Mark of the Web

Scenario: In this exercise you are responsible for protecting www.match.com. You have always been reactive in investigations after the attack was discovered by customers or other employees. Now, you want to be on the offensive and be more proactive and to find the attacker as early as possible in the attack kill chain during the setup and weaponization phases.

Goal: Look at your own infrastructure, www.match.com, and see what is normal or legitimate. You will leverage new threat hunting techniques to identify suspicious or malicious infrastructure used by threat actors.

You will have two objectives to accomplish during this investigation.

Objective 1: Which data set could be helpful in finding malicious infrastructure?

Objective 2: Identify common techniques shared amongst results in order to find more malicious content.

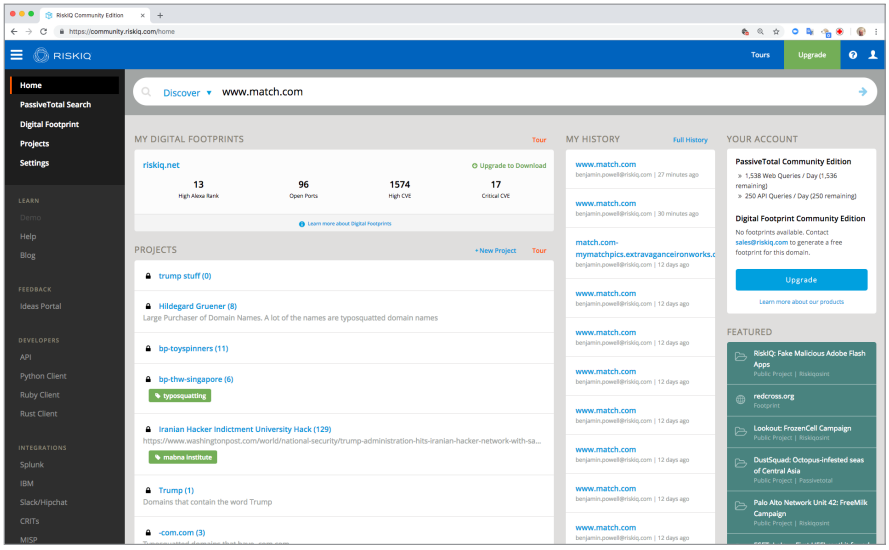
We are going to start with your known good domain, www.match.com, and look for bad things that are linked to it, this will allow us to be more proactive in your threat hunting.

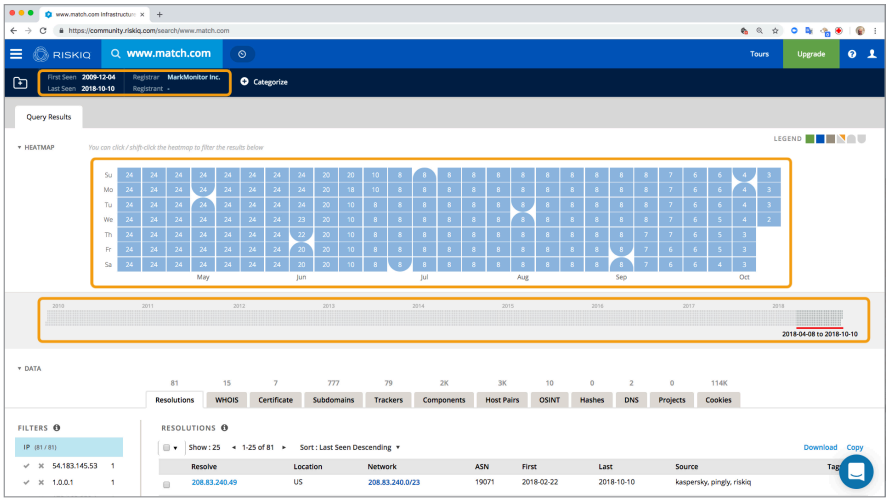
Log into https://community.riskiq.com with your web browser.

STEP 1: **Perform a search for www.match.com**

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

In the search window, search for www.match.com





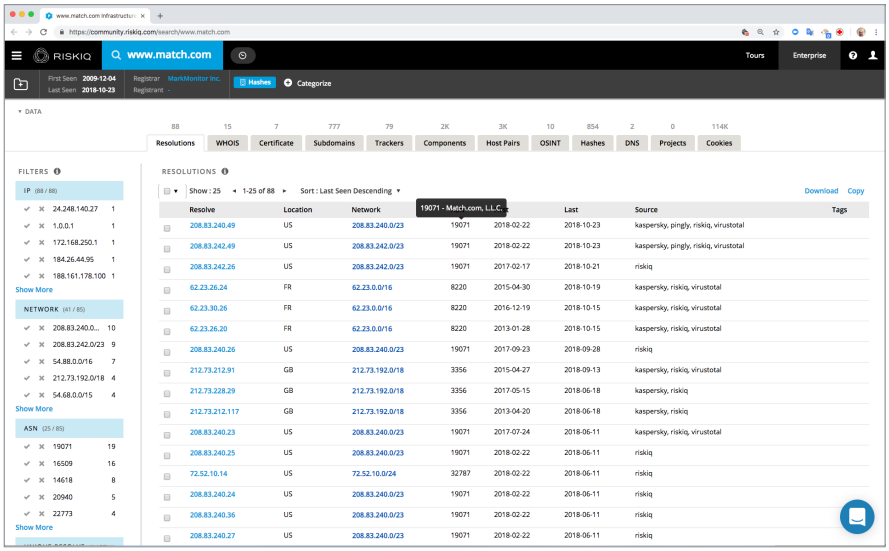
Step 2: **Review results (Heatmap, data bar, first last seen)**

Here are some key characteristics of a legitimate domain.

A legitimate domain will have a large or complete heatmap. For match.com, the heatmap indicates the website has been seen on the internet with a routable IP address for the last six months. Threat actors will sometimes part their domain to a non-routable IP address (127.0.0.1) when there are not using their domain to prevent discovery or investigation. www.match.com has had between 24 different IP address and now has two different IP addresses associated with this domain.

The data map shows RiskIQ has data on www.match.com going back to before 2010. First and Last seen on the top of the screen shows the domain was first seen 12-4-2009 and then whenever it was last seen by by RiskIQ.

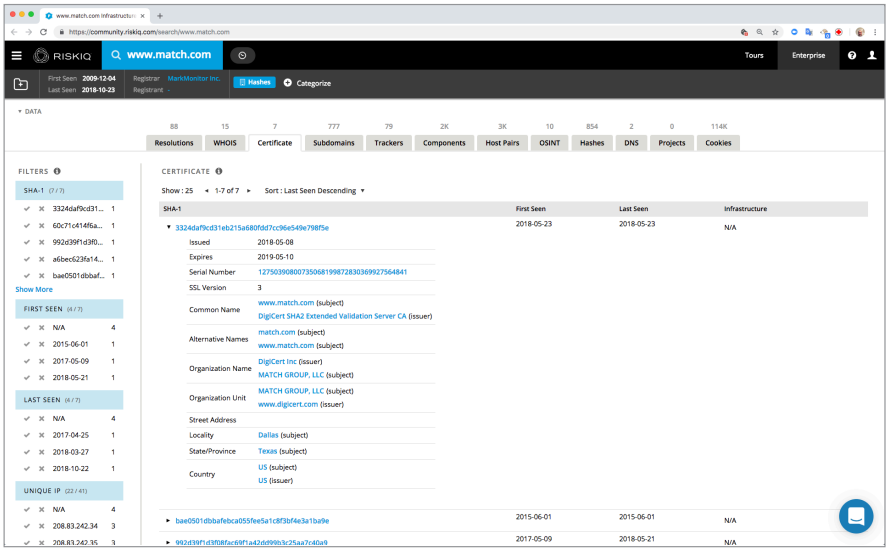
Look at the resolutions on the bottom of the page.



Step 3: **Review the Resolution tab www.match.com**

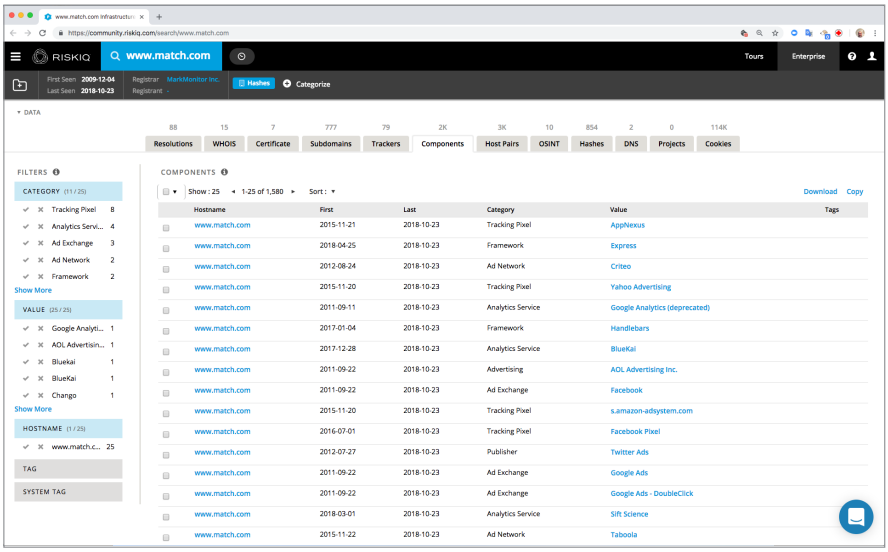
From the resolutions tab, you can see the passive DNS information on the DNS "A" records. The PDNS information shows the domain's IP history. We can understand the hosting history by reviewing the data below. We can see that www.match.com has been hosted on numerous IP addresses in many different geographic locations, including the US (United States), GB (Great Britain), and FR (France). If you hover over the ASN, it will display additional information. The ASN 19071 is registered to Match.com LLC. This is a good indicator that this is a legitimate domain because threat actors don't usually get their own ASN assigned to them.

Step 4: **Review the Certificate tab and expand the first result**



We see the SSL certificate issued by www.digicert.com which is a paid certificate for Match Group, LLC. If you see a paid certificate, this can sometimes be another indicator it is a legitimate domain. However, we *have* seen threat actors purchase certificates in the past.

Step 5: **Components tab**

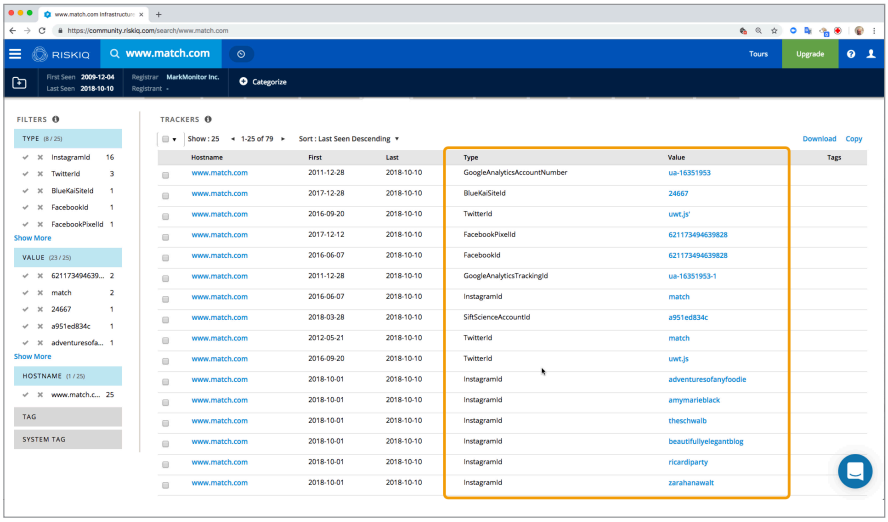


There are over 1000 components listed. This indicates a lot of infrastructure and multiple types of underlying architecture and applications. Threat actors generally only setup the bare minimum to perform their attacks. It costs money to setup, maintain, and support the servers and infrastructure. We generally see threat actors only setting up the fewest components necessary when perform attacks.

Step 6: **The Proactive Investigation begins**

Go to the Trackers tab and look at the results.

Now we will begin to be proactive in our threat hunting to identify threat actors attacking the domain www.match.com.



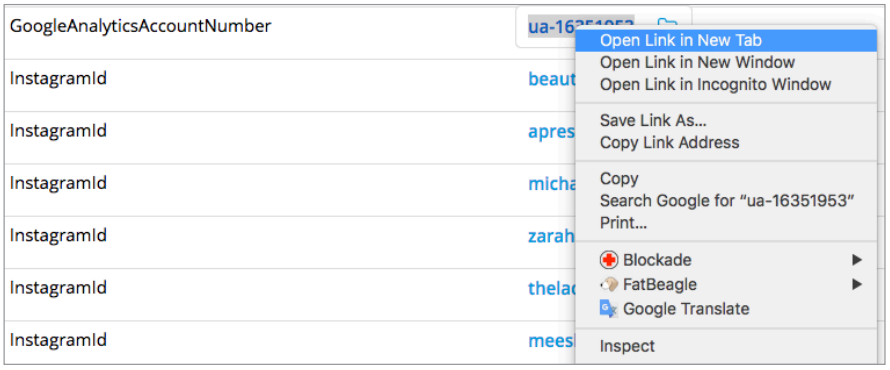
In the screen shot above, you see the trackers that RiskIQ has identified that are being served and used by www.match.com. When a threat actor phishes or attacks your domain, they will sometimes duplicate your real website. The duplicated domain might also contain your legitimate trackers.

Step 7: **Pivoting on trackers**

Now we are going to perform a few pivot queries on some trackers to help surface threat actors that have duplicated the domain www.match.com.

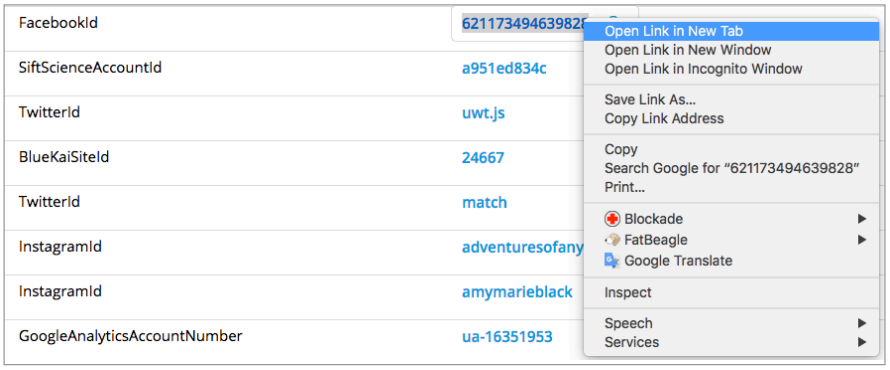
Right click on the value for the GoogleAnalyticsAccountNumber ua-16351953 and open it in a new tab. We will come back to this tab in a later section.

Community.riskiq.com query:
https://community.riskiq.com/search/trackers/GoogleAnalyticsAccountNumber/ua-16351953

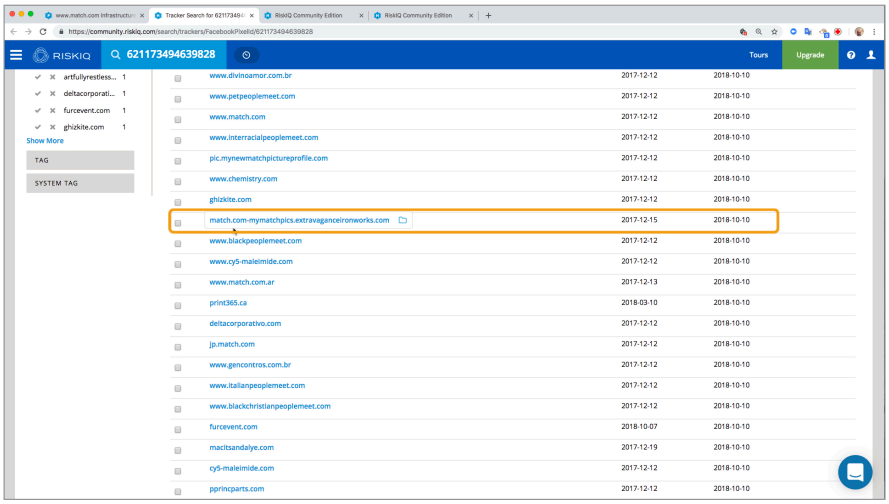


Right click on the value for the FacebookPixelid 62117349639828 and open it in a new tab.

Community.riskiq.com query:
https://community.riskiq.com/search/trackers/FacebookPixelId/621173494639828



Click on the tab for the Facebook tracker.



Step 8: **Review FacebookPixelid tracker**

All of the results shown indicated the same FacebookPixelid 62117349639828 is being served for all of the domains listed.

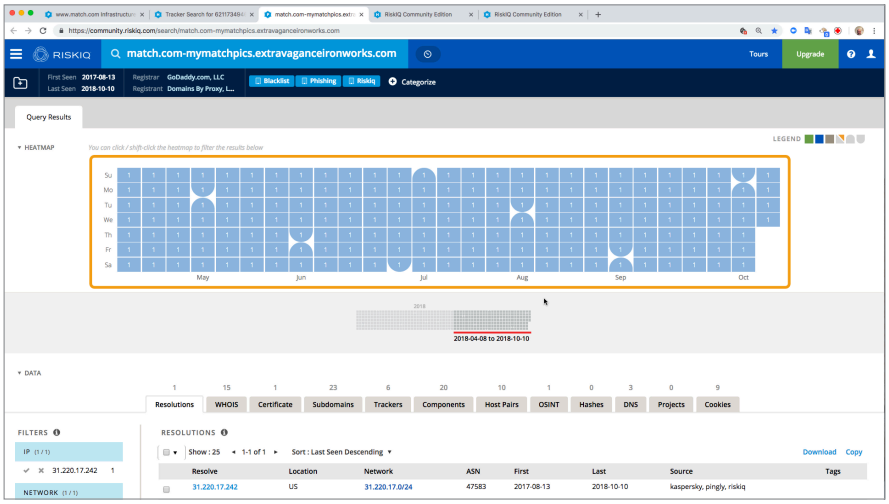
Threat actors will sometimes use the legitimate domain names in their attacks. Match.com-mymatchpics.extravaganceironworks.com does not appear to be legitimate. It appears to be typosquatting www.match.com.

Step 9: **Investigate the domain mymatchpics.extravaganceironworks.com**

To further investigate this domain, right click on the domain match.com-mymatchpics.extravaganceironworks.com and open it in a new tab.

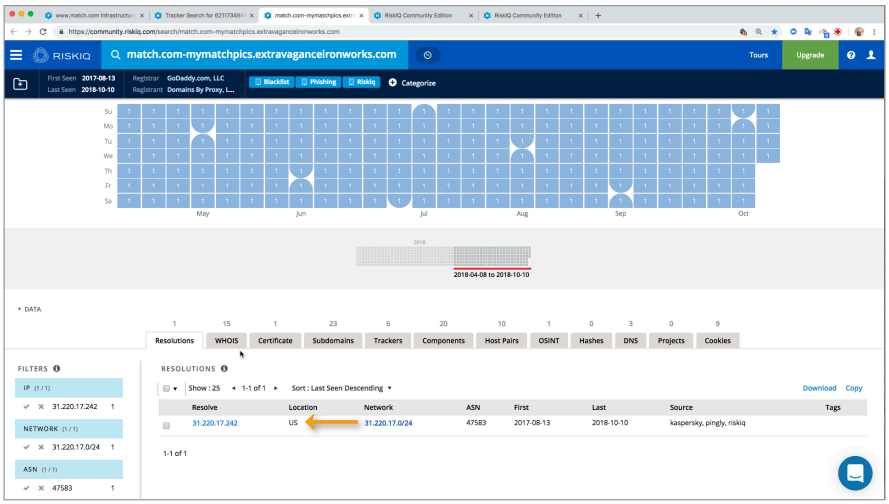
Community.riskiq.com query:
https://community.riskiq.com/search/match.com-mymatchpics.extravaganceironworks.com

Step 9A: **Review Heatmap, databar, first and last seen**



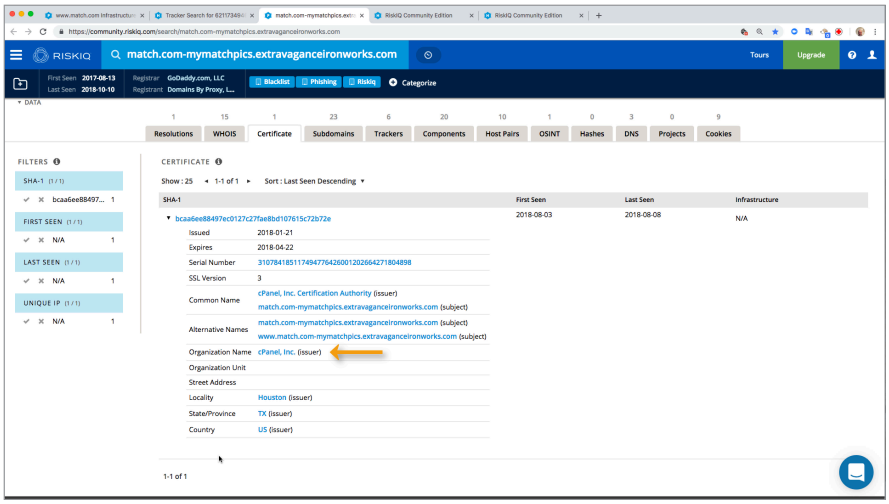
In the screen shot above, we see a complete heatmap with the same IP address seen for the last six months. No non-routable IP address has been seen. So far, this looks legitimate.

Just below the heatmap is the data bar. The data bar shows that RiskIQ has data going back to August 13, 2017. The top left of the screenshot shows the first and last seen dates for this domain. This could also indicate a legitimate domain.



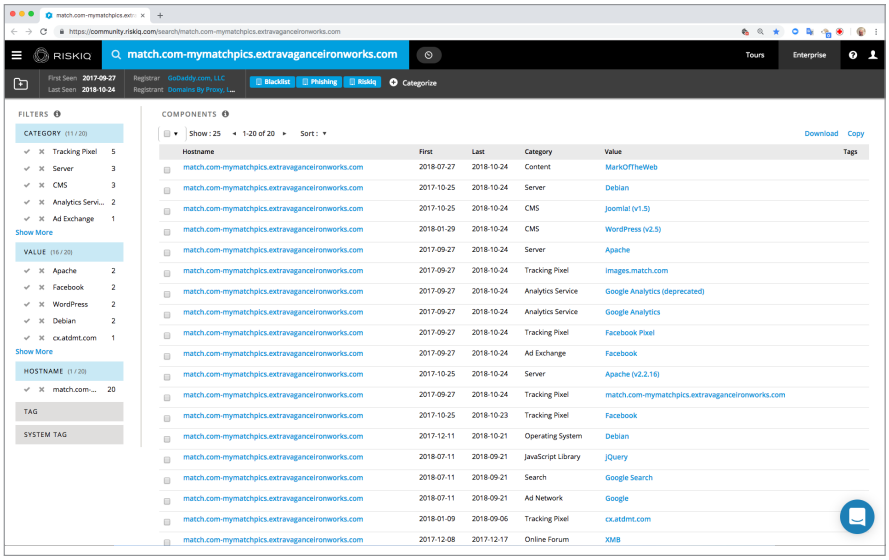
The IP's location information shows that is based in the US. The IP address has been the same one for the entire time it has been on the internet. This also is an indication of a legitimate domain.

Examine the certificate tab now.



The certificate that is being utilized by this domain was issued by cPanel, Inc. This is a paid certificate usually given when someone is doing their hosting with a provider. Since this is a paid certificate, it also seems to give credibility that this is a legitimate domain.

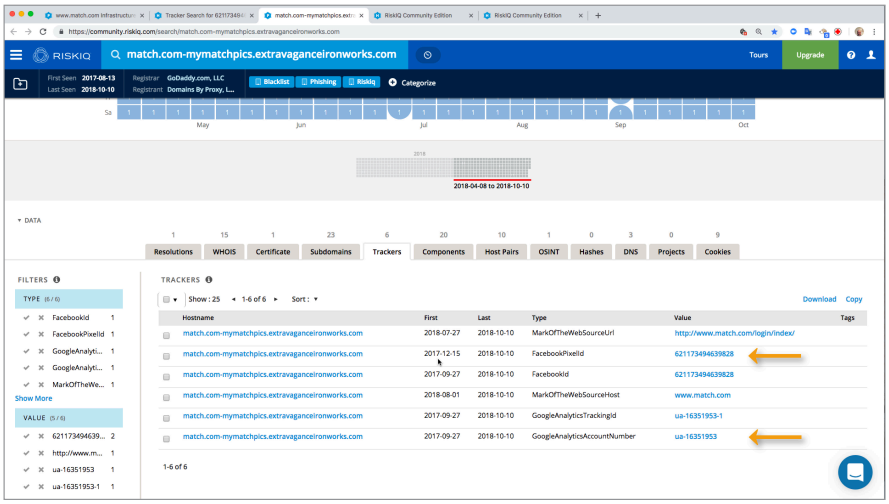
Review the components.



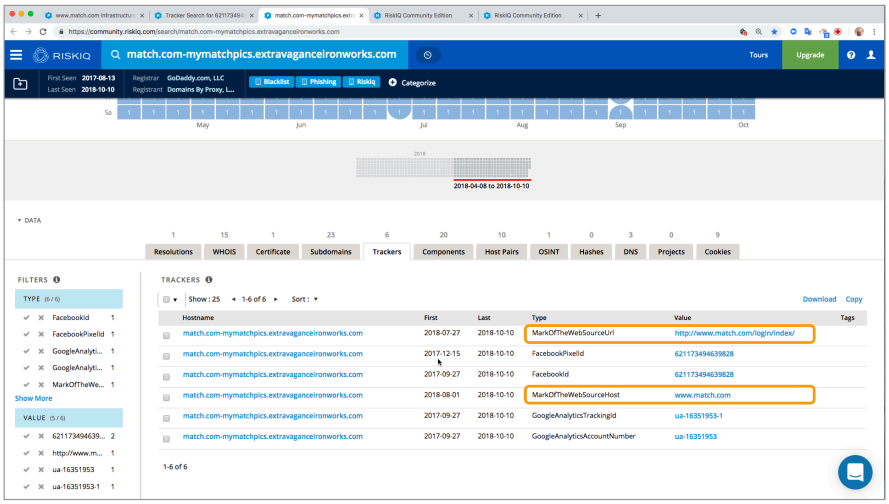
We see in the components many familiar things listed from Debian, Joomla, Apache, JQuery, and WordPress. It looks like a full stack of web infrastructure is being used by this domain, which appears legitimate. However, I do see something that could be suspicious in the list of components: MarkOfTheWeb. We will investigate this component later.

Step 10: **Review Trackers**

Click on the tracker tab.



In the screenshot above we see the FaceBookPixelid and the GoogleAnalyticsAccountNumber from www.match.com. This domain is serving these trackers to visitors to this domain, just like they do www.match.com.



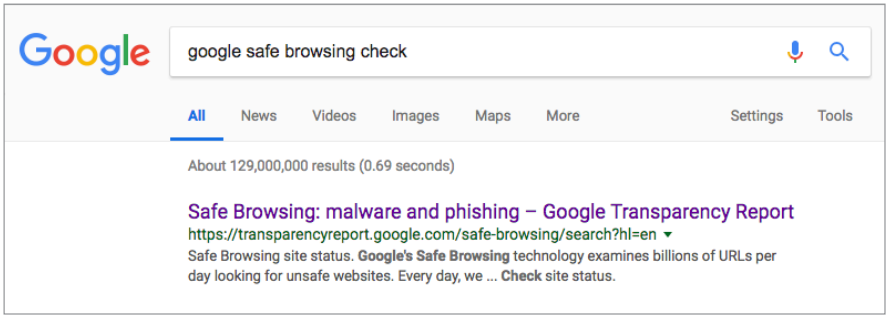
In the screenshot above we see MarkOfTheWebSourceUrl and MarkOfTheWebSourceHost. When someone saves a website using a Microsoft web browser it creates some watermarks to identify where the original website was copied from. For example, mymatchpics.extravaganceironworks.com website is a copy from http://www.match.com/login/index/. This is very suspicious, and this type of tracker can easily identify domain infringement or potential phishing associated with the domain that was copied. Now that we suspect that the domain mymatchpics.extravaganceironworks.com could be malicious, we need to investigate it safely without visiting the website.

Step 11: **Verify if the domain is legitimate with Google Safe Browsing**

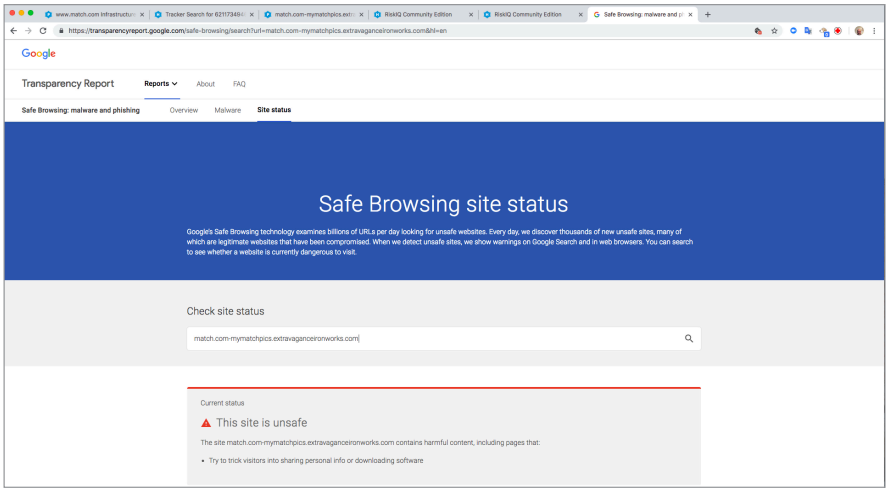
We can check to see if Google has classified this domain as unsafe without having to visit the threat actor's domain mymatchpics.extravaganceironworks.com.

In a new tab, search for "Google Safe Browsing check" and click on the result for "Safe Browsing: malware and phishing – Google Transparency Report"

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



In the check site status, search for the domain match.com-mymatchpics.extravaganceironworks.com.



The results indicated that match.com-mymatchpics.extravaganceironworks.com is unsafe due to the website tricking visitors into sharing personal info or downloading software.

Now we have confirmed the domain is unsafe. We have identified a domain that is coping, the legitimate trackers and serving them on their own domain.

Objective 1 Complete: Which data set could be helpful in finding malicious infrastructure?

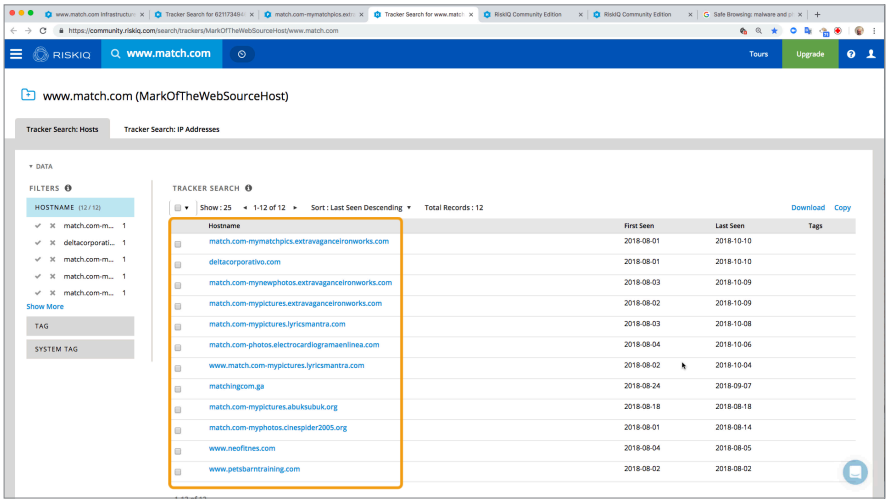
We have learned that we can utilize many different data sets to surface suspicious infrastructure. We learned that threat actors that duplicate websites also duplicate legitimate trackers. Searching on legitimate trackers can surface suspicious or malicious domains that are also utilizing those same trackers. In the exercise, we searched on the FaceBookPixelid and the GoogleAnalyticsAccountNumber used by www.match.com. We identified a domain match.com-mymatchpics.extravaganceironworks.com that appeared to be typosquatting the legitimate domain www.match.com.

While investigating the domain match.com-mymatchpics.extravaganceironworks.com it appeared to be legitimate with a long history of utilizing the same IP address from the United States and had a full web application stack. We identified a single web component that we were not familiar with MarkOfTheWeb. While investigating trackers we identified that the domain match.com-mymatchpics.extravaganceironworks.com had copied its website from www.match.com. Using Google Safe Browsing check we confirmed our suspicions that match.com-mymatchpics.extravaganceironworks.com was malicious tricking users into sharing personal information and downloading software.

Step 12: **Identify if anyone else is attacking www.match.com**

Objective 2: Identify common techniques shared amongst results in order to find more malicious content.

Keeping objective two in mind, if you search on the MarkOfTheWebSourceHost for www.match.com, this will identify all other websites that are copies of www.match.com.



In the screenshot above we have now identified 12 other domains that are copies of www.match.com. All of the websites should be investigated because they are all utilizing a copy of the legitimate website www.match.com and do not appear to be affiliated with them.

If you bookmark the URL you can easily access this query at any time in the future. https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/www.match.com

Objective 2 Complete: Identify common techniques shared amongst results in order to find more malicious content.

Utilizing the MarkOfTheWeb tracker you can identify all domains that are copied from the identified source. Below are a few interesting domains that are utilizing MarkOfTheWeb compenents and trackers.

To help you in finding interesting domains to investigate, below is a list to get you started.

All Domains that are utilizing MarkOfTheWeb.

https://community.riskiq.com/search/components/Content/MarkOfTheWeb

Targeted Domains That Contain MarkOfTheWeb Data

MarkOfTheWebSourceHost

www.netflix.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/www.netflix.com

get.uber.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/get.uber.com

www.match.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/www.match.com

outlook.office365.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/outlook.office365.com

login.microsoftonline.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/login.microsoftonline.com

login.live.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/login.live.com

facebook.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/www.facebook.com

www.westernunion.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/www.westernunion.com

www.dropbox.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/www.dropbox.com

www.expedia.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/www.expedia.com

itunes.apple.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/itunes.apple.com

accounts.google.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/accounts.google.com

creditcards.chase.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/creditcards.chase.com

www.linkedin.com
https://community.riskiq.com/search/trackers/MarkOfTheWebSourceHost/www.linkedin.com

RISKIQ®

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

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com