OSINT Investigation

Investigation of IOCs from an Open Source Intelligence publication

Scenario:

Your CEO has forwarded you an article from Kaspersky.
https://securelist.com/apt-phantomlance/96772/#infrastructure.

The CEO wanted you to review the publication and see if your organization has anything to worry about, and if your organization has been affected by this attack.

Goal: **Read the article and then investigate the Command and Control domains and IP address and see what you can find out.**
Important Note: During your investigation you have informed your team not to directly visit the website in order to prevent any potential malware from entering the organization.

Objective 1: What are the aspects of the attacks?
Objective 2: Is it still active?
Objective 3: Does your organization need to worry about this attack?
Objective 4: Have you seen any traffic to the IOCs?
In this exercise I will highlight the differences in RiskIQ PassiveTotal account types and integrations.

Free Community Account
PassiveTotal Enterprise with the CrowdStrike integration enabled.

Initial Searches
From the article you have decided to review one IP and the OceanLotus Windows backdoor domains

Article: https://securelist.com/apt-phantomlance/96772/ - infrastructure

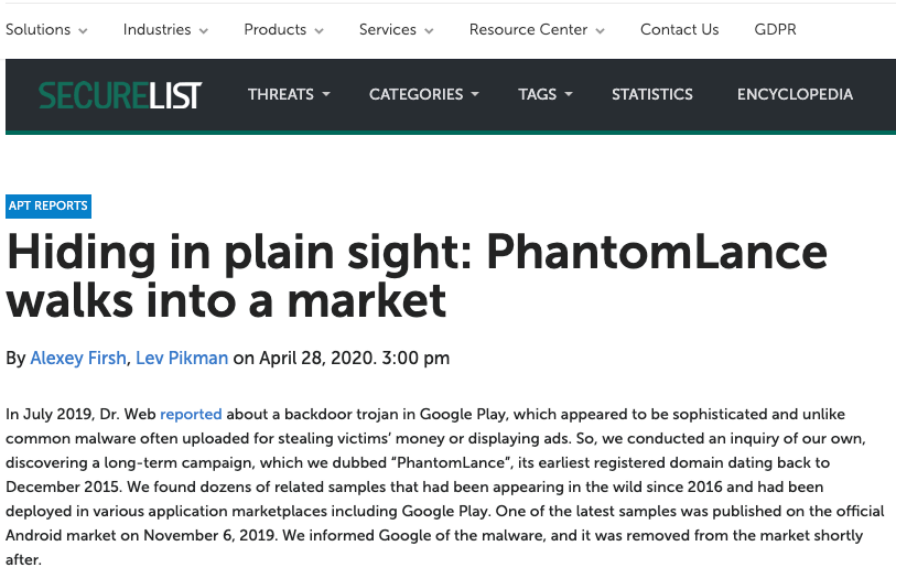
88[.]150[.]138.77
https://community.riskiq.com/search/88.150.138.77/resolutions

ps[.]andreagahuvrauvin[.]com
https://community.riskiq.com/search/ps.andreagahuvrauvin.com

paste[.]christienollmache[.]xyz
https://community.riskiq.com/search/paste.christienollmache.xyz/resolutions

att[.]illagedrivestralia[.]xyz
https://community.riskiq.com/search/att.illagedrivestralia.xyz

Step 1: OSINT Publication Review
https://securelist.com/apt-phantomlance/96772/ - infrastructure


kaspersky

Solutions Industries Products Services Resource Center Contact Us GDPR

SECURELIST THREATS CATEGORIES TAGS STATISTICS ENCYCLOPEDIA

APT REPORTS

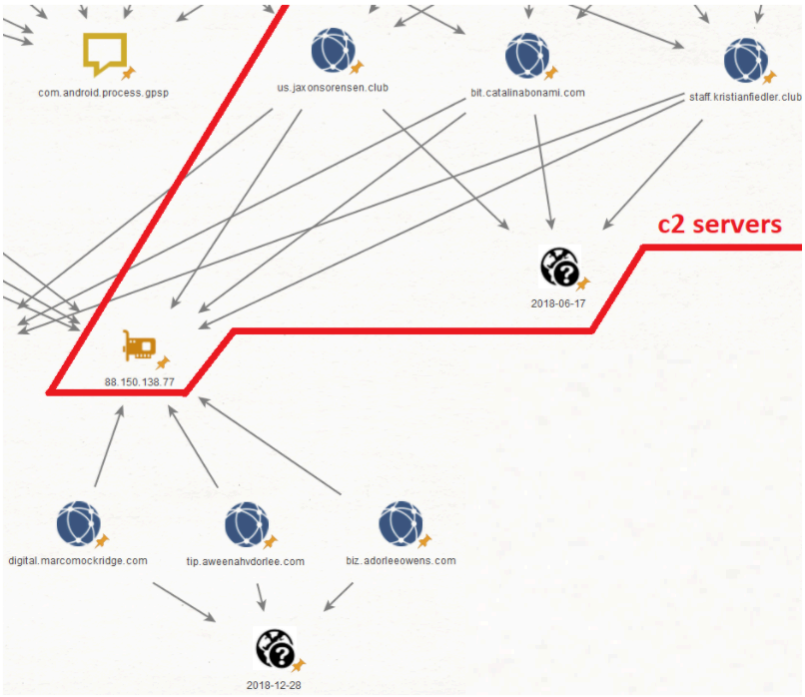
Hiding in plain sight: PhantomLance walks into a market

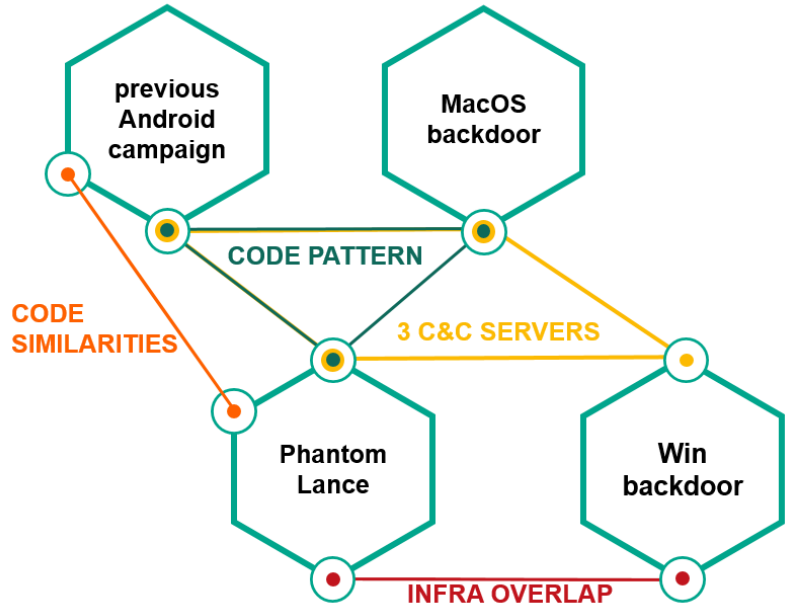
By Alexey Firsh, Lev Pikman on April 28, 2020. 3:00 pm

In July 2019, Dr. Web reported about a backdoor trojan in Google Play, which appeared to be sophisticated and unlike common malware often uploaded for stealing victims' money or displaying ads. So, we conducted an inquiry of our own, discovering a long-term campaign, which we dubbed "PhantomLance", its earliest registered domain dating back to December 2015. We found dozens of related samples that had been appearing in the wild since 2016 and had been deployed in various application marketplaces including Google Play. One of the latest samples was published on the official Android market on November 6, 2019. We informed Google of the malware, and it was removed from the market shortly after.

SECURELIST THREATS CATEGORIES TAGS STATISTICS ENCYCLOPEDIA

infrastructure.





Summary of overlaps

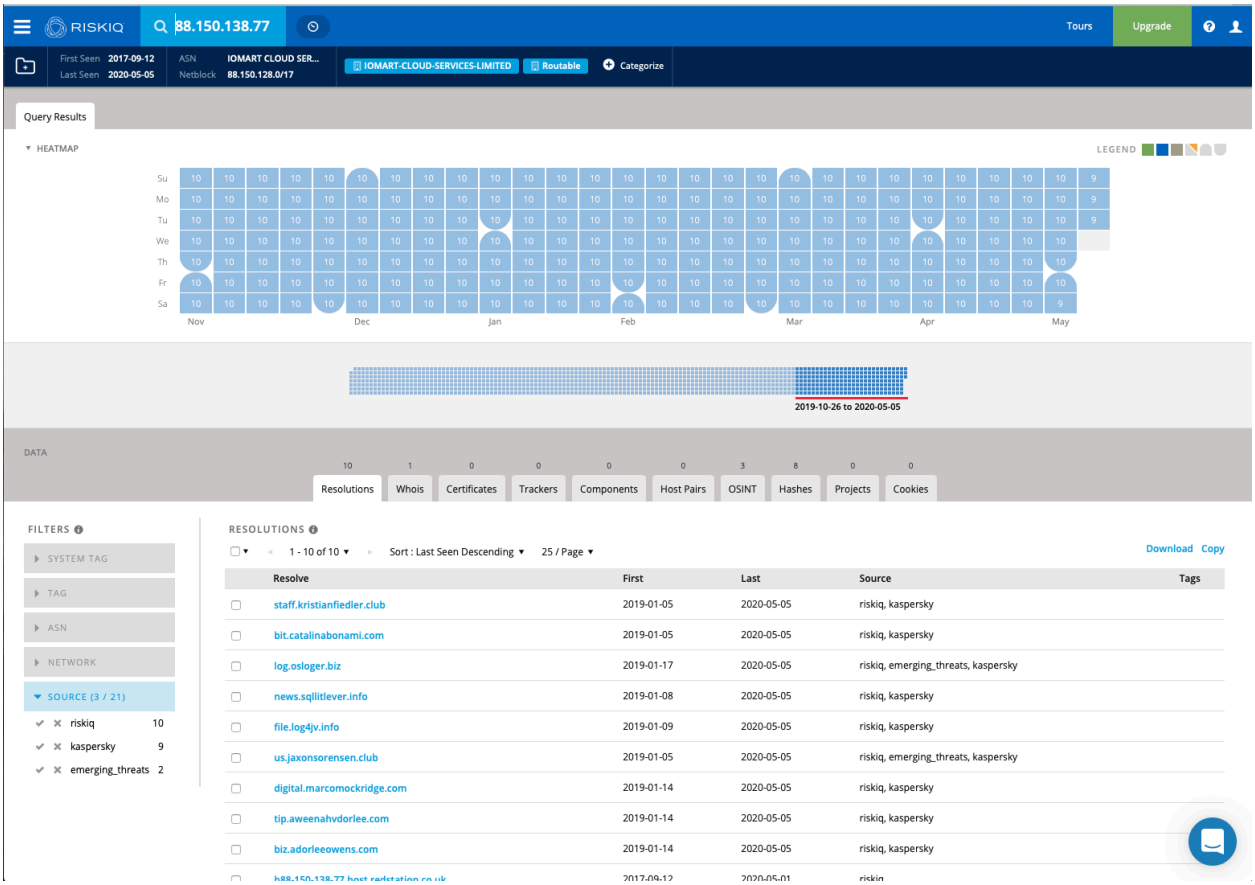
Another notable attribution token that applies to most of OceanLotus malware across platforms is usage of three redundant, different C2 servers by each sample, mostly subdomains. Below is an example of this from the samples examined above and OceanLotus Windows malware described in our private report.

MD5	C2 servers	Description
0d5c03da348dce513bf575545493f3e3	mine.remaariegarcia[.]com egg.stralisemariegar[.]com api.anaehler[.]com	PhantomLance Android
d1eb52ef6c2445c848157beaba54044f	sadma.knrowz[.]com ckoen.dmkatti[.]com itpk.mostmkru[.]com	OceanLotus Android campaign 2014-2017
306d3ed0a7c899b5ef9d0e3c91f05193	ssl.arkouthrie[.]com s3.hiahornber[.]com widget.shoreoa[.]com	OceanLotus MacOS backdoor
51f9a7d4263b3a565dec7083ca00340f	ps.andreagahuvrauvin[.]com paste.christienollmache[.]xyz att.illagedrivestralia[.]xyz	OceanLotus Windows backdoor

From the article you have decided to review one of the IP address and the OceanLotus Windows backdoor domains.

Step 2: Using Free Community Account

Open your browser and go to https://community.riskiq.com/home. Search for the IP address 88[.]150[.]138[.]77.

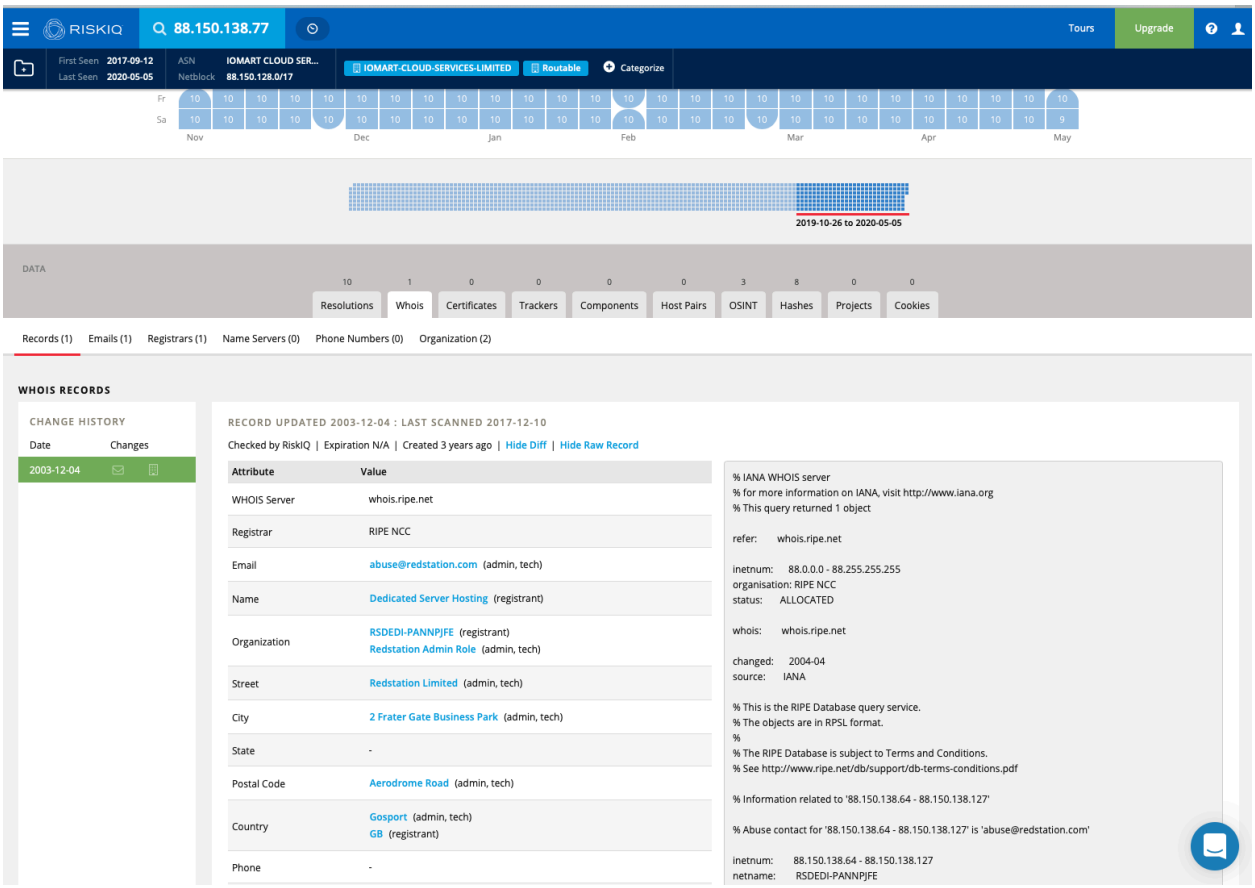


https://community.riskiq.com/search/88.150.138.77/resolutions

This IP address has 10 active domains associated with IP address. Some of the domains have been around since 2017. The numbers in the heatmap show that there have been between 10 and 9 domains active each day.

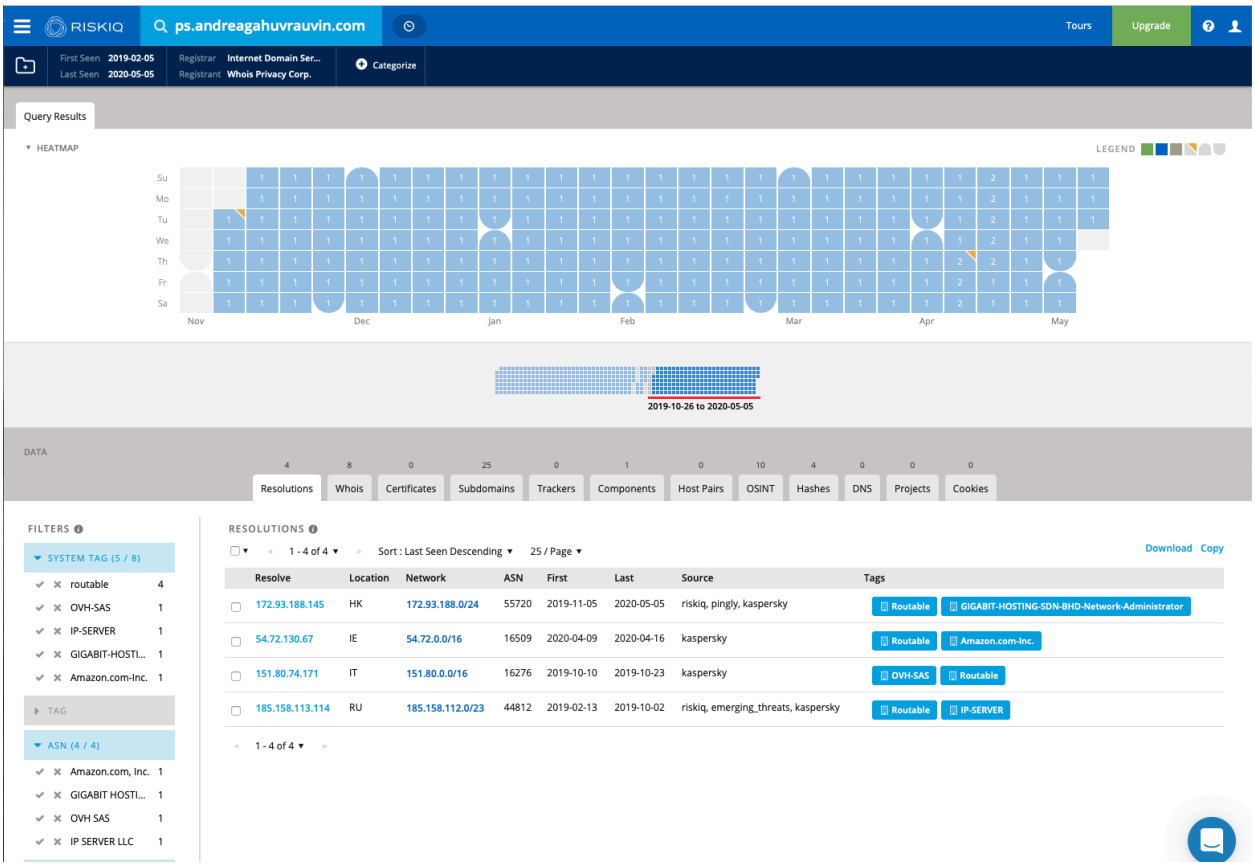
Step 3: Click on the Whois tab

https://community.riskiq.com/search/88.150.138.77/whois



The IP address is located in Great Britian. There is not Whois history available in the free community version of PassiveTotal.

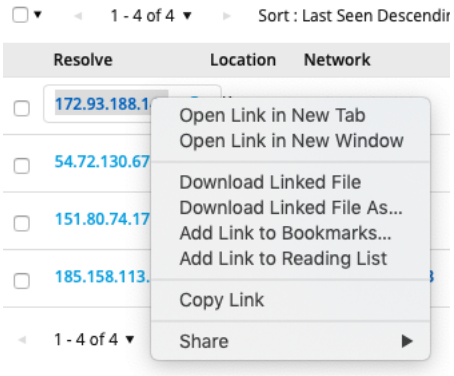
Step 4: In PassiveTotal Search for ps[.]andreagahuvrauvin[.]com
https://community.riskiq.com/search/ps.andreagahuvrauvin.com

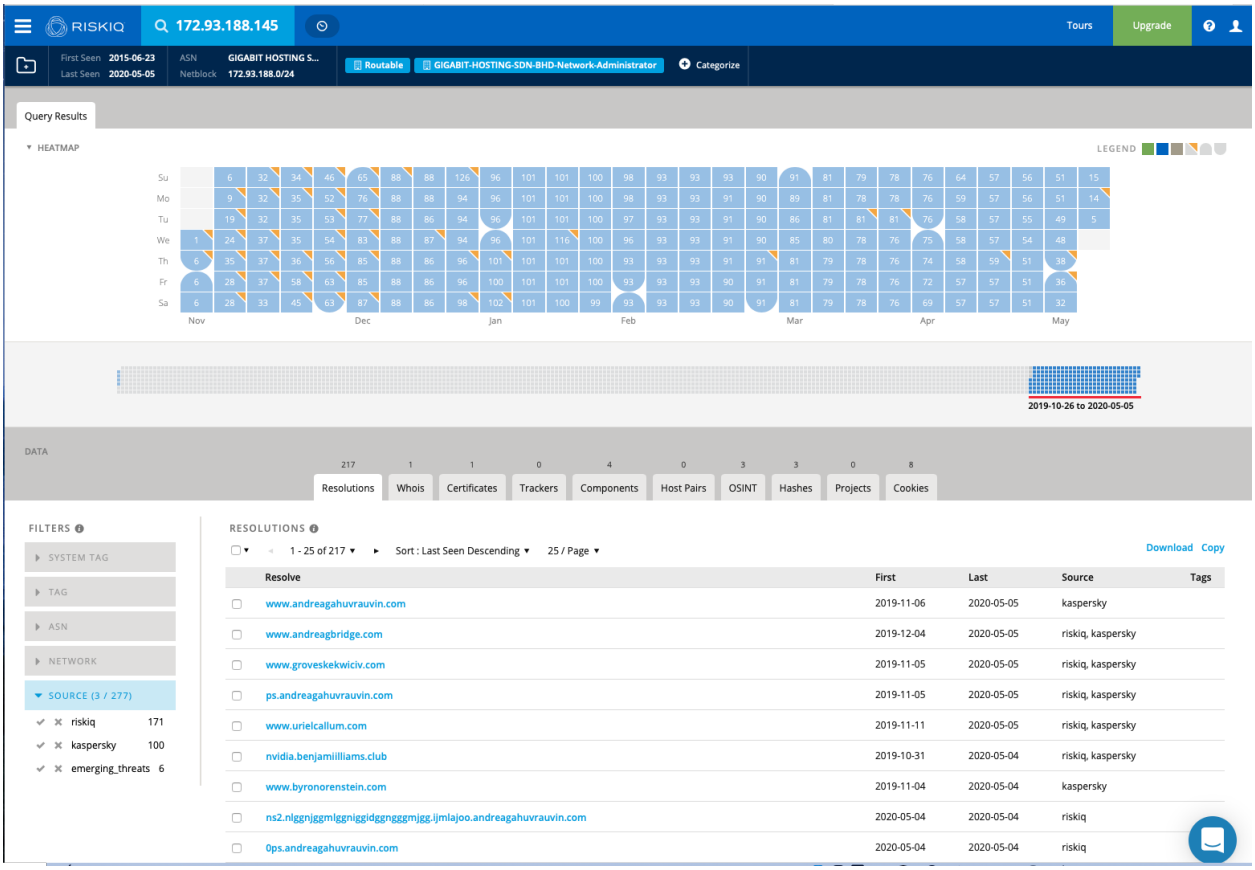


The IP address 172[.]93[.]188[.]145 has been active since November 2019 and is based out of Hong Kong. You can see this next to the listed IP address, first, last, and location country.

Step 5: Pivot search on the IP address 172[.]93[.]188[.]145.

Right click on the IP address and open it in a new tab



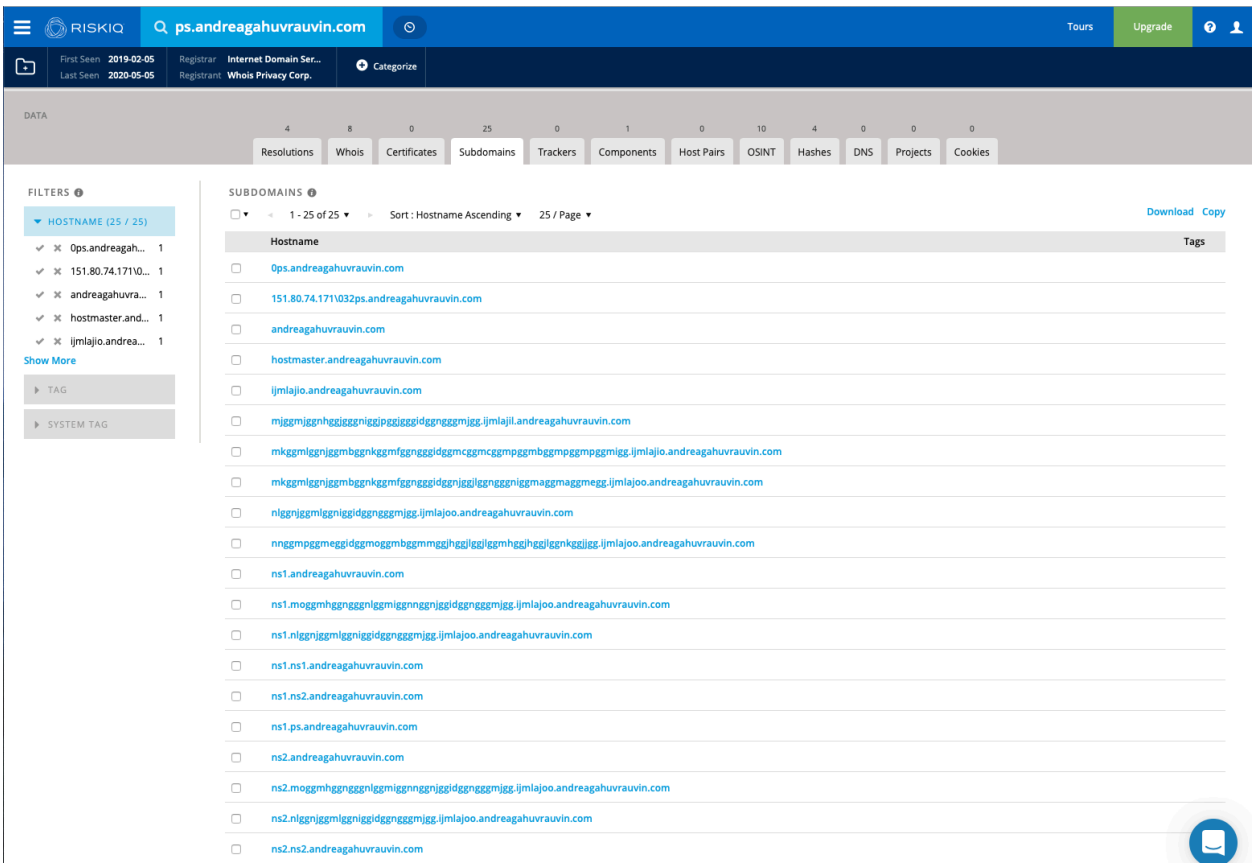


https://community.riskiq.com/search/172.93.188.145

We can see 217 IP addresses most have recent activity on the domains going back to a few months ago.

Go back to the domain ps.andreagahuvrauvin.com
https://community.riskiq.com/search/ps.andreagahuvrauvin.com/resolutions

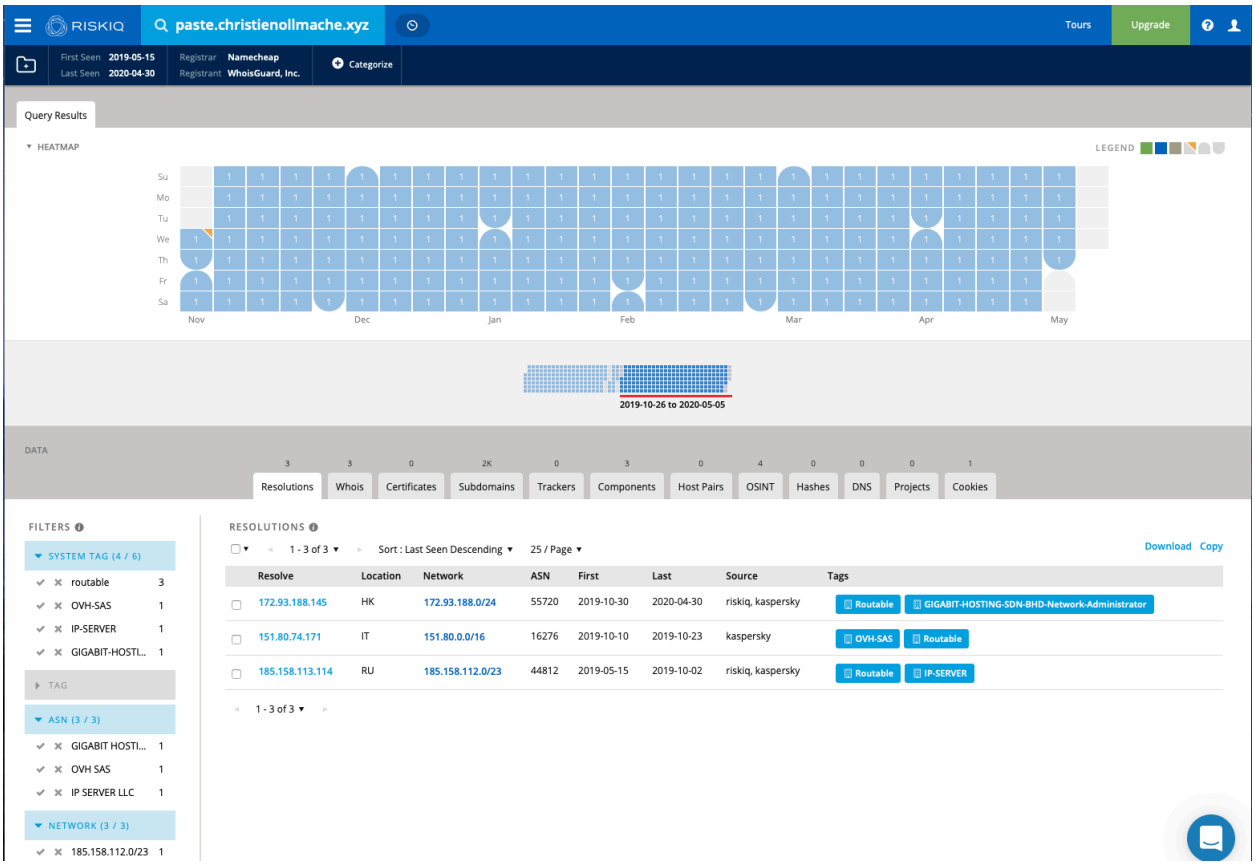
Step 6: Click on the Subdomains tab.
https://community.riskiq.com/search/ps.andreagahuvrauvin.com/subdomains



We can see 25 subdomains associated with this domain. All of the subdomains can be associated with completely different infrastructure and should be investigate individually to fully understand the for extent of this attack. But, for this exercise we will just focus on the Windows backdoor domains.

Step 7: Search on the next domain from the article paste[.]christienollmache[.]xyz

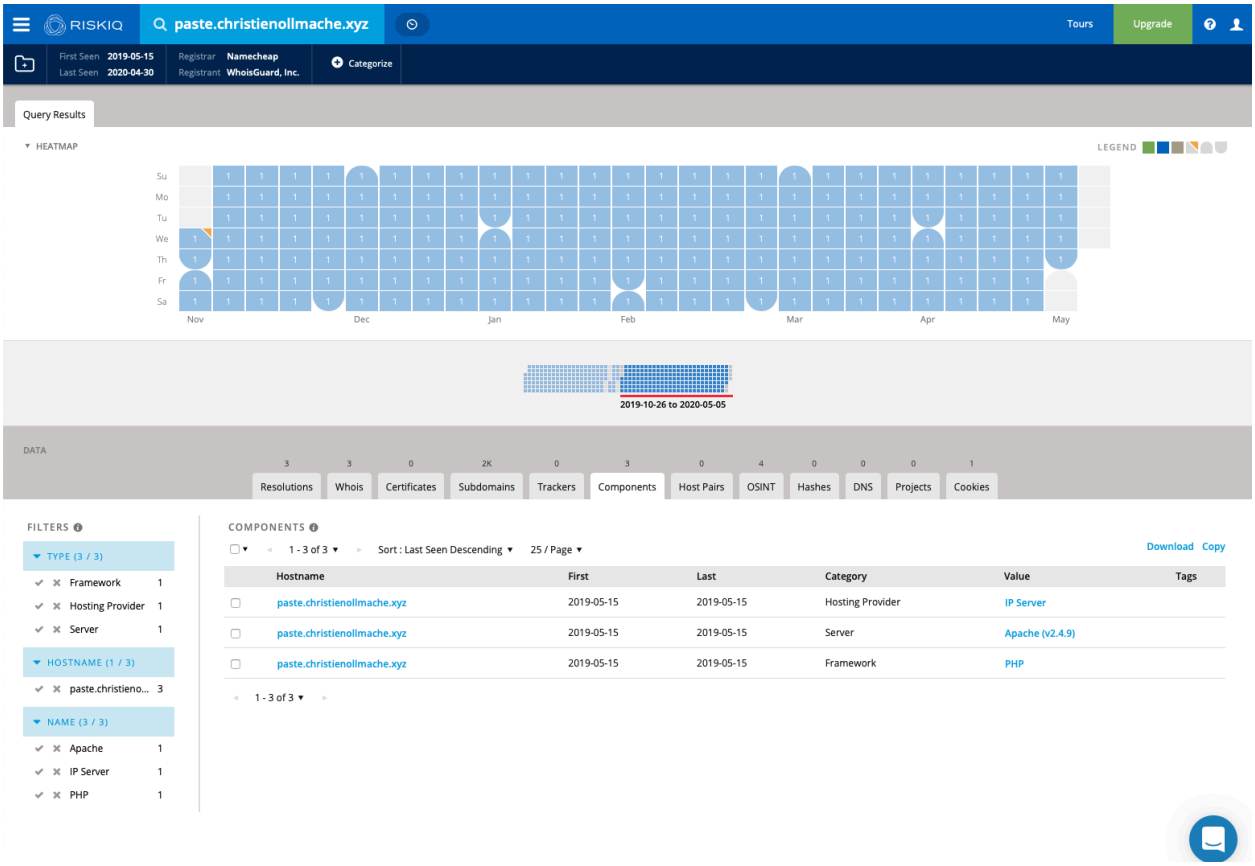
https://community.riskiq.com/search/paste.christienollmache.xyz/resolutions



Here we see 3 fairly recent IP addresses and the latest one is hosted in Hong Kong. Previous ones were hosted in Italy and Russia.

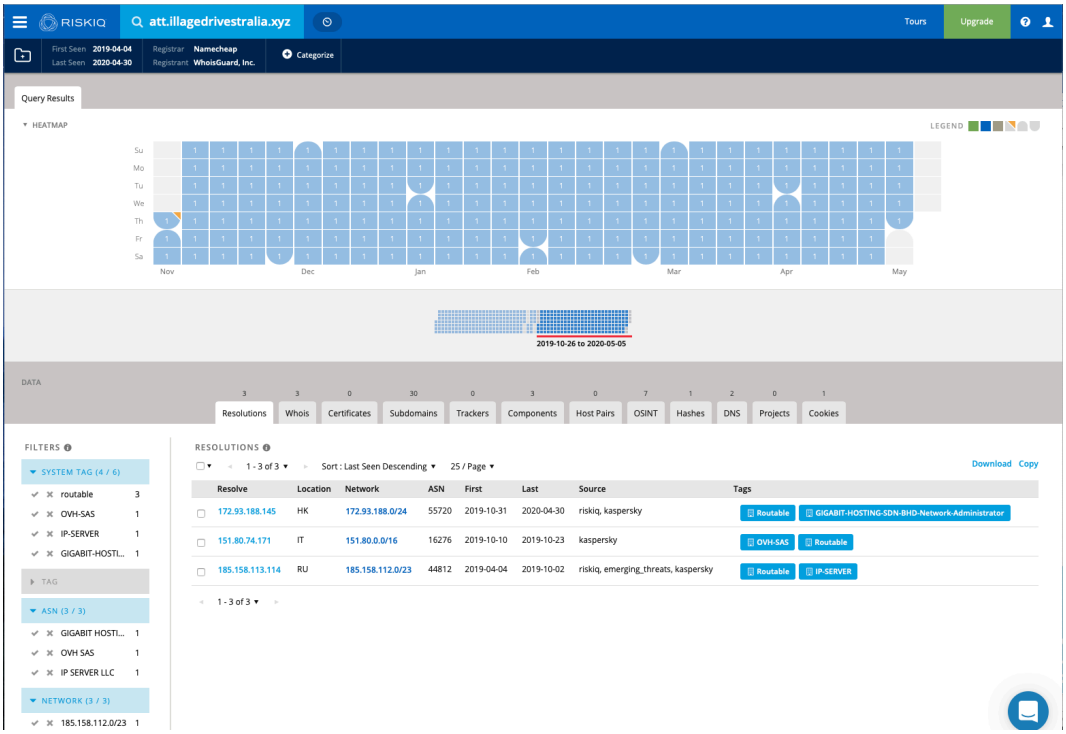
Step 8: Click on Components

https://community.riskiq.com/search/paste.christienollmache.xyz/components



We can see that this domain is running Apache v2.4.9 and PHP.

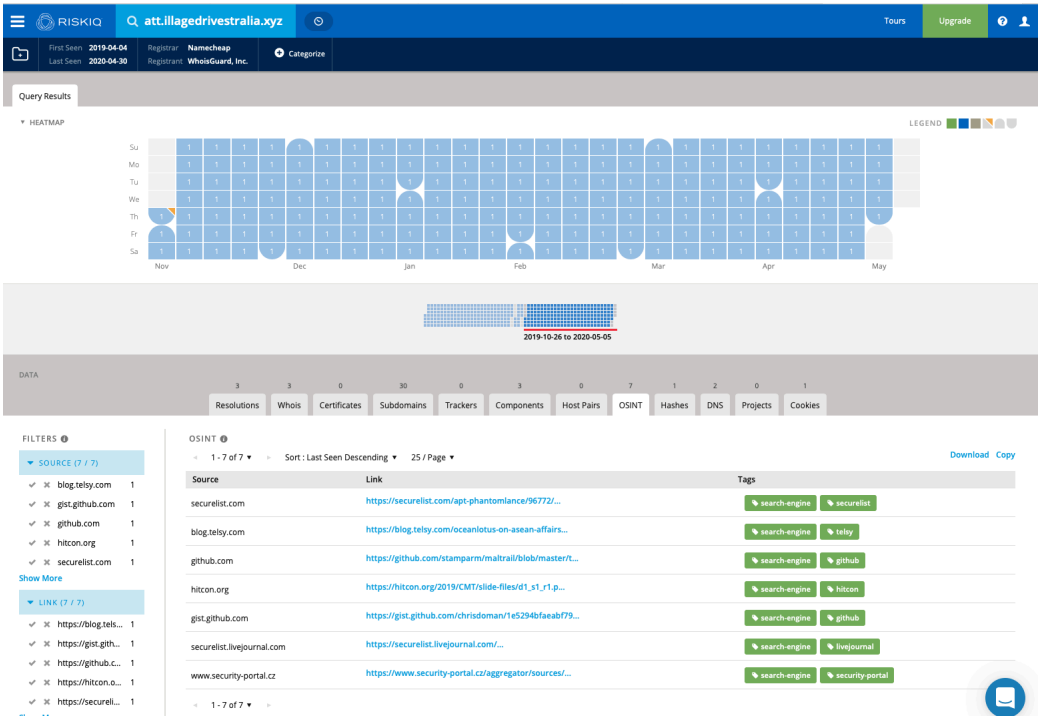
Step 9: Search the last domain att[.]illagedrivestralia[.]xyz
https://community.riskiq.com/search/att.illagedrivestralia.xyz



We see the same hosting locations HK, IT, RU. The IP addresses are actually the same as the previous domains.

Step 10: Click on the OSINT Tab

https://community.riskiq.com/search/att.illagedrivestralia.xyz/osint



The OSINT tab list a special google search for matches on searched IOC related to security blogs and organizations. Listed here are seven different links with information related to att[.]illagedrivestralia[.]xyz.

Community User Conclusion:

At this point we can conclude that the hosting was in Great Britain, Hong Kong, Italy, and Russia. We do not have information about the threat actor or whether it is related to known bad infrastructure or bad domains.

Objective 1: What are the aspects of the attacks?

Android, MacOS, Windows attack vectors according to the publication.

Objective 2: Is it still active?

Inconclusive, needs further investigation

Objective 3: Does your organization need to worry about this attack?

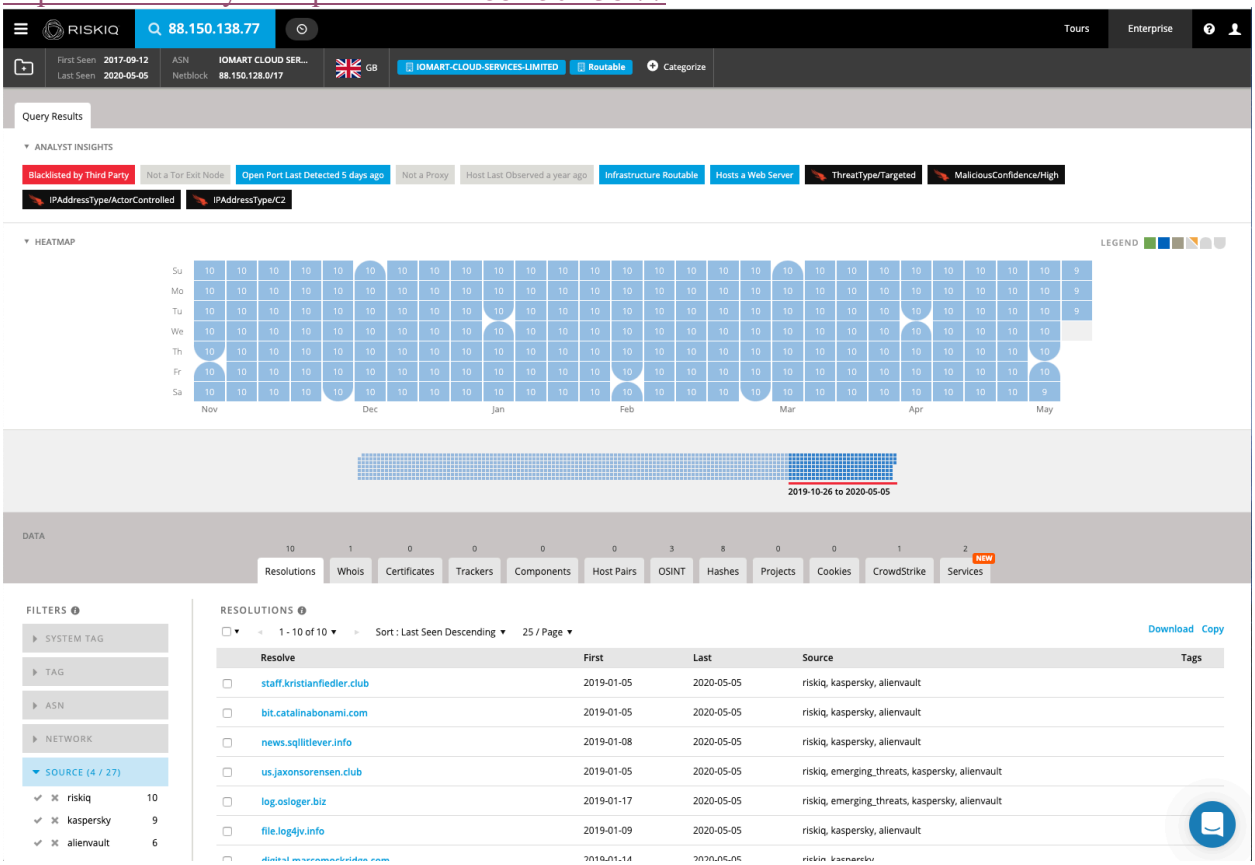
Inconclusive, needs further investigation

Objective 4: Have you seen any traffic to the IOCs?
Inconclusive, needs further investigation

Now I will look at the same tabs using an Enterprise PassiveTotal Account with the CrowdStrike Integration enabled.

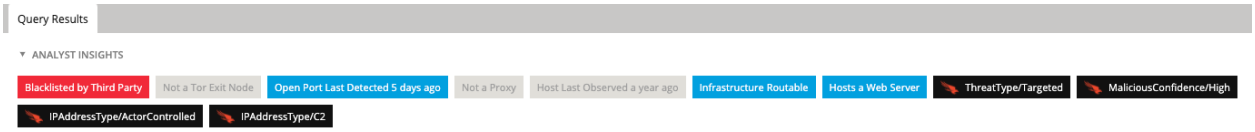
Step 11: Using Enterprise PassiveTotal Account
Open your browser and go to https://community.riskiq.com/home. Search for the IP address 88[.]150[.]138[.]77.

https://community.riskiq.com/search/88.150.138.77



Immediately we see some differences. I will explain what is different in the display and the additional information you gain with RiskIQ PassiveTotal Enterprise paid account.

At the top of the screen you can immediately see where the IP is located and it has a flag of the country so you can visually recognize the country.



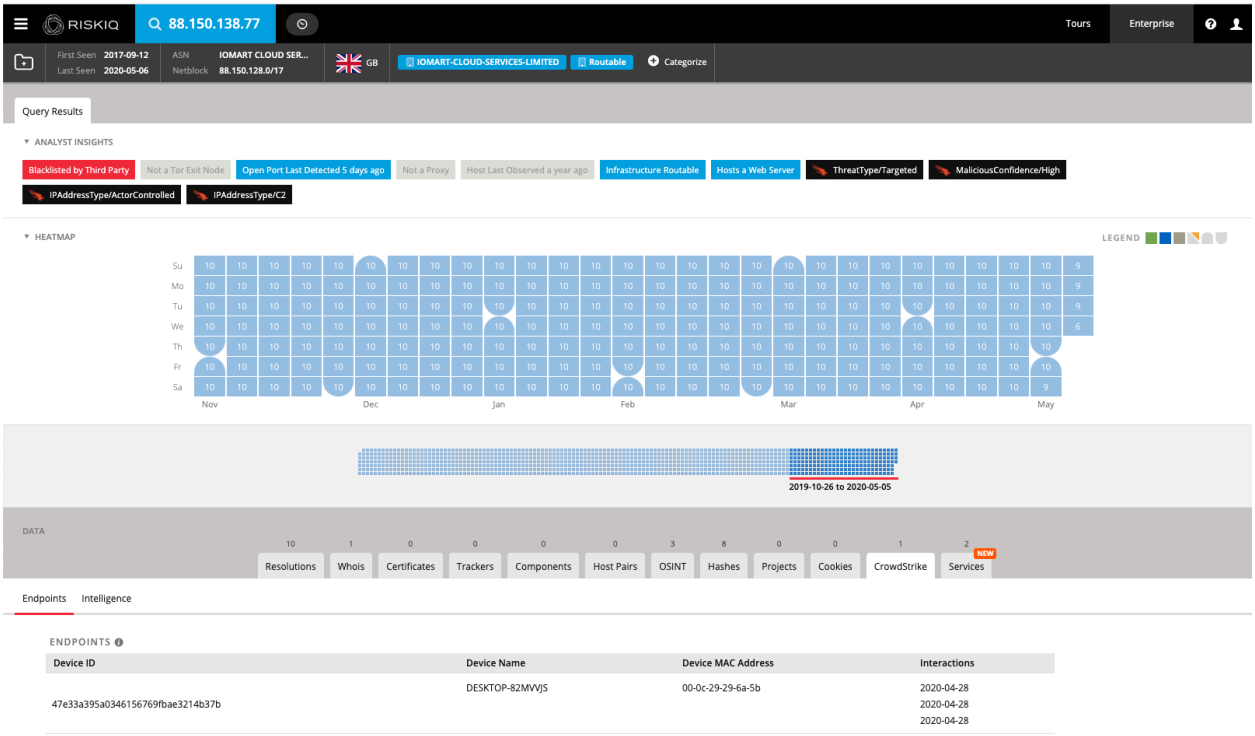
The next area you will see is Analyst Insights. We worked with our professional cyber investigators and polled them to find out the question they needed to answer during an investigation to determine if something was suspicious, malicious, benign.
The Black colored insights are due to the CrowdStrike Integration. These insights are pulled when you perform a search in PassiveTotal. This ensures that you have the latest intelligence from CrowdStrike during your investigation.

From the results here we see that this is a known bad site that was blacklisted by a third-party. It has open ports just five days ago and the infrastructure (IP address) was routable and was hosting a webserver.

CrowdStrike Intelligence informs the analyst that this is part of a targeted attack. This IP is malicious with a high confidence. The IP address is controlled by the threat actor and it is a command and control server IP address.

That is a lot of information in a very condensed area. This allows for smart, and faster incident response.

Step 12: Click on the CrowdStrike tab.
https://community.riskiq.com/search/88.150.138.77/crowdstrike

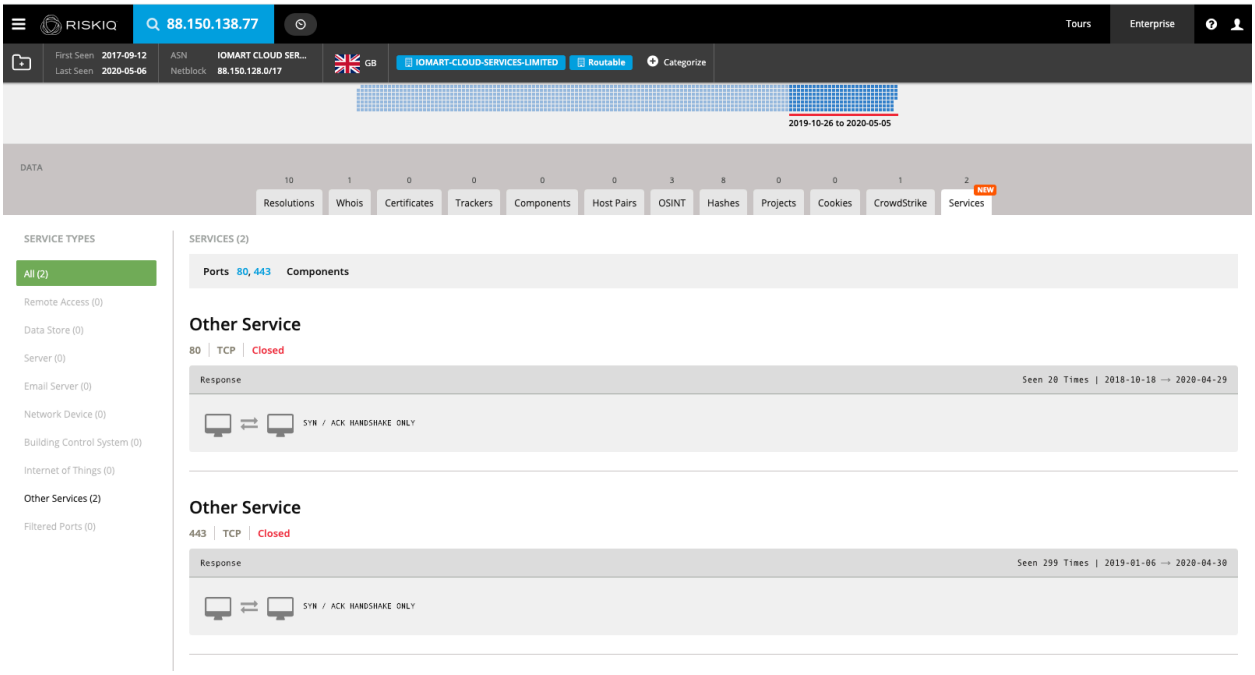


CrowdStrike is protecting the organizations endpoint. Falcon sees everything inside the organization and RiskIQ see everything outside the firewall on the internet.

This tab informs the analyst what devices have communicated with the IOC you searched in PassiveTotal. The analyst can immediately know that a single desktop has communicated 3 time on April 28th to this known command and control IP address.

Now the analyst knows that he needs to work with the use to make sure the organization is safe from this attacker.

Step 13: Click on the Service Tab
https://community.riskiq.com/search/88.150.138.77/services

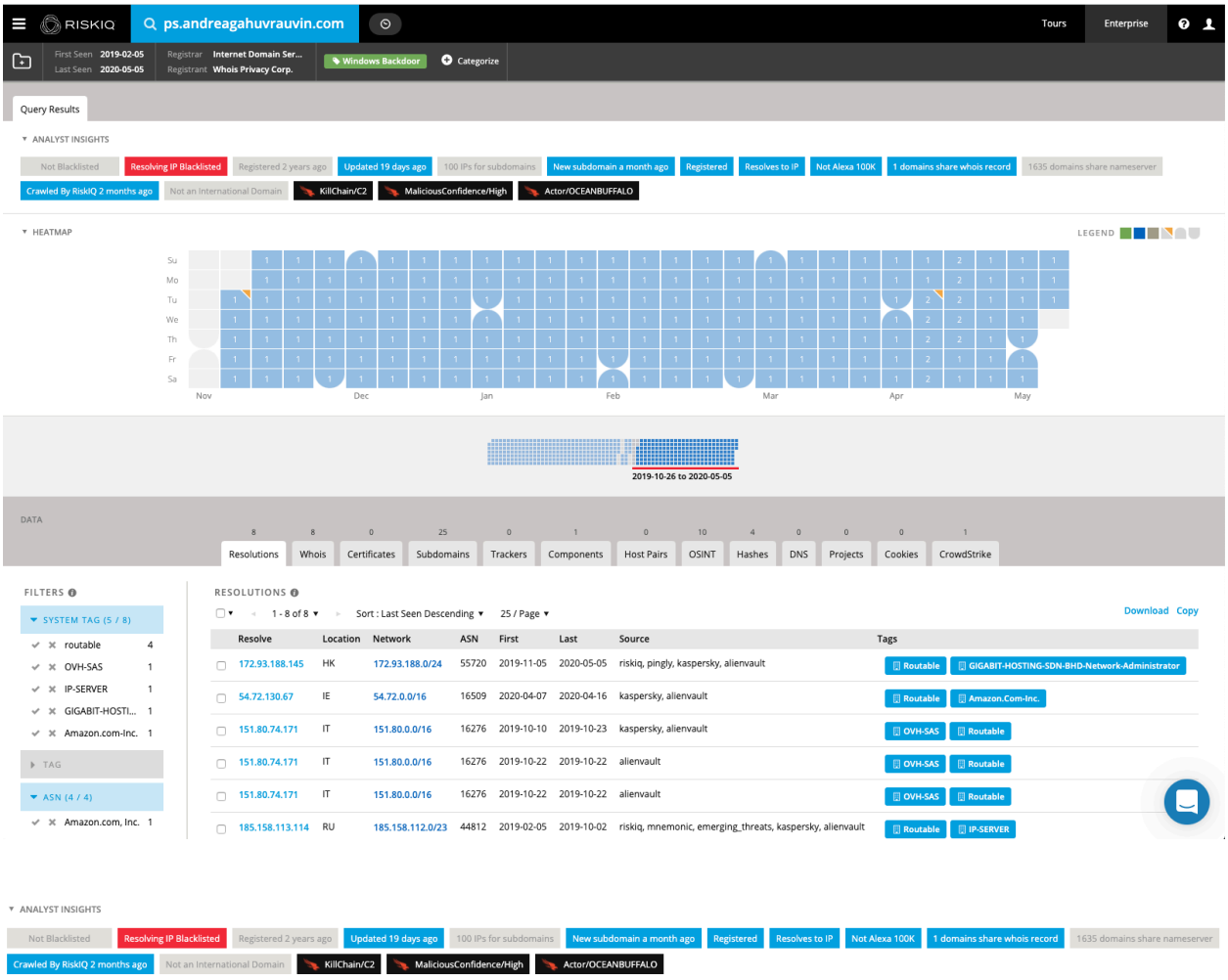


The Services tab is a feature is only available to PassiveTotal Enterprise users and is not available to free community users.

Analyst can now know if the services (Ports) are open, closed, filtered and see the actual response during the scan.

From here we can see that the IP address is no longer active at this particular time.

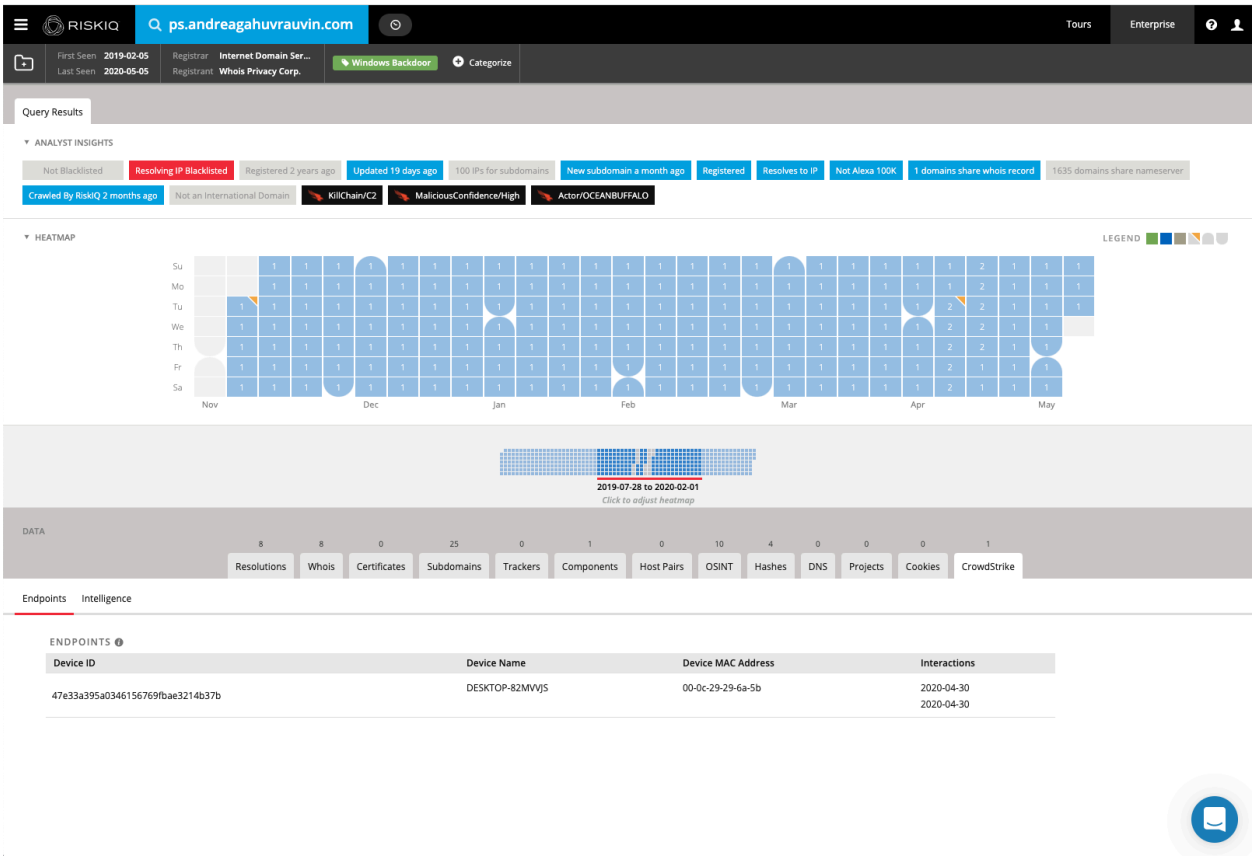
Step 14: In PassiveTotal Search for ps[.]andreagahuvrauvin[.]com
https://community.riskiq.com/search/ps.andreagahuvrauvin.com



From the Analyst Insights RiskIQ informs the analyst that the domain is resolving to known blacklisted IP address, the IP address changed 19 days ago. A new subdomain was seen a month ago.

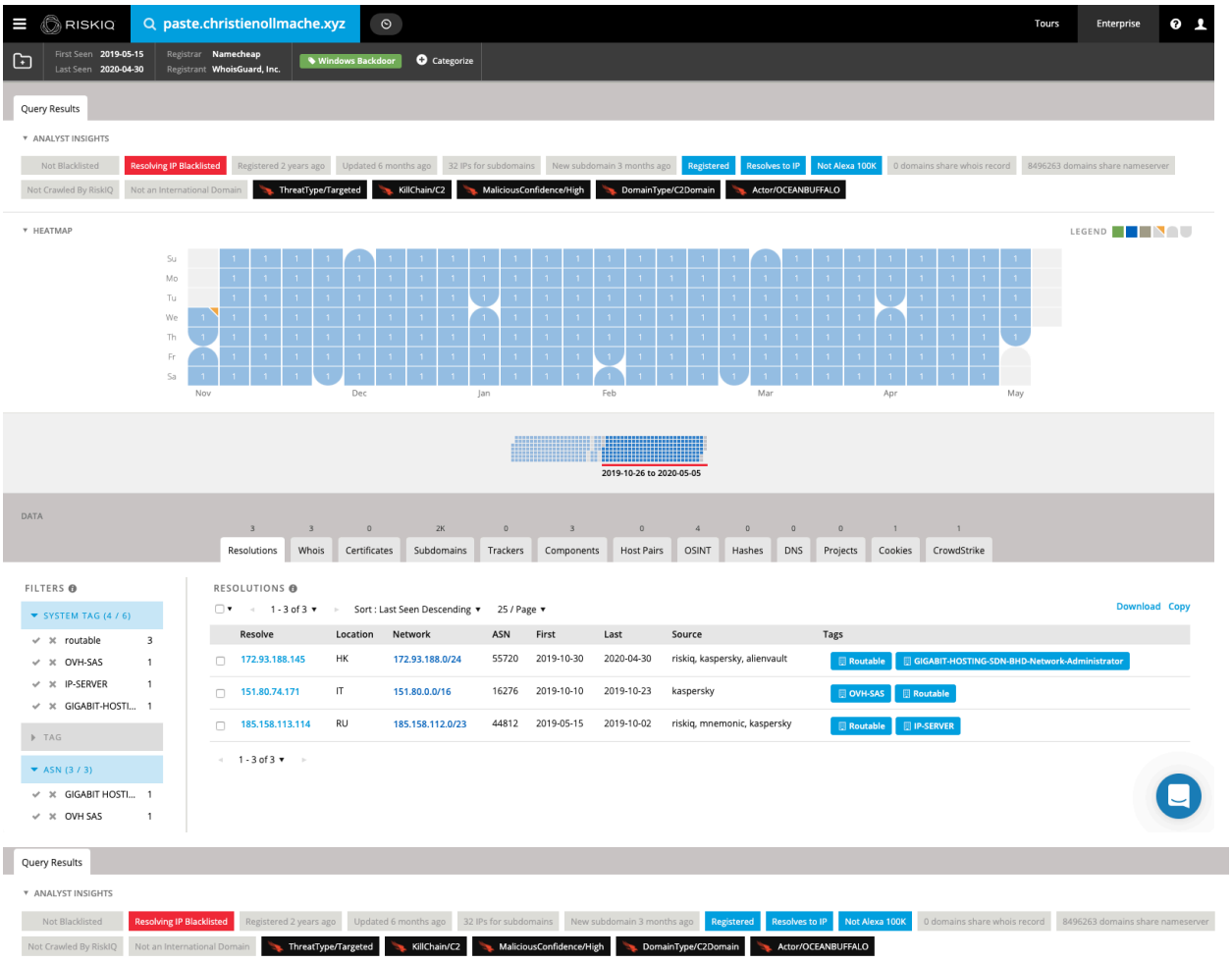
CrowdStrike informs the analyst that this attack is malicious, and the threat actor is Ocean Buffalo. It is part of the command and control in the kill chain.

Step 15: Click on the CrowdStrike Tab.
https://community.riskiq.com/search/ps.andreagahuvrauvin.com/crowdstrike



We see that the same device that reached out to the known bad IP address reached out to this particular domain twice on April 30th.

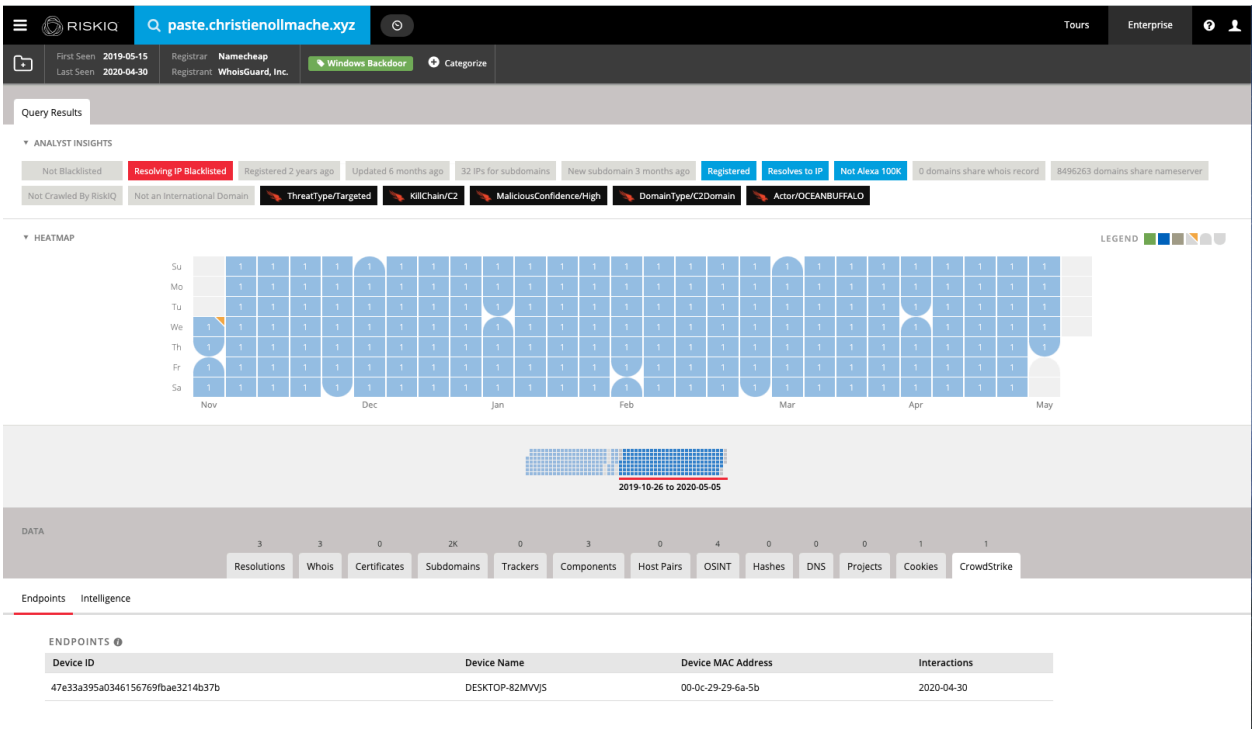
Step 16: Search on the next domain from the article paste[.]christienollmache[.]xyz
https://community.riskiq.com/search/paste.christienollmache.xyz/resolutions



RiskIQ informs the analyst that the domain was registered 2 years ago, it is connected to a resolving blacklisted IP address.

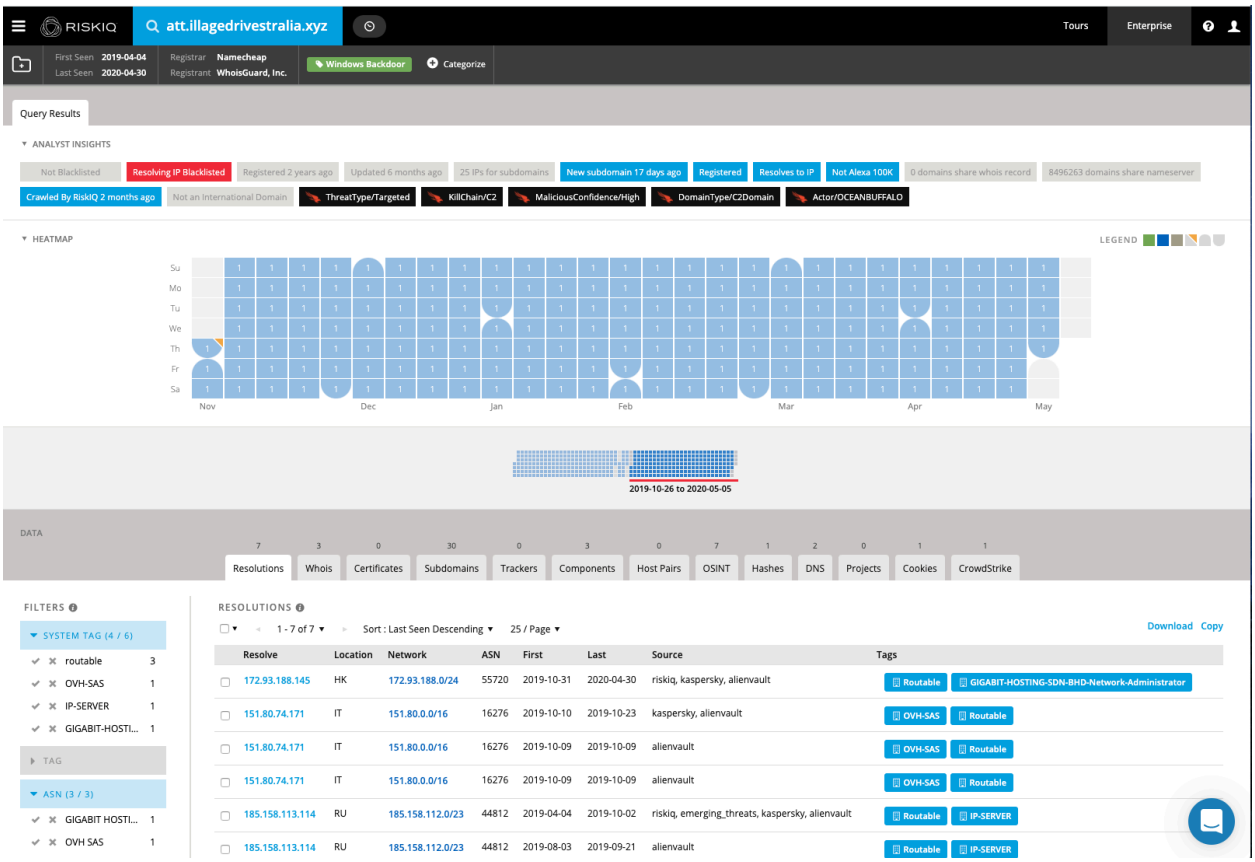
CrowdStrike informs the analyst that it is part of a targeted attack, it is malicious, part of the command and control section of the kill chain. The threat actor is Ocean Buffalo.

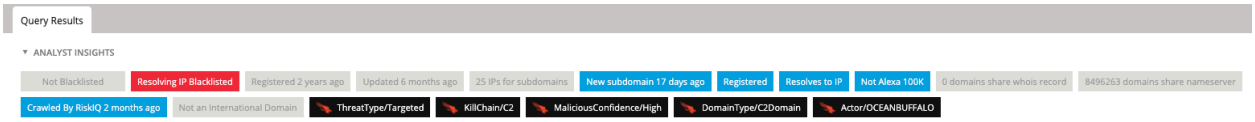
Step 17: Click on the CrowdStrike Tab
https://community.riskiq.com/search/paste.christienollmache.xyz/crowdstrike



CrowdStrike informs the analyst protect asset Desktop-82mvjs reached out to this malicious domain on April 30th.

Step 18: Search the last domain att[.]illagedrivestralia[.]xyz
https://community.riskiq.com/search/att.illagedrivestralia.xyz





RiskIQ informs that analyst that the domain's IP address is blacklisted. New subdomain was added 17 days ago.

CrowdStrike informs the analyst that this is a targeted attack, part of the command and control section of the kill chain. The domain is malicious and is associated with the threat actor Ocean Buffalo.

Conclusion:

Objective 1: What are the aspects of the attacks?

Android, MacOS, Windows attack vectors according to the publication.

Objective 2: Is it still active?

The IP address is not currently active at this time.

Objective 3: Does your organization need to worry about this attack?

Yes, a single device DESKTOP-82MVVJS reached out the C2 IP address and all three windows backdoor domains.

Objective 4: Have you seen any traffic to the IOCs?

Yes, a single device DESKTOP-82MVVJS reached out the C2 IP address and all three windows backdoor domains.