



Advanced Use Case:

www[.]flowerexplosion[.]com

Part 2 - JQuery[.]su infrastructure investigation

Scenario:

You work for Flower Explosion as a Security Analyst. You have confirmed that your website www[.]flowerexplosion[.]com was compromised. The compromised script linked to jquery[.]su in Ukraine.

Now you need to further investigate the compromise to see the extent of the attack and try to identify the threat actor's infrastructure.

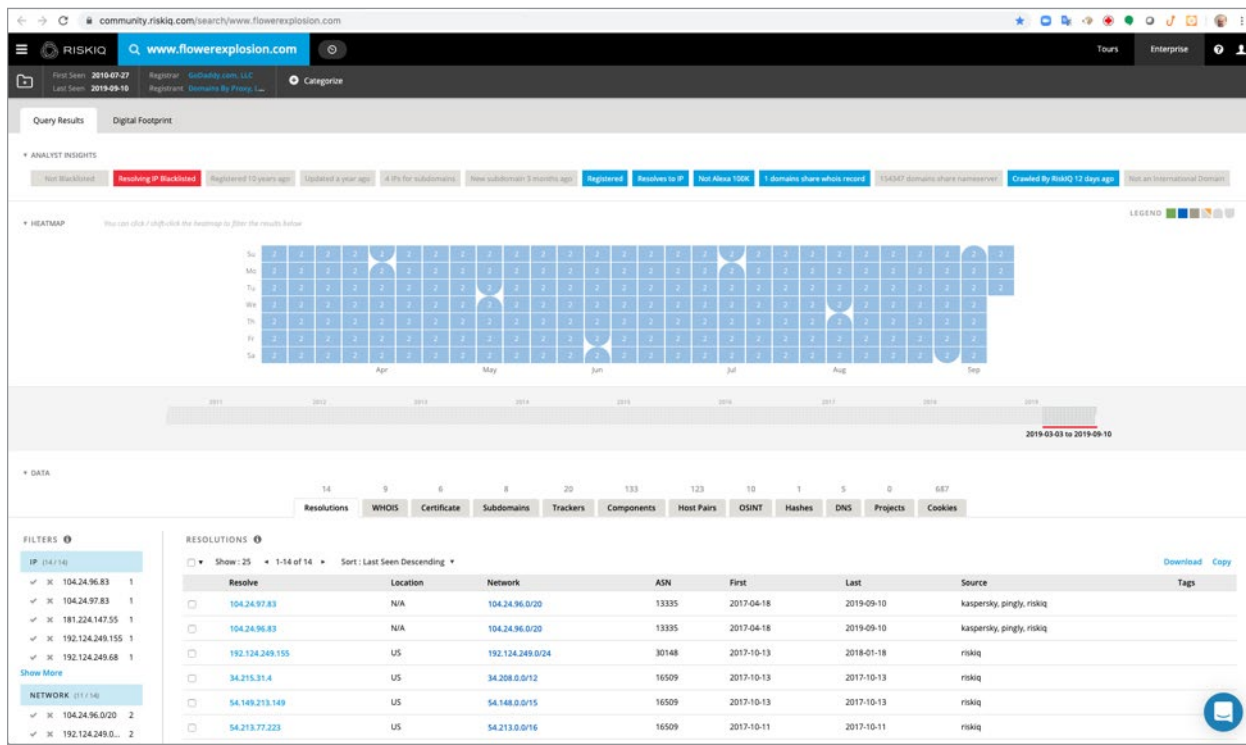
Step 1: In your web browser go to <https://community.riskiq.com>

The screenshot displays the RiskIQ community dashboard. The left sidebar contains navigation links: Home, PassiveTotal Search, Digital Footprint, Projects, Settings, LEARN (Overview, Help, Blog), FEEDBACK (Ideas Portal), DEVELOPERS (API, Python Client, Ruby Client, Rust Client), and INTEGRATIONS (Splunk, IBM, Slack/Hipchat, CIBTs, MSP, Maltego). The main content area is divided into three sections: MY DIGITAL FOOTPRINTS, MY HISTORY, and YOUR ACCOUNT. MY DIGITAL FOOTPRINTS shows a table with data for riskiq.net and riskiq.com. MY HISTORY lists various domains and their associated data. YOUR ACCOUNT section provides information about the user's subscription and offers an upgrade option. A sidebar on the right lists featured content, including APT134 leaked tools, FIN7 Cyber Espionage Group, and Gift Card Sharks.

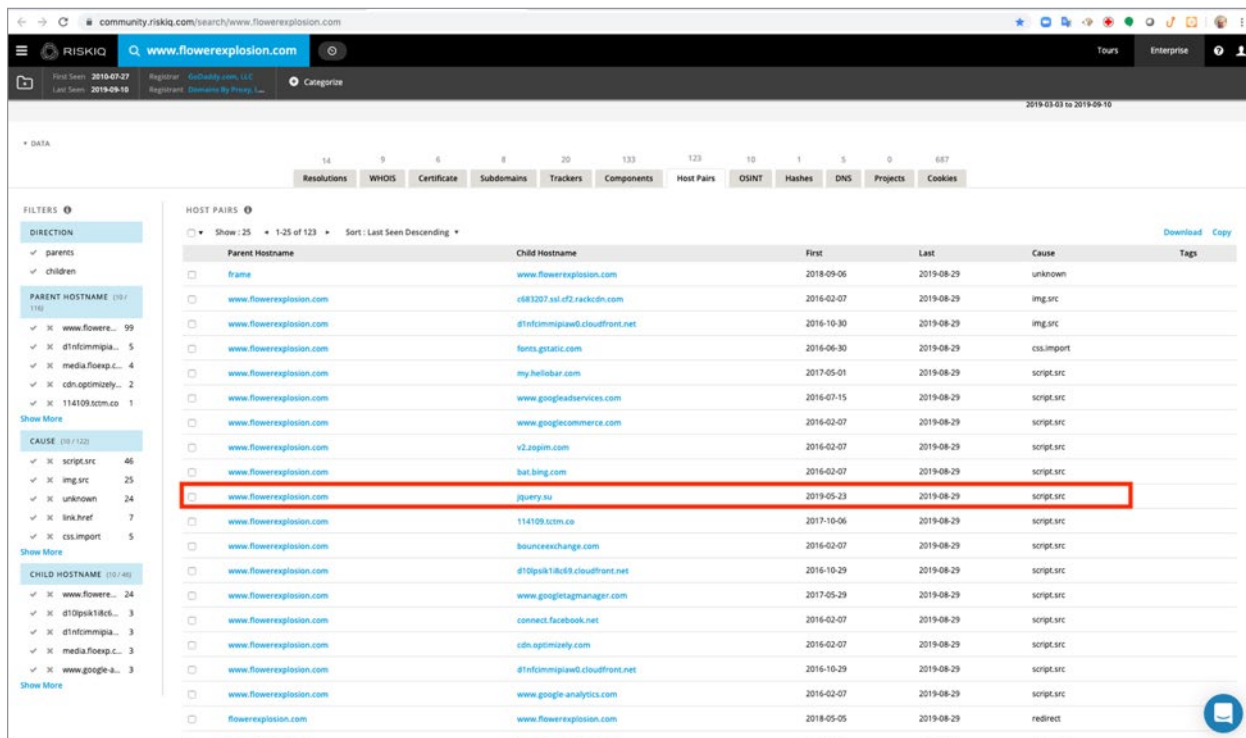
Domain	High Alexa Rank	Open Ports	High CVE	Critical CVE
riskiq.net	13	96	1574	17
riskiq.com	14	3771	1100	19

Step 2: Search for the domain www.flowerexplosion.com

<https://community.riskiq.com/search/www.flowerexplosion.com>



Step 3: Click on the Host Pair tab



The malicious Magecart script came from jquery.su.

Step 4: Pivot search on jquery[.]su

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

<https://community.riskiq.com/search/jquery.su>

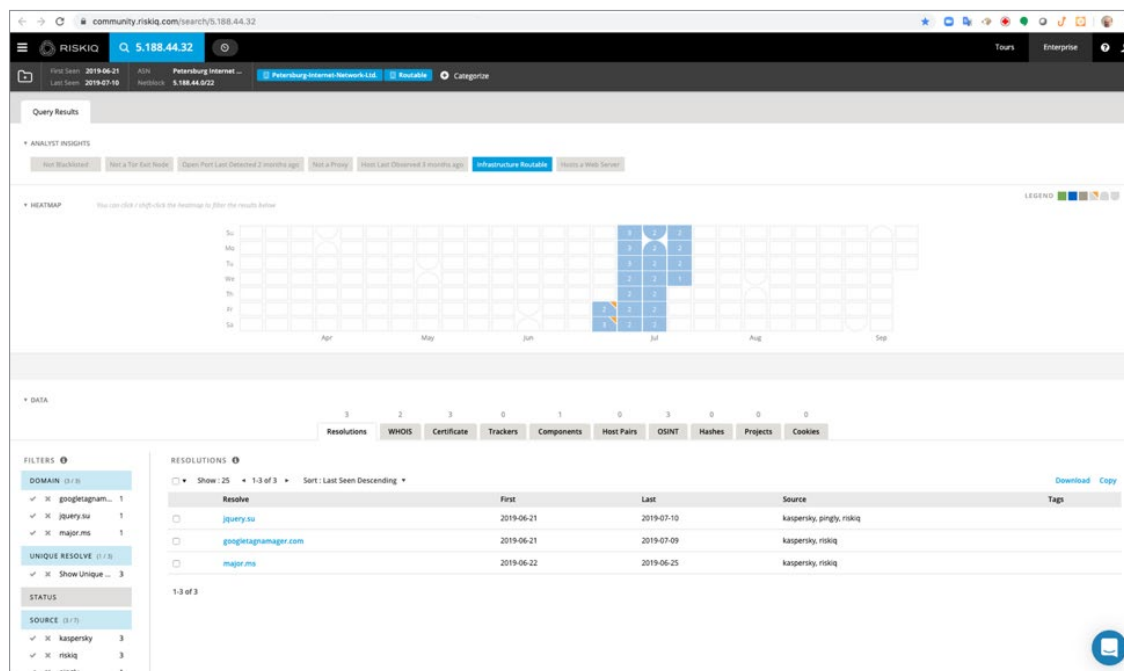
The screenshot shows the RiskIQ search interface for the domain **www.flowerexplosion.com**. The 'HOST PAIRS' tab is active, displaying a table with columns: Parent Hostname, Child Hostname, First, Last, Cause, and Tags. A right-click context menu is open over the entry for **jquery.su**, with the option 'Open Link in New Window' selected. The table lists various hostnames associated with the parent domain, including **www.flowerexplosion.com**, **cdn.optimizely.com**, **media.flowerexplosion.com**, and **jquery.su**.

The screenshot shows the RiskIQ search interface for the domain **jquery.su**. The 'RESOLUTIONS' tab is active, displaying a table with columns: Resolve, Location, Network, ASN, First, Last, Source, and Tags. A red box highlights the 'Location' column, showing 'UA' (Ukraine) and 'RU' (Russia). The table lists various IP addresses associated with the domain, including **176.119.1.112**, **5.188.44.32**, **217.8.117.140**, **194.58.56.17**, and **194.58.56.167**.

The threat actor web site resolves to IP addresses hosted in Ukraine and Russia.

Step 5: Pivot search on 5[.]188[.]44[.]32 and open it in a new tab.

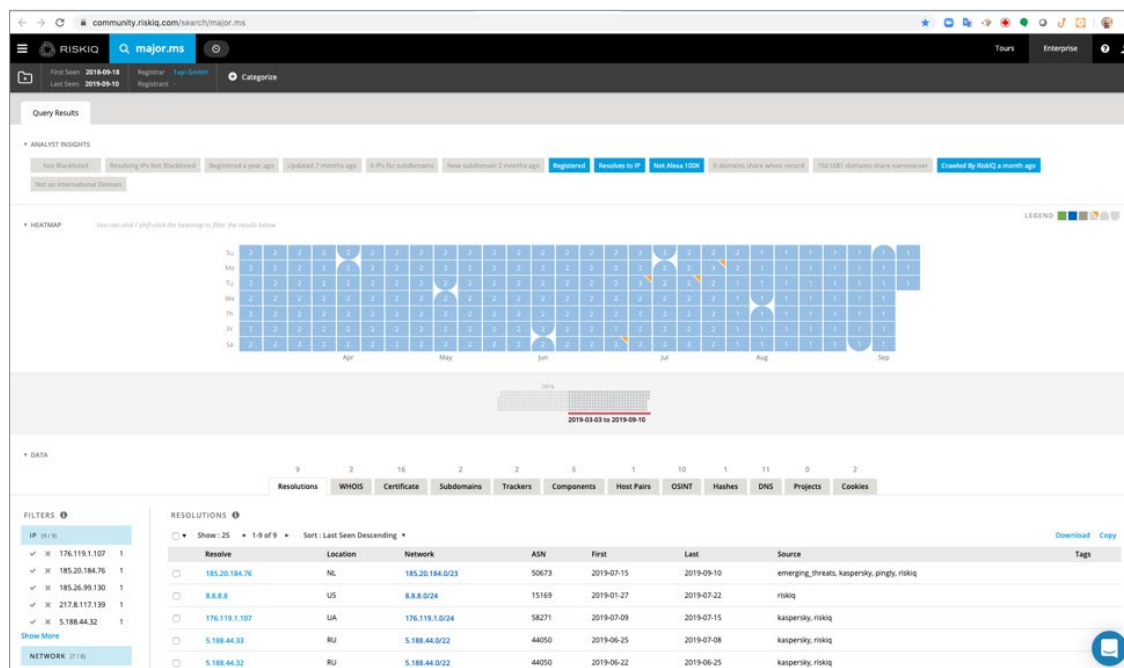
<https://community.riskiq.com/search/5.188.44.32>



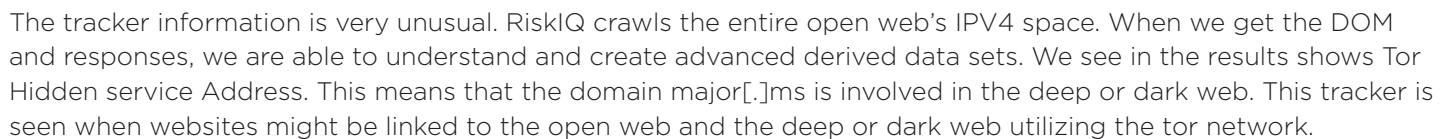
Pivot searching on the IP address now give us 3 domains, jquery[.]su, googletagmanager[.]com (appears to be a typosquatted domain for google tag manager), major[.]ms.

Step 6: Pivot search on major[.]ms and open it in a new tab.

<https://community.riskiq.com/search/major.ms>



The location information shows the Netherlands, the United States, and Russia.



<https://community.riskiq.com/search/trackers/verified2ebdpvms>

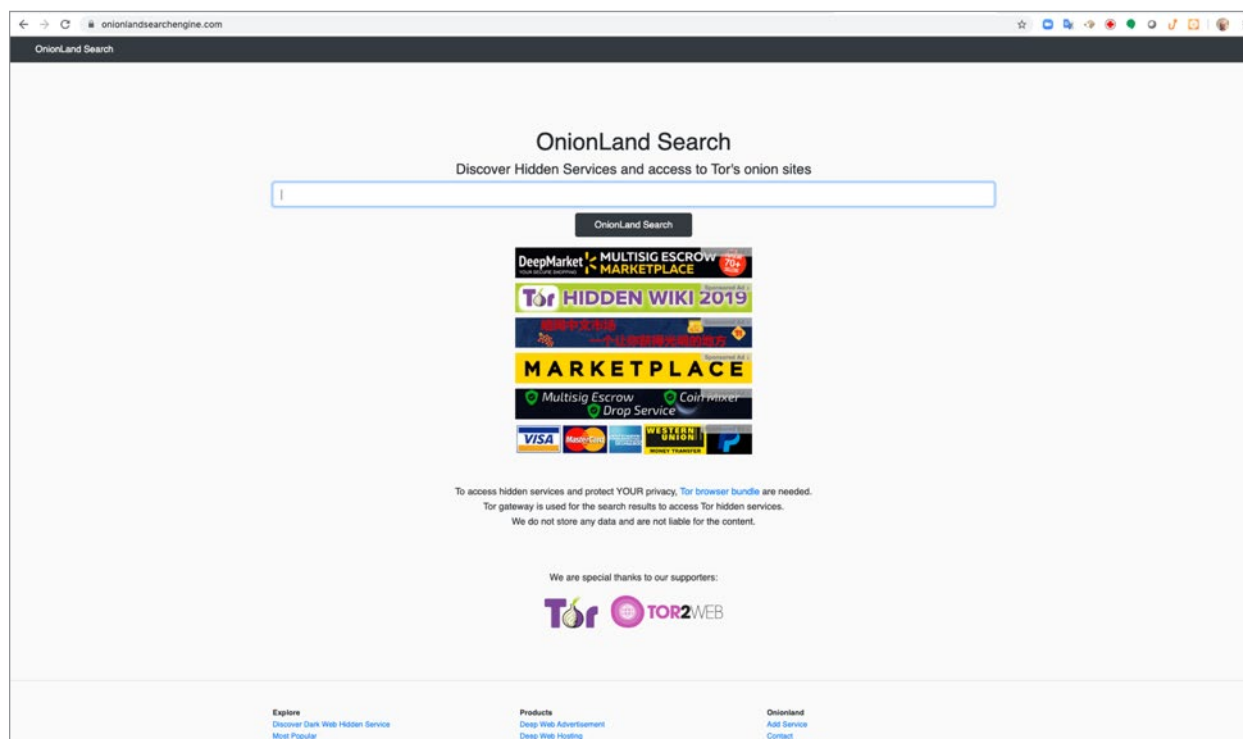
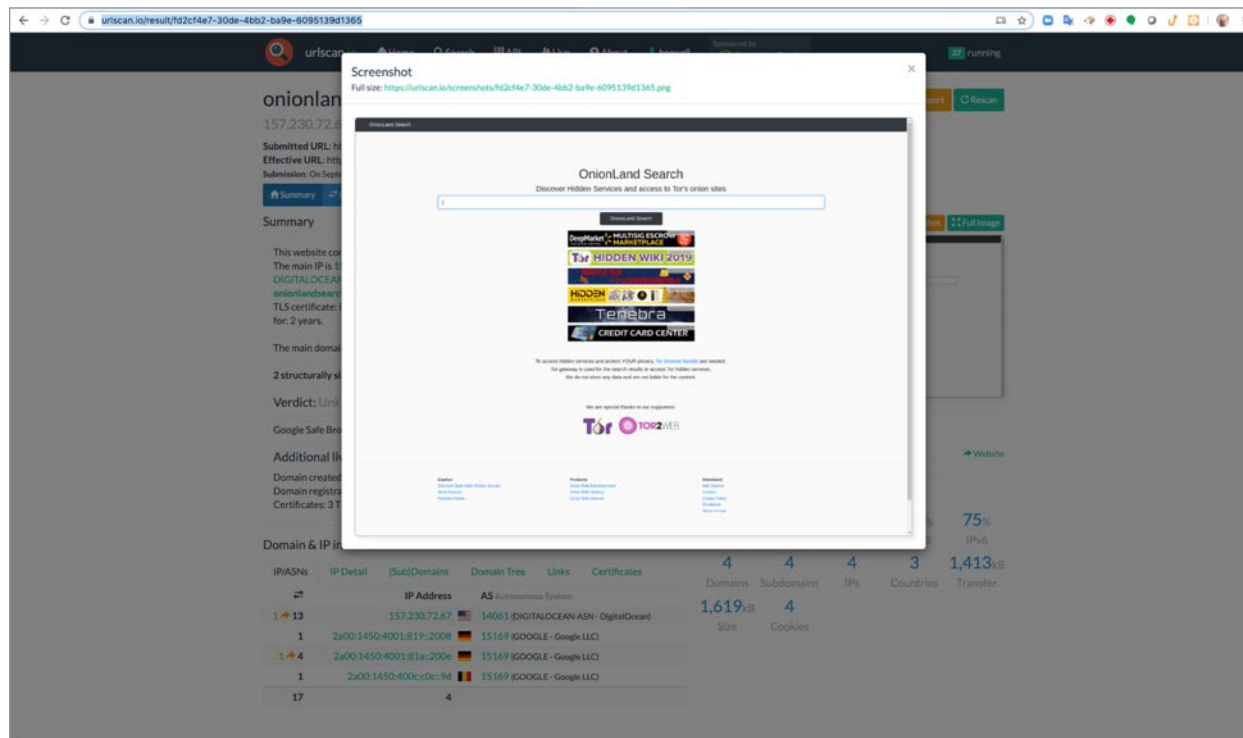
The results show 45 different hosts that are associated with the tracker.

Utilizing urlscan.io we can safely see what each website looks like and what business they are in.

Each one of the websites listed is involved in the Dark Web. The websites bridge the open internet and the Dark Web.

Onionlandsearchengine[.]com

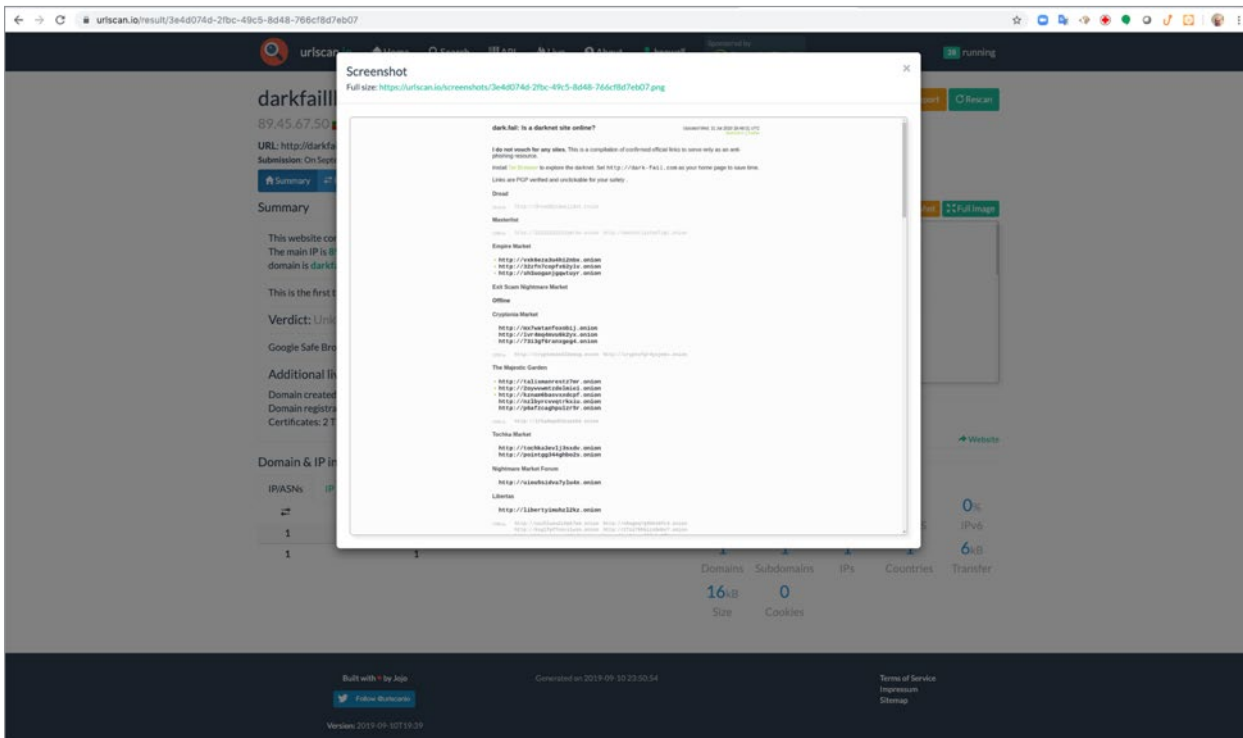
<https://urlscan.io/result/fd2cf4e7-30de-4bb2-ba9e-6095139d1365>



This website appears to be a way to search for things on the dark web.

darkfaillnkf4vf.com

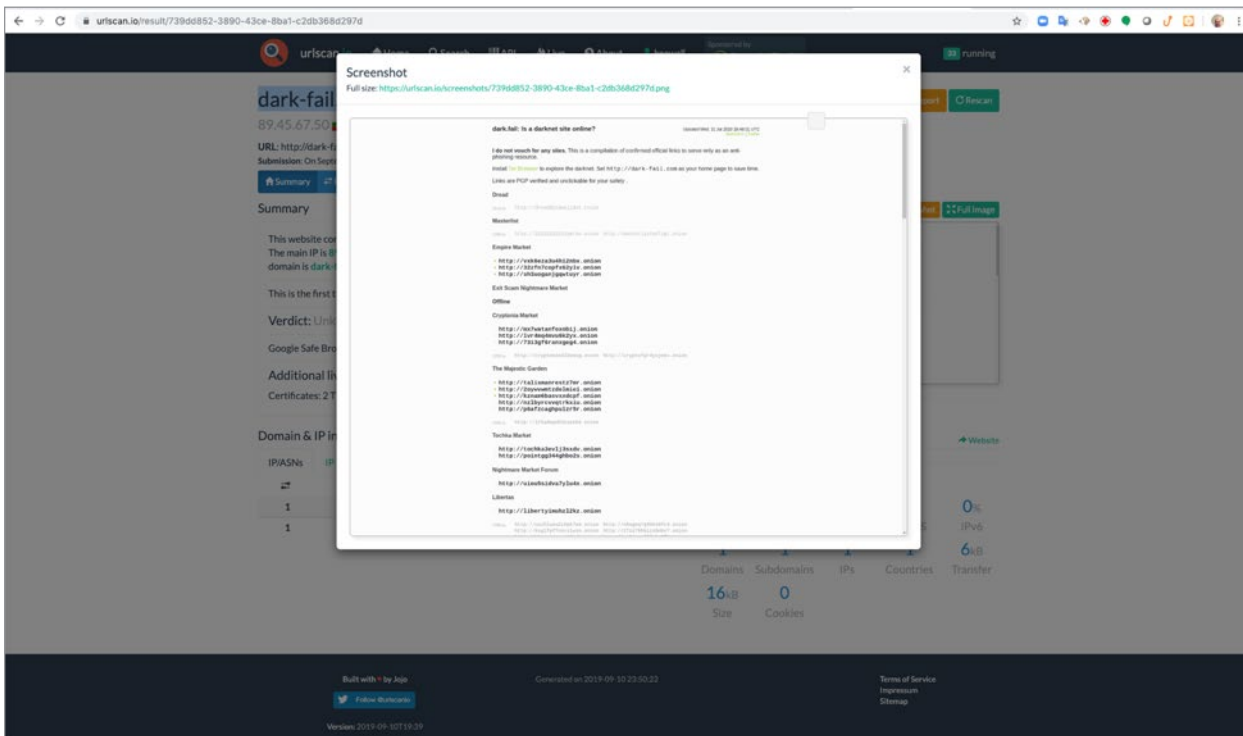
<https://urlscan.io/result/3e4d074d-2fbc-49c5-8d48-766cf8d7eb07>



This website appears to list a dark web website featuring different marketplaces where payment cards can be bought and sold.

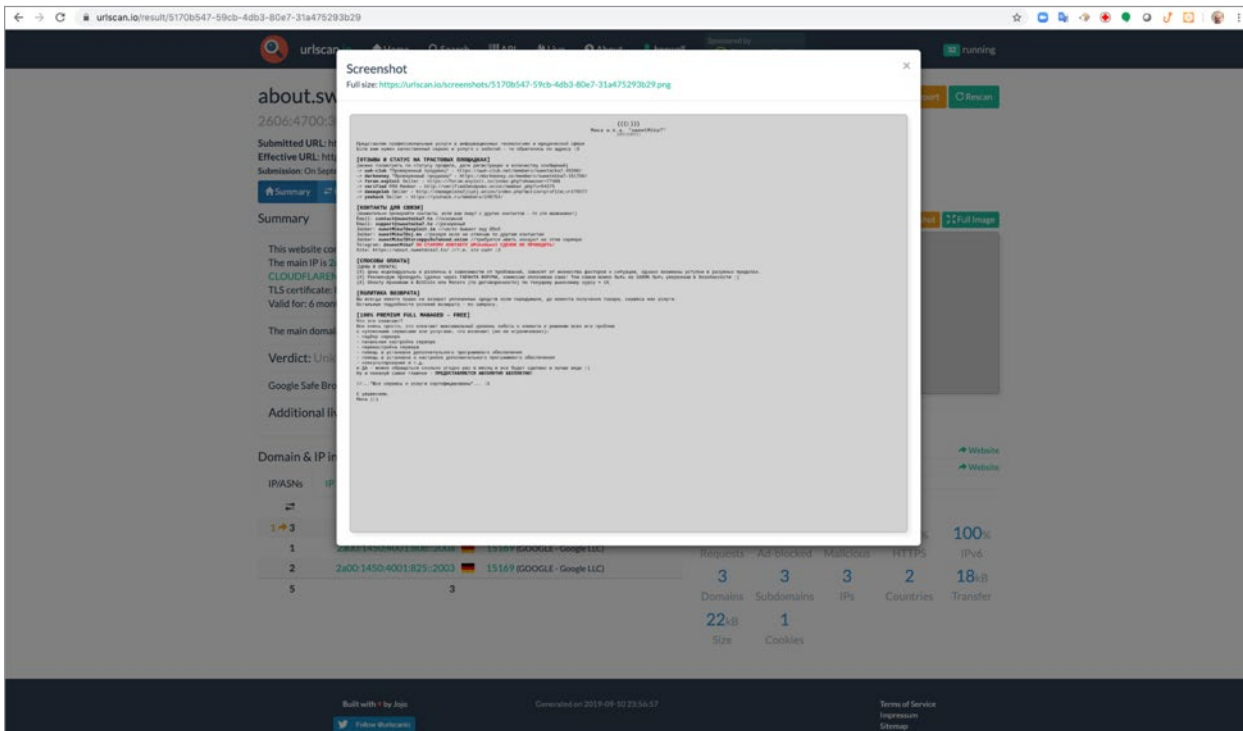
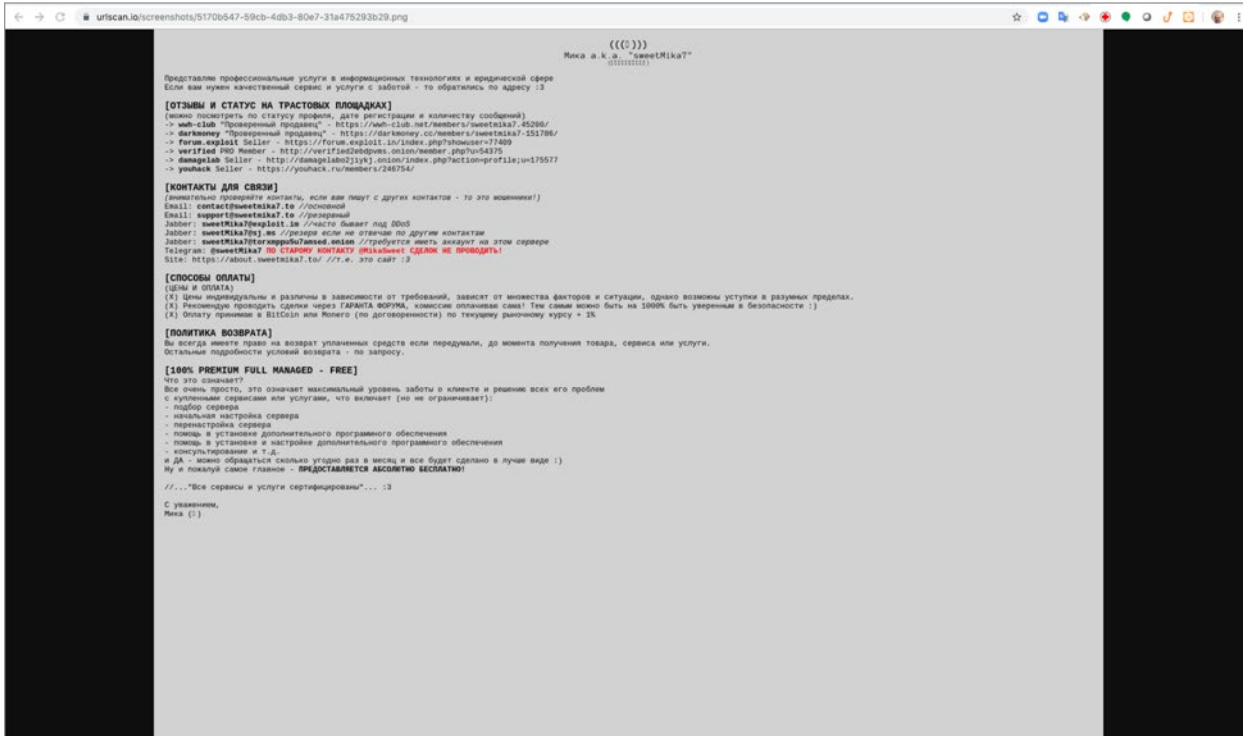
dark-fail.org

<https://urlscan.io/result/739dd852-3890-43ce-8ba1-c2db368d297d>



This website appears to list a dark web website featuring different marketplaces where payment cards can be bought and sold.

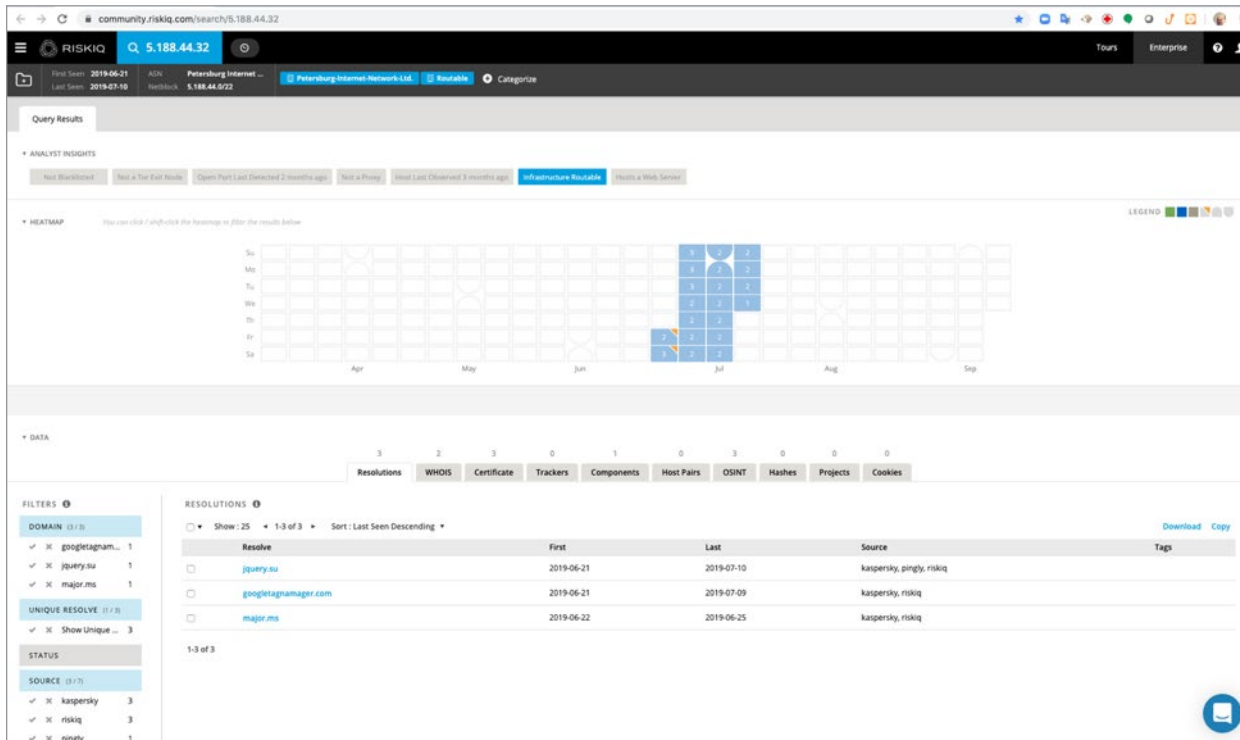
about.sweetmika7[.]to
<https://urlscan.io/result/5170b547-59cb-4db3-80e7-31a475293b29>



This website appears to list how and whom to contact for different dark web services.

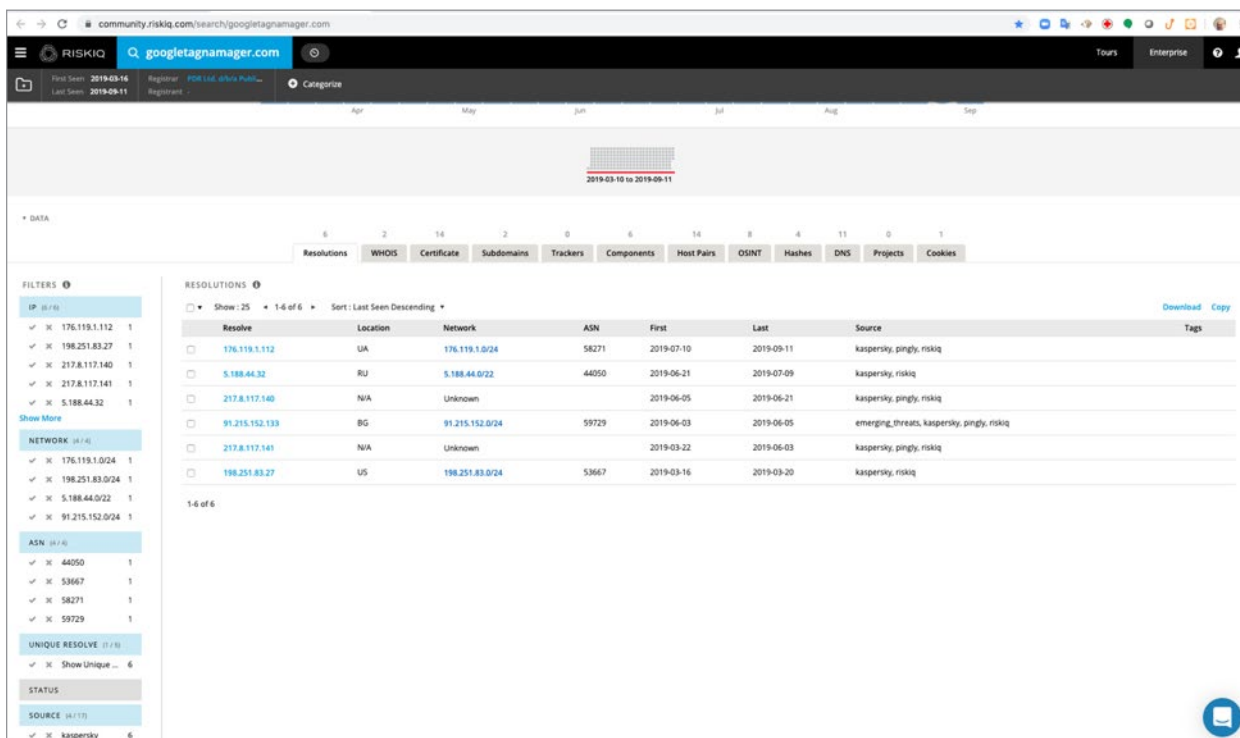
Step 9: go back to the tab 5[.]188[.]44[.]32

<https://community.riskiq.com/search/5.188.44.32>



Pivot search for googletagmanager[.]com and open it in a new tab.

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



Here we see several IP addresses located in Ukraine, Russia, and Bulgaria.

Step 10: click on the WHOIS tab.

The screenshot shows the RiskIQ community search interface. The search query is 'googletagmanager.com'. The 'WHOIS' tab is selected, displaying a record from 2019-07-08. The record shows the domain is registered to Alexander Kolmakov in Moscow, Russia. The contact information includes an email address: alexander.colmakov2017@yandex.ru. The record also shows the domain's expiration date as 2020-03-16T14:36:54Z.

Attribute	Value
WHOIS Server	whois.PublicDomainRegistry.com
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com
Email	alexander.colmakov2017@yandex.ru (registrant, admin, tech)
Name	Alexander Kolmakov (registrant, admin, tech)
Organization	
Street	Iverskoy 18 kv 12 (registrant, admin, tech)
City	Moscow (registrant, admin, tech)
State	Moscow (registrant, admin, tech)
Postal	121345 (registrant, admin, tech)
Country	RUSSIAN FEDERATION (registrant, admin, tech)
Phone	79267355576 (registrant, admin, tech)
NameServers	a83327a.bitcoin-dns-hosting a8336824.bitcoin-dns-hosting

The WHOIS information is not privacy protected. It is registered to Alexander Kolmakov in Moscow.

Step 11: Pivot search on the email address alexander[.]colmakov2017@yandex[.]ru

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

The screenshot shows the RiskIQ community search interface with the search query 'alexander.colmakov2017@yandex.ru'. The 'WHOIS SEARCH' tab is selected, displaying a table of results. The table has columns for Focus, Email, Registered, Expires, and Tags. The results show three domains: googletagmanager.com, jquery.su, and serversoftwarebase.com, all registered to alexander.colmakov2017@yandex.ru.

Focus	Email	Registered	Expires	Tags
googletagmanager.com	alexander.colmakov2017@yandex.ru	2019-03-16	2020-03-16	
jquery.su	alexander.colmakov2017@yandex.ru	2019-02-27	2020-02-27	
serversoftwarebase.com	alexander.colmakov2017@yandex.ru	2018-10-18	2019-10-18	

We see a new avenue of investigation serversoftwarebase[.]com

Step 12: Right-click on serversoftwarebase[.]com and open it in a new tab.

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

community.riskiq.com/search/serversoftwarebase.com

First Seen: 2018-10-18
Last Seen: 2019-08-11

Resolutions

Resolve	Location	Network	ASN	First	Last	Source	Tags
190.97.166.189	PA	190.97.166.0/24	3356	2019-05-17	2019-09-11	emerging_threats, kaspersky, pingly, riskiq	
190.97.167.116	PA	190.97.167.0/24	3356	2018-10-19	2019-05-15	emerging_threats, kaspersky, pingly, riskiq	
198.251.83.27	US	198.251.83.0/24	53667	2018-10-18	2018-10-18	riskiq	

1.3 of 3

Filters: IP (3/3), NETWORK (3/3), ASN (2/3), UNIQUE RESOLVE (1/3), STATUS, SOURCE (4/3)

IP location information is from Panama and the United States.

Step 13: Click on the OSINT tab

Here we see a list of internet articles that are related to serversoftwarebase[.]com. Click on the article for [www\[.\]redpacketsecurity\[.\]com](https://www.redpacketsecurity.com/new-golang-brute-forcer-discovered-amid-rise-in-e-commerce-attacks/), <https://www.redpacketsecurity.com/new-golang-brute-forcer-discovered-amid-rise-in-e-commerce-attacks/>

redpacketsecurity.com/new-golang-brute-forcer-discovered-amid-rise-in-e-commerce-attacks/

Are you using a VPN? If not I suggest using PrivateVPN. Port forwarding supported. [Check it out!](#)

HOME NEWS TUTORIALS

Home » News » New Golang brute-forcer discovered amid rise in e-commerce attacks

NEWS

New Golang brute-forcer discovered amid rise in e-commerce attacks

by admin | Published February 28, 2019

E-commerce websites continue to be targeted by online criminals looking to steal personal and payment information directly from unaware shoppers. Recently, attacks have been conducted via skimmer, which is a piece of code that is either directly injected into a hacked site or referenced externally. Its purpose is to watch for user input, in particular around online shopping carts, and send the perpetrators that data, such as credit card numbers and passwords, in clear text.

RECENT POSTS

- Julian Assange arrested: WikiLeaks founder arrested in London
- CVE-2019-0803: Cisco Routers - Critical glib CVESS Score
- CVE-2019-0804: New Elevation of Privilege Vulnerability Found in Cisco WebEx Meetings
- Chrome Zero-Day Exploited to Harvest User Data via PDF Files
- Government-funded researchers investigate vulnerabilities in EV charging stations

SEARCH

ARCHIVES

- April 2019
- February 2019
- October 2018
- May 2018

Please follow me on:

Twitter Telegram

Compromising e-commerce sites can be achieved in more than one way. Vulnerabilities in popular

We use cookies to ensure that we give you the best experience on our website. If you continue to use this site we will assume that you are happy with it.

redpacketsecurity.com/new-golang-brute-forcer-discovered-amid-rise-in-e-commerce-attacks/

Are you using a VPN? If not I suggest using PrivateVPN. Port forwarding supported. [MORE INFO](#)

Indicators of Compromise (IOCs)

Skimmer domain

```
googletagmanager[.]eu
```

Delphi downloader

```
cbe74b47bd7ea953268b5df3378d11926bf97ba72d326d3ce9e0d78f3e0dc786
```

Delphi C2

```
anaphyteplie1dup[.]xyz
tolmeta[.]info
serversoftwarebase[.]com
```

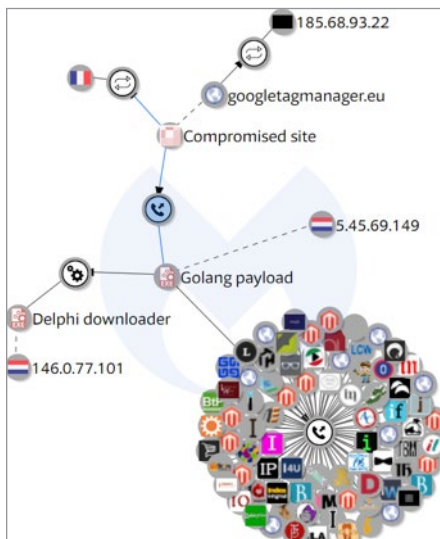
Golang bruteforcer

```
fdc3e15d2bc80b092f69f89329ff34b7b828be976e5cbe41e3e5720f7896c140
```

Similar Golang bruteforcers

```
46fd1e8d08d06c0b9d91e2fe19a1173821dfffa051315626162e9d4b38223bd4a
05073af551fd4064cced8a8b13a4491125b3cd1f08dfe3d3970b8211c46e6b2
fdc3e15d2bc80b092f69f89329ff34b7b828be976e5cbe41e3e5720f7896c140
96a5b2a8fcd28b560f92937720ad0dc5c30c705e4ce88e3f82c2a5d3ad085aa
```

We use cookies to ensure that we give you the best experience on our website. If you continue to use this site we will assume that you are happy with it. [Ok](#)



According to the article serversoftwarebase.com is a Delphi C2 server.

Step 14: Go back to the tab for googletagmanager[.]com

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

Click on the OSINT tab.

The screenshot shows the RiskIQ community search interface. The search term is 'googletagmanager.com'. The 'OSINT' tab is selected, displaying a table of results. The table has columns for 'Source', 'Link', and 'Tags'. The results list various sources like bgs.he.net, uriscan.io, github.com, www.reddit.com, uriscan.io, www.rdbx.com, uriscan.io, bgs.he.net, mescan.s3.amazonaws.com, and bgs.he.net, each with a corresponding link and tags such as 'search-engine', 'github', 'reddit', 'uriscan', 'rdbx', 'he', and 'amazonaws'.

Step 15: Click on the link to the Reddit article.

https://www.reddit.com/r/Magento/comments/chy3lm/fake_google_domains_used_in_evasive_magento/?ref=readnext

The screenshot shows a Reddit post from the r/Magento community. The post title is 'Fake Google Domains Used in Evasive Magento Skimmer'. The post content describes a security incident where a Magento website was infected with a credit card skimmer. The skimmer was using a JavaScript script from a domain that was a variation of 'google-analytics.com'. The post includes a source link: <https://blog.sucuri.net/2019/07/fake-google-domains-used-in-evasive-magento-skimmer.html>. The post has 3 comments and is sorted by 'BEST'. The comments section shows a discussion about the incident, with one comment mentioning that the domains were down at the time and another mentioning that the domains were on-line and serving malicious scripts again.

The information in the Reddit post talk about the two domains we are investigating, googletagmanager[.]com and jquery[.]su. They describe cleaning up a credit card “CC” skimmer. Our analysis seems to be correct that the two domains are involved in skimming payment card information.

One more thing to note. The post above is unrelated to our attack but points out how sneaker threat actors are in their typosquatted domains. If you notice that google-analytics[.]com (or in ASCII xn--google-analytcs-xpb[.]com). The letter “i” is called an i-circumflex used in languages like French, Turkish, and Italian. When examining your website’s logs or the DOM this could easily be overlooked as a regular letter “i”. Please be careful when examining your logs to check for these types of attacks.

Step 16: Go back to the tab for googletagmanager[.]com

Click on the Host Pairs tab.

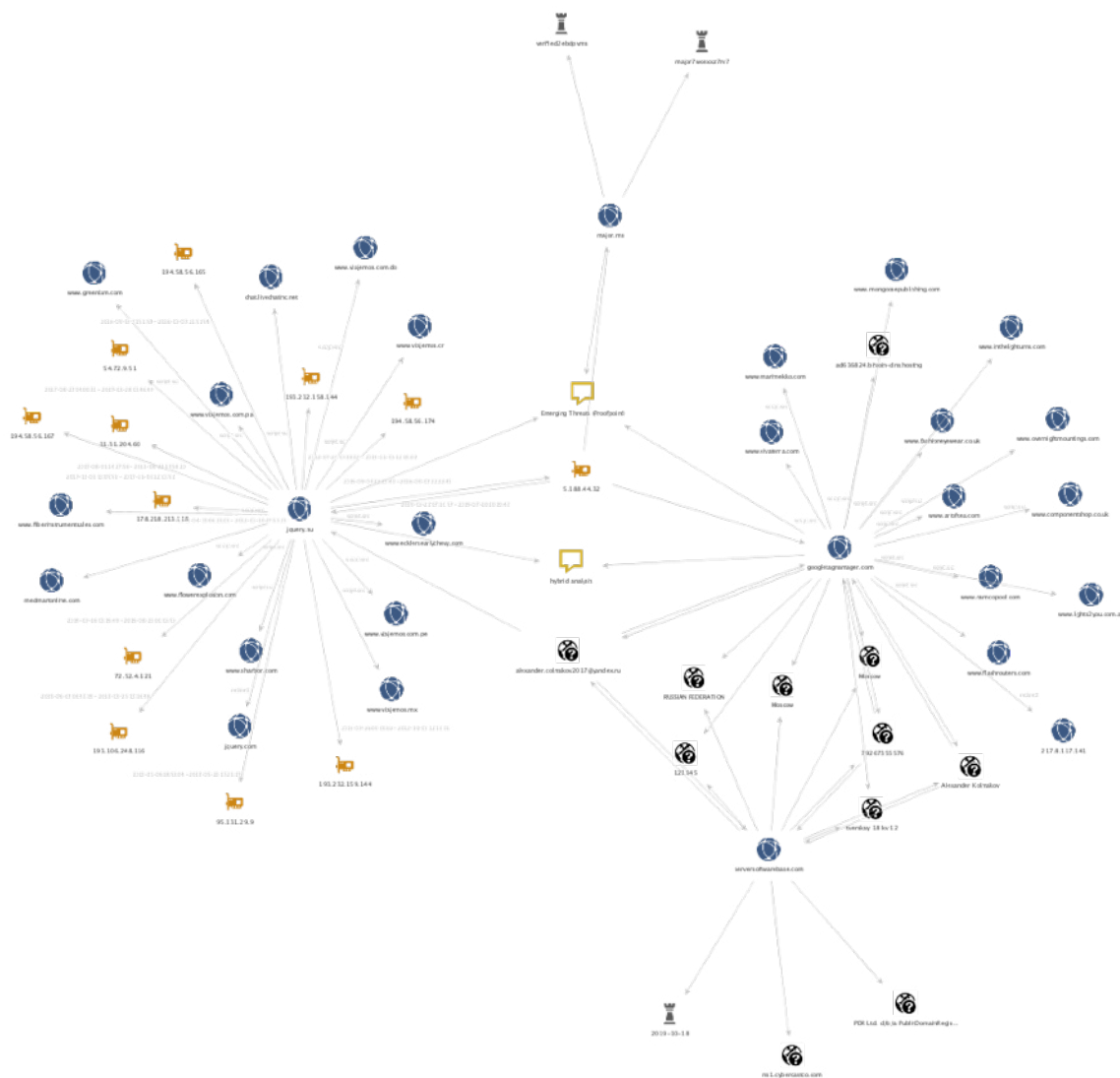
The screenshot shows the RiskIQ search interface for **googletagmanager.com**. The 'Host Pairs' tab is active, displaying a table of parent and child hostnames. The table lists various domains like **www.vivatera.com**, **www.inthelightturns.com**, and **www.componentshop.co.uk**, all linked to **googletagmanager.com** as the child. The cause for most is **script.src**, and the first seen dates range from May 2019 to August 2019.

Parent Hostname	Child Hostname	First	Last	Cause	Tags
googletagmanager.com	jquery.com	2019-05-12	2019-08-14	redirect	
www.inthelightturns.com	googletagmanager.com	2019-06-05	2019-06-19	script.src	
www.componentshop.co.uk	googletagmanager.com	2019-06-13	2019-06-13	script.src	
www.artoftea.com	googletagmanager.com	2019-06-02	2019-06-05	script.src	
www.lights2you.com.au	googletagmanager.com	2019-06-03	2019-06-03	script.src	
www.marimekko.com	googletagmanager.com	2019-06-03	2019-06-03	script.src	
www.flashrouters.com	googletagmanager.com	2019-06-01	2019-06-01	script.src	
www.overnightmountings.com	googletagmanager.com	2019-06-01	2019-06-01	script.src	
www.mongoosepublishing.com	googletagmanager.com	2019-05-25	2019-05-25	script.src	
217.8.117.141	googletagmanager.com	2019-05-21	2019-05-23	redirect	
www.namcopool.com	googletagmanager.com	2019-05-22	2019-05-22	script.src	
www.vivatera.com	googletagmanager.com	2019-05-11	2019-05-13	script.src	
www.vivatera.com	googletagmanager.com	2019-05-12	2019-05-12	unknown	
www.fashioneyewear.co.uk	googletagmanager.com	2019-04-08	2019-04-08	script.src	

All of the Parent Hostnames associated with googletagmanager[.]com have been observed running a script for this server. This means all of the domains listed a child relationship to googletagmanager[.]com with a cause of a script are also likely compromised as well. If you look at the first seen date you can see when RiskIQ discovered the attack and the Last date shown is when RiskIQ showed the site was no longer seen as compromised.

Now we know that the same threat actor that attack flower explosion is related to these other attacks.

Below is a Maltego map of this exercise showing the compromised websites and how they were connected to jquery[.]su and googletagmanager[.]com.



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

✉ sales@riskiq.net

☎ 1 888.415.4447

Learn more at riskiq.com

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