



## 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>

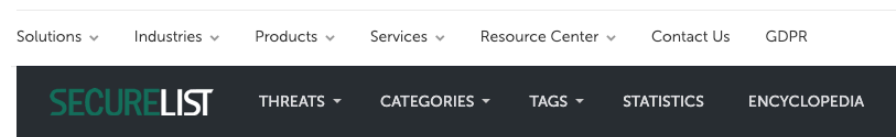
att[.]illagedrivestralia[.]xyz

<https://community.riskiq.com/search/att.illagedrivestralia.xyz>

## Step 1: OSINT Publication Review

<https://securelist.com/apt-phantomlance/96772/- infrastructure>

kaspersky

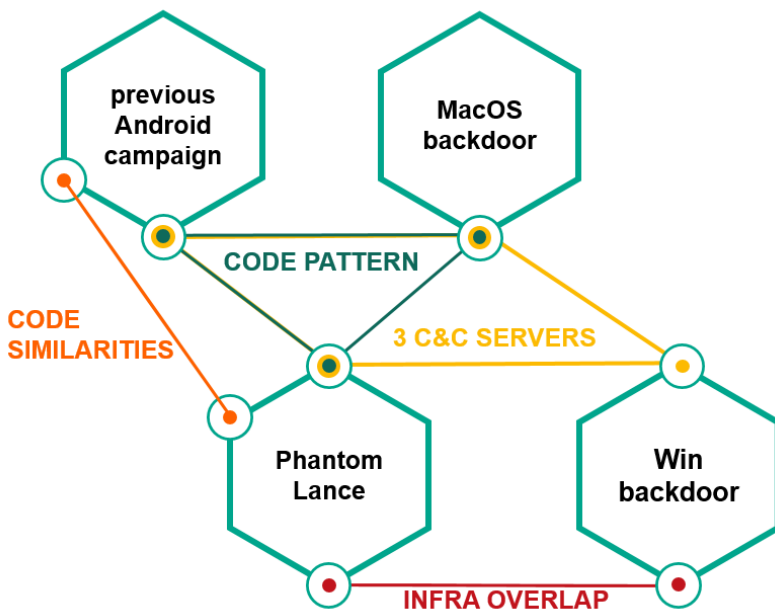
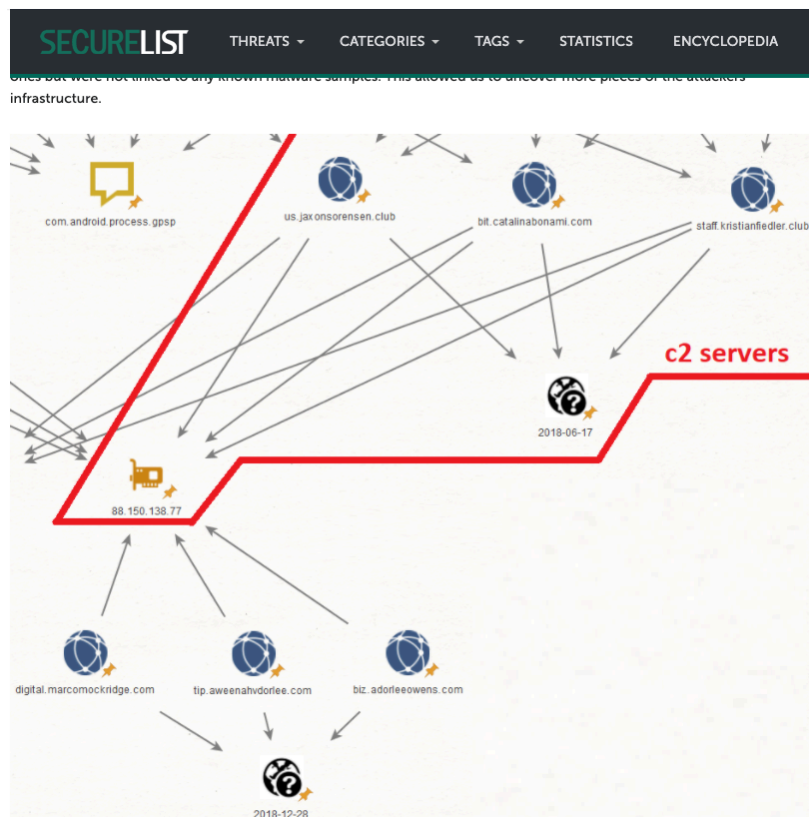


### APT REPORTS

## 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.



## Summary of overlaps

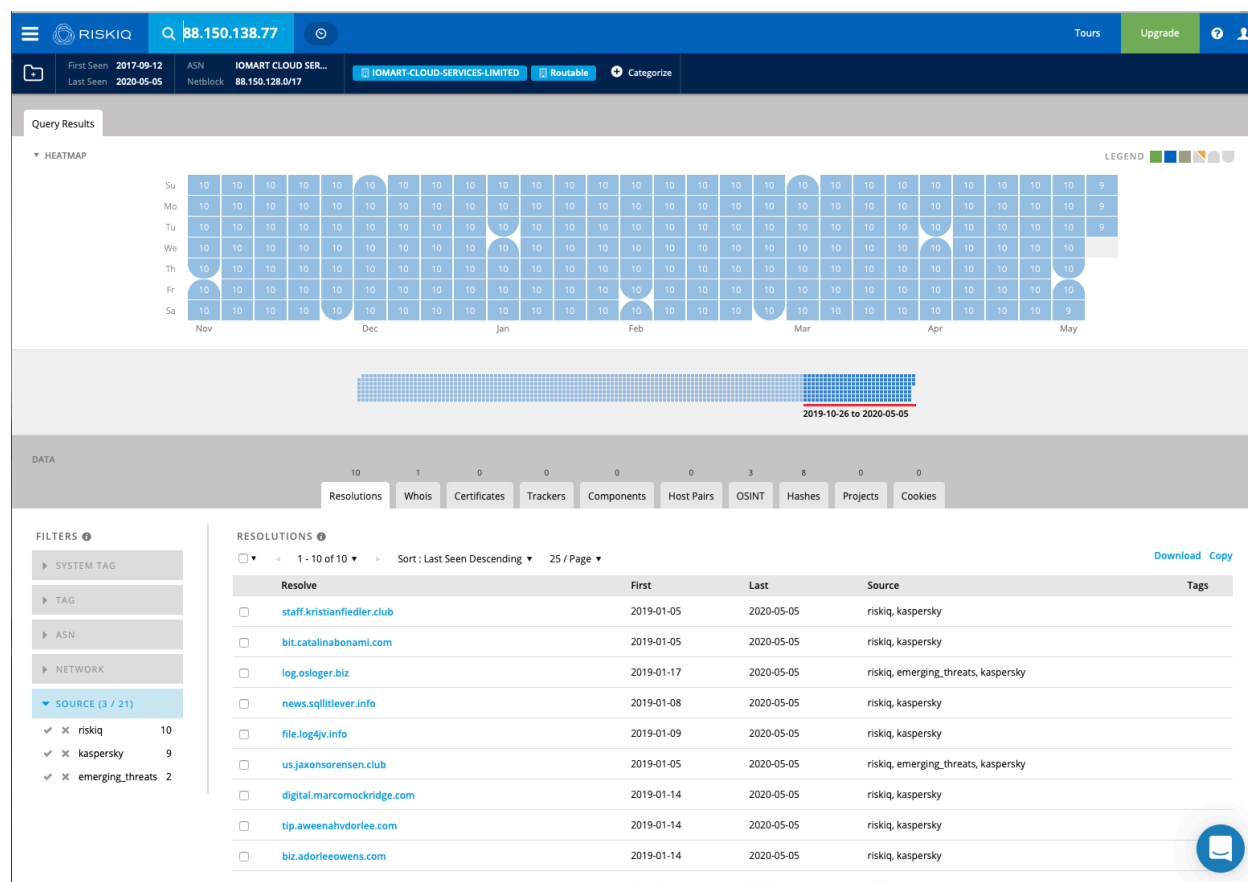
Another notable attribution token that applies to most of OceanLotus malware across platforms is usage of three redundant, different C2 servers by each sample, mostly subdomains. Below is an example of this from the samples examined above and OceanLotus Windows malware described in our private report.

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

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 screenshot shows the RiskIQ community search interface. At the top, the search bar contains the IP address 88.150.138.77. Below the search bar, there's a navigation bar with tabs for Resolutions, Whois, Certificates, Trackers, Components, Host Pairs, OSINT, Hashes, Projects, and Cookies. The 'Whois' tab is currently selected. The main content area displays the Whois record for the IP address 88.150.138.77, which is associated with the domain 88.150.138.77. The record includes details such as the Registrar (RIPE NCC), Email (abuse@redstation.com), Name (Dedicated Server Hosting), Organization (RSDEDI-PANNPJE), Street (Redstation Limited), City (2 Frater Gate Business Park), State (-), Postal Code (Aerodrome Road), Country (Gosport), and Phone (-). The record was updated on 2003-12-04 and last scanned on 2017-12-10. A 'CHANGE HISTORY' table on the left shows the record was updated on 2003-12-04. The right side of the record contains additional information, including the IANA WHOIS server, the RIPE Database query service, and the abuse contact for the IP address.

**WHOIS RECORDS**

CHANGE HISTORY

Date	Changes
2003-12-04	[icon]

RECORD UPDATED 2003-12-04 : LAST SCANNED 2017-12-10  
 Checked by RiskIQ | Expiration N/A | Created 3 years ago | [Hide Diff](#) | [Hide Raw Record](#)

Attribute	Value
WHOIS Server	whois.ripe.net
Registrar	RIPE NCC
Email	<a href="mailto:abuse@redstation.com">abuse@redstation.com</a> (admin, tech)
Name	<a href="#">Dedicated Server Hosting</a> (registrant)
Organization	<a href="#">RSDEDI-PANNPJE</a> (registrant) <a href="#">Redstation Admin Role</a> (admin, tech)
Street	<a href="#">Redstation Limited</a> (admin, tech)
City	<a href="#">2 Frater Gate Business Park</a> (admin, tech)
State	-
Postal Code	<a href="#">Aerodrome Road</a> (admin, tech)
Country	<a href="#">Gosport</a> (admin, tech) <a href="#">GB</a> (registrant)
Phone	-

% IANA WHOIS server  
 % for more information on IANA, visit <http://www.iana.org>  
 % This query returned 1 object

refer: whois.ripe.net

inetnum: 88.0.0.0 - 88.255.255.255  
 organisation: RIPE NCC  
 status: ALLOCATED

whois: whois.ripe.net

changed: 2004-04  
 source: IANA

% This is the RIPE Database query service.  
 % The objects are in RPSL format.  
 %  
 % The RIPE Database is subject to Terms and Conditions.  
 % See <http://www.ripe.net/db/support/db-terms-conditions.pdf>

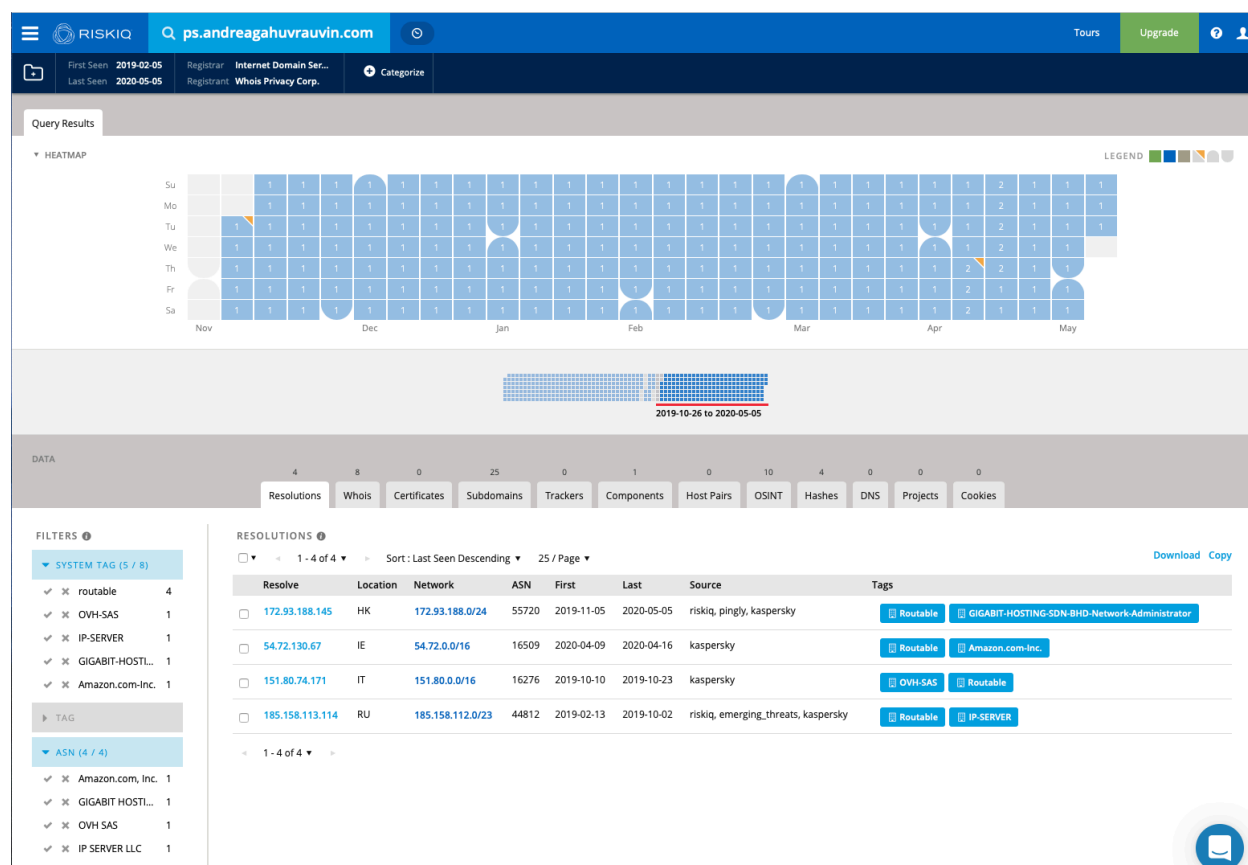
% Information related to '88.150.138.64 - 88.150.138.127'

% Abuse contact for '88.150.138.64 - 88.150.138.127' is 'abuse@redstation.com'

inetnum: 88.150.138.64 - 88.150.138.127  
 netname: RSDEDI-PANNPJE

The IP address is located in Great Britain. 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

The screenshot displays the RiskIQ community search results for the IP address 172.93.188.145. The interface includes a search bar at the top with the IP address entered. Below the search bar, there are tabs for 'Query Results' and 'HEATMAP'. The 'HEATMAP' tab shows a calendar view with activity levels indicated by colored squares. The 'Query Results' tab shows a list of resolutions with columns for 'Resolve', 'First', 'Last', 'Source', and 'Tags'. The 'Filters' section on the left allows filtering by system tag, tag, ASN, network, and source. The 'Resolutions' section on the right shows a list of resolutions with columns for 'Resolve', 'First', 'Last', 'Source', and 'Tags'.

**Query Results**

HEATMAP

LEGEND

DATA

217 1 1 0 4 0 3 3 0 8

Resolutions Whois Certificates Trackers Components Host Pairs OSINT Hashes Projects Cookies

**FILTERS**

SYSTEM TAG

TAG

ASN

NETWORK

SOURCE (3 / 277)

riskiq 171

kaspersky 100

emerging\_threats 6

**RESOLUTIONS**

1 - 25 of 217 Sort: Last Seen Descending 25 / Page

Resolve	First	Last	Source	Tags
<a href="#">www.andreagahuvrauin.com</a>	2019-11-06	2020-05-05	kaspersky	
<a href="#">www.andreagabridge.com</a>	2019-12-04	2020-05-05	riskiq, kaspersky	
<a href="#">www.groveskekiv.com</a>	2019-11-05	2020-05-05	riskiq, kaspersky	
<a href="#">ps.andreagahuvrauin.com</a>	2019-11-05	2020-05-05	riskiq, kaspersky	
<a href="#">www.urielcallum.com</a>	2019-11-11	2020-05-05	riskiq, kaspersky	
<a href="#">nvidia.benjamilliams.club</a>	2019-10-31	2020-05-04	riskiq, kaspersky	
<a href="#">www.byronorenstein.com</a>	2019-11-04	2020-05-04	kaspersky	
<a href="#">ns2.nlggnjggmgnidgngggmjjg.lmlajoo.andreagahuvrauin.com</a>	2020-05-04	2020-05-04	riskiq	
<a href="#">Ops.andreagahuvrauin.com</a>	2020-05-04	2020-05-04	riskiq	

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

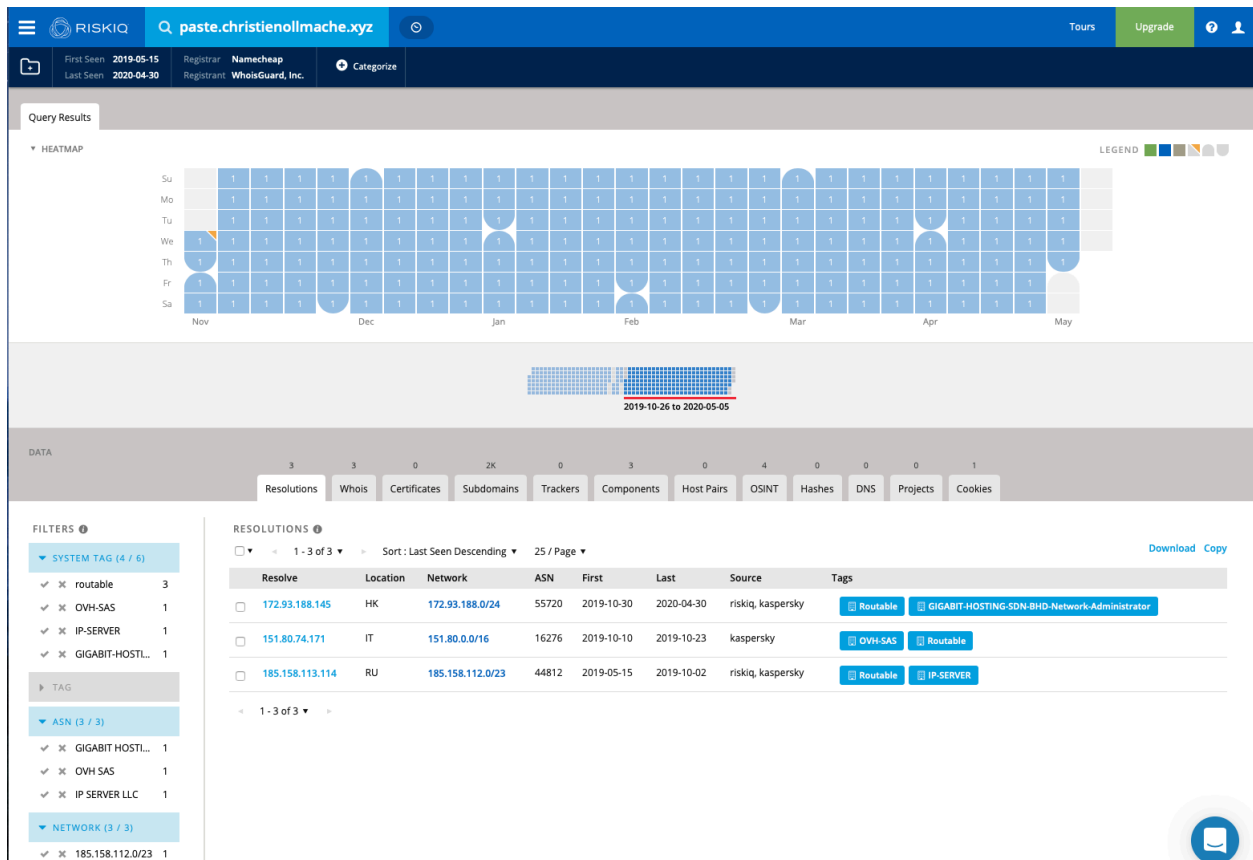
We can see 217 IP addresses most have recent activity on the domains going back to a few months ago.





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

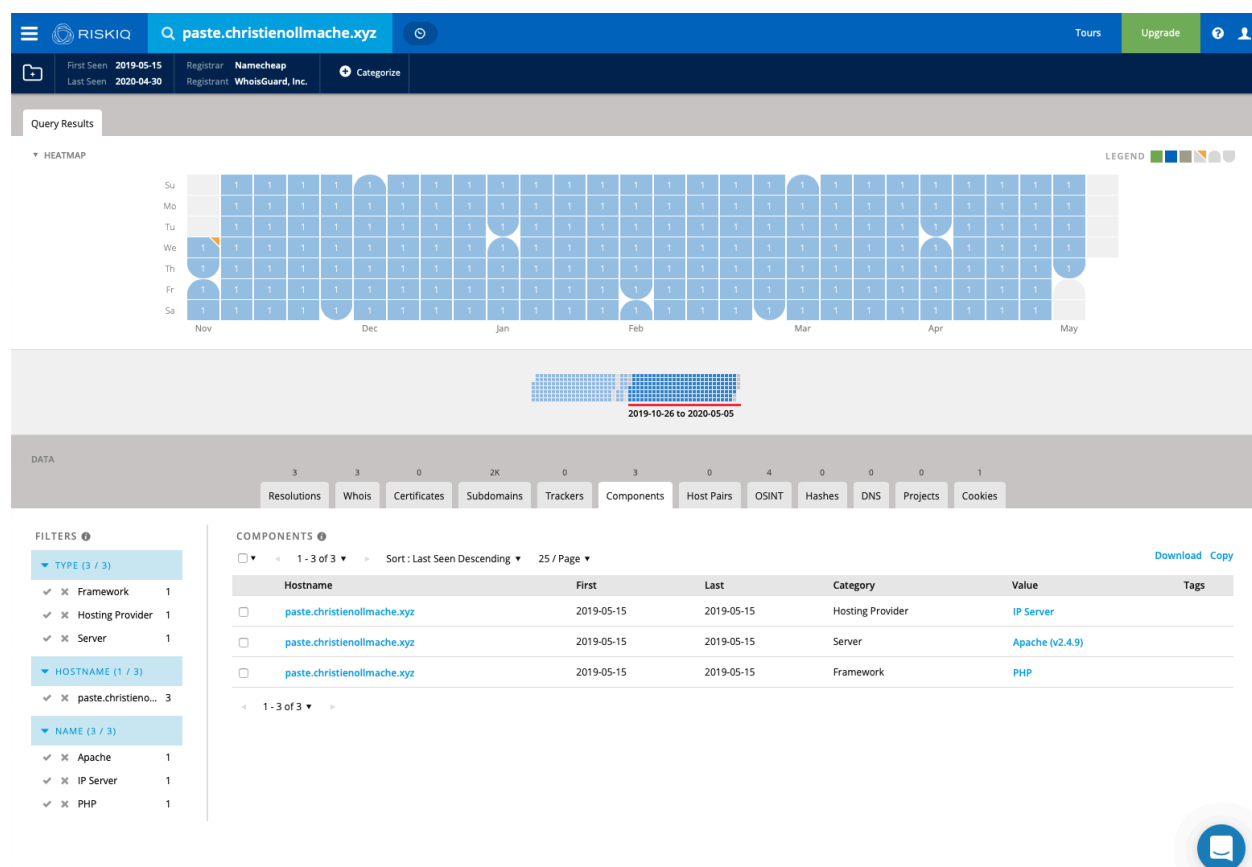
<https://community.riskiq.com/search/paste.christienollmache.xyz/resolutions>



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.

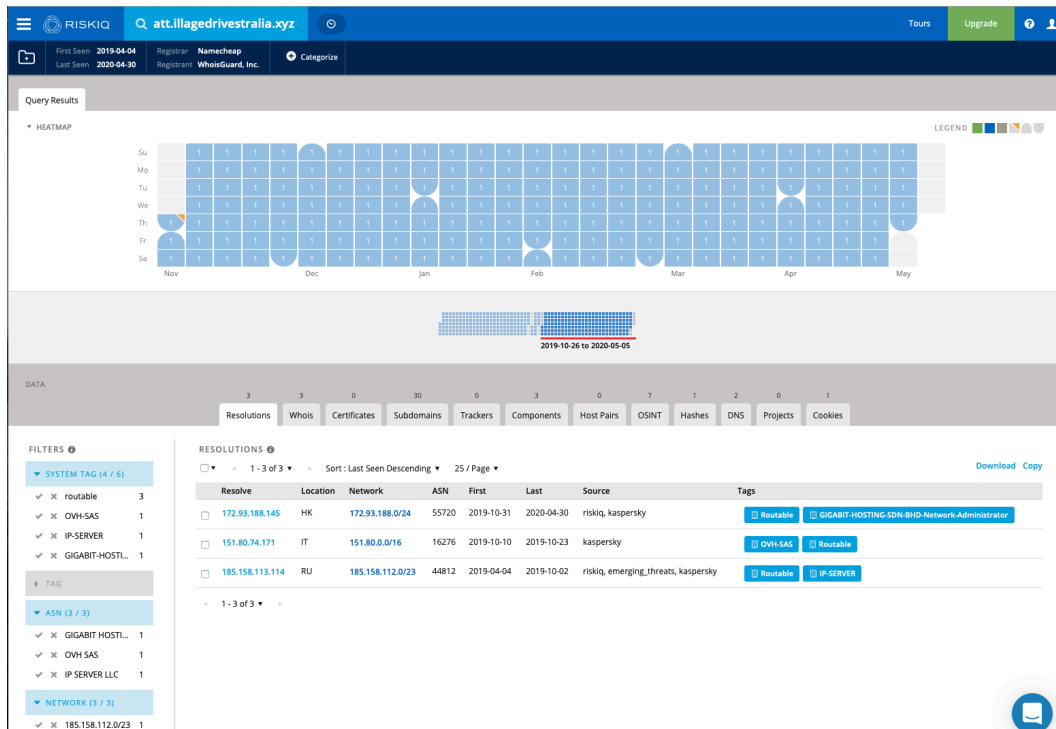
## Step 8: Click on Components

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



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

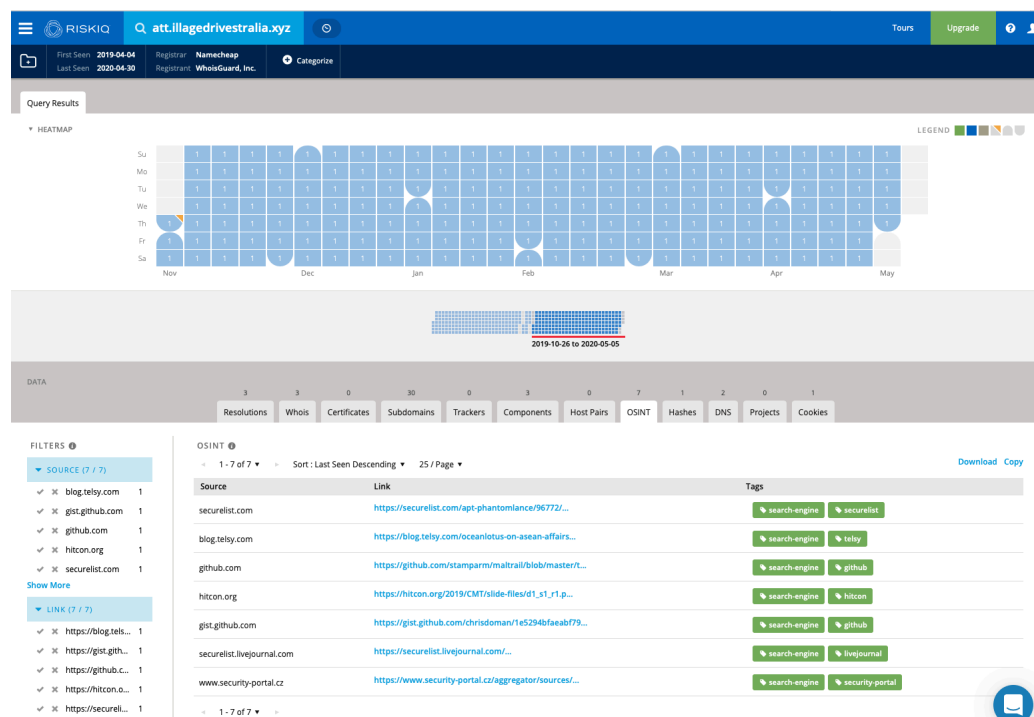
**Step 9:** Search the last domain att[.]illagedrivestralia[.]xyz  
<https://community.riskiq.com/search/att.illagedrivestralia.xyz>



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

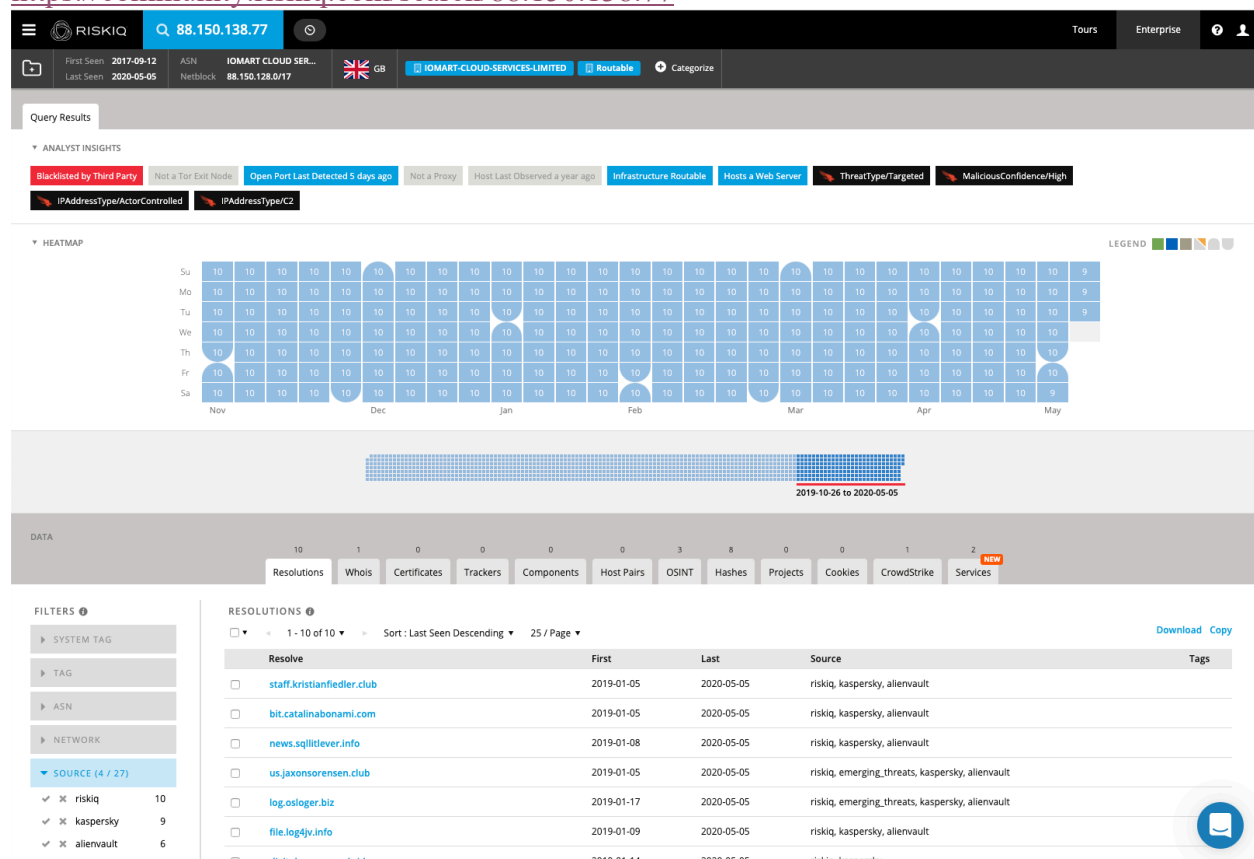
**Objective 4:** Have you seen any traffic to the IOCs?  
Inconclusive, needs further investigation

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.

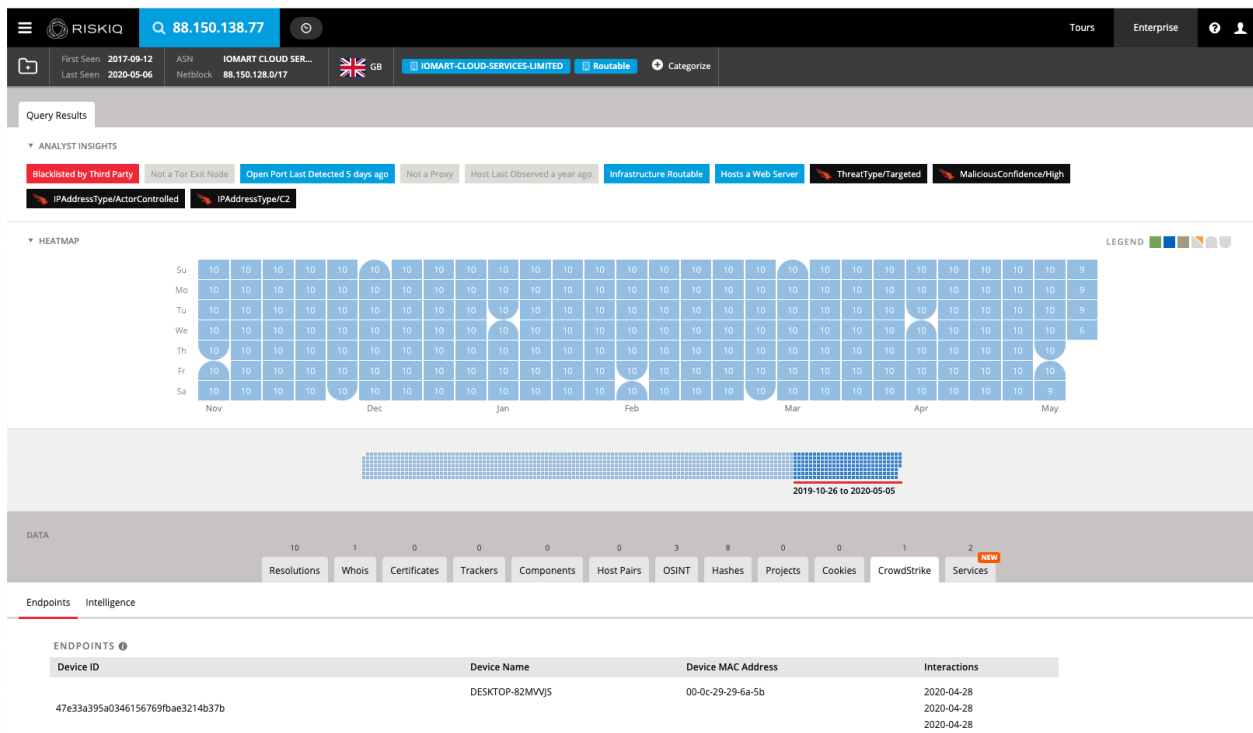
From the results here we see that this is a known bad site that was blacklisted by a third-party. It has open ports just five days ago and the infrastructure (IP address) was routable and was hosting a webserver.

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 28<sup>th</sup> 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 screenshot displays the RiskIQ community search interface. The top navigation bar includes the RiskIQ logo, a search bar with the IP address 88.150.138.77, and links for Tours and Enterprise. Below the navigation bar, a header section shows the IP address 88.150.138.77, its location (GB), and associated domains (IOMART-CLOUD-SERVICES-LIMITED, Routable). A timeline bar indicates the period from 2019-10-26 to 2020-05-05. The main content area is divided into two sections: SERVICE TYPES and SERVICES (2). The SERVICE TYPES section lists various categories like Remote Access, Data Store, Server, Email Server, Network Device, Building Control System, Internet of Things, and Other Services (2). The SERVICES (2) section shows two entries for 'Other Service'. The first entry is for port 80, TCP, Closed, with a response icon and a timeline from 2018-10-18 to 2020-04-29. The second entry is for port 443, TCP, Closed, with a response icon and a timeline from 2019-01-06 to 2020-04-30. Both entries show a response icon and the text 'SYN / ACK HANDSHAKE ONLY'.

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>

**Query Results**

**ANALYST INSIGHTS**

- Not Blacklisted
- Resolving IP Blacklisted**
- Registered 2 years ago
- Updated 19 days ago
- 100 IPs for subdomains
- New subdomain a month ago
- Registered
- Resolves to IP
- Not Alexa 100K
- 1 domains share whois record
- 1635 domains share nameserver
- Crawled By RiskIQ 2 months ago
- Not an International Domain
- KillChain/C2
- MaliciousConfidence/High
- Actor/OCEANBUFFALO

**HEATMAP**

2019-10-26 to 2020-05-05

**DATA**

8 Resolutions 8 Whois 0 Certificates 25 Subdomains 0 Trackers 1 Components 0 Host Pairs 10 OSINT 4 Hashes 0 DNS 0 Projects 0 Cookies 1 CrowdStrike

**FILTERS**

- SYSTEM TAG (5 / 8)
  - routeable 4
  - OVH-SAS 1
  - IP-SERVER 1
  - GIGABIT-HOSTING 1
  - Amazon.com-Inc. 1
- TAG
- ASN (4 / 4)
  - Amazon.com, Inc. 1

**RESOLUTIONS**

Sort: Last Seen Descending 25 / Page

Resolve	Location	Network	ASN	First	Last	Source	Tags
172.93.188.145	HK	172.93.188.0/24	55720	2019-11-05	2020-05-05	riskiq, pingly, kaspersky, alienvault	Routeable, GIGABIT-HOSTING-SDN-BHD-Network-Administrator
54.72.130.67	IE	54.72.0.0/16	16509	2020-04-07	2020-04-16	kaspersky, alienvault	Routeable, Amazon.Com-Inc.
151.80.74.171	IT	151.80.0.0/16	16276	2019-10-10	2019-10-23	kaspersky, alienvault	OVH-SAS, Routeable
151.80.74.171	IT	151.80.0.0/16	16276	2019-10-22	2019-10-22	alienvault	OVH-SAS, Routeable
151.80.74.171	IT	151.80.0.0/16	16276	2019-10-22	2019-10-22	alienvault	OVH-SAS, Routeable
185.158.113.114	RU	185.158.112.0/23	44812	2019-02-05	2019-10-02	riskiq, mnemonic, emerging_threats, kaspersky, alienvault	Routeable, IP-SERVER

**ANALYST INSIGHTS**

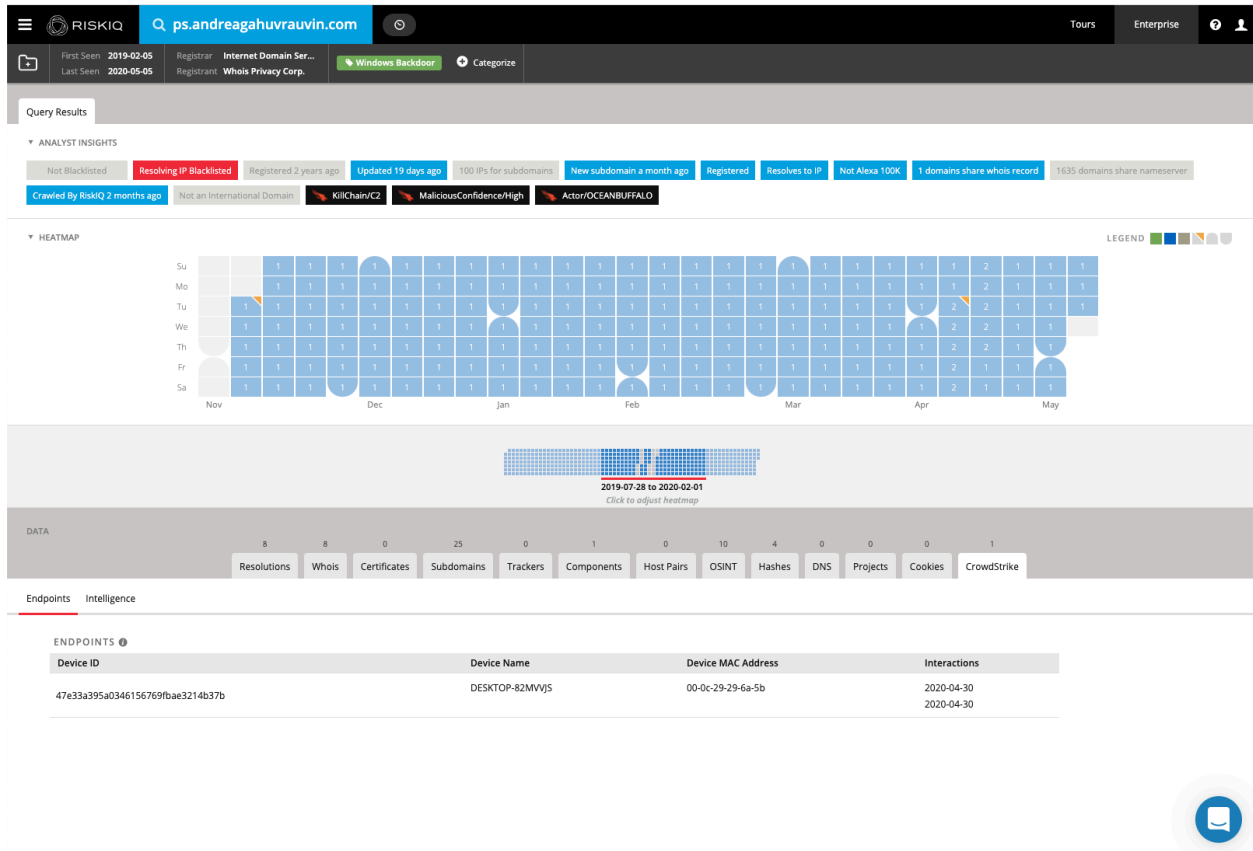
- Not Blacklisted
- Resolving IP Blacklisted**
- Registered 2 years ago
- Updated 19 days ago
- 100 IPs for subdomains
- New subdomain a month ago
- Registered
- Resolves to IP
- Not Alexa 100K
- 1 domains share whois record
- 1635 domains share nameserver
- Crawled By RiskIQ 2 months ago
- Not an International Domain
- KillChain/C2
- MaliciousConfidence/High
- Actor/OCEANBUFFALO

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.andreaghuvrauvin.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 30<sup>th</sup>.

**Step 16:** Search on the next domain from the article

paste[.]christienollmache[.]xyz

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

**Query Results**

**ANALYST INSIGHTS**

- Not Blacklisted
- Resolving IP Blacklisted**
- Registered 2 years ago
- Updated 6 months ago
- 32 IPs for subdomains
- New subdomain 3 months ago
- Registered
- Resolves to IP
- Not Alexa 100K
- 0 domains share whois record
- 8496263 domains share nameserver
- Not Crawled By RiskIQ
- Not an International Domain
- ThreatType/Targeted
- KillChain/C2
- MaliciousConfidence/High
- DomainType/C2Domain
- Actor/OCEANBUFFALO

**HEATMAP**

LEGEND

2019-10-26 to 2020-05-05

**DATA**

3 Resolutions 3 Whois 0 Certificates 2K Subdomains 0 Trackers 3 Components 0 Host Pairs 4 OSINT 0 Hashes 0 DNS 0 Projects 1 Cookies 1 CrowdStrike

**FILTERS**

**SYSTEM TAG (4 / 6)**

- ✓ X routable 3
- ✓ X OVH-SAS 1
- ✓ X IP-SERVER 1
- ✓ X GIGABIT-HOSTL... 1

**TAG**

**ASN (3 / 3)**

- ✓ X GIGABIT HOSTL... 1
- ✓ X OVH SAS 1

**RESOLUTIONS**

1 - 3 of 3 Sort: Last Seen Descending 25 / Page

Resolve	Location	Network	ASN	First	Last	Source	Tags
<input type="checkbox"/> 172.93.188.145	HK	172.93.188.0/24	55720	2019-10-30	2020-04-30	riskiq, kaspersky, alienvault	<a href="#">Routable</a> <a href="#">GIGABIT-HOSTING-SDN-BHD-Network-Administrator</a>
<input type="checkbox"/> 151.80.74.171	IT	151.80.0.0/16	16276	2019-10-10	2019-10-23	kaspersky	<a href="#">OVH-SAS</a> <a href="#">Routable</a>
<input type="checkbox"/> 185.158.113.114	RU	185.158.112.0/23	44812	2019-05-15	2019-10-02	riskiq, mnemonic, kaspersky	<a href="#">Routable</a> <a href="#">IP-SERVER</a>

1 - 3 of 3

**Query Results**

**ANALYST INSIGHTS**

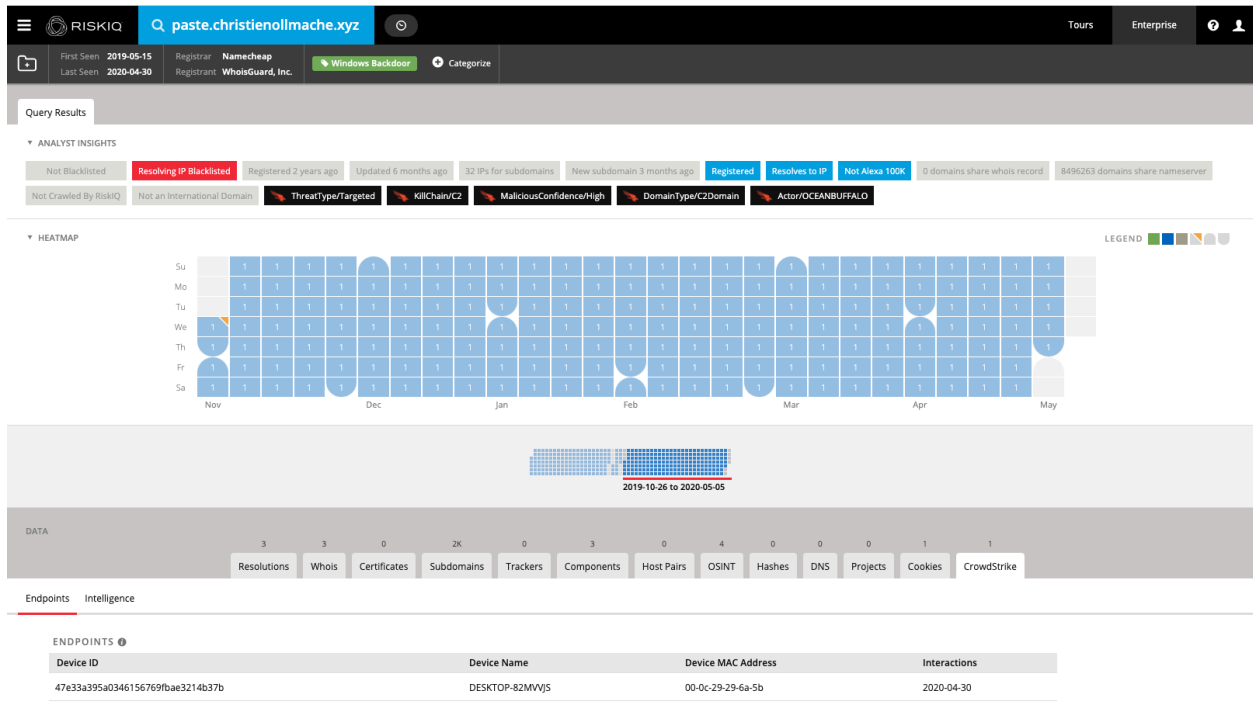
- Not Blacklisted
- Resolving IP Blacklisted**
- Registered 2 years ago
- Updated 6 months ago
- 32 IPs for subdomains
- New subdomain 3 months ago
- Registered
- Resolves to IP
- Not Alexa 100K
- 0 domains share whois record
- 8496263 domains share nameserver
- Not Crawled By RiskIQ
- Not an International Domain
- ThreatType/Targeted
- KillChain/C2
- MaliciousConfidence/High
- DomainType/C2Domain
- Actor/OCEANBUFFALO

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.

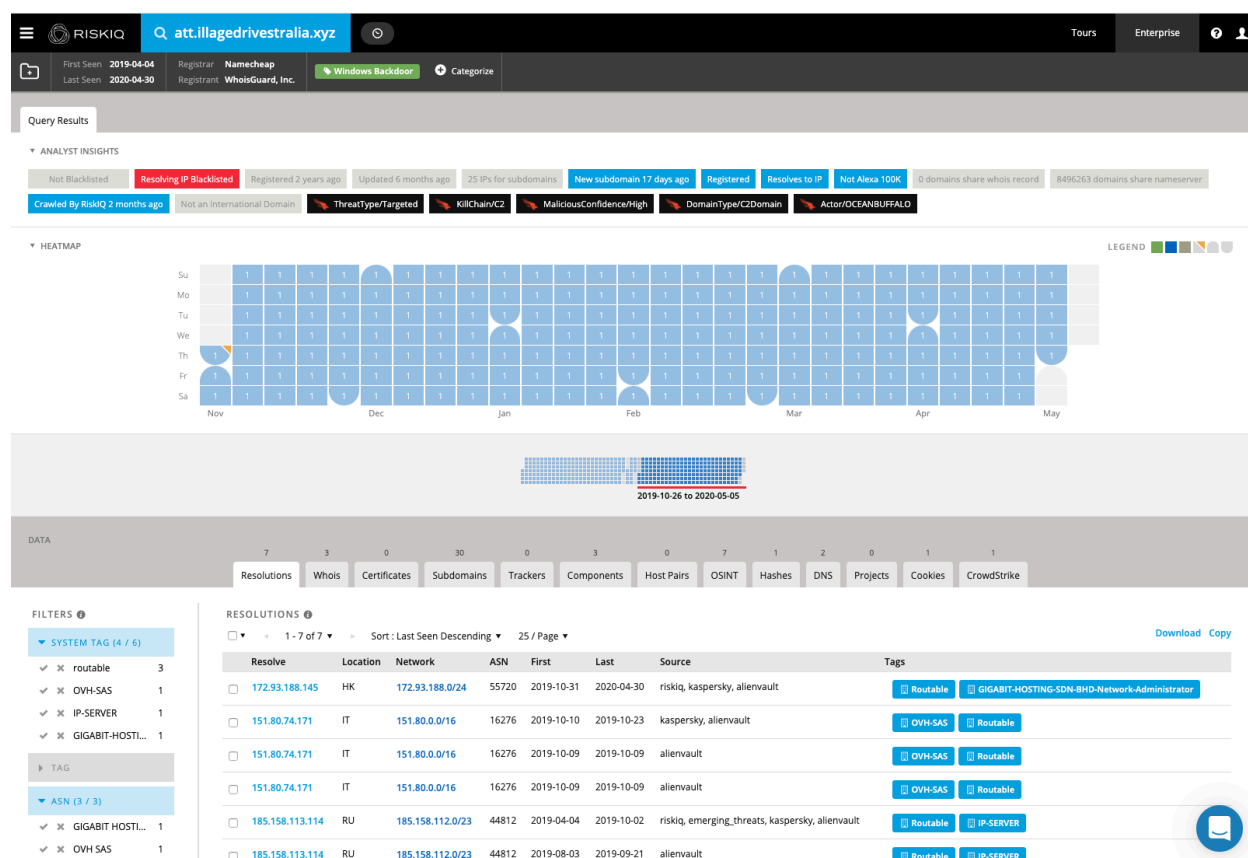
## Step 17: Click on the CrowdStrike Tab

<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 30<sup>th</sup>.

## 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.