

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

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

The URL should now be:

https://transparencyreport.google.com/safebrowsing/search?url=www.almamaterstore.in&hl=en

← → C (â transparencyrepo	rt.google.com/safe-browsing/search?url=www.almamaterstore.in&hl=en	□ ★ □ N	 👍 w. 😑	1 1
	ncy Report			
Overview Malware Site sta	tus			
	Safe Browsing site status			
	Google's Safe Browsing technology examines billions of URLs par day looking for unsafe websites. Every day, we discover thousands of new unsafe websites the legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web brows search to see whether a website is currently dangerous to visit.	afe sites, many of ers. You can		
	Check site status			
	www.almamaterstore.in	Q		
	Current status			
	No unsafe content found			
	Site info			
	This info was last updated on Feb 26, 2020.			
	Site safety can change over time. Check back for updates.			

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 <u>https://www.google.com</u>

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+skim ming+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 are common payment card skimming attacks targeting online retails		
🔍 All 🔟 News 🖕 Images 🖉 Shopping 🗈 Videos 🗄 More	attings Tools	
About 16,700,000 results (0.75 seconds)		
www.nbonews.com > tech > tech-news > what-magecart-credit-card-st *		
What is Magecart? Credit card-stealing malware proves he Dec 14, 2013 - In 2018, multiple large-scale caller retailers like Tickermater and B attacks have become so common and consistent that information While the digit cardid carling, known as skimming, is non new, attacks on payment pages data to including those of Home Depot and Target.	- The If of Me	
People also ask		
What is a Magecart attack?	~	
What is Magecart malware?	~	
What is e skimming?	~	
Can malware steal credit card info?	v	
	Feedback	
www.cnbc.com > 2020/01/31 > e-skimming-cyberattack-is-growing-a *		
E-skimming cyberattack is growing along with online shop	a	
Jan 31, 2020 - Skimmers, or hidden devices designed to steal credit card A cybe	k known	
as e-skimming is getting more common with the rise of online shopping Compare	inge and	
small have been hit by e-skimming attacks in the past "As the majority of exploit target software installations that are	10	
www.csoonline.com > article > what is magecart-how-this-hacker-gro •		
What is Magecart? How this hacker group steals payment	d	
Magecart is a consortium of malicious hacker groups who target online shopping	ystems,	
usually the Magento system, to steal customer payment card information. This is k	as a	

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

\rightarrow C $\hat{\mathbf{a}}$ communi	ity.riskiq.com/home	* •	🛓 🗇 🖲 🎈 🦓 🚾 🕌
RISKIQ			Tours Enterprise 🔿
me isiveTotal Search	Q Discover • www.almamaterstore.in		÷
tal Footprint			
ects	PROJECTS +New Project	TEAM HISTORY My History	YOUR ACCOUNT
ngs	Sainsburys Phishing Feb 2020 (59) Domains Gathered by Jake	vamsikrishna.food.blog miguel.rodriguez@riskiq.net a minute ago	PassiveTotal Enterprise Edition No query limit set
	AliKM Bulletproof Hosting ()	google.com carlos.gonzalez@risklq.net 3 minutes ago	Upgrade
	Vijay Test11 (2)	google.com carlos.gonzalez@riskiq.net 7 minutes ago	EEATI IDED
	Azure Blob Phishing (304) Instances of Azure Blob storage being used for phishing campaigns.	52.1.173.203 hiten.sharma@riskiq.net 16 minutes ago	Fox Kitten Campaign: Widespread Iranian Espionage-Offensive Campaign
	USPS - Phishing Campaign (1)	seguroscrediscotia cardif.com pe	Public Project Riskiqosint
	A Junaine IEB Infeatouriure //E70)	josh.ginnings@riskiq.net 19 minutes ago	Charming Kitten: Fake Interview
	tantani Gr Imizadu Guile (1770) This project elses to catality farianis RF Infrastructure and net ranges based of RiskiQ IP Whois and PDNS Data. This project includes IP addre tran 159 Telecommunications Infrastructure	media.noonnikemocaptainannguynoky bt3@riskiq.net 25 minutes ago	APT40 - Leviathan - Malaysia Cert Fubic Project Jangrossinov
	OurSainsburys, Websites (7)	nike.com bh3@riskiq.net 27 minutes ago	Public Project Riskig
	bofa test (2)	dl2.dropbox-download-eu.com bh3@riskip.ret 32 minutes ago	Palo Alto Unit 42:The Fractured Statue Campaign - U.S. Governme Targeted in Spear-Phishing Attack
	BNPP - PHISH Investigation (10) ChiPP_Cmail Peak	159.89.196.89 bh2@riskie.net 37 minutes ago	Public Project Riskiquesint
	CrowdStrike Phishing GetAndGoLoader malware (10)	di2.onedrive-us-en.com	Sequel Public Project Riskiqosint
	Demo for CrowdStrike Integration	bh2@riskiq.net 37 minutes ago	Kaspersky: Shlayer Trojan a one in ten macOS users

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

\leftrightarrow \rightarrow C $$ community.riskiq	q.com/search/www.alman	aterstore.in	📼 ★ 🖸 隆 🚸 🖲	🎈 👍 w. 🔤	: 🌒
	v.almamaterstore.ii	\odot	Tours	Enterprise	01
First Seen 2010-07-28 Registra Last Seen 2020-02-26 Registra	rar GoDaddy.com, LLC rant last minute films	Categorize			
FILTERS	SUBDOMAINS 🕲				
▼ HOSTNAME (22 / 22)	□ • 1 - 22 of 22	 Sort : Hostname Ascending		Downloa	d Copy
✓ X almamaterstor 1		Hostname	Ta	gs	
🗸 🗶 app01.almamat 1		almamaterstore.in			
✓ ≍ aws01.almamat 1		app01.almamaterstore.in			
✓ X blog.almamater 1		aws01.almamaterstore.in			
Show More		blog.almamaterstore.in			
▶ TAG		cpanel.almamaterstore.in			
▶ SYSTEM TAG		crm.almamaterstore.in			
		dev.almamaterstore.in			
		flash.almamaterstore.in			
		html.almamaterstore.in			
		m.almamaterstore.in			
		mail1.almamaterstore.in			
		mob.almamaterstore.in			
		new.almamaterstore.in			
		old.almamaterstore.in			
		shop.almamaterstore.in			
		staging.almamaterstore.in			
		staging01.almamaterstore.in			
		store.almamaterstore.in			E

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

\leftrightarrow \rightarrow C \triangleq community.riskig	q.com/search/www.almamaterstore.in				📼 ★ 📮 🗣 📀	🖡 🗸 🚾 🛛 🧶 🗄
	w.almamaterstore.in				Tours	Enterprise ? 👤
First Seen 2010-07-28 Registr Last Seen 2020-02-26 Registr	trar GoDaddy.com, LLC • Categorize trant last minute films					
FILTERS 🕲	TRACKERS ()					
TYPE (10 / 22)	□ 🔹 🖂 1 - 27 of 27 💌 🕞 Sort : L	ast Seen Descending 🔻	50 / Page 🔻			Download Copy
✓ × Facebookid 3	Hostname	First	Last	Туре	Value	Tags
✓ X GoogleAnalytics 3	www.almamaterstore.in	2019-06-25	2020-02-24	DocumentBaseHost	www.almamaterstore.in	
✓ X GoogleAnalytics 3	www.almamaterstore.in	2018-05-01	2020-02-24	InstagramId	almamaterstore	
✓ X GoogleTagMan 3	www.almamaterstore.in	2012-03-07	2020-02-24	Facebookld	almamaterstore	
Show More	www.almamaterstore.in	2017-12-16	2020-02-24	FacebookPixelId	1538473942840080	
▼ HOSTNAME (1 / 27)	www.almamaterstore.in	2019-04-20	2020-02-24	GoogleTagManagerId	gtm-wsl637z	
√ ೫ www.almamat 27	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-5jqrs5z	
	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	AddThisPubld	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	ucjshifid0hrkhw5xtd_i8cw	0
	www.almamaterstore.in	2019-04-09	2019-06-05	Bitlyld	getsizebug1	U

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



\leftrightarrow \rightarrow C $$ community.riskiq.	🖻 C 🗯 community.riskiq.com/search/www.almamaterstore.in 🗅 🛧 💿 🍇 🚸 🍨 🦕 👍 🐝 📟 ا 🌡 🚦									
	almamaterstore.in				Tours	Enterprise 🕜 👤				
First Seen 2010-07-28 Registra Last Seen 2020-02-26 Registra	rr GoDaddy.com, LLC Categorize									
DATA	9 4 36 Resolutions Whois Certificates Subd	22 27 omains Trackers Corr	156 102 hponents Host Pairs	10 0 4 0 OSINT Hashes DNS Projects	2K 1 Cookies CrowdStrike					
FILTERS 🕑	COMPONENTS 🕑									
▼ TYPE (10 / 126)	□ 🔹 🔄 1 - 156 of 156 💌 🕞 Sort : Last Seen Desc	ending 🔻 250 / Page 🔻				Download Copy				
✓ × Tracking Pixel 53	Hostname	First	Last	Category	Value	Tags				
✓ ≍ JavaScript Libr 30	www.almamaterstore.in	2019-04-04	2020-02-24	Operating System	Ubuntu					
 Analytics Service 8 	www.almamaterstore.in Api	il 4th 2019, 2:09:08 am	2020-02-24	Server	nginx (v1.14.0)					
✓ × CDN 7	www.almamaterstore.in	2019-04-04	2020-02-24	Hosting Provider	Google Cloud					
Show More	www.almamaterstore.in	2019-04-05	2020-02-24	JavaScript Library	Bootstrap (v3.3.5)					
▼ HOSTNAME (1 / 156)	www.almamaterstore.in	2015-12-01	2020-02-24	Ad Network	Google					
✓ X www.almam 156	www.almamaterstore.in	2013-11-27	2020-02-24	Ad Exchange	Google Ads - DoubleClick					
▼ NAME (10 / 32)	www.almamaterstore.in	2019-04-05	2020-02-24	JavaScript Library	Swiper (v3.4.2)					
✓ X jQuery 7	www.almamaterstore.in	2015-11-20	2020-02-24	Tracking Pixel	Google Analytics					
✓ × PHP 5	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					
✓ X Google 3	www.almamaterstore.in	2018-12-09	2020-02-24	JavaScript Library	mustache.js (v0.8.1)					
Show More	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	9				

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

← → C								
	mamaterstore.i	n e						
First Seen 2010-07-28 Registrar Last Seen 2020-02-26 Registrant	GoDaddy.com, LLC last minute films	🛨 Categori:	ze					
DATA	9	4	36	22	27	156		
	Resolutions	Whois	Certificates	Subdomains	Trackers	Components		
FILTERS ()	COMPONENTS				250 / 2			
TYPE (10 / 126)	■ ■ ■ 1 - 156 of 1	56 ▼ ►	Sort : Last See	en Descending 🔻	2507 Page	•		
🗸 🗶 Tracking Pixel 53	Hostname			First	25	Last		
🗸 🗶 JavaScript Libr 30	www.almama	terstore.in		2019-0	50	2020-02-24		
✓ X Analytics Service 8	www.almama	terstore.in		2019-0	100	2020-02-24		
✓ ★ CDN 7	www.almama	terstore.in		2019-0	250	2020-02-24		
 Ad Exchange Show More 	www.almama	terstore.in		2019-0-	500 4-05	2020-02-24		
▼ HOSTNAME (1 / 156)	www.almama	terstore.in		2015-1	2-01	2020-02-24		



← → C 🔒 community.riskic	.com/search/www.flower	explosion.com												*	🗅 🔤 🛷	۰ (o J 🖸	@ :
	v.flowerexplosion.co	om o														Tours	Enterprise	01
First Seen 2010-07-27 Registr	rar GoDaddy.com, LLC	 Categorize 																
Last Seen 2019-09-18 Registr	Trant Domains By Proxy, L																	
		14 Resolutions	WHOIS	6 Certificate	Subdomains	Trackers	137 Components	128 Host Pairs	OSINT	Hashes	DNS	Projects	Cookies					
FILTERS ()	COMPONENTS O			- December -													Developed	6
/ 107)	↓ Show:250 4	1-13/ 01 13/ F	ort : First See	n Descending	Eiset	L art		Category				Value					Download	Сору
✓ X Tracking Pixel 41	Hostname	ralasian com			2019-09-10	201	9.09.10	Online Vid	805			Value	uba				Tags	
✓ X JavaScript Lib 19		posion.com			2019-09-10	201		Online Vio	e03			Tour	uue					
✓ X CDN 10	www.flowerex	plosion.com			2019-09-10	201	9-09-10	JavaScript	Library			Word	Press Emoji (v5.2.2)				
✓ X Analytics Servi 8	www.flowerex	plosion.com			2019-09-10	201	9-09-10	CMS				Word	Press (v5.2.2'')					
Show More	www.flowerex	plosion.com			2019-09-10	201	9-09-10	JavaScript	Library			Word	Press Embeds (v5.)	2.2)				
HOSTNAME (1/137)	www.flowerex	plosion.com			2019-07-05	201	9-09-17	Server				Cloud	iFlare					
✓ × www.flower 137	www.flowerex	plosion.com			2019-05-02	201	9-09-17	Customer	Engagement			ZenD	esk Chat					
NAME (10/27)	www.flowerex	plosion.com			2019-02-07	201	9-02-07	Tracking P	ixel			www	google.es					
✓ × WordPress 6	www.flowerex	plosion.com			2018-12-31	201	9-09-17	JavaScript	Library			Boots	itrap (v3.3.1)					
✓ X CloudFlare 5	www.flowerex	plosion.com			2018-11-10	201	8-11-10	Wordpress	s Plugin			Akisn	net Anti-Spam					
✓ × Admeta 2	www.flowerex	plosion.com			2018-11-10	201	9-09-10	Wordpres:	s Plugin			Insta	gram Feed					
✓ X Amazon Web 2	www.flowerex	plosion.com			2018-11-10	201	9-09-10	Developm	ent Tool			AddT	oAny					
Show More	www.flowerex	plosion.com			2018-11-10	201	9-09-10	Wordpres:	s Plugin			AddT	oAny Share Button	s				
	www.flowerex	plosion.com			2018-11-10	201	9-09-10	Sharing				Locke	erz Share					
	www.flowerex	plosion.com			2018-11-10	201	9-09-10	CDN				Boot	Strap CDN					
	www.flowerex	plosion.com			2018-11-10	201	9-09-10	Web Desig	'n			Font	Awesome (v4.7.0)					
	www.flowerex	plosion.com			2018-11-10	201	8-11-10	Publisher				Insta	gram					
	www.flowerex	plosion.com			2018-11-10	201	8-11-10	CMS				Word	Press (v4.9.8)					
	www.flowerex	plosion.com			2018-08-13	201	9-08-29	Tracking P	ixel			hi.he	llobar.com					
	www.flowerex	plosion.com			2018-08-10	201	9-09-17	JavaScript	Library			Credi	t Card Validation Ja	wascript				
	www.flowerex	plosion.com			2018-06-23	201	8-06-23	CDN				Goog	le Hosted Libraries					0
	www.flowerex	plosion.com			2018-06-23	201	8-06-23	JavaScript	Library			jQue	ry (v1.8.0)					y
•		mlarian com			2018-06-23	201	8.06.73	CDN				6000	A Alay (TA)					

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.



\leftrightarrow \rightarrow C $$ community.risking	q.com/search/www.flowerexplosion.com	* 🗅 🕸 👁 🖲	• • J 🖸 🗑 :			
	w.flowerexplosion.com				Tours	Enterprise 😯 👤
First Seen 2010-07-27 Regist	trar GoDaddy.com, LLC • Categorize					
Cast Seen 2019-09-18 Negati	14 9	6 8 21 13	128 10	0 1 5 0	769	
	Resolutions WHOIS	Certificate Subdomains Trackers Compo	onents Host Pairs OSI	NT Hashes DNS Projects	Cookies	
FILTERS 🚯	HOST PAIRS ()					
DIRECTION	□ Show : 25 I - 25 of 128 Sort : Last Seen	Descending 🔻				Download Copy
✓ parents	Parent Hostname	Child Hostname		First	Last Cause	Tags
🗸 children	frame	www.flowerexplosion.com		2018-09-06	2019-09-17 unknown	
PARENT HOSTNAME (107	www.flowerexplosion.com	c683207.ssl.cf2.rackcdn.com		2016-02-07	2019-09-17 img.src	
✓ × www.flower 103	www.flowerexplosion.com	d1nfcimmipiaw0.cloudfront.net		2016-10-30	2019-09-17 img.src	
✓ × d1nfcimmipia 5	www.flowerexplosion.com	fonts.gstatic.com		2016-06-30	2019-09-17 css.import	
✓ ≍ media.floexp.c 4	www.flowerexplosion.com	www.flowerexplosion.com my.heliobar.com 2017-05-01 2019-09-17				
✓ × con.optimizely 2 ✓ × static.addtoan 2	www.flowerexplosion.com	www.googleadservices.com 2016-07-15 2019-09-17				
Show More	www.flowerexplosion.com	www.googlecommerce.com		2016-02-07	2019-09-17 script.src	
CAUSE (10/124)	www.flowerexplosion.com	v2.zopim.com		2016-02-07	2019-09-17 script.src	
✓ × script.src 46	www.flowerexplosion.com	bat.bing.com		2016-02-07	2019-09-17 script.src	
✓ × unknown 24	www.flowerexplosion.com	114109.tctm.co		2017-10-06	2019-09-17 script.src	
✓ × link.href 7	www.flowerexplosion.com	bounceexchange.com		2016-02-07	2019-09-17 script.src	
✓ × css.import 5 Show More	www.flowerexplosion.com	d10lpsik1i8c69.cloudfront.net		2016-10-29	2019-09-17 script.src	
CHILD HOSTNAME (107.48)	www.flowerexplosion.com	www.googletagmanager.com		2017-05-29	2019-09-17 script.src	
✓ × www.flowere 26	www.flowerexplosion.com	connect.facebook.net		2016-02-07	2019-09-17 script.src	
✓ ≍ d10lpsik1i8c6 3	www.flowerexplosion.com	cdn.optimizely.com		2016-02-07	2019-09-17 script.src	
✓ × d1ntcimmipia 3 ✓ × media.floexp.c 3	www.flowerexplosion.com	d1nfcimmipiaw0.cloudfront.net		2016-10-29	2019-09-17 script.src	
✓ × www.google-a 3	www.flowerexplosion.com	www.google-analytics.com		2016-02-07	2019-09-17 script.src	
Show More	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	0
	www.flowerexplosion.com	www.flowerexplosion.com		2019-09-07	2019-09-16 parentPage	
L	· · · · · · · · · · · · · · · · · · ·			2010 00 07	3010-00-10 321-00-010-00	

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) × × img.src 25 \checkmark 25 script.src 25 × unknown × link.href 6 × redirect 6 \checkmark **Show More**

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

HOST PAIRS ()



← → C 🔒 community.riskie	q.com/search/www.flowerexplosion.com			* 🗅 🌬 🧇 🖲 🗣 🥥 🖞 🖸 😰 :
	w.flowerexplosion.com			Tours Enterprise 🕜 👤
First Seen 2010-07-27 Regist	rar GoDaddy.com, LLC Categorize			
Last Seen 2019-09-18 Regist	rant. Domains By Proxy, L			
	14 9 6 8 Resolutions WHOIS Certificate Subdom	21 1.37 1.28 10 1 ains Trackers Components Host Pairs OSINT Hashes	DNS Projects Cookies	
	HOST BAIRS O			
DIRECTION	□ ▼ Show : 25 ◀ 1-25 of 46 ► Sort : First Seen Descending ▼			Download Copy
✓ parents	Parent Hostname	Child Hostname	First Last	Cause Tags
✓ children	www.flowerexplosion.com	jquery.su	2019-05-23 2019-09-	13 script.src
PARENT HOSTNAME (107	www.flowerexplosion.com	www.shopperapproved.com	2019-01-22 2019-02-	13 script.src
✓ × www.flower 103	www.flowerexplosion.com	kinfirighbetted.host	2018-11-24 2019-01-	27 script.src
✓ × d1nfcimmipia 5	www.flowerexplosion.com	load.sumo.com	2018-11-10 2019-09-	10 script.src
✓ ※ media.floexp.c 4	www.flowerexplosion.com	static.addtoany.com	2018-11-10 2019-09-	10 script.src
✓ X cdn.optimizely 2 ✓ X static addtoan 2	114109.tctm.co	www.flowerexplosion.com	2018-11-08 2018-11-	08 script.src
Show More	www.flowerexplosion.com	www.g-statistic.com	2018-08-10 2019-01-	27 script.src
CAUSE (10/124) 26	www.flowerexplosion.com	ajax.googleapis.com	2018-06-23 2018-06-	23 script.src
✓ × script.src 46	www.flowerexplosion.com	ajax.cloudflare.com	2018-05-13 2018-05-	13 script.src
✓ × img.src 26 ✓ × unknown 24	www.flowerexplosion.com	stats.wp.com	2018-04-28 2018-04-	28 script.src
√ × link.href 7	www.flowerexplosion.com	secure.gravatar.com	2018-04-28 2018-04-	28 script.src
✓ X css.import 5	www.flowerexplosion.com	s0.wp.com	2018-04-28 2018-04-	28 script.src
CHILD HOSTNAME (10/40)	www.flowerexplosion.com	114109.tctm.co	2017-10-06 2019-09-	17 script.src
✓ × www.flowere 26	www.flowerexplosion.com	www.googletagmanager.com	2017-05-29 2019-09-	17 script.src
✓ X d10lpsik1i8c6 3	www.flowerexplosion.com	my.hellobar.com	2017-05-01 2019-09-	17 script.src
✓ X d1nfcimmipia 3	www.flowerexplosion.com	assets.pcrl.co	2017-05-01 2017-11-	15 script.src
✓ X media.idexp.c 3 ✓ X www.google-a 3	www.flowerexplosion.com	load.sumome.com	2017-02-11 2018-04-	28 script.src
Show More	www.flowerexplosion.com	html5shim.googlecode.com	2017-02-11 2018-04-	28 script.src
	d1nfcimmipiaw0.cloudfront.net	www.flowerexplosion.com	2017-02-11 2019-09-	10 script.src
	www.flowerexplosion.com	cs.luckyorange.net	2017-01-28 2017-04-	04 script.src
	www.flowerexplosion.com	d10lpsik1i8c69.cloudfront.net	2016-10-29 2019-09-	17 script.src

From the list you can see a typosquatted domain.



\leftrightarrow \rightarrow C $$ community.riskig	.com/search/www.almamaterstore.in			E 📵 ★	🖸 💺 👁 💌 🖣	💪 w. 😐	: 🚯
	v.almamaterstore.in O		manager.com	2/2 ^ ~ X	Tours	Enterprise	01
First Seen 2010-07-28 Registr Last Seen 2020-02-26 Registr	rar GoDaddy.com, LLC Categorize Categorize						
of X years it arear 2	www.itcareermakers.com	www.almamaterstore.in	2016-04-29	2016-11-19	script.src		
Show More	vww.almamaterstore.in	ajax.googleapis.com	2016-05-09	2016-07-18	script.src		
▼ CAUSE (10 / 100) 🛛 🗙	www.almamaterstore.in	www.googleadservices.com	2016-12-24	2019-04-09	script.src		
✓ × img.src 25	www.almamaterstore.in	code.jquery.com	2017-04-11	2018-07-29	script.src		
✓ × script.src 25	www.almamaterstore.in	platform.twitter.com	2017-05-02	2018-07-26	script.src		
✓ × link.href 6	www.almamaterstore.in	apis.google.com	2017-05-02	2018-07-15	script.src		
✓ X redirect 6	www.almamaterstore.in	assets.pinterest.com	2017-05-02	2018-07-26	script.src		
Show More	connect.facebook.net	www.almamaterstore.in	2017-11-09	2018-05-05	script.src		
 CHILD HOSTNAME (10 / 58) 	www.almamaterstore.in	cdn.izooto.com	2018-05-05	2019-04-01	script.src		
✓ × www.almamat 34	www.almamaterstore.in	dev.almamaterstore.in	2018-05-08	2018-06-24	script.src		
✓ ≍ cdn.staticans.co 4	www.almamaterstore.in	www.googletag <mark>manager.com</mark>	2018-06-30	2020-02-24	script.src		
✓ X www.tacebook 4 ✓ X assets.pinterest 3	vww.almamaterstore.in	ssl.google-analytics.com	2018-08-05	2019-04-01	script.src		
✓ 🗶 ik.imagekit.io 3	www.almamaterstore.in	app.wigzo.com	2018-08-13	2018-08-20	script.src		
Show More	www.almamaterstore.in	server.connecto.lo	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		
	vww.almamaterstore.in	googleteg <mark>manager.com</mark>	2019-08-09	2020-02-24	script.src		
	vww.almamaterstore.in	static.hotjar.com	2020-01-13	2020-02-24	script.src		_
	vww.almamaterstore.in	tag.cottonusa.org	2020-01-13	2020-01-15	script.src		
	< 1 - 25 of 25 V						

www.googletagmanager.com and googletegmanager[.]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.

\leftrightarrow \rightarrow C $$ community.riskig	.com/search/www.almamaterstore.in			۵ 🖈	🗅 🔤 🧇 🖲 🖣	ථ <mark>ආ</mark> w. 😐 🗶 ፤
	v.almamaterstore.in		manager.com	2/2 ^ ~ X	Tours	Enterprise 😯 👤
First Seen 2010-07-28 Registr Last Seen 2020-02-26 Registr	ar GoDaddy.com, LLC ant last minute films					
▼ CAUSE (10 / 100) 🗙	www.almamaterstore.in	www.googleadservices.com	2016-12-24	2019-04-09	script.src	
✓ × img.src 25	www.almamaterstore.in	code.jquery.com	2017-04-11	2018-07-29	script.src	
✓ × script.src 25	www.almamaterstore.in	platform.twitter.com	2017-05-02	2018-07-26	script.src	
✓ × unknown 25	www.almamaterstore.in	apis.google.com	2017-05-02	2018-07-15	script.src	
✓ × redirect 6	www.almamaterstore.in	assets.pinterest.com	2017-05-02	2018-07-26	script.src	
Show More	connect.facebook.net	www.almamaterstore.in	2017-11-09	2018-05-05	script.src	
 CHILD HOSTNAME (10 / 58) 	www.almamaterstore.in	cdn.izooto.com	2018-05-05	2019-04-01	script.src	
✓ × www.almamat 34	www.almamaterstore.in	dev.almamaterstore.in	2018-05-08	2018-06-24	script.src	
✓ ೫ cdn.staticans.co 4	www.almamaterstore.in	www.googletag <mark>manager.com</mark>	2018-06-30	2020-02-24	script.src	
 × www.facebook 4 × assets pinterest 3 	www.almamaterstore.in	ssl.google-analytics.com	2018-08-06	2019-04-01	script.src	
✓ × ik.imagekit.io 3	www.almamaterstore.in	app.wigzo. Open Link in New Tab	2018-08-13	2018-08-20	script.src	
Show More	www.almamaterstore.in	Open Link in New Window Open Link in Incognito Window	2018-09-04	2020-02-24	script.src	
	www.almamaterstore.in	ik.imagekit Send Link to Benjamin	2019-04-05	2020-02-24	script.src	
	www.almamaterstore.in	cdn.onesig Copy Link Address	2019-04-05	2020-02-24	script.src	
	www.almamaterstore.in	s7.addthis. Copy	2019-04-27	2020-01-15	script.src	
	www.almamaterstore.in	googletegn Print	2019-08-09	2020-02-24	script.src	
	www.almamaterstore.in	static.hotja	2020-01-13	2020-02-24	script.src	
	www.almamaterstore.in	tag.cottont	2020-01-13	2020-01-15	script.src	
	 1 - 25 of 25 v 					
https://community.riskia.com/search/apople	ofermanager.com and confidential; do not distribute without prior appro	val. Privacy P(Services				

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 is might not be a legitimate google domain.

Step 9: Click on the WHOIS tab.

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



\leftrightarrow \rightarrow C $$ community.ris	kiq.com/search/googletegr	manager.com	II 🖈 🖸 隆 🧇 🛞	🌒 🥠 w. 😐	: 🌒
	ogletegmanager.con		Tours	Enterprise	01
First Seen 2017-11-29 Reg Last Seen 2020-02-26 Reg	gistrar URL Solutions, Inc. gistrant Private Person	Categorize			
Records (4) Emails (3) Registrars	s (2) Name Servers (11) Ph	one Numbers (3) Organization (2)			
WHOIS RECORDS					
CHANGE HISTORY Date Changes	RECORD UPDATED 2 Checked by RisklQ Ex	2019-04-04:LAST SCANNED 2020-01-08 spires in a month Created a year ago Hide Diff Hide Raw Record			
2019-04-04 🖂 📞 🛄 🖨	Attribute	Value	Domain Name: GOOGLETEGMANAGER.COM		
2018-11-28 🖂 📞 🛄 😁	WHOIS Server	C whois.pananames.com	Registry Domain ID: 2376490214_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.pananames.com		
2017-12-20 🖂 📞 🛄 🖨	initia server	whois.PublicDomainRegistry.com	Registrar URL: http://www.pananames.com Updated Date: 2019-04-04T00:56:29Z		
2017-11-27 🖂 🤇 🛄 🖨	Registrar	URL Solutions, Inc.	Creation Date: 2019-04-04T00:56:27Z Registry Expiry Date: 2020-04-04T00:56:27Z		
		Smrimur@yandex.ru (registrant, admin, tech)	Registrar: URL Solutions, Inc. Registrar IANA ID: 1449		
	Email	B-	Registrar Abuse Contact Email: abuse@pananames.com Registrar Abuse Contact Phone: +1.9727369998		
	Name	Alan Lauer (registrant, admin, tech)	Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.PANAMASERVER.COM		
	Name	B -	DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/		
	Organization	C Private Person (registrant, admin, tech)	>>> Last update of whois database: 2019-04-04T20:52:07Z <<<		
		a)	For more information on Whois status codes, please visit https://icann.org/epp		
	Street	10188 SE Ellis st (registrant, admin, tech)	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		
	City	Portland (registrant, admin, tech)	view the registrar's reported date of expiration for this registration.		
		 a) 	TERMS OF USE: You are not authorized to access or query our Whois		
		OR (registrant, admin, tech)	automated except as reasonably necessary to register domain names or		
	State		modity existing registrations; the Data in VeriSign Global Registry		

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 googletegmanager[.]com.

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

https://community.riskiq.com/search/googletegmanager.com/domaincertific ates



← → ♂ ■ community.riskiq.com/search/googletegmanager.com	* 🖸 🕸 🧇	📀 🍨 🛵 w. 🔤	ء 🐌
E RISKIQ Q googletegmanager.com		Fours Enterprise	0 I
First Seen 2017-11-29 Registrar URL Solutions, Inc. Categorize Last Seen 2022-02-26 Registrant Private Person Categorize			
DATA 4 4 15 2 0 7 14 4 1 13 3 0 1 Resolutions Whois Certificates Subdomains Trackers Components Host Pairs OSINT Hashes DNS Projects Cookles Crowc Filtrens O Certificates Subdomains Trackers Components Host Pairs OSINT Hashes DNS Projects Cookles Crowc	1 dStrike		
✓ SHA-1 (15 / 15) × 1 - 15 of 15 ▼ Sort: Last Seen Descending ▼ 25 / Page ▼			
✓ × 048bf633221 1 SHA-1 First Seen	Last Seen	Infrastructure	
× 25938/67495af 1 Succassibis 1:esc/p450/edf/2600516:65:072:86 2020-03:10 2020-03:10 2020-03:10 2020-03:10 Secassibis 1:esc/p450/edf/260051:0:55:55:75:70 Secassibis 1:esc/p450/edf/260051:0:53:56:27163:4085:75:5470 Secassibis 1:esc/p450/edf/260051:0:53:56:27163:4085:75:5470 Secassibis 1:esc/p450/edf/260051:0:50	2020-02-24		
✓ × 1554744841411 1	2020-01-19	91.134.122.252	
X 1561682973228 1 cd5bc555020aeb384d2c2e954eaac9993cb56ae 2019-12-11	2019-12-13		-
✓ X 1561822590918 1 + 60ecca54a268ed166a3c6c3909bc1ef3c877630 2019-12-10	2019-12-12		
Show More 517eb808305490x9/7/3ca7b5271cea1d6e9229f 2019-12-11 2019-12-11	2019-12-11		

The results show that the domain googletegmanager.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.

\leftrightarrow \rightarrow \bigcirc $\stackrel{\circ}{_{\oplus}}$ https://communit	ty.riskiq.com/search/googleteg	manager.com/subdomains							x 🖸 🌬 🧇 🖲 🖣	🥑 w. 🔤 🎩 E
👖 Apps 📄 THW 201 📄 THW 301	🛅 investigations 🥆 Dashboa	ard Dash 🚸 Benjamin Powell	1 Tracker Search for	calendar.google.c	RisklQ, Inc Sec	J ≽ TriNet Plat	form 🕕 Prezi Suppor	rt Cen 🔗 Item List: My	Bids	» Dther Bookmarks
	letegmanager.com	0							Tours	Enterprise 🕜 👤
First Seen 2019-04-03 Registra	ar URL Solutions, Inc.									
Last Seen 2020-03-30 Registra	ant Private Person	tegorize								
Query Results										
 ANALYST INSIGHTS 										
Blacklisted 12 days ago Resolving IPs No	ot Blacklisted Registered a year ago	Updated a year ago 4 IPs for subdom	ains New subdomain 4 mc	inths ago Registered	Resolves to IP Not Alex	a 100K 1 domains t	share whois record 155	56 domains share nameserver	Crawled By RiskiQ 11 days ago	
Not an International Domain										
* НЕАТМАР										EGEND
	Su 1 1			1 1 1	1 1 1 1	1 1 1	1 1 1 1			
	Mo 1 1									
	Tu Tu Tu									
	Th									
	Fr 1 1	1 1 1 1 1 1								
	Sa 1 0	1 1 1 1 1 1 Det Nov	Dec		1 1 1 1 Ian	Feb	Mar			
				2019-05	21 to 2020-03-30					
DATA										
		4 4 17	2 0 Subdamaine Tracker	8 Componentr Ho	21 4	0 13	1 0 Projecto Cookier	1 CrowdStrike		
	N.	resolutions millions certificates	Suburnains Trackers	components no	Craits Osini P	asires Dina P	Tojecis Cookies	crowdstrike		
FILTERS ()	SUBDOMAINS O	Sect. Mastering Assessing - 35 (D								Download Copy
HOSTNAME (2 / 2)	0. 1.202.	Hostname	age •						Taes	
✓ × googletegmana 1 ✓ × www.googleteg 1		googletegmanager.com							8*	
h TAG	0	www.googletegmanager.com								
	1.2 of 2 ¥									
▶ SYSTEM TAG										

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.



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

Step 12: Click on the Components tab

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



\leftrightarrow \rightarrow \mathcal{C} \textcircled{e} community.riskiq.com/search	ch/googletegmanager.com				* 🗳 🍇 👁 🖲	🕨 👍 🚧 😐 🗧 🐌 🗄
	anager.com 💿				Tours	Enterprise 💡 👤
First Seen 2017-11-29 Registrar URL Solu Last Seen 2020-02-26 Registrant Private P	vtions, Inc. Person					
		20	19-08-17 to 2020-02-26			
DATA	4 4 15 2 Resolutions Whois Certificates Subdomains	0 7 Trackers Components	14 4 Host Pairs OSINT	1 13 3 0 Hashes DNS Projects Cookies	1 CrowdStrike	
FILTERS ● COMP(▼ TYPE (4 / 7)	ONENTS ④ ≪ 1 - 7 of 7 ▼ ⇒ Sort : Last Seen Descending ▼ 2	5/Page 🔻				Download Copy
✓ X Server Module 3	Hostname	First	Last	Category	Value	Tags
✓ × Framework 2	googletegmanager.com	2019-04-23	2020-02-24	Server Module	mod_fcgid (v2.3.9)	
V X Operating Syste 1	googletegmanager.com	2019-04-23	2020-02-24	Server Module	OpenSSL (v1.0.2k-fips)	
✓ × Server 1	googletegmanager.com	2019-04-23	2020-02-24	Operating System	CentOS	
▼ HOSTNAME (1 / 7)	googletegmanager.com	2019-04-23	2020-02-24	Server Module	PHP (v7.0.31)	
✓ ≍ googletegmana 7	googletegmanager.com	2019-04-23	2020-02-24	Framework	PHP (v7.0.31)	
▼ NAME (5 / 7)	googletegmanager.com	2019-04-23	2020-02-24	Server	Apache (v2.4.6)	
✓ × PHP 3	eoogletegmanager.com	2019-06-05	2020-02-20	Framework	PHP	
✓ X Apache 1	8868888					
✓ × CentOS 1 1	-7 of 7 🔻 🕞					
✓ X OpenSSL 1						
✓ ≍ moa_icgia 1						
						Q
5.475.0 © 2020, RisklQ Inc. All Rights Reserved. Prop						

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/googletegmanager.com/hostpairs

\leftarrow \rightarrow C $$ community.riskiq.com/searce	rch/googletegmanager.com				* 🕒 🍇 👁 🖲	🌒 🛵 w. 🔤 🇶 E
	anager.com 📀				Tours	Enterprise 😯 👤
First Seen 2017-11-29 Registrar URL Solu	lutions, Inc.					
Last Seen 2020-02-26 Registrant Private F	Person					
		20	019-08-17 to 2020-02-26			
DATA	4 4 15	2 0 7	14 4	1 13 3 0	1	
	Resolutions Whois Certificates	Subdomains Trackers Components	Host Pairs OSINT	Hashes DNS Projects Cooki	ies CrowdStrike	
	CONENTS O					
	< 1 - 7 of 7 ▼ ► Sort : Last Seen D	escending 🔻 25 / Page 🔻				Download Copy
✓ X Server Module 3	Hostname	First	Last	Category	Value	Tags
✓ X Framework 2	googletegmanager.com	2019-04-23	2020-02-24	Server Module	mod_fcgid (v2.3.9)	
✓ X Operating Syste 1	googletegmanager.com	2019-04-23	2020-02-24	Server Module	OpenSSL (v1.0.2k-fips)	
✓ × Server 1	googletegmanager.com	2019-04-23	2020-02-24	Operating System	CentOS	
▼ HOSTNAME (1 / 7)	googletegmanager.com	2019-04-23	2020-02-24	Server Module	PHP (v7.0.31)	
✓ X googletegmana 7	googletegmanager.com	2019-04-23	2020-02-24	Framework	PHP (v7.0.31)	
▼ NAME (5 / 7)	googletegmanager.com	2019-04-23	2020-02-24	Server	Apache (v2.4.6)	
✓ X PHP 3	googletegmanager.com	2019-06-05	2020-02-20	Framework	РНР	
✓ X CentOS 1 < 1.	-7 of 7 🔻 🕨					
✓ X OpenSSL 1						
√ × mod_fcgid 1						
	prietary and confidential: do not distribute w	thout prior approval. Privacy Policy Terr				

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[.]191and open it in a new tab.

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





\leftrightarrow \rightarrow C \cong community.riskic	.com/search/92.63.192.191	★ 🗅 🔤 🖲 🌒 🧃 👐 🧱 🗄
E CRISKIQ Q 92.6	3.192.191 0	Tours Enterprise 🕜 👤
First Seen 2016-07-23 ASN	LLCDigital Network RU E Routable LLCDigital-Hitework C Categorie	
	W1 J S A A A B B B F T </th <th></th>	
	2019-10-20 00-05-05	
DATA	13 2 9 0 13 1 2 1 0 0 2 to 2 Resolutions Whois Centificates Trackers Components Host Paris OSINT Hashes Projects Cookes CrowdStrike Services	
FILTERS O	RESOLUTIONS ©	Download Copy
▶ SYSTEM TAG	Resolve First Last Source	Tags
▶ TAG	googletegmanager.com 2019-12-11 2020-04-11 riskiq, kaspersky, allenvault	-
▶ ASN	www.googletegmanager.com 2019-12-11 2020-04-10 riskiq, allervault	
▶ NETWORK	gorlon.in.ua 2019-12-11 2020-03-24 riskiq alienvault	
▼ SOURCE (4 / 19)	www.gorlon.in.ua 2019-12-12 2020-03-24 riskig, emerging, threats, alienvault	
√ × riskiq 12	92.63.192.1911032www.gorlon.in.ua 2020.02-27 2020.03-16 riskiq	
✓ × alienvault 4	mail.gorlon.in.ua 2020-02-02 2020-03-09 riskiq	
✓ × kaspersky 2	webmailgorion.in.ua 2020-01-05 2020-03-05 riskiq	
· · · · · · · · · · · · · · · · · · ·	webdisk.gorion.in.ua 2020-01-05 2020-03-04 riskiq	
	cpanel.gorion.in.ua 2020-01-03 2020-02-09 riskig	
	autodiscover.gorion.in.ua 2020-01-03 2020-02-09 riskig	
	dc-3849d5a216df.mandarincc.info 2019-12-14 2019-12-18 riskiq	
	promorgasky.com 2017-06-11 2017-09-17 riskiq	
	spiralsteer.com 2016-07-23 2016-10-21 kaspersky	
	1-13 of 13 • •	Q

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 <u>https://urlscan.io</u>



Search for www[.]almamaterstore[.]in

C 🗎 urlscan.io			* 🗅 🕸
	urlscan.io तHome Q Search ⅢAPI ∳Live Ə About LLogin	Sponsored by	54 runninį
	urlscan.io		
	www.almamaterstore.in	► Public Scan	Options
Recents	Scans 🖑 Updates every 10s - Last update: 16:29:59		器API L Manual @ Auto
🔒 URL		Submitted	Size 🗰 IPs 🏴 🏦
🔒 miarrob	pa.com/	36 seconds ago	3 MB 139 37 7 📕
info.x1.	com/UnsubscribePage.html?mkt_unsubscribe=1&mkt_tok=eyJpIjoiWkRnNU9XUTRZ	37 seconds ago	66 KB 16 5 3 💻
O chouita	r.nl/vw8iYxnSOIBs1&subid2=wgi100gq8adcro7t1gm39ga4	38 seconds ago	244 KB 2 3 3 🚍
O www.xd	1.com/error.html	38 seconds ago 👫 7	720 KB 50 24 6 💻
O america	ancapitalone.com/	40 seconds ago	12 KB 2 1 1
🔒 chestyi.	.com/suntrust/login.online-banking.suntrust.com/SunTrust/1/1.html?%3C?ph	41 seconds ago	1 MB 66 10 7 🖸
a www.va	akantieveilingen.nl/producten.html?utm_source=selligent&utm_medium=email&u	41 seconds ago	1 MB 38 12 4 🚍
O eu1-us1	1.ckcdnassets.com/448/creatives/33077/hydrestore-start.jpg?platform=hoots	44 seconds ago	65 KB 1 1 1 📕
O www.xd	1.com/error.html	45 seconds ago	719КВ 50 24 5 💻
O ww1.wa	almarcapitalone.com/?sub1=2eb03d38-58f8-11ea-9614-bc2ca8556ef0	45 seconds ago	104 KB 8 4 2 💻
	21982077 public scans - 45909605 in total		
	Construction T	noc	
	* Security Iralis	Tell your extension story	

Step 18: Review the results

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

\leftrightarrow \rightarrow C $\stackrel{\text{\tiny left}}{}$ urlscan.io/result	/2b115d7c-95a8	3-422b-b00d-	76aee0733ef1							* 💷 🔤 🧇 🧕) 🌒 👍 w. 🔤 🇶 E
	Q ur	Iscan.io	♠Home Q	Search 🛄 API	🔲 Live	• About	Login	Sponsored by SecurityTrails		61 running	
	www.	almama	aterstor	e.in				QLoo	okup 🕶 🔿 Go To	Report C Rescan	
	35.200.1	39.97									
	Submitted U Effective UR Submission: O	IRL: http://www L: https://www n February 26 via	w.almamaterstor w.almamaterstor wanual (February	e.in e.in/ 26th 2020, 9:25:33 pn	n) from US 🌉	I.					
	☆ Summary	≓HTTP 137		🖵 Behaviour 🛛 💠 Io	Cs 🔗 Sim	nilar 🚺 🗐 DO	M 🕒 Con	itent 躍API			
	Summary							Screenshot	💠 Live s	creenshot	
	This webs transactic The main main dom TLS certifi	ite contacted 2 ons. IP is 35.200.13 ain is www.alm icate: Issued by	3 IPs in 8 countr 9.97, located in A materstore.in. Let's Encrypt Aut	ies across 22 doma Ascension Island an hority X3 on Januar	ins to perfo d belongs to y 28th 2020	orm 137 HTTP o GOOGLE, US. Th 0. Valid for: 3 mon	e :hs.				
	The main	domain was sca	anned 11 times o	n urlscan.io		Show Scan	5 11		₹299/- EA	CH SHOP NOW	
	1782 stru	cturally simila	r pages on differ	ent IPs, domains an	d ASNs four	nd Show Scans	1782		Annini, You Cuys		
	Verdict:	No classific	ation								
	Google Sa	fe Browsing: 🔇	Clean (Current	Classification)							
	Additio	aal live infor	mation					Detected technology	gies		
	Current D	NS A record: 3	5 200 139 97 (A	\$15169 - GOOGLE	115)			🔕 Ubuntu (Operating System	ns)	→ Website	
	current b	HIS ATCORD. 0	5.200.107.77	515107 0000LL	00)			Bootstrap (Web Framewo	rks)	→ Website	
	Domain &	IP informat	ion					G Nginx (Web Servers)		✓ Website	
								Zendesk Chat (Live Chat)	neworks)	✓ Website	
	IP/ASNs	IP Detail	(Sub)Domains	Domain Tree	Links	Certificates		Facebook (Widgets)		→ Website	
	#			IP Address	AS Aut	onomous System		Font Awesome (Font Scri	ipts)	→ Website	
	1 🔶 69			35.200.139.97	15169	(GOOGLE)		🔀 Google Analytics (Analyt	tics)	→ Website	
	2		2a00:1450	:4001:81a::200a	15169	(GOOGLE)		Google Analytics Enhan	rints)	Malytics) 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 googletegmanager[.]com

← → C 🏻 urlscan.io/result/2b115d7c-95a8-4	22b-b00d-76aee0733ef1#transactions					☆ (i 👁 🖲 🗣 👍 w. 🔤 i 🌒 E
🚔 GET 200 Н/1.1 ок	clip-rotate.css /catalog/view/theme/default/stylesheet/d_social_login/pre_loader	3 KB 1 KB	2364ms 362ms	Stylesheet text/css	35.200.139.97 GOOGLE		୍	2
GET 200 H/1.1 OK	styles.css /catalog/view/theme/default/stylesheet/d_social_login	5 KB 2 KB	2383ms 368ms	Stylesheet text/css	35.200.139.97 GOOGLE		୍	3
▲ GET 200 H2	swiper.jquery.js ik.imagekit.lo/xqgyjenzqsmnk/catalog/view/javascript/jquery/s wiper/js	204 KB 31 KB	183ms 81ms	Script application/javascript	13.225.73.74		٩	3
GET 200 H/1.1 OK	supermenu-responsive.js?v=30 Show response /catalog/view/javascript/supermenu	4 KB 2 KB	2728ms 364ms	Script application/javascript	35.200.139.97 GOOGLE		٩	3
GET 200 H/1.1 OK	jquery:hoverIntent.minified.js Show response /catalog/view/javascript/supermenu	1 KB 1020 B	2754ms 370ms	Script application/javascript	35.200.139.97 GOOGLE		୍	3
GET 200 H/1.1 OK	spin.min.js /catalog/view/javascript/d_social_Jogin	6 КВ 3 КВ	2756ms 372ms	Script application/javascript	35.200.139.97 GOOGLE		୍	3
GET 200 H/1.1 OK	gae.js /catalog/controller/extension/analytics	2 KB 1 KB	2844ms 363ms	Script application/javascript	35.200.139.97 GOOGLE		୍	3
GET 200 H/1.1 OK	common.js /catalog/view/javascript	16 KB 5 KB	2879ms 364ms	Script application/javascript	35.200.139.97 GOOGLE		୍	3
■ GET 200 H2	OneSignalSDK.js cdn.onesignal.com/sdks	8 КВ 3 КВ	28ms 11ms	Script application/javascript	2606:4700::6812:e234		୍	3
GET 200	js?id=AW-1003588398 Show response www.googletagmanager.com/gtag	75 KB 28 KB	42ms 39ms	Script application/javascript	2a00:1450:4001:825::2008	3	ଭ	3
GET 200 H/1.1 OK	embed.min.js googletegmanager.com	14 KB 14 KB	771ms 129ms	Script application/javascript	92.63.192.191		୍	3
GET 200 H/1.1 OK	google.svg /image/catalog/d_social_login	1 KB 872 B	579ms 366ms	Image image/svg+xml	35.200.139.97 GOOGLE		ଭ	3
GET 200 H/1.1 OK	facebook.svg /image/catalog/d_social_login	816 B 1 KB	402ms 371ms	Image image/svg+xml	35.200.139.97 GOOGLE		୍	3
GET 200 H/1.1 OK	twitter.svg /image/catalog/d_social_login	1 KB	2121ms 2111ms	Image image/svg+xml	35.200.139.97 GOOGLE		٩	3
➡ GET 200 H/1.1 OK	linkedin.svg /image/catalog/d_social_login	1 KB 892 B	377ms 367ms	Image image/svg+xml	35.200.139.97 GOOGLE		୍	3
GET 200 H/1.1 OK	logo.png /image/catalog	5 KB 6 KB	385ms 374ms	Image image/png	35.200.139.97 GOOGLE		ଭ	3
■ GET 200	closemenu.png	176 B	318ms	Image	13.225.73.83			

Click on show response button



← → C (🕯 urlscan.io/responses/69e2eaa52fabf1fb62f352d5b8e8a718e1b39fe62e5756054c5cc3fe71d7fb7b/	Be ⊀	<u>አ</u>			•	🧞 w.	•••	ء 🐌
<pre>if (typeof JSON !== "object") { JSON = ();</pre>								
<pre>} use strict; use strict;</pre>								
<pre>function f(n) { return n < 10 7 "0" + n : n; }</pre>								
<pre>function this_value() { return this value() { f(typeof Date.prototype.toJSON !== "function") { Date.prototype.toJSON = function() { Date.prototype.toJSON = function() { Date.prototype.toJSON = function() { this.valueOf()) ? this.getUTCPullYear() + "-" + f(this.getUTCMonth() + 1) + "-" + f(this.getUTCDate()) + "T" + f(this.getUTCDate()) + f</pre>	TCHour	:s())	* ":" ·	+ f(this	.getUT	CMinute	s()) 4	x 121 +
<pre>function str(key, holder) { var i; var i; var i; var evaluation of the structure of the</pre>								
return quote(value);								

This script is a variant of Magecart credit JavaScript skimmer. To see when this domain was infected if you look at the hostpair tab for www[.]almamaterstore[.]in. you can see the first and last seen dates for traffic reaching out to googletegmanager[.]com

Sear	ched domain	child relationship	Frist Seen	Last Seen	cause
	www.almamaterstore.in	www.googletagmanager.com	2018-06-30	2020-02-24	script.src

From this information you can see that his website has been compromised since June 30, 2018 and is still compromised.

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 collogues.

