	Script	35.200.139.97	GOOGLE	
H/1.1	OK	/catalog/view/javascript	5 KB	364ms	application/javascript	35.200.139.97	GOOGLE	
GET	200	OneSignalSDK.js	8 KB	28ms	Script	2606:4700:6812:e234	CLOUDFLARENET	
H2	OK	cdn.onesignal.com/sdks	3 KB	11ms	application/javascript	2606:4700:6812:e234	CLOUDFLARENET	
GET	200	js?id=AW-1003588398	75 KB	42ms	Script	2a00:1450:4001:825::2008	GOOGLE	
I	OK	www.googletagmanager.com/itag	28 KB	39ms	application/javascript	2a00:1450:4001:825::2008	GOOGLE	
GET	200	embed.min.js	14 KB	771ms	Script	92.63.192.191	FOPSERVER	Show response
H/1.1	OK	googletagmanager.com	1.4 KB	371ms	application/javascript	92.63.192.191	FOPSERVER	
GET	200	google.svg	1 KB	579ms	Image	35.200.139.97	GOOGLE	
H/1.1	OK	/image/catalog/d_social_login	872 B	366ms	image/svg+xml	35.200.139.97	GOOGLE	
GET	200	facebook.svg	816 B	402ms	Image	35.200.139.97	GOOGLE	
H/1.1	OK	/image/catalog/d_social_login	1 KB	371ms	image/svg+xml	35.200.139.97	GOOGLE	
GET	200	twitter.svg	1 KB	2121ms	Image	35.200.139.97	GOOGLE	
H/1.1	OK	/image/catalog/d_social_login	1 KB	2111ms	image/svg+xml	35.200.139.97	GOOGLE	
GET	200	linkedin.svg	1 KB	377ms	Image	35.200.139.97	GOOGLE	
H/1.1	OK	/image/catalog/d_social_login	892 B	367ms	image/svg+xml	35.200.139.97	GOOGLE	
GET	200	logo.png	5 KB	385ms	Image	35.200.139.97	GOOGLE	
H/1.1	OK	/image/catalog	6 KB	374ms	image/png	35.200.139.97	GOOGLE	
GET	200	closemenu.one	176 B	318ms	Image	13.225.73.83		

Click on show response button

Searched domain	child relationship	Frist Seen	Last Seen	cause
<input type="checkbox"/> www.almamaterstore.in	www.googletagmanager.com	2018-06-30	2020-02-24	script.src

Note: RiskIQ has notified this domain over the years about being infected with Magecart and they have never cleaned up their domain.

Conclusion:

While investigating it is best to utilize tools that safeguard your systems from possible compromised and limiting the threat actor from finding out you are investigating them.

PassiveTotal was able to show that a script was modified in late June of 2018. By examining the DOM from `www[.]almamaterstore[.]in` (using <https://urlscan.io>) we were able to determine exactly what script the web site was calling from `googletegmanager[.]com`.

But to prevent future compromises we needed to determine the vulnerabilities that exist on the web site so it can be patched or upgraded to prevent malicious code from being inserted back on the website.

We hope you enjoyed this use case and share it with your friends and colleagues.