Advanced Use Case:

www[.]flowerexplosion[.]com

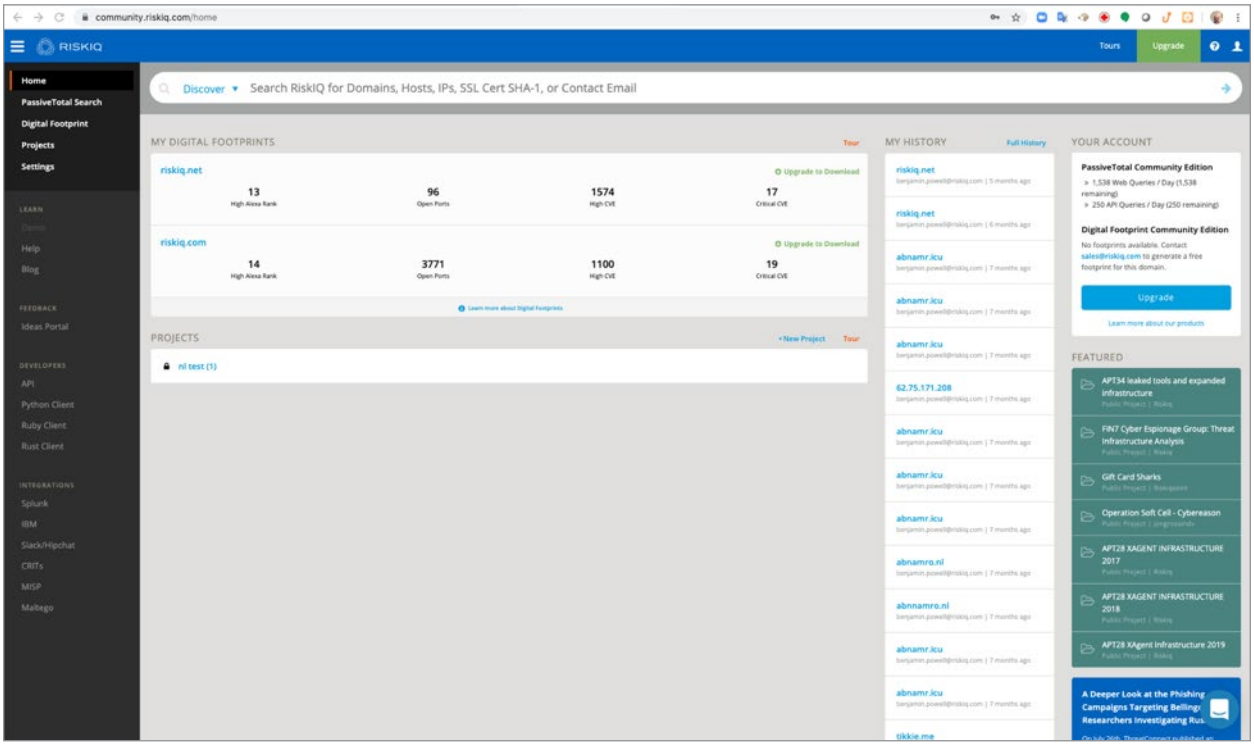
Part 2 - Jquery[.]su infrastructure investigation

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.

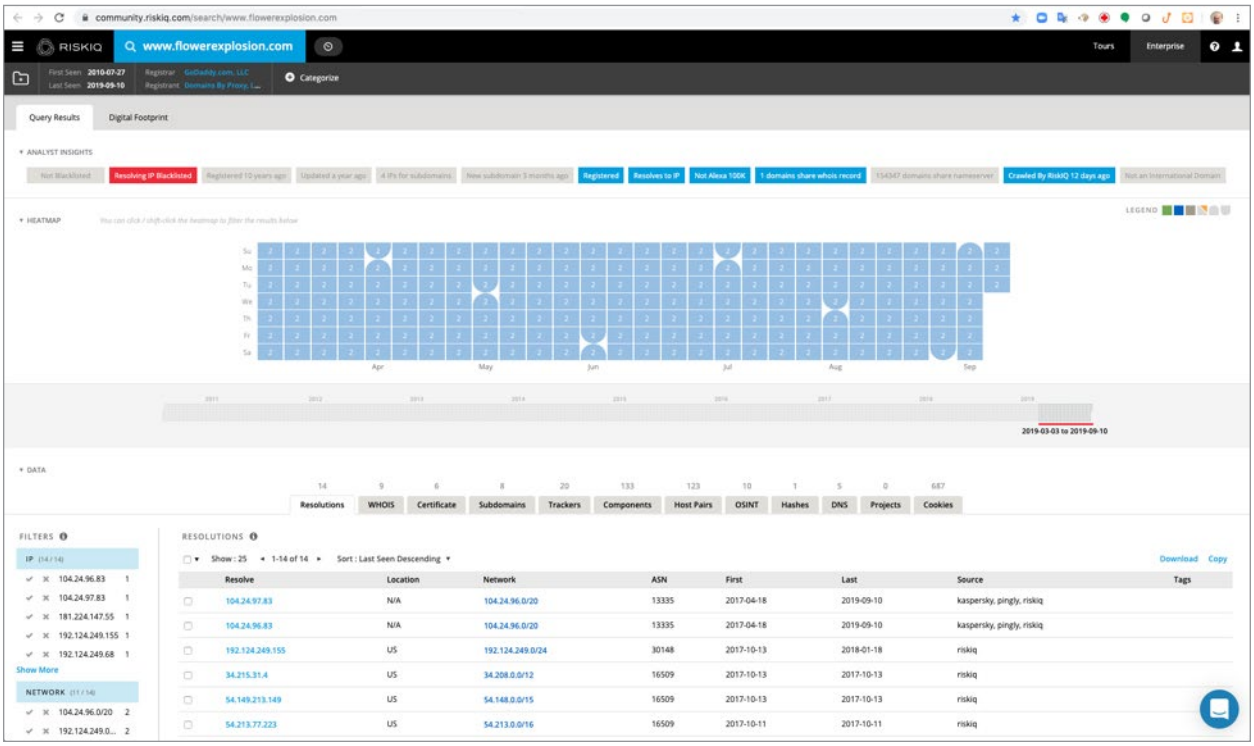
Now you need to further investigate the compromise to see the extent of the attack and try to identify the threat actor's infrastructure.

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

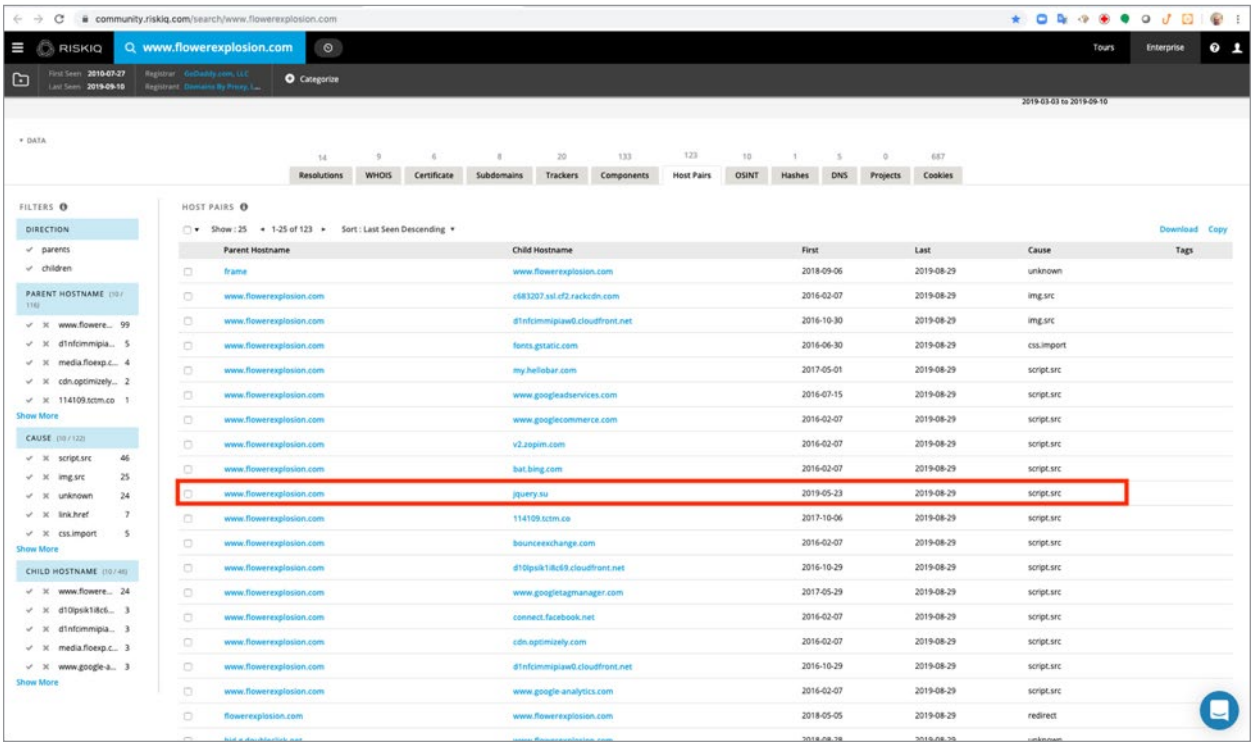


Step 2: Search for the domain www.flowerexplosion.com

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



Step 3: Click on the Host Pair tab

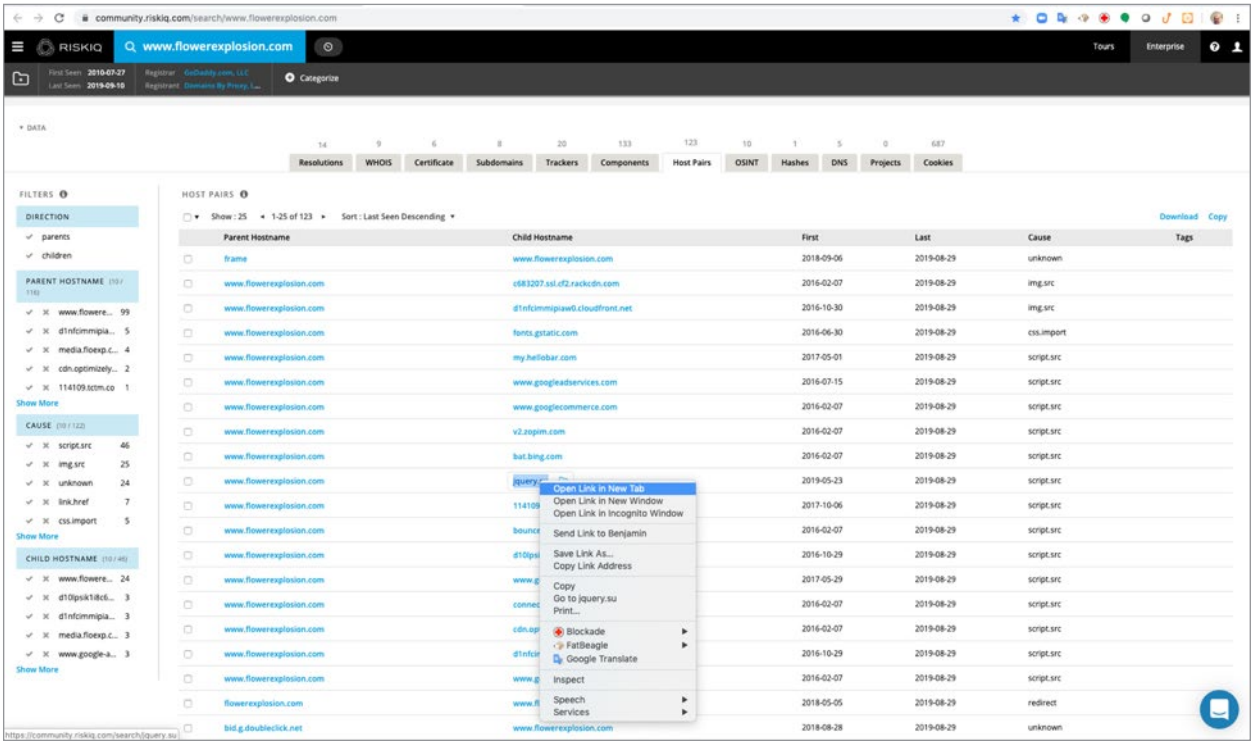


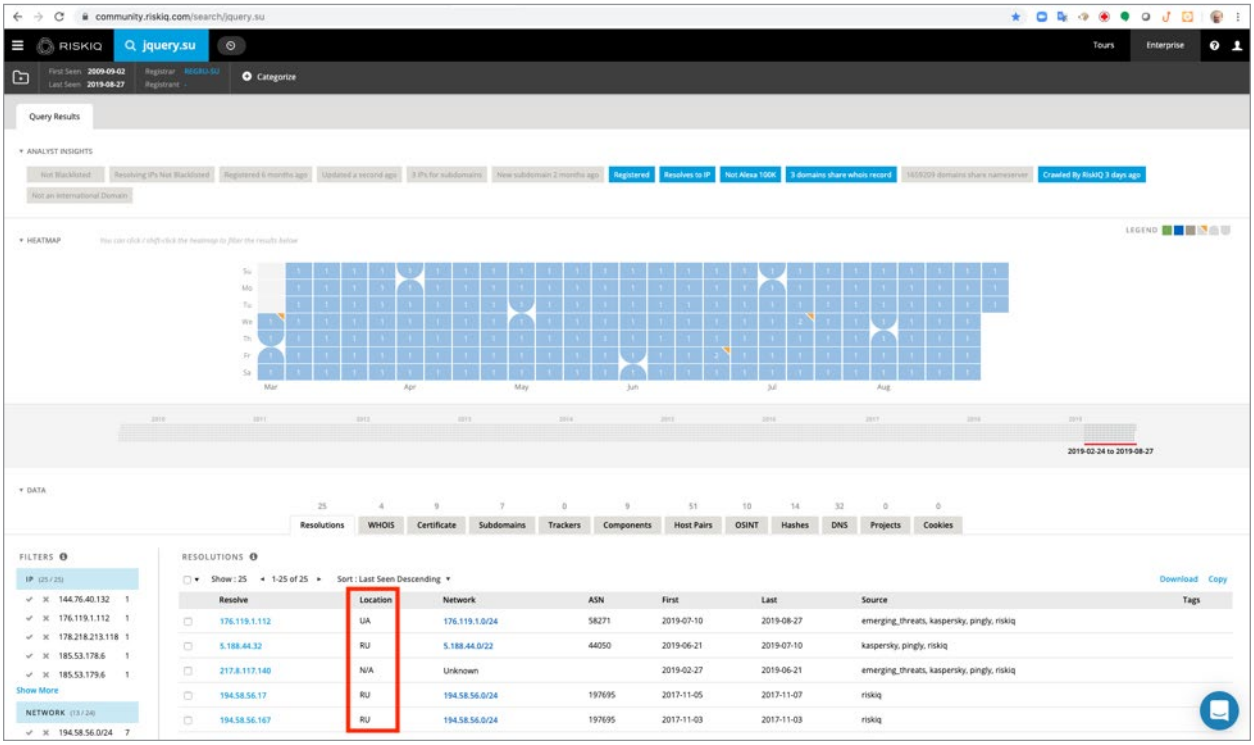
The malicious Magecart script came from jquery.su.

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

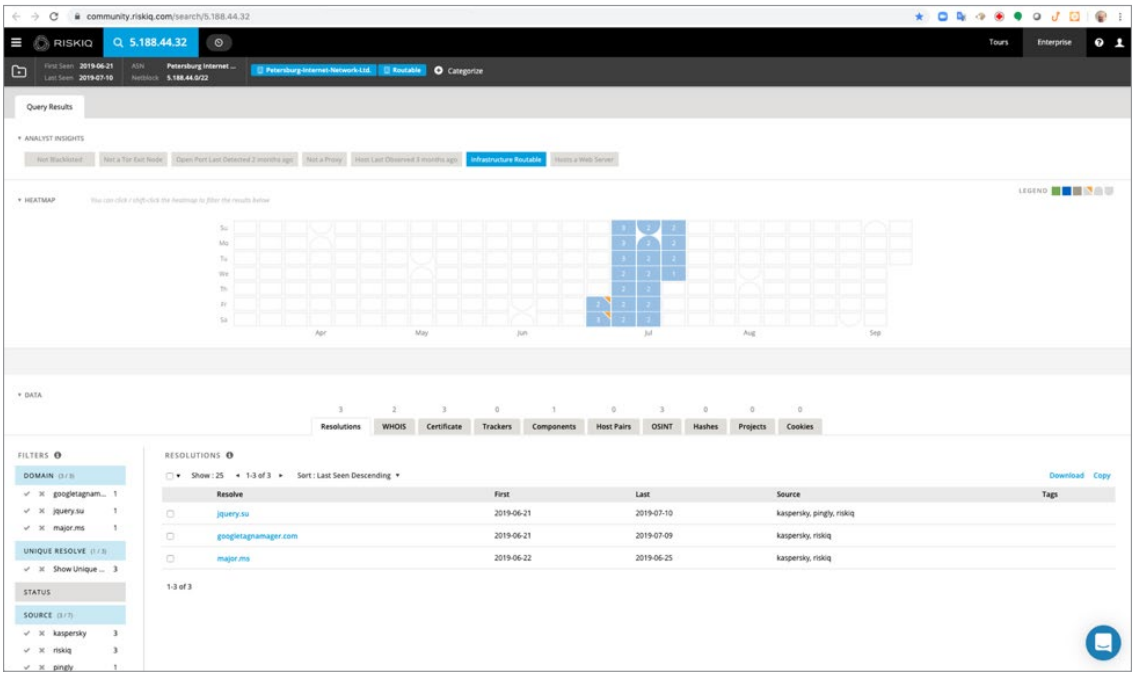




The threat actor web site resolves to IP addresses hosted in Ukraine and Russia.

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

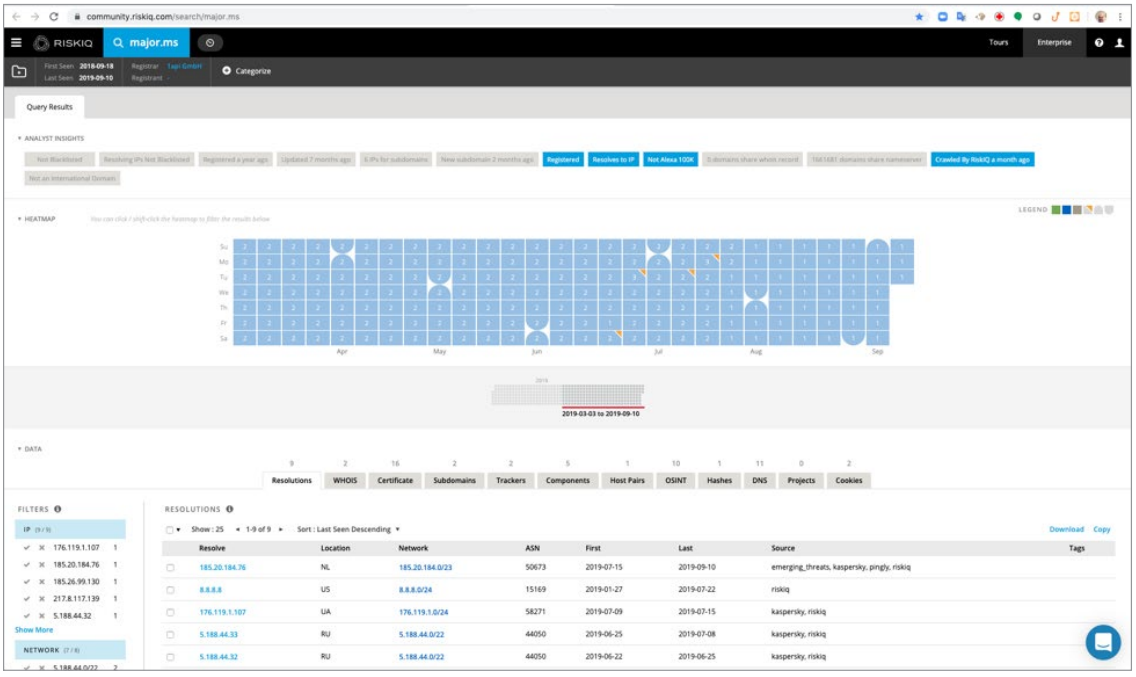
https://community.riskiq.com/search/5.188.44.32



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

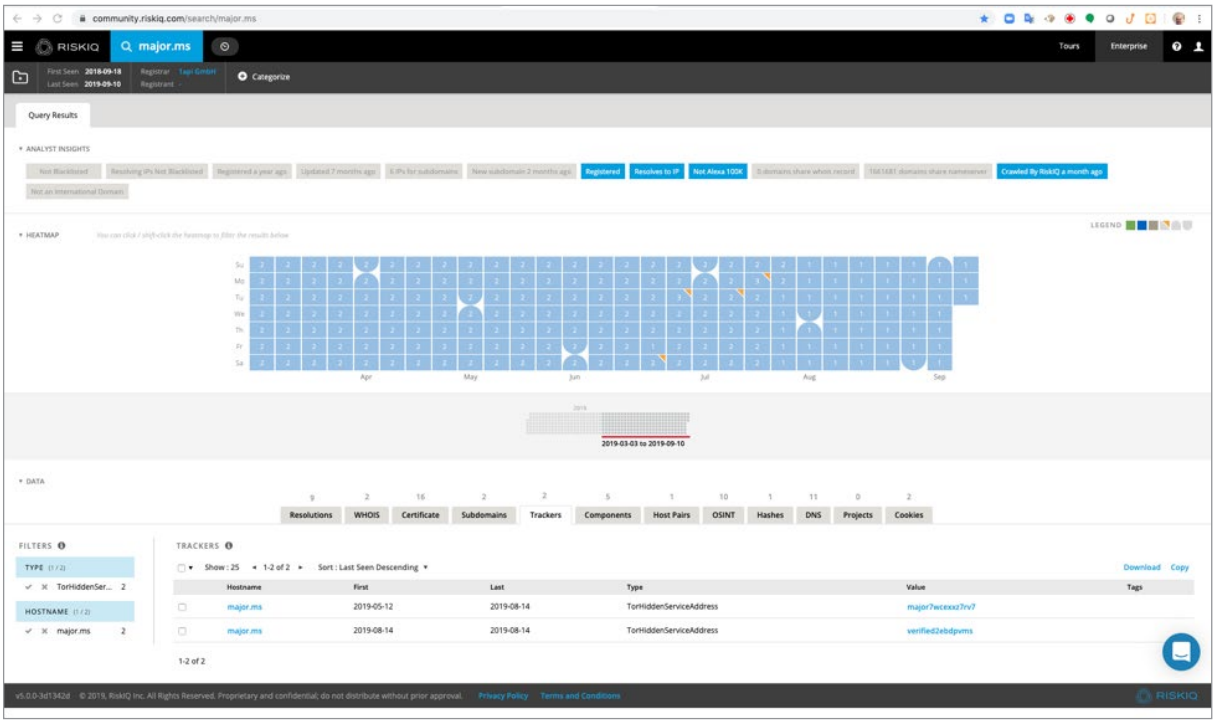
Step 6: Pivot search on major[.]ms and open it in a new tab.

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



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

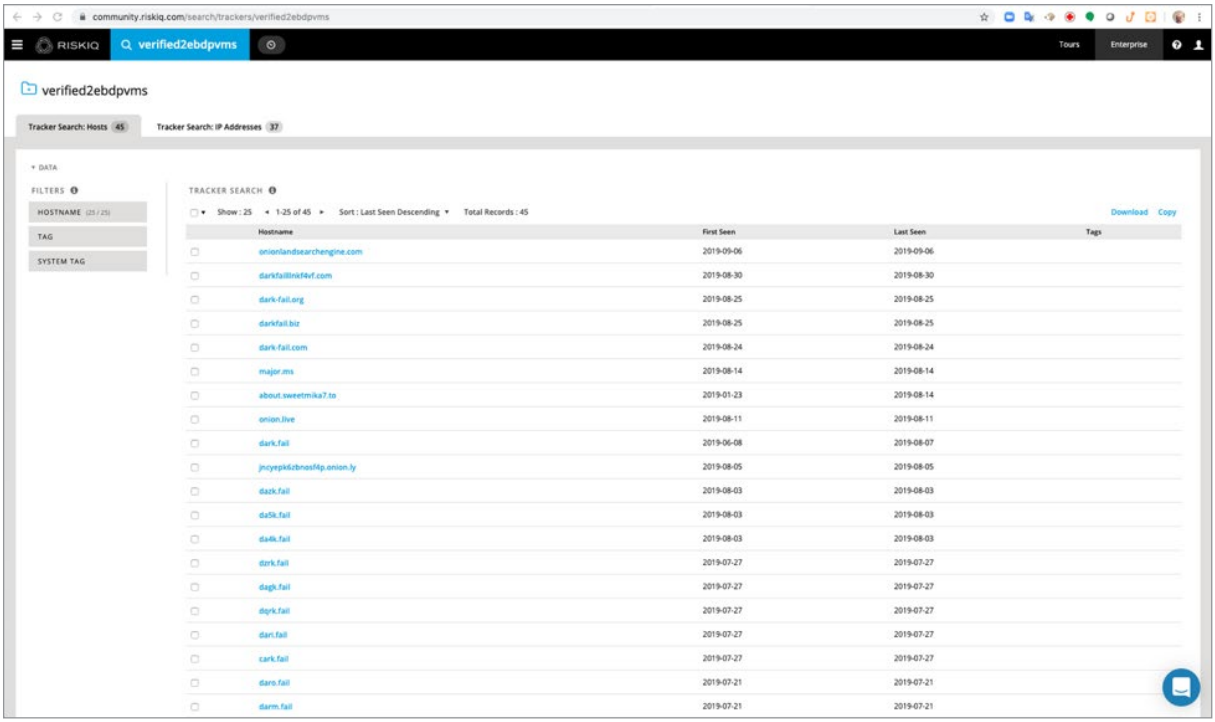
Step 7: click on the trackers tab



The tracker information is very unusual. RiskIQ crawls the entire open web's IPV4 space. When we get the DOM and responses, we are able to understand and create advanced derived data sets. We see in the results shows Tor Hidden service Address. This means that the domain major[.]ms is involved in the deep or dark web. This tracker is seen when websites might be linked to the open web and the deep or dark web utilizing the tor network.

Step 8: Pivot search on the value verified2ebdpvms and open it in a new tab.

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

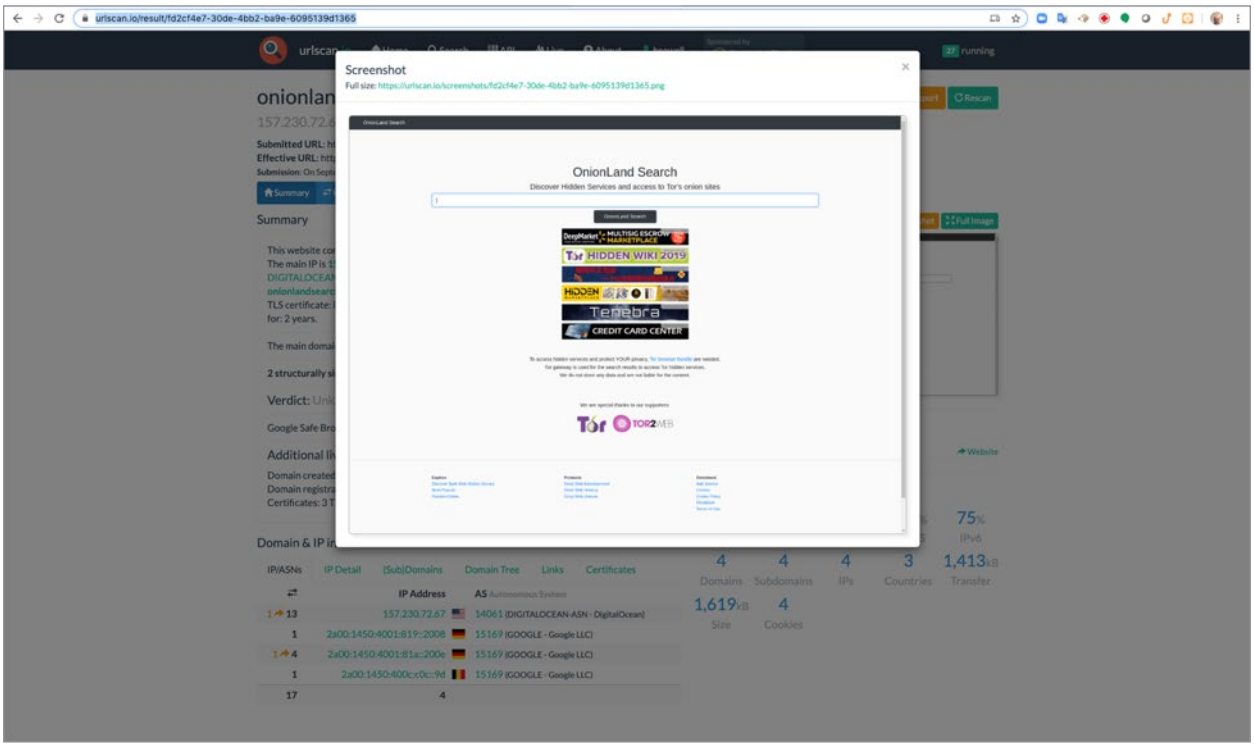


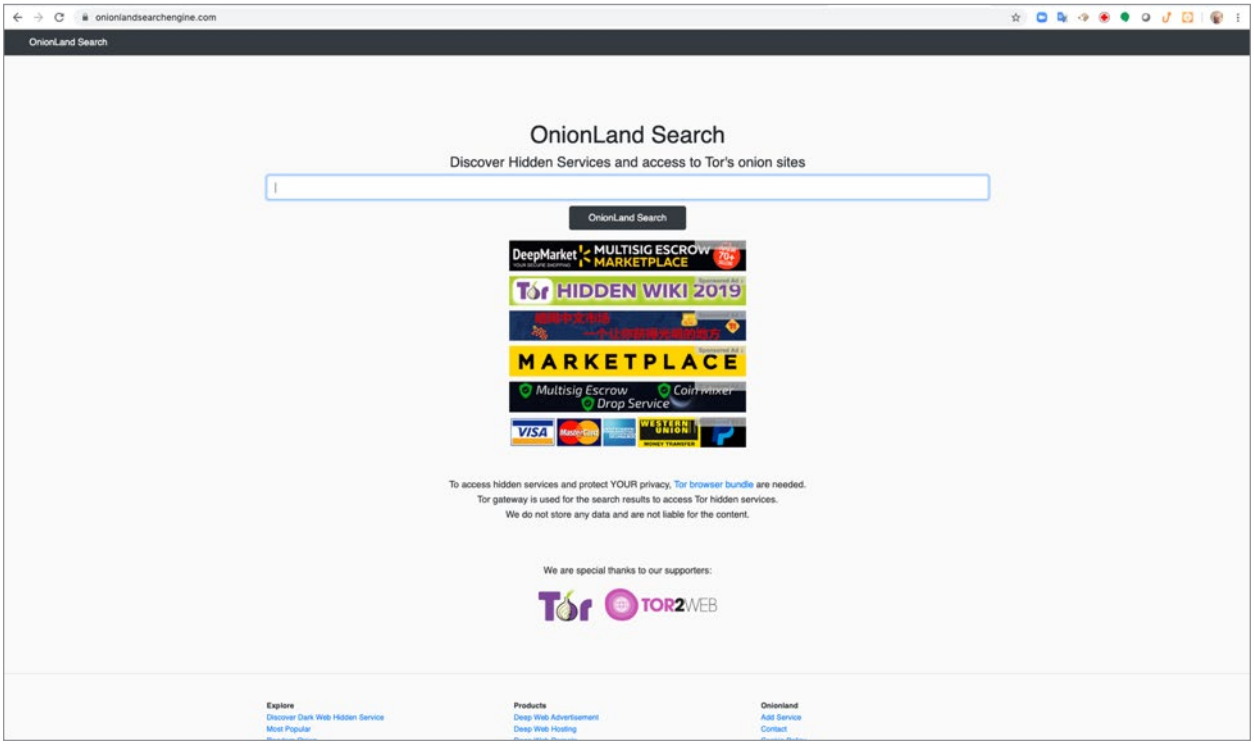
The results show 45 different hosts that are associated with the tracker.

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.

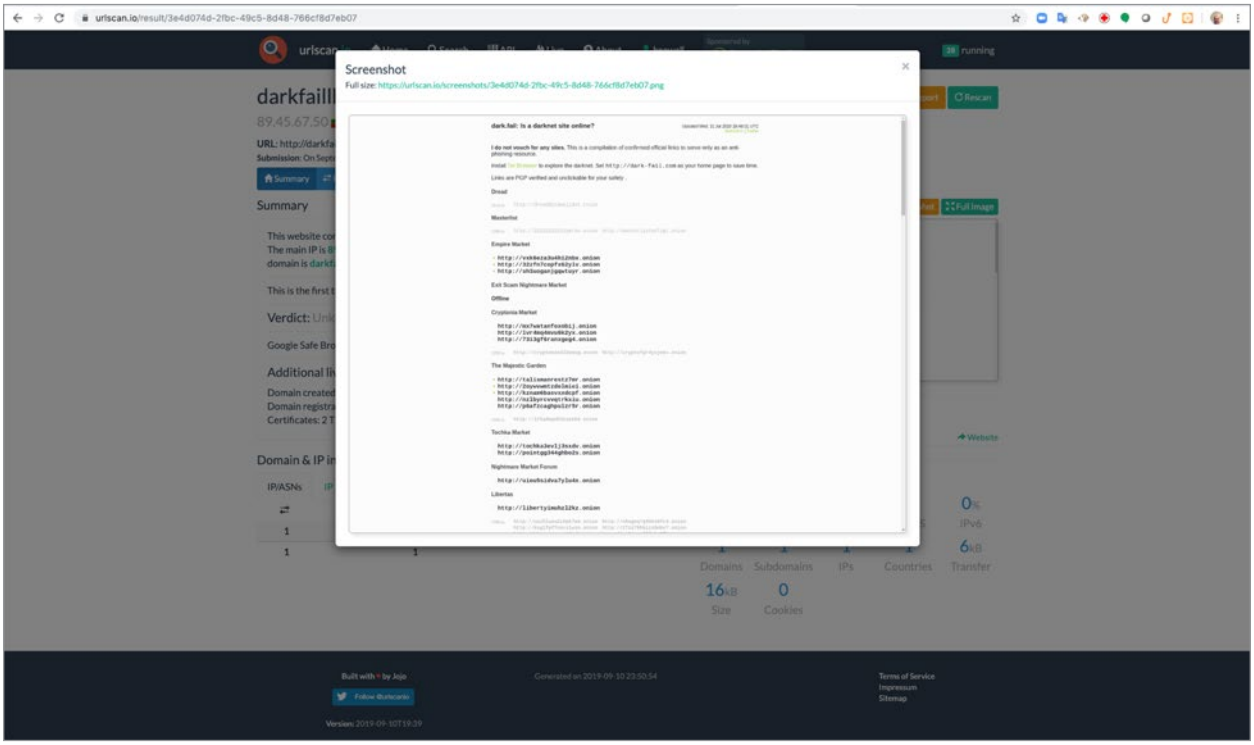
Onionlandsearchengine[.]com
https://urlscan.io/result/fd2cf4e7-30de-4bb2-ba9e-6095139d1365





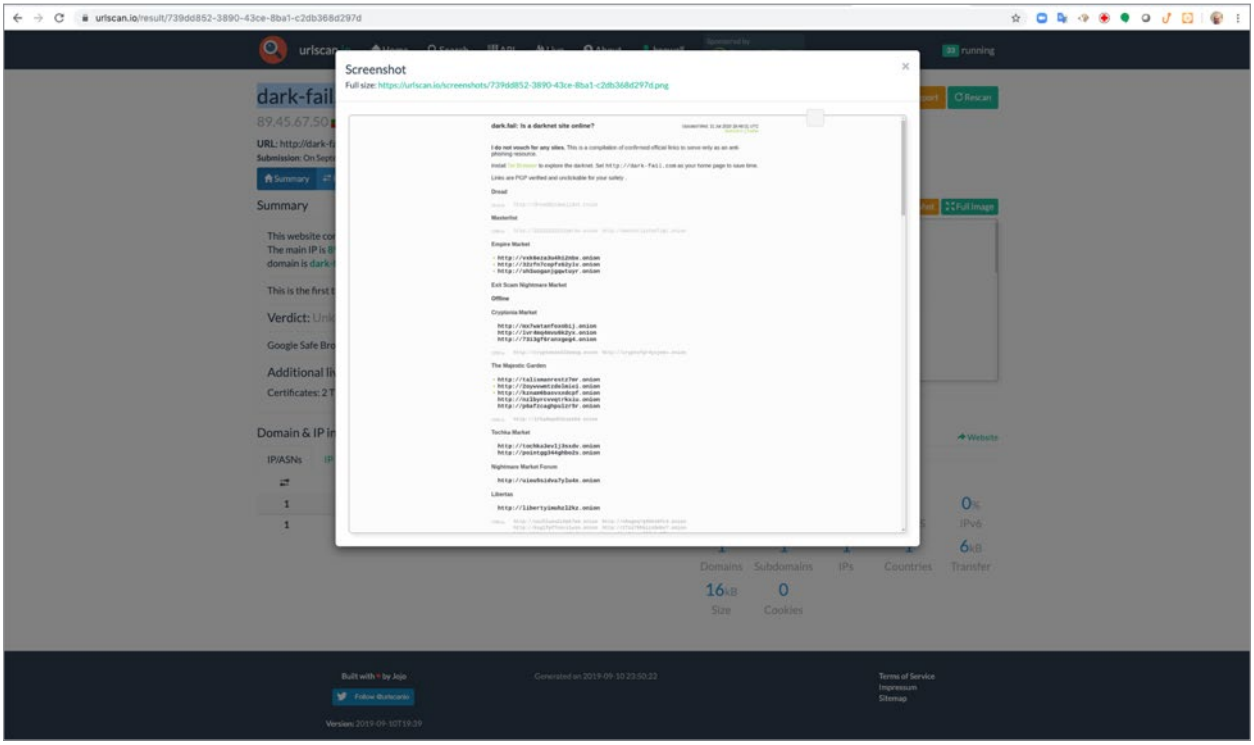
This website appears to be a way to search for things on the dark web.

darkfaillInkf4vf[.]com
https://urlscan.io/result/3e4d074d-2fbc-49c5-8d48-766cf8d7eb07



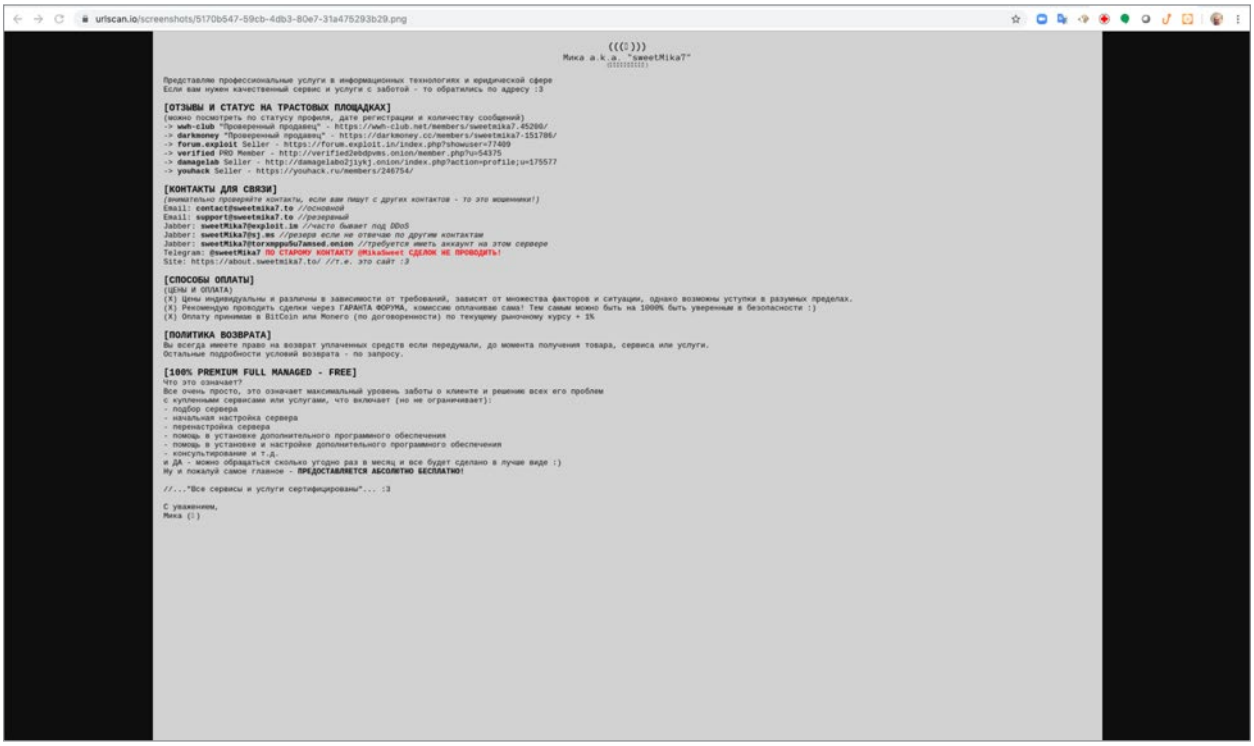
This website appears to list a dark web website featuring different marketplaces where payment cards can be bought and sold.

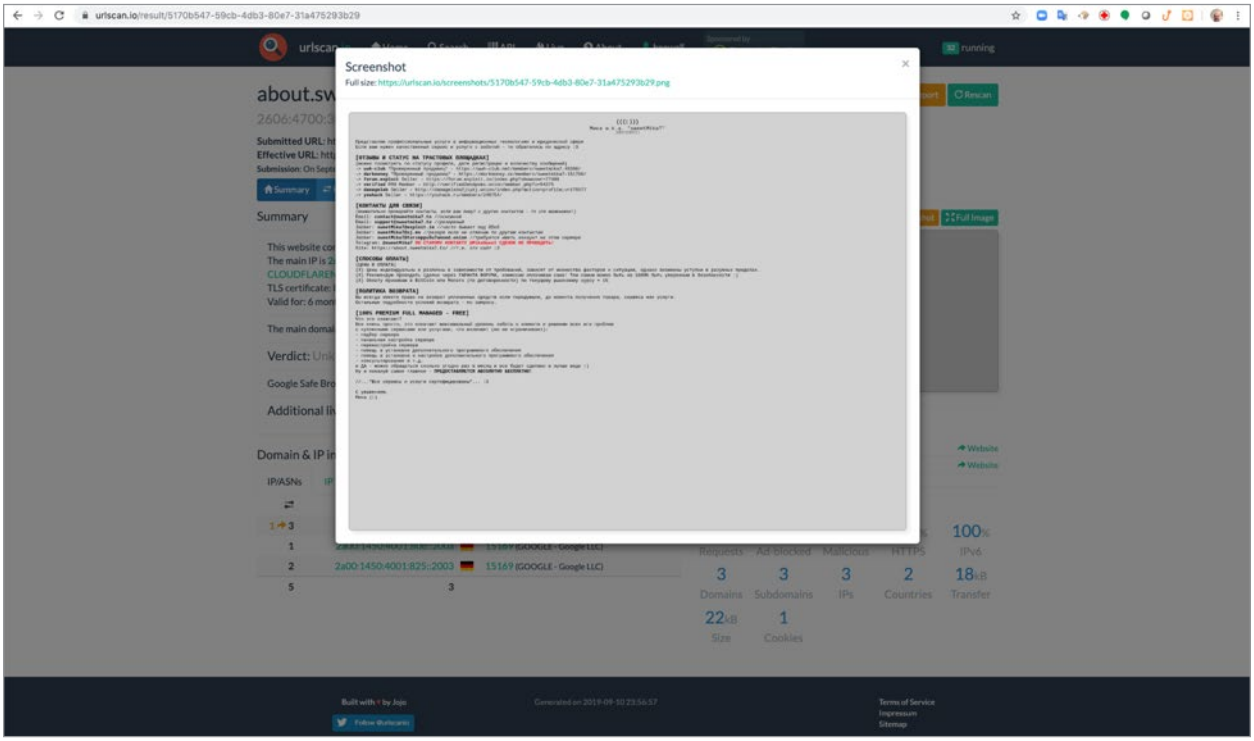
dark-fail[.]org
https://urlscan.io/result/739dd852-3890-43ce-8ba1-c2db368d297d



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

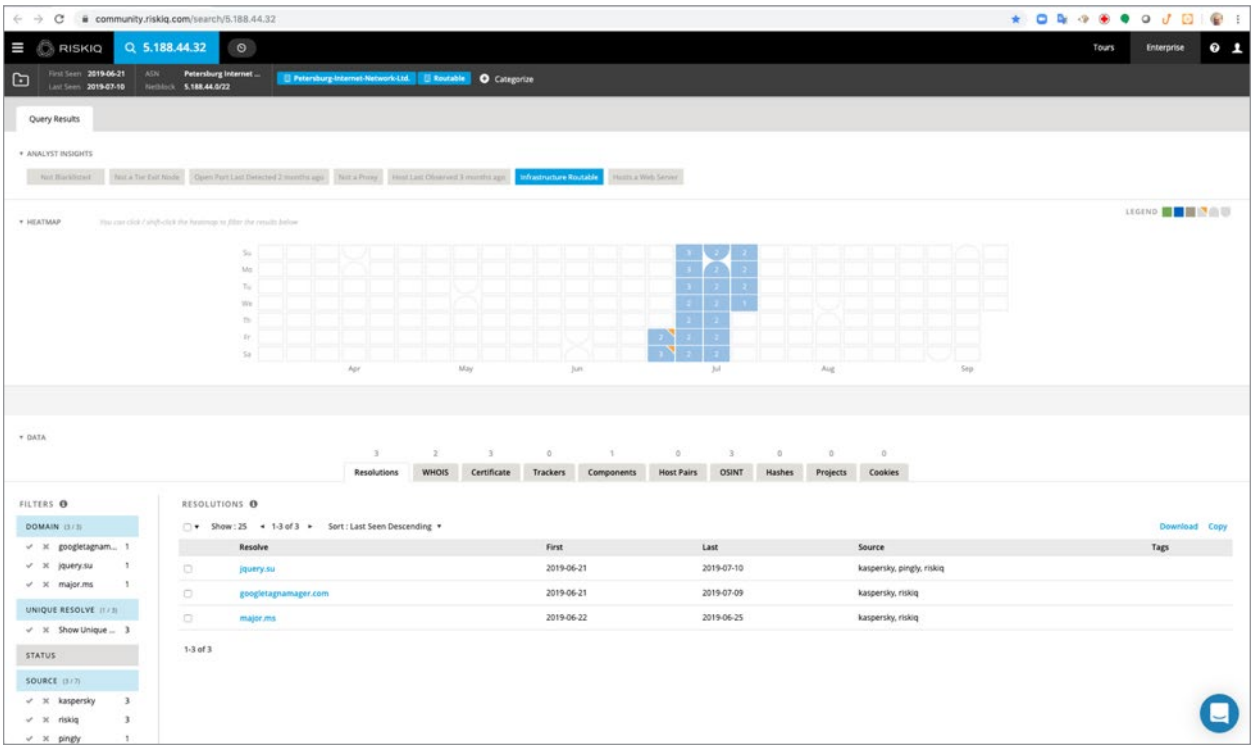




This website appears to list how and whom to contact for different dark web services.

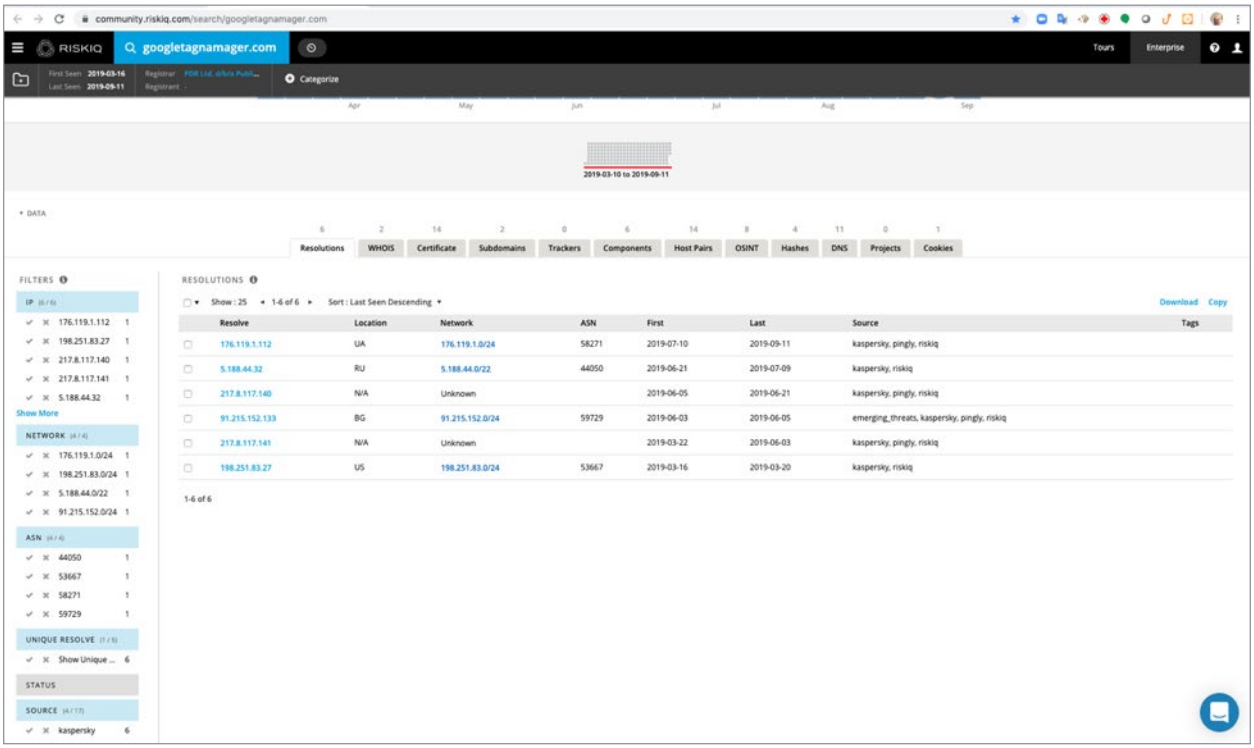
Step 9: go back to the tab 5[.]188[.]44[.]32

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



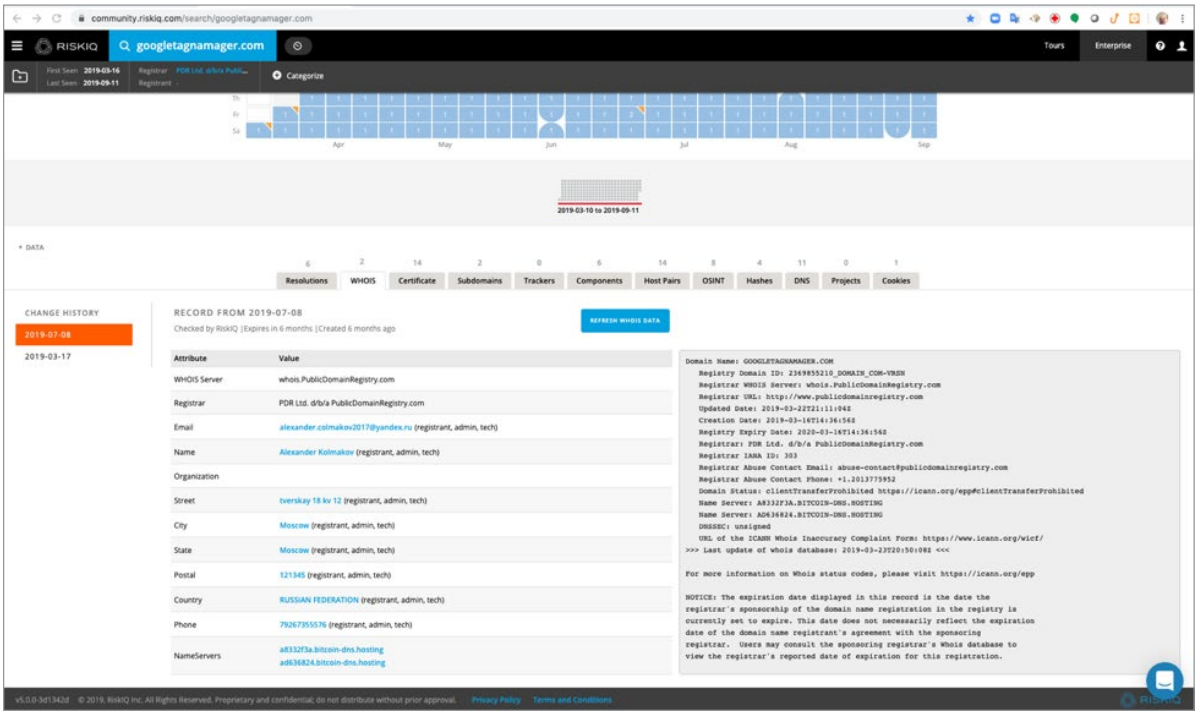
Pivot search for googletagnamager[.]com and open it in a new tab.

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



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

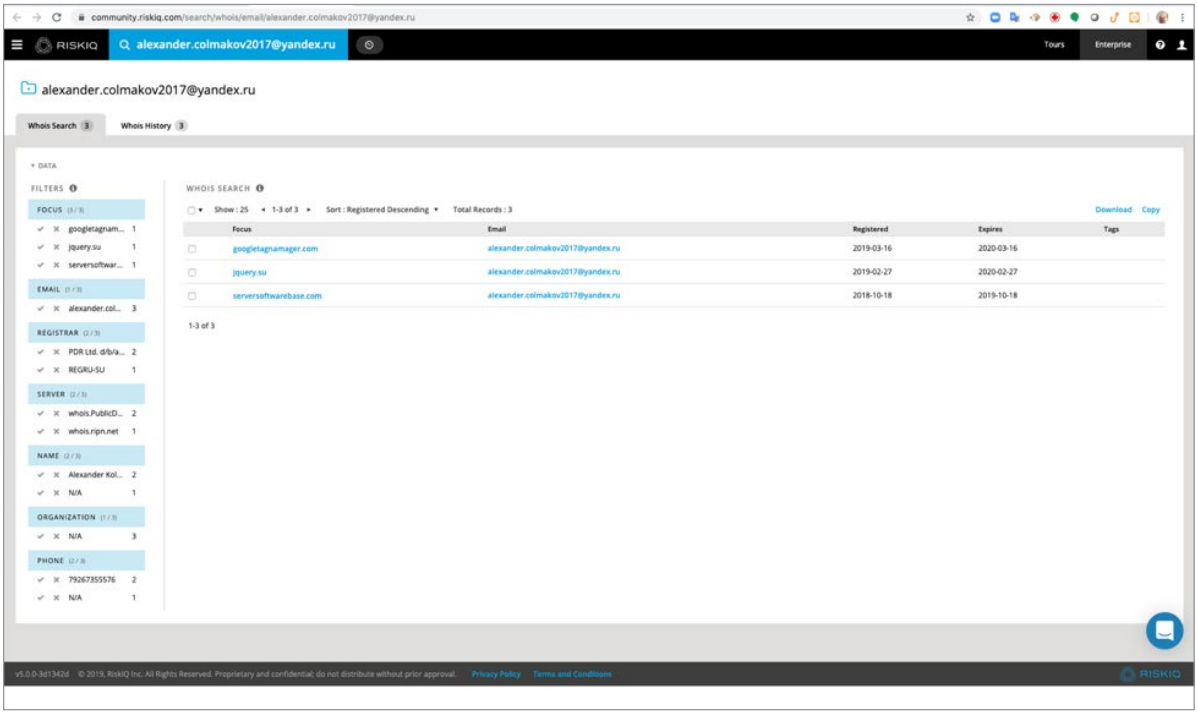
Step 10: click on the WHOIS tab.



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

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

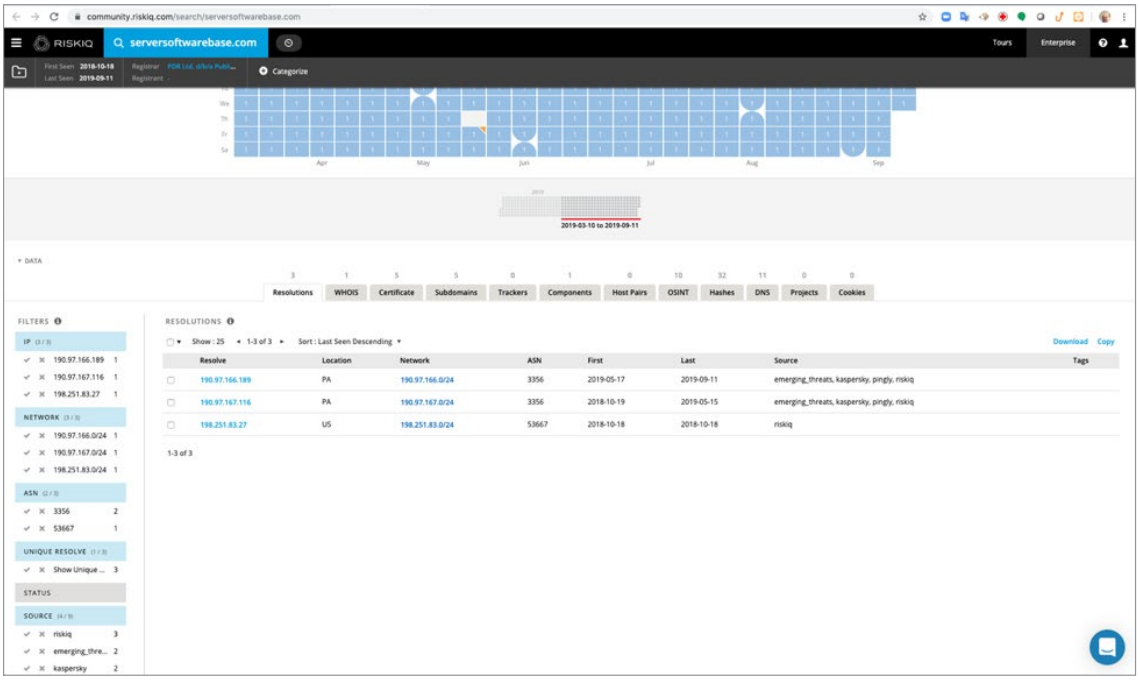
https://community.riskiq.com/search/whois/email/alexander.colmakov2017@yandex.ru



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

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

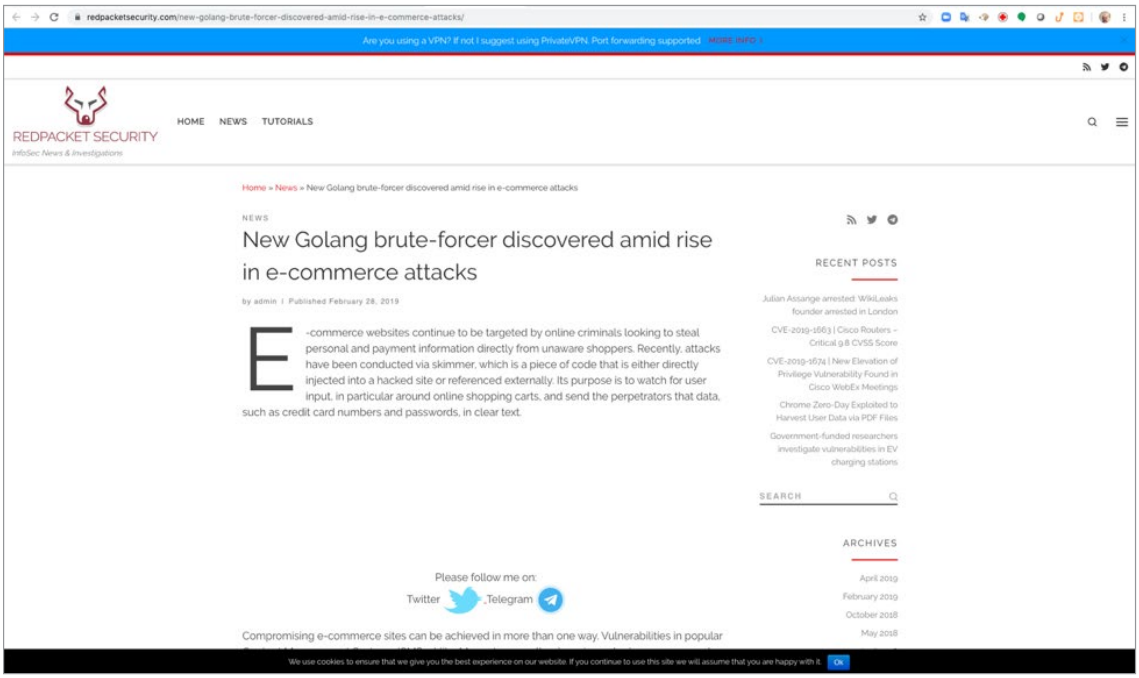
https://community.riskiq.com/search/serversoftwarebase.com

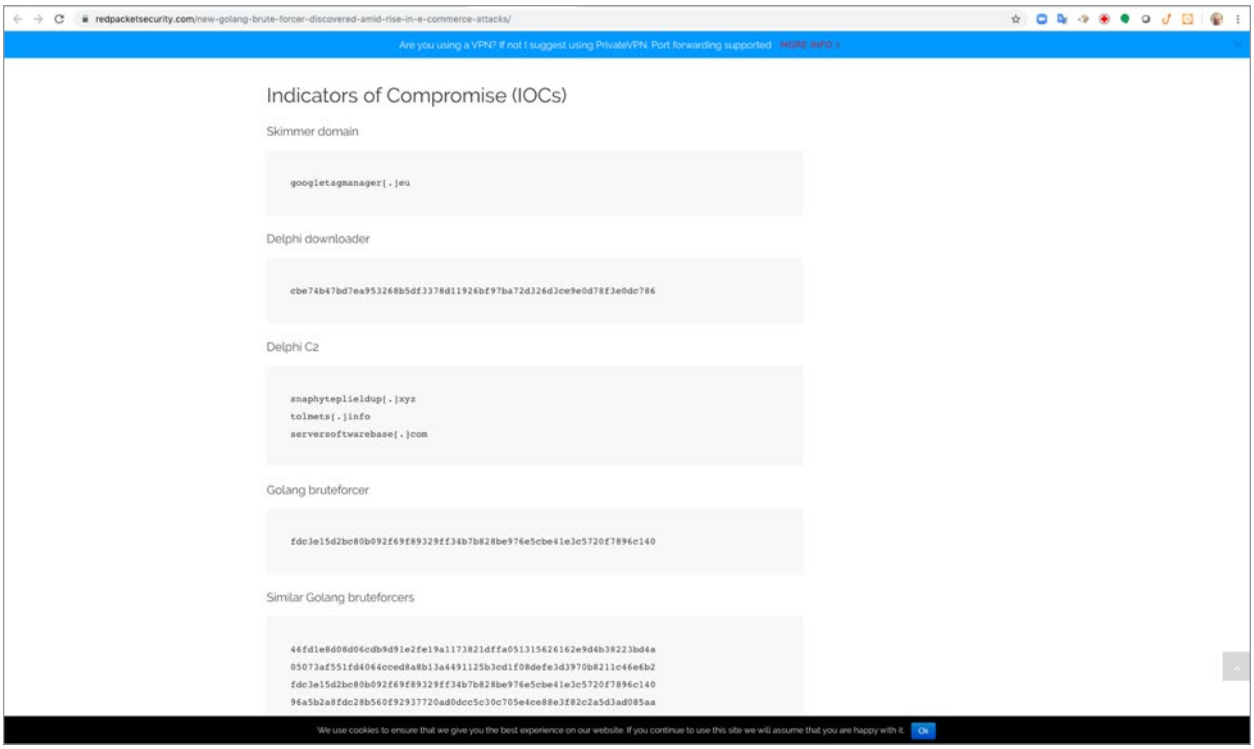


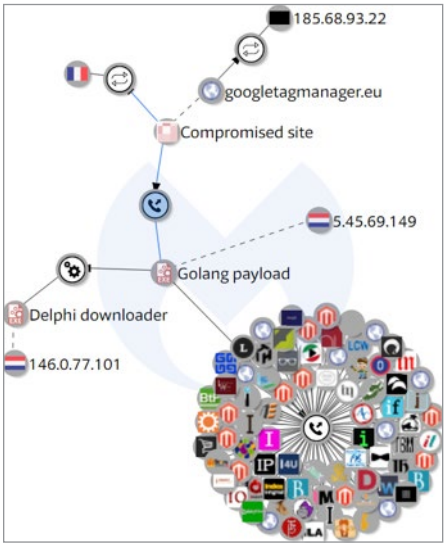
IP location information is from Panama and the United States.

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[.] redbacketsecurity[.]com, https://www.redpacketsecurity.com/new-golang-brute-forcer-discovered-amid-rise-in-e-commerce-attacks/





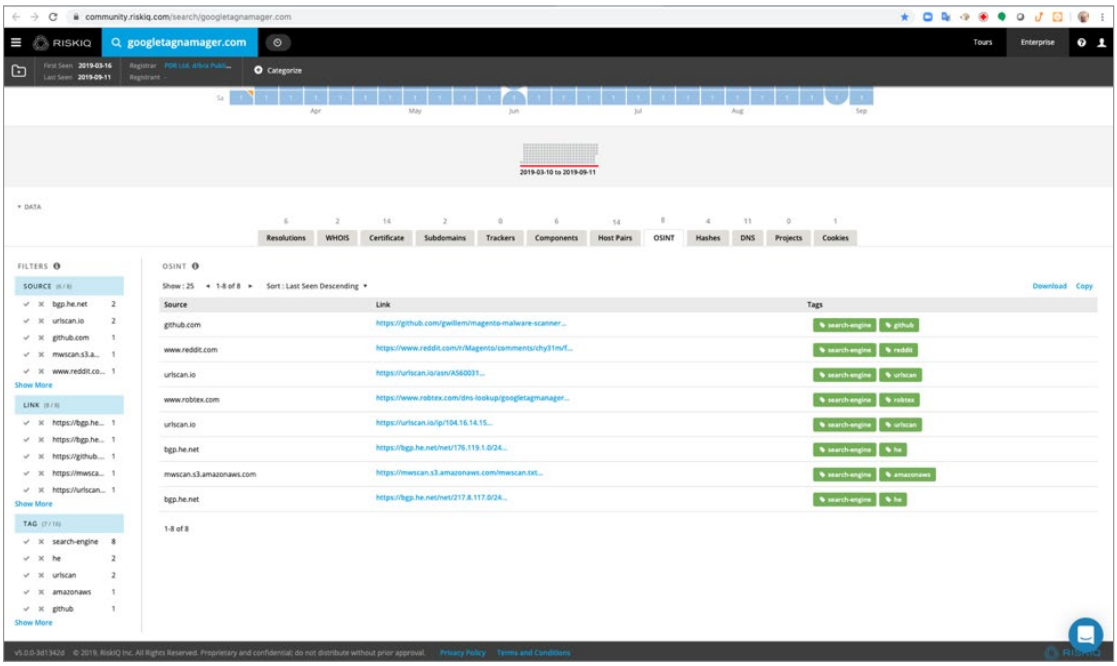


According to the article serversoftwarebase[.]com is a Delphi C2 server.

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

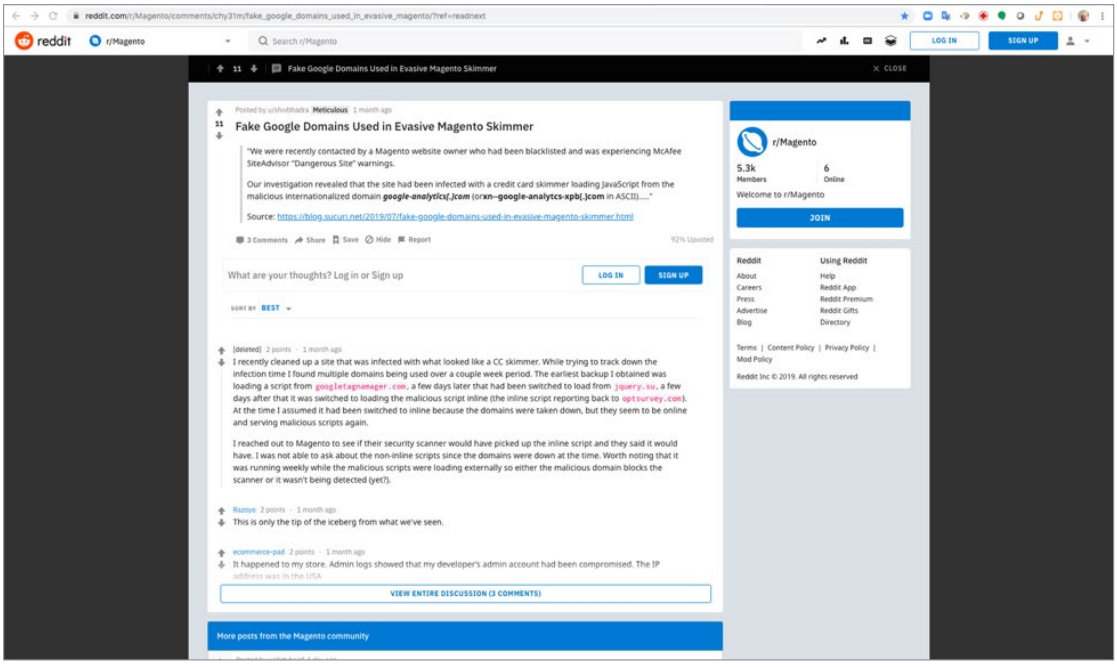
https://community.riskiq.com/search/googletagnamager.com

Click on the OSINT tab.



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

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

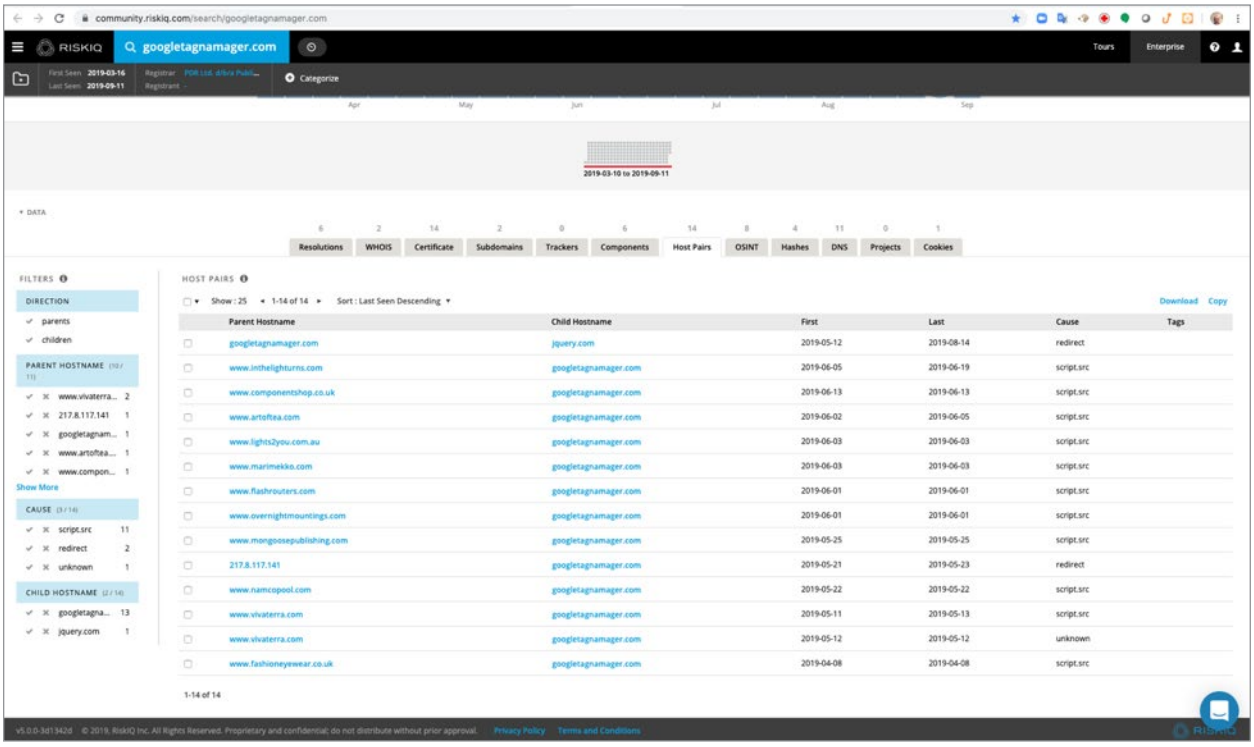


The information in the Reddit post talk about the two domains we are investigating, googletagnamager[.]com and jquery[.]su. They describe cleaning up a credit card "CC" skimmer. Our analysis seems to be correct that the two domains are involved in skimming payment card information.

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-analytîcs[.]com (or in ASCII xn--google-analytcs-xpb[.]com). The letter "î" 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 googletagnamager[.]com

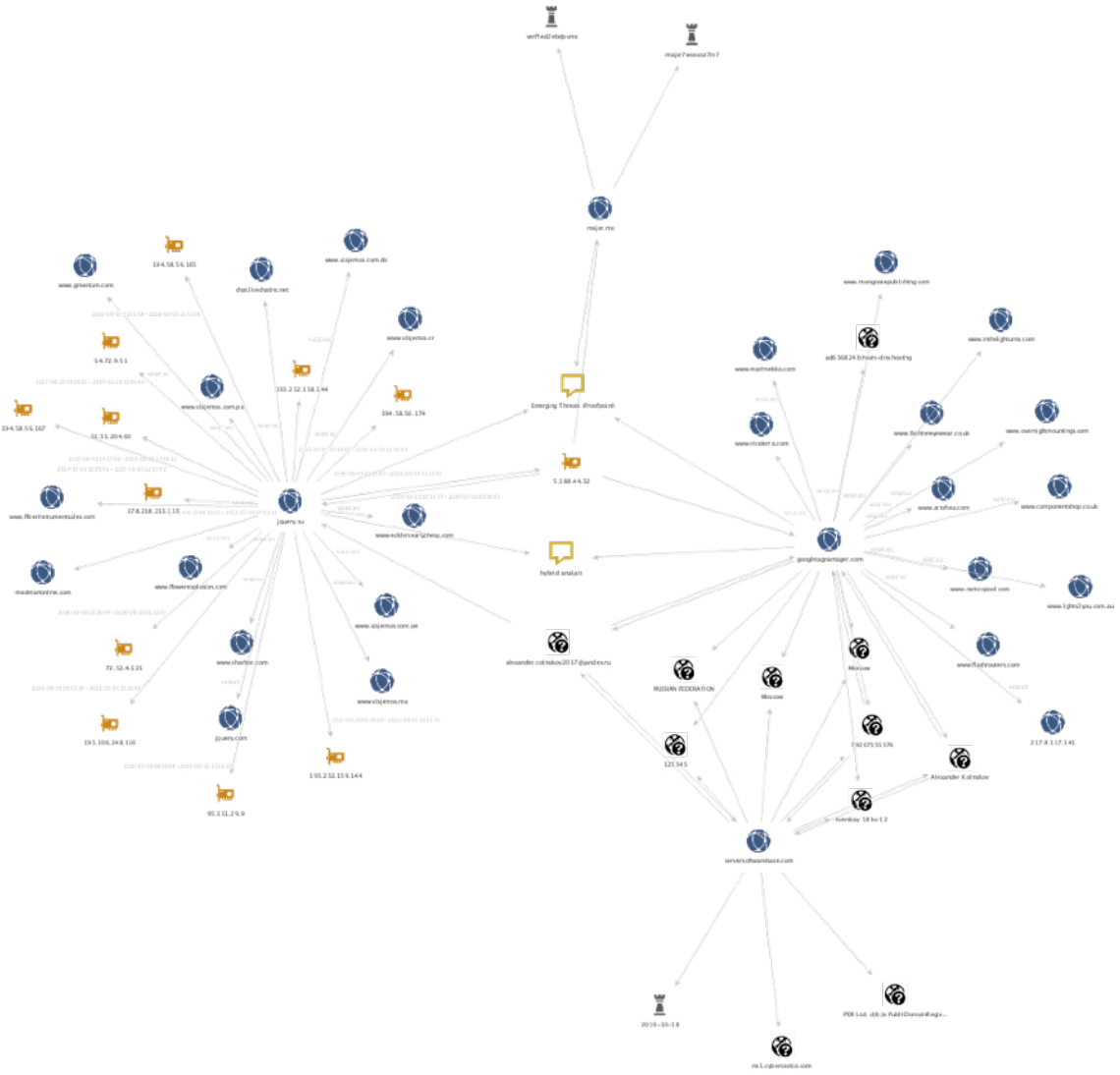
Click on the Host Pairs tab.



All of the Parent Hostnames associated with googletagnamager[.]com have been observed running a script for this server. This means all of the domains listed a child relationship to googletagnamager[.]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 googletagnamager[.]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