How to Treat False Positive with Threat Hunting

ZUP Security Labs at Zup Innovation

Researcher & CyberSecurity Manager: Filipi Pires

Introduction

The purpose of this document, to conduct an investigation on a ***Malops (Malware Operations)*** that were recurring in our environment. The existence of the same domain was observed, being accessed by many machines from different teams, on different days, at different times.

This report was based on one of the pillars for **IOA (Indicator of Attack)** research, multiple alarm events from the many different host for a single domain.

Validating that the domain was really malicious and verifying if there could be some APT underway in our environment, and we performed a lot of research and analysis was carried out regarding the appropriate behaviors.

With the final product, the front responsible for the product will have an instrument capable of guiding a process of mitigation and / or correction, as well as optimized improvement, based on the criticality of risks.

2.0.1 Scope

The conduction this investigation had as a target the Domain = "(`https://cookiesync.slyngshot.io/`)", validating if this domain is malicious or not, first information are provied by Cyberearon are represented in the Malops Incident (`Cybereason Cloud Console malop | AAAA01y6vOZhchYQ`) where we found more than 40 machine doing communication with this domain;

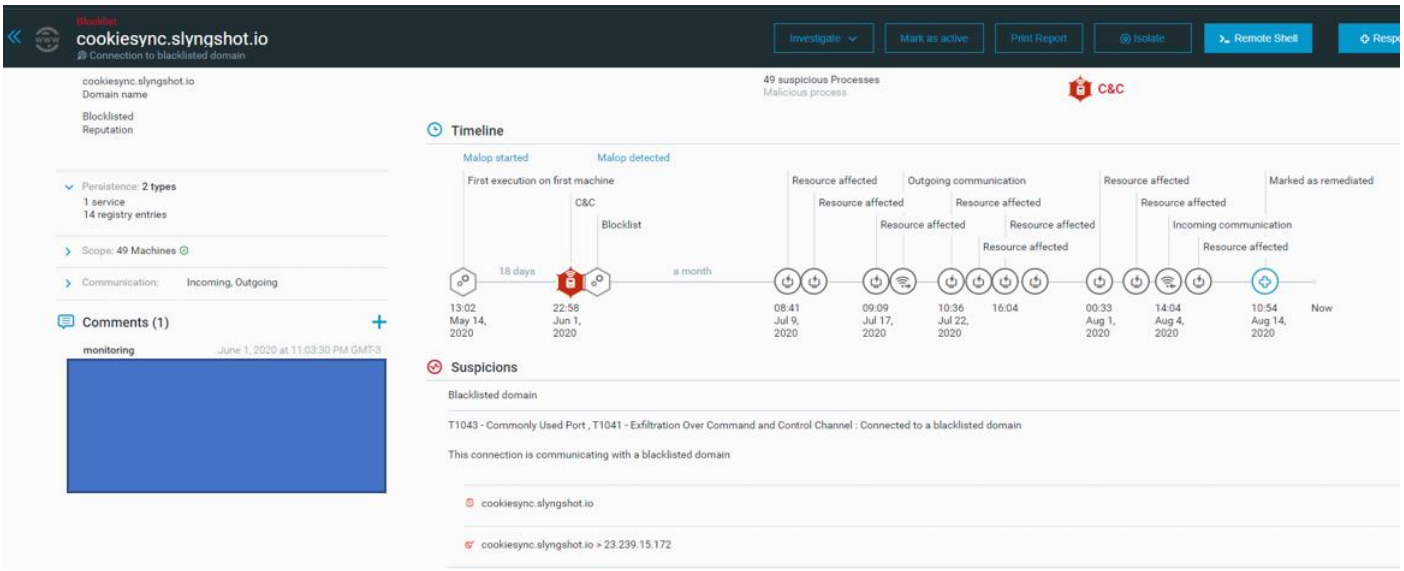


Image 1.1: Malops Incident Detection

2.0.2 Project Summary

The execution of the investigation analysis of the Threat Hunting team it was carried out through the analyze of the log's information provided by Malops Incident reports, other research on the internet, to understands the domain is malicious or not, execution this domain in controlled environment, this investigation occurred during **1 day**. The investigation started on the **11th of August** of the year 2020 and the elaboration this report on the **19th of August** of the same year.

1 Running the Investigation

3.1 First Step

The first step in this investigation it was understand the Malops report and your information's, as we can see in the malops information, the possible attack could be started in May and still happen on August, below we have saw 49 Machine in the scope, the communication looks like to be inbound and outbound and maybe can affect next to 27 users inside de company.

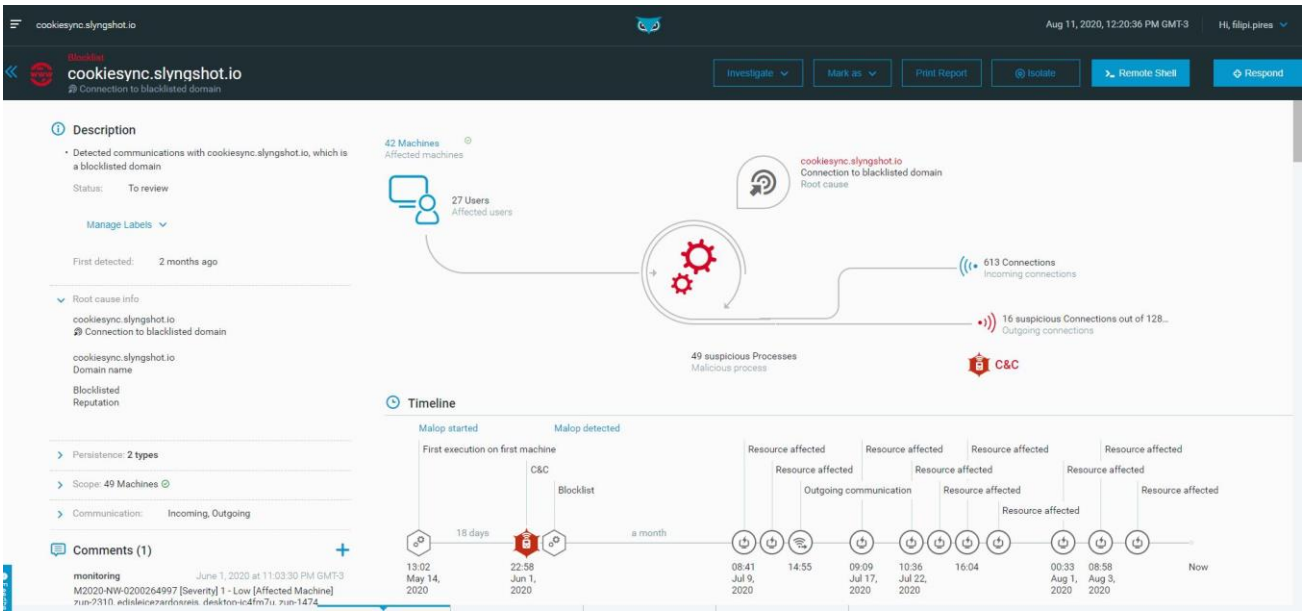


Image 1.2: Overview Malops incident

When we look the malops report we can find others information like a 49 malicious process and 16 suspicious connection, and theses process can be many different malwares being download to the environment, as we can see in the image below, we have many processes related a different extension like a [`.exe / chorme.exe / core.exe /msmpeng.exe and 17x unkown process`]

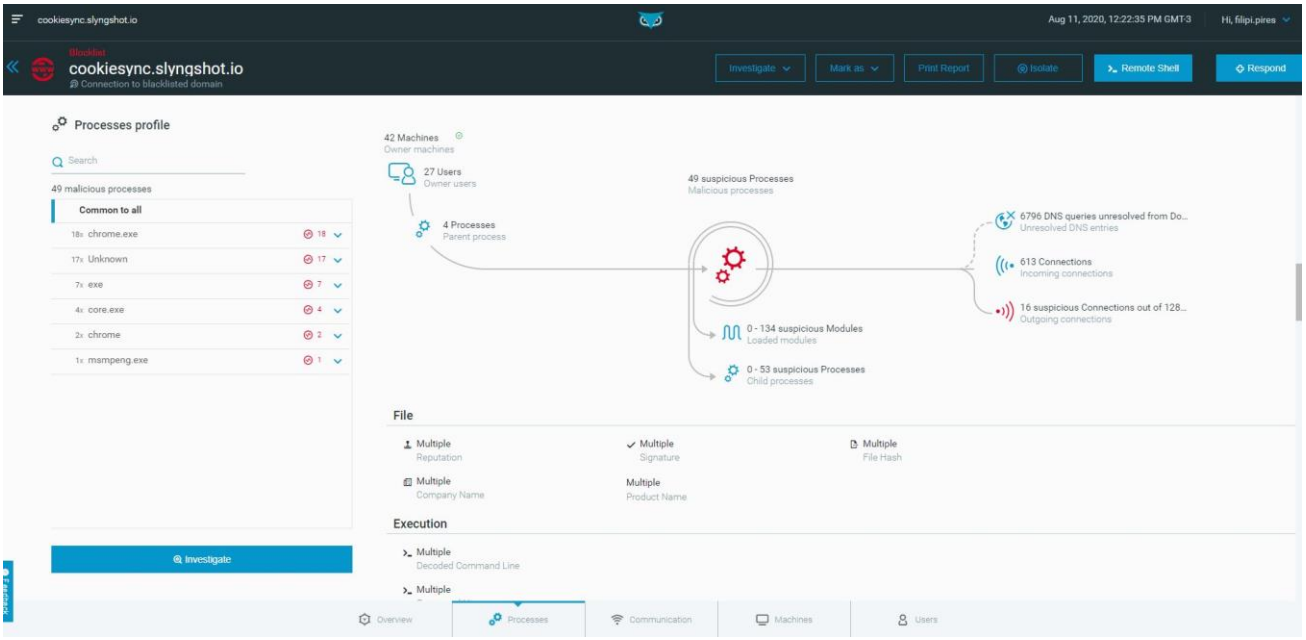


Image 1.3: Process information by Malops Report

3.2 Second Step

In this stage we started to work with some **hypotheses**, however for this happen we needed to understand the "possible" timeline of this incident, looking inside the Malops Report (in PDF), we can find the data, which can have started this incident.

On 14th May it was started the first execution, after 14 days on 1st Jun, it was triggered as C&C Blocklisted Domain, and the next day, continued "infecting" many other machines in our environment, all these machines would be accessing `cookiesync.slyngshot.io,` with the `IP 23.239.15.172`.

All these *triggers* are based on Cybereason Documentation:

Triggering item *- The process that caused Cybereason to create a Malop.* ***Detection type*** *- Category of detection that recognized the malicious behavior.* ***Root cause*** *- The underlying reason why an activity is considered malicious.*

(`https://nest.cybereason.com/documentation/product-documentation/201/what-malop`)

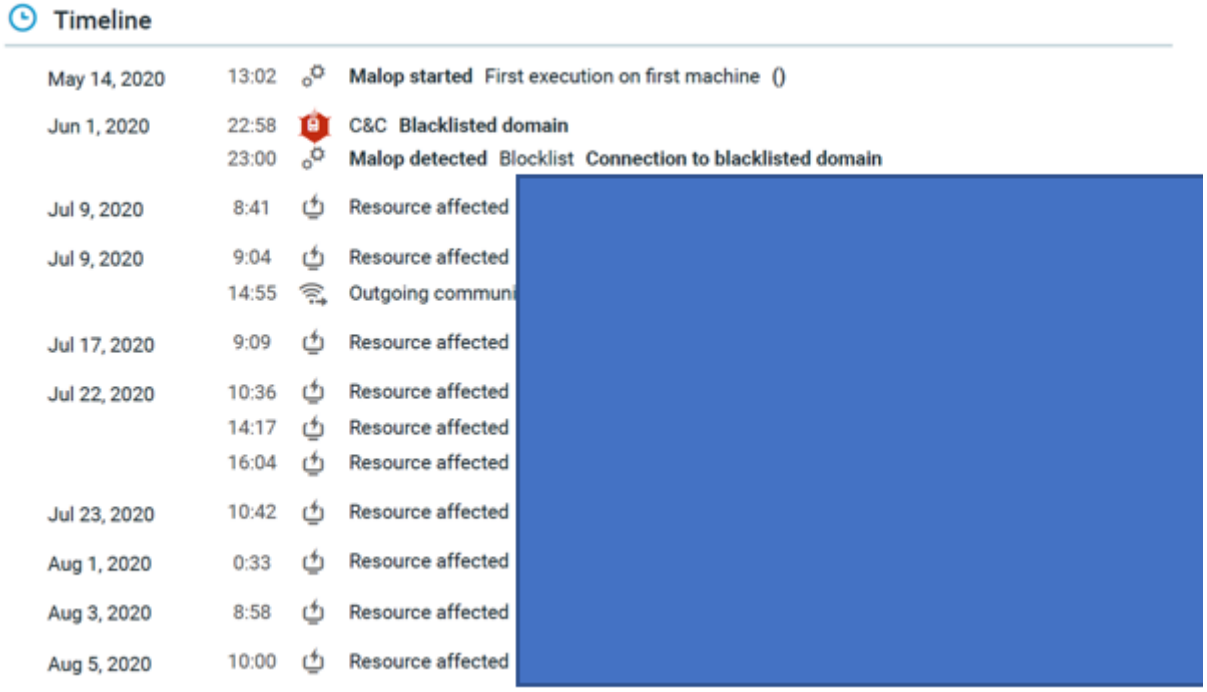


Image 1.4: Timeline of the Incident

3.3 Third Step

Based in this information, we started other researches, locking for a tool that works as a antivirus scanning know as a VIRUS TOTAL.

We performed two tests running the URL “malicious” and de root domain and our tests, both of them are safe.

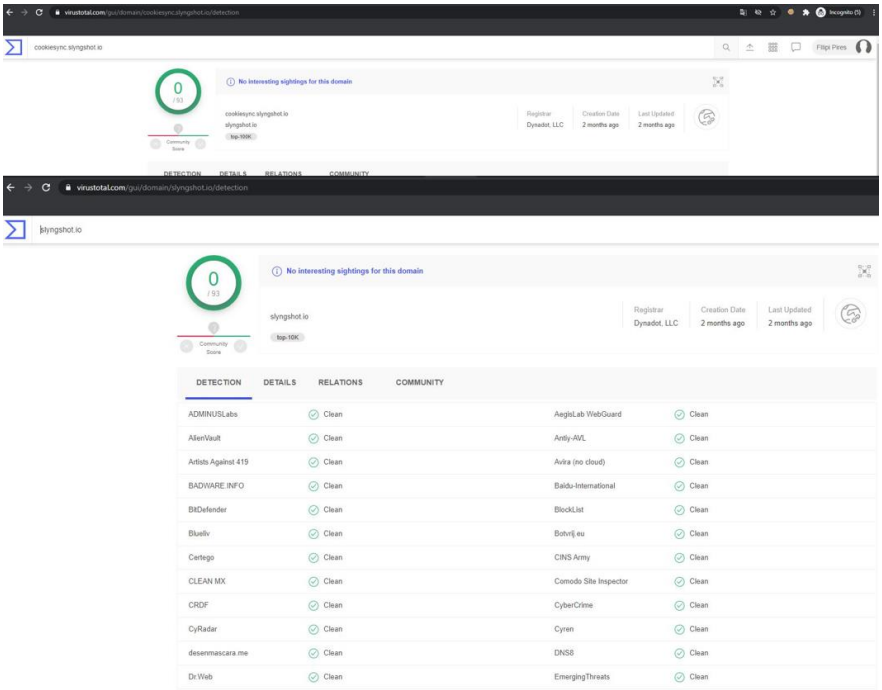


Image 1.5: Research VirusTotal Platform

We tried to access the domain in a controlled environment to see the behavior, however the

domain it is inaccessible with 404 Not Found error, could be caused by many possibilities, like as: *incorrect url, incompatible extension, disable page or unstable server*.

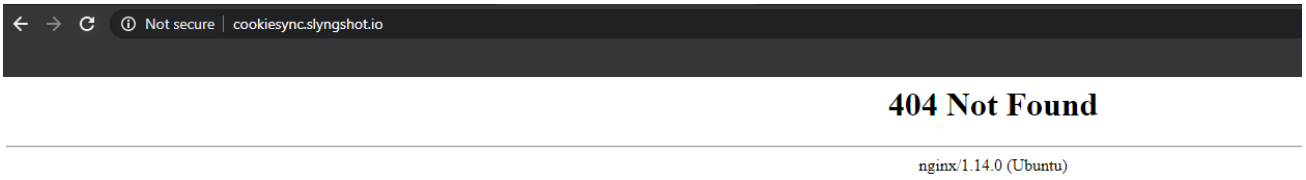


Image 1.6: Testing the domain

Other perspective is to try find any information in another kind of platforms, or others databases and to try find any reputation for this domain, I made an testing in **Hybrid Analysis** platform, that is a Sandbox in cloud to execute many tests in URLs/Files/Hashes and so on, The result of this test, brought to us that this domain **is Safe** and the behavior was the same our environment, as you can see in the *prescreen* below provide by HybridAnalysis Sandbox.

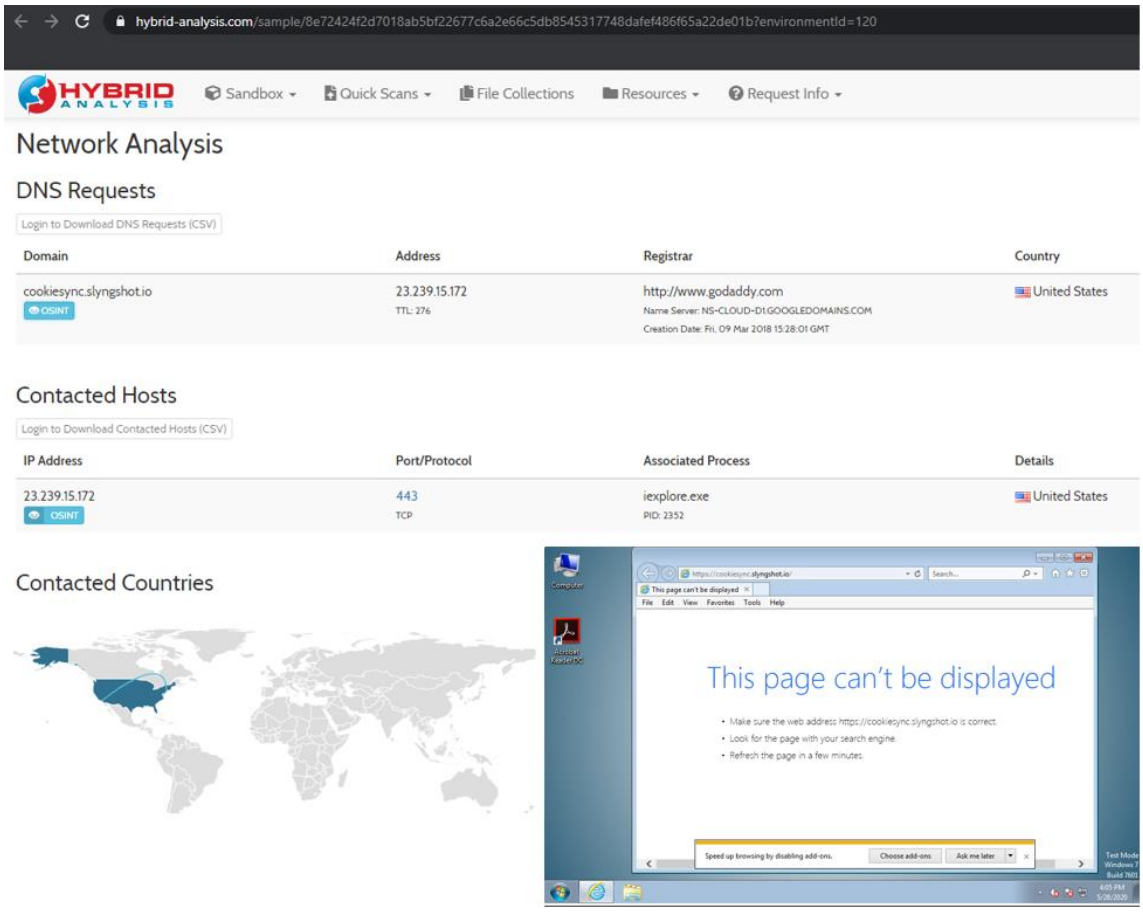


Image 1.7: Hybrid Analysis Sandbox

After this , I made other test in **APP.Any.Run** platform, that is a Sandbox in cloud to execute many tests in URLs/Files/Hashes and so on, The result of this test, brought to us the same result **Safe Domain** and the behavior was the same our environment, as you can see in the *prescreen* below provide by app.any.run Sandbox.

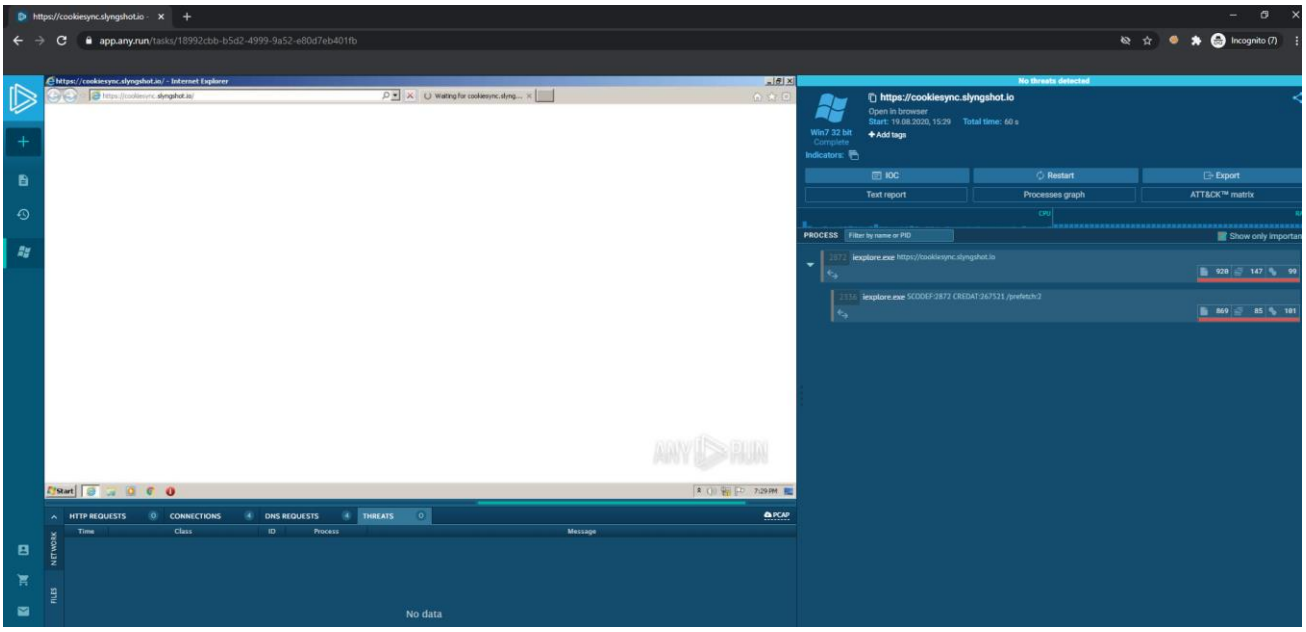


Image 1.8: App.any.Run Sandbox

After that we performed this analyzes based in all evidences, is clear that this domain is safe, another important point is that Cybereason documentation, explain that:

"*VirusTotal domain classification is also factored into certain threat calculations, but core decision-making is based on the techniques described above..*"

(https://nest.cybereason.com/knowledgebase/14192).

However in this incident, the "engine or mayba API" from VirusTotal was used.

2 Impact

At the end of this test, it was possible to verify that this domain or this alerts is totally safe, and this can be many unnecessary alerts as you can see below:

- Many alerts with false positive in internal SOC (Customer Environment);
- Many customers could be impacted with the false positive, because they're using the Global Threat Intelligence database by Cybereason;
- Many alerts with false positive in Cybereason SOC, because they respond for all Malops case in customer environment;

3 Recommendation Actions

As we mentioned before, to conduct an investigation on a ***Malops (Malware Operations)*** that were recurring in our environment. At the end of this test, the following actions were taken to improve the assets of the protection environment:

- You can use some tips below used in Threat Hunting Investigation to evaluate the **IOA (Indicator of Attack)** analysis
    - Internal hosts with bad destinations/suspicious
    - Many internals hosts accessing the same domain/IP/URL
    - Recurrence of the same malware on different machines.
    - Internal hosts with non-standard ports
    - Public Servers/DMZ to Internal hosts
    - Network scans by internal hosts
    - Multiple alarm events from a single host
    - The system is reinfected with malware
    - Multiple Login from different regions
    - Internal hosts use much SMTP
    - Internal hosts many queries to External/Internal DNS
- Open support case with the manufacture the try solve this false positive.

4 Answers from Cybereason Company

As we mentioned before, to conduct an investigation on a **Malops** that were recurring in our environment. The existence of the same domain was observed, being accessed by many machines from different teams, on different days, at different times, after our analyses following actions will be taken to improve the protection environment of our assets:

- **This investigation was sent to Cybereason support by Support case number: #00** [redacted]

  Our idea is this issue was to understand how works the **engine of detection**, how Global Threat Intelligence by Cybereason classify this information and the correlations.

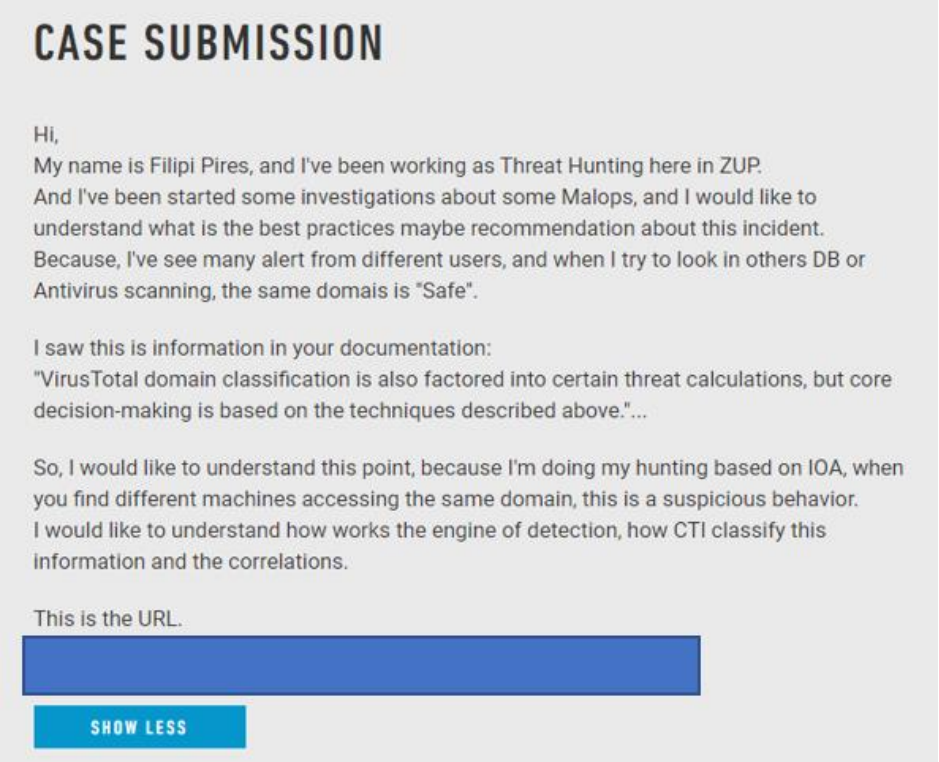


Image 1.9: Support Case

We just receive a generic information by support:

"*To establish some grounds: We use both EDR and NGAV. I know your environment is using our latest version too so that includes a lot of different detection features*".

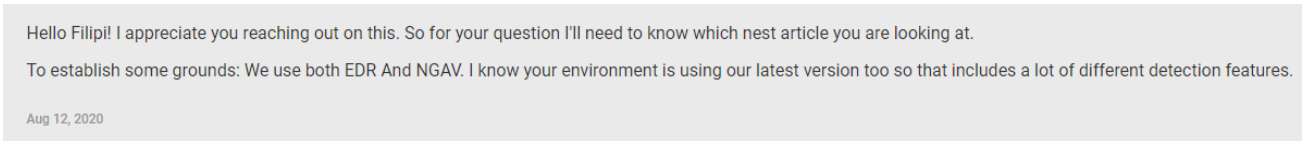


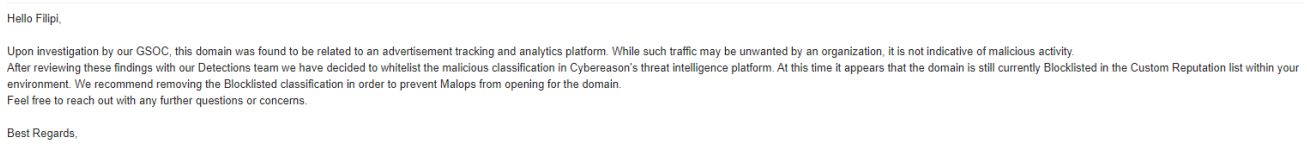
Image 1.10: Answer by Support

After that our Customer Success sent me an email, requesting me that I should send an email to de AMS Team, after sending the email to the AMS team, we received the good answer.

"*Hello Filipi,*

Upon investigation by ***our GSOC****, this domain was found to be related to an advertisement tracking and analytics platform. While such traffic may be unwanted by an organization,* ***it is not indicative of malicious activity****.*

After reviewing these findings with ***our Detections team,*** *we have* ***decided to whitelist the malicious classification in Cybereason's threat intelligence platform***"


Hello Filipi,

Upon investigation by our GSOC, this domain was found to be related to an advertisement tracking and analytics platform. While such traffic may be unwanted by an organization, it is not indicative of malicious activity.
After reviewing these findings with our Detections team we have decided to whitelist the malicious classification in Cybereason's threat intelligence platform. At this time it appears that the domain is still currently Blocklisted in the Custom Reputation list within your environment. We recommend removing the Blocklisted classification in order to prevent Malops from opening for the domain.
Feel free to reach out with any further questions or concerns.

Best Regards,

Image 1.11: Answer by Support