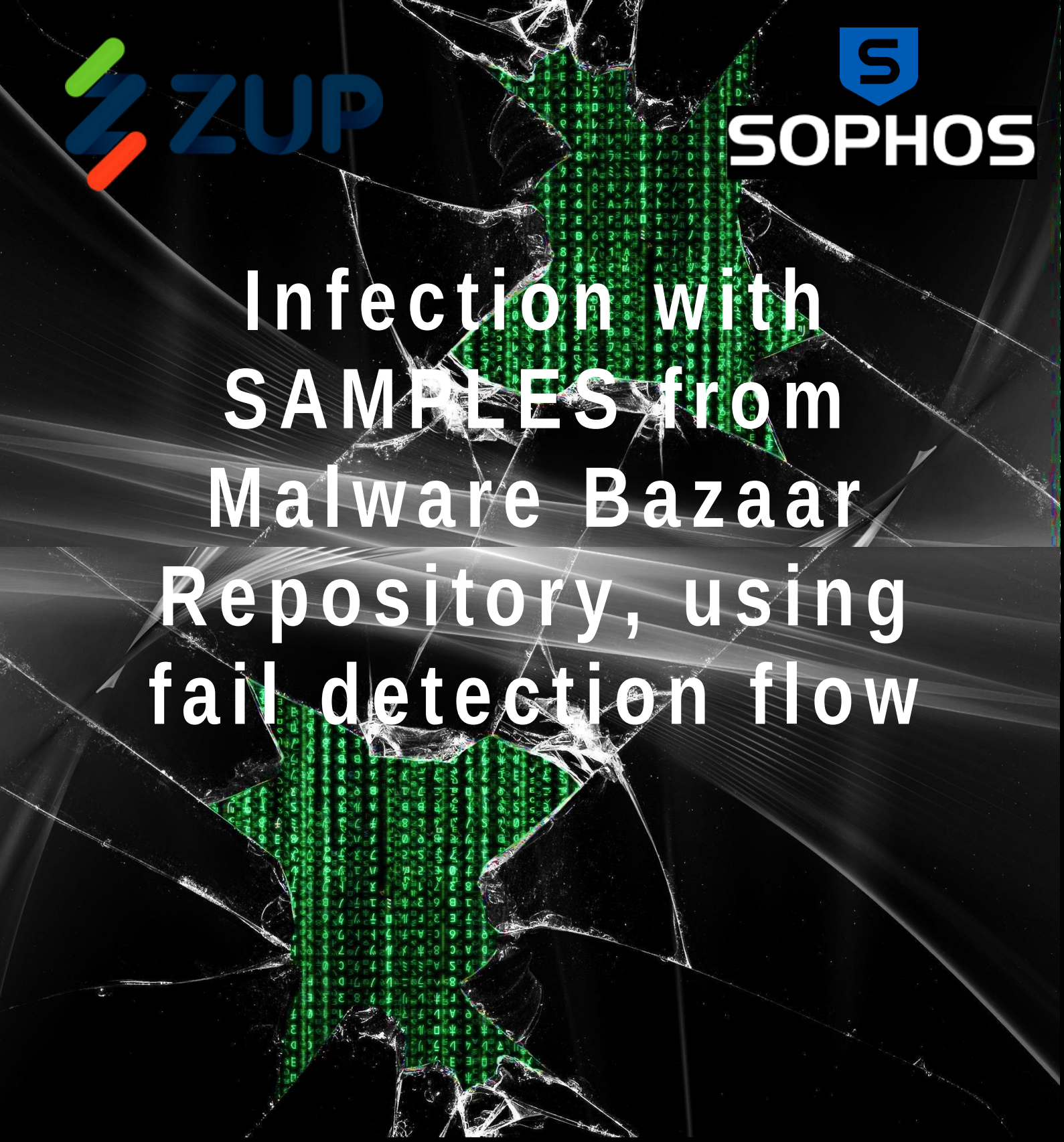


Infection with SAMPLES from Malware Bazaar Repository, using fail detection flow

ZUP Security Labs at Zup Innovation

Researcher and CyberSecurity Manager (s): Filipi Pires

1 Introduction

The purpose of this document, it was to execute several efficiency and detection tests in our endpoint solution, provided by Sophos, this document brings the result of the defensive security analysis with an offensive mindset performing a download manually and executing of daily batches of malware sample created by **MalwareBazaar** in our environment.

Regarding the test performed, the first objective it was to simulate targeted attacks using known malware to obtain a panoramic view of the resilience presented by the solution, with regard to the efficiency in its detection by signatures, NGAV and Machine Learning, downloading these artifacts directly on the victim's machine in manually way from daily batches provide by MalwareBazaar. The second objective consisted of analyzing the detection of those same malwares (or those not detected yet) when they were changed directories, the idea here is to work with manipulation of samples (without execution).

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 efficiency and detection analysis had as target the Cybereason Endpoint Protection application (`https://cloud.sophos.com`) in **Version:**

- **Agent Version = 10.8.9 VE3.79.0**
- **Core Agent – 2.10.7 BETA**
- **Endpoint Advanced 10.8.9.1 BETA**
- **Sophos Intercept X 2.0.17 BETA**
- **Device Encryption 2.0.82**

Installed in the windows machine `Windows 10 Pro`;
Hostname - `Threat-Hunting-Win10-POC`, as you can see in the picture below:

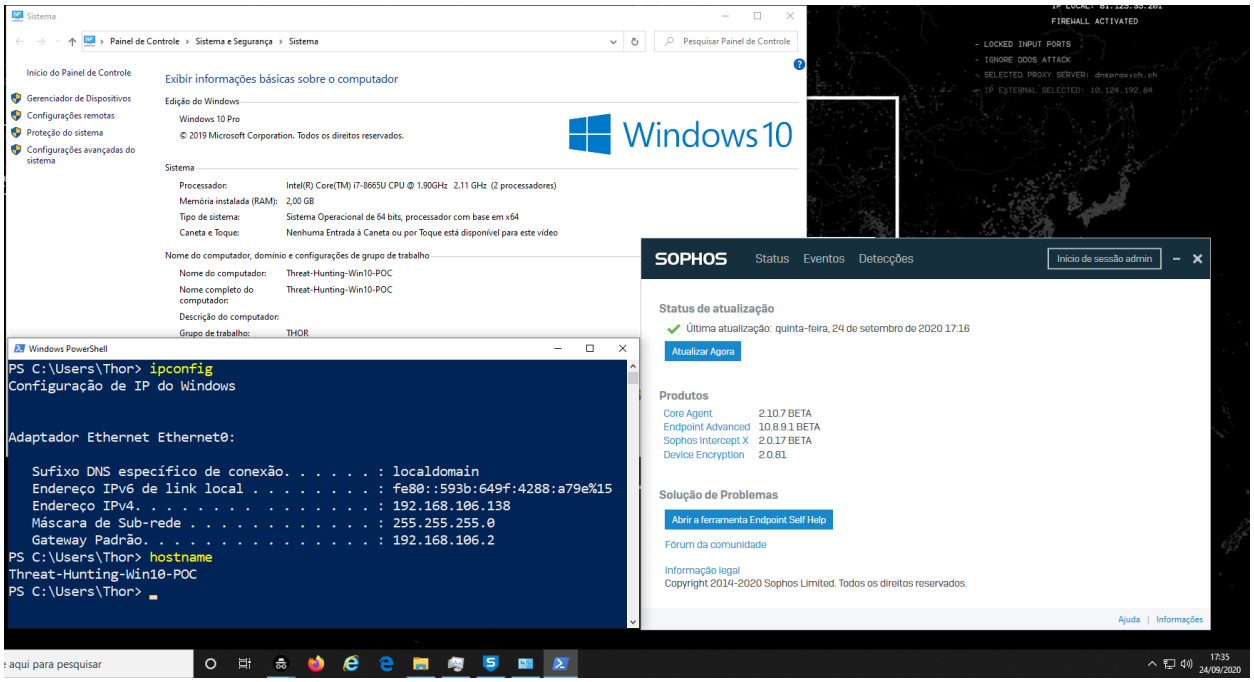


Image 1.1: Windows 10 Pro 2019 Virtual Machine

2.0.2 Project Summary

The execution of the security analysis tests of the Threat Hunting team it was carried out through the execution of daily batches of malware sample created by **MalwareBazaar** with more than **1150 Malwares** in a virtualized environment in a controlled way, simulating a real environment, together with their respective best practices of the security policies applied, the test occurred during **2 day**, without count the weekend, along with the making of this document. The intrusion test started on the **24th of September** of the year 2020 and it was completed on the **28th of September** of the same year.

2 Running the Tests

3.1 Description

A virtual machine with Windows 10 operating system it was deployed to perform the appropriate tests, as well as the creation of a security policy on the management platform (`Threat-Hunting-Win10-POC`) e and applied to due device.

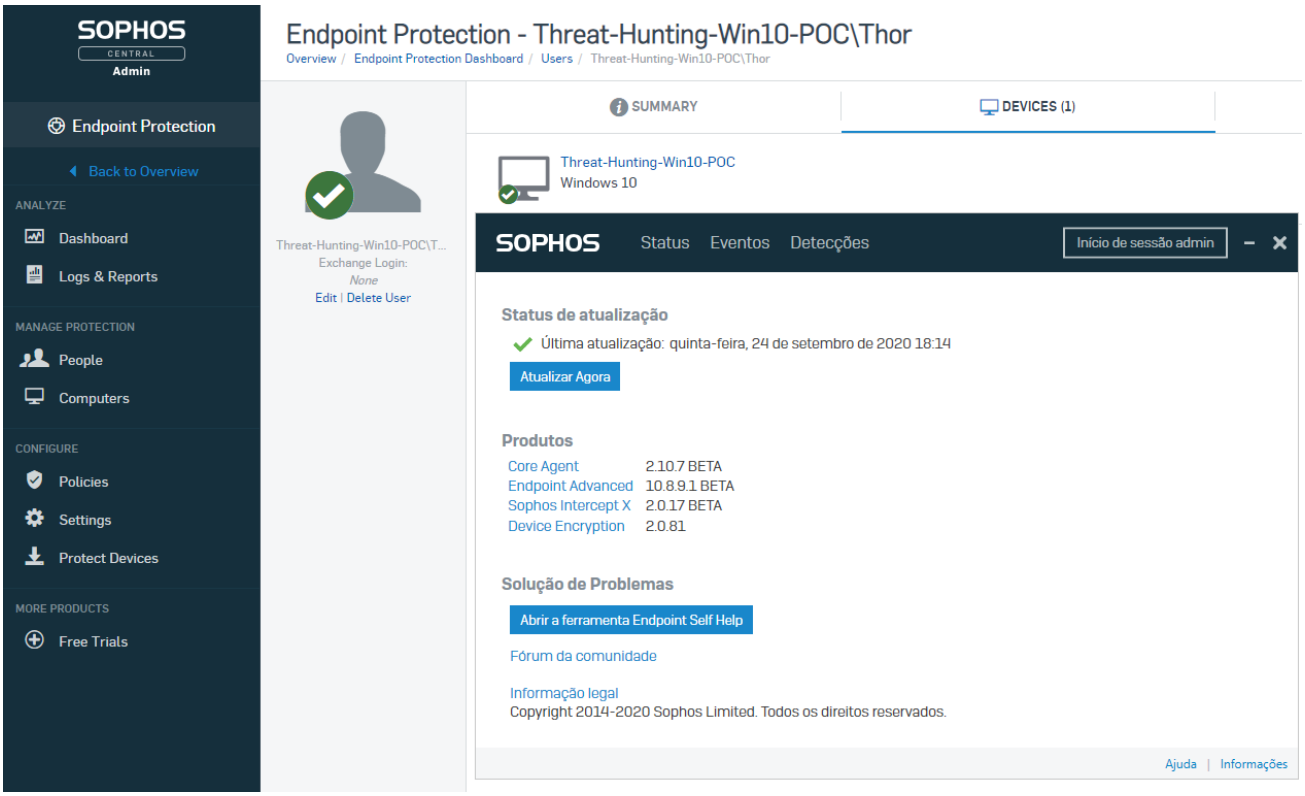


Image 1.2: Virtual Machine with Policy applied

The policy created was named **`Threat-Hunting-Win10-POC`**, following the best practices recommended by the manufacturer, and, for testing purposes, all due actions were based on an aggressive detection method.

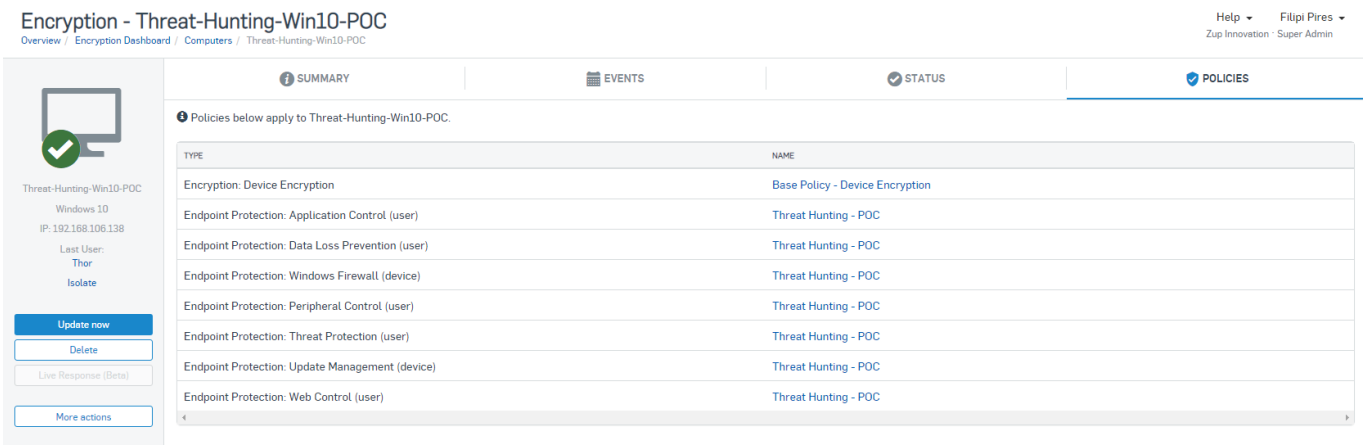


Image 1.3: Policy created by Sophos Central

3.2 First Test

The first stage of the tests was through the download more than **1150 Malwares** in a virtualized environment, that it was uploaded from public repository known and maintained by the security community called **MalwareBazzar** (https://bazaar.abuse.ch/);

> *MalwareBazaar is a project from abuse.ch with the goal of sharing malware samples with the infosec community, AV vendors and threat intelligence providers.*

MalwareBazaar creates daily batches of malware sample). The daily batches are created once a day at midnight (00:00 UTC). Please consider that it takes a few minutes to create the batch. So, I kindly ask you to not fetch the daily batch before 00:15 UTC.

The day choose for this test it was 2020-09-15

(https://mb-api.abuse.ch/downloads/2020-09-15.zip);

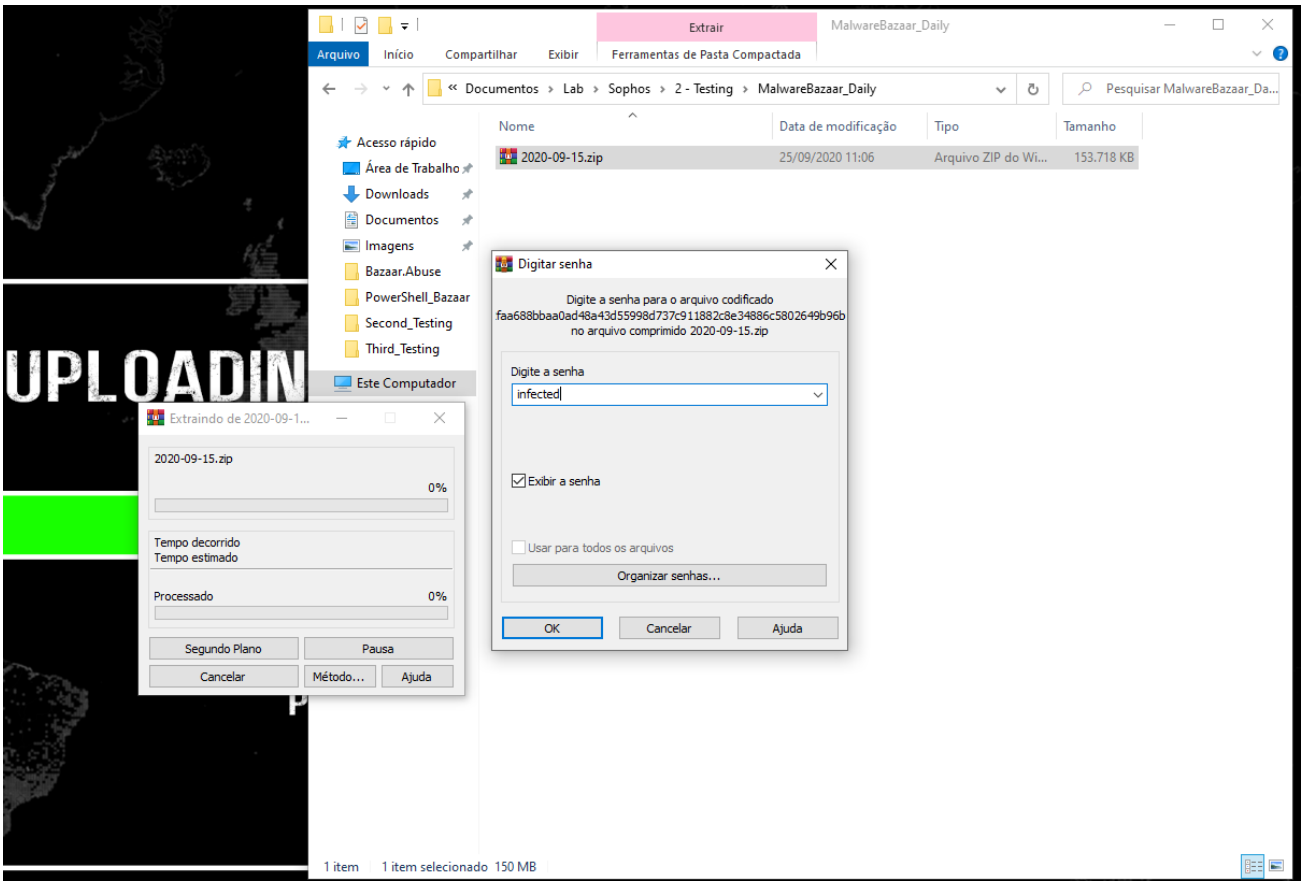


Image 1.4: Download more than 1150 Malwares inside this Folders

The purpose of this test, it was to simulate the same process as a user receiving a zipped file (`.zip`) and performing the extraction of these artifacts in their own environment.

During this test, one thing called my attention:

- **First Detection** happened on **September 24, 2020 at 11:14 AM GMT-3**
- **Last Detection** happened on **September 28, 2020 at 12:11 AM GMT-3**

That is, we have a time gap with more than **4 days** between the first and the last detection, that was the time it took for malwares to be detected

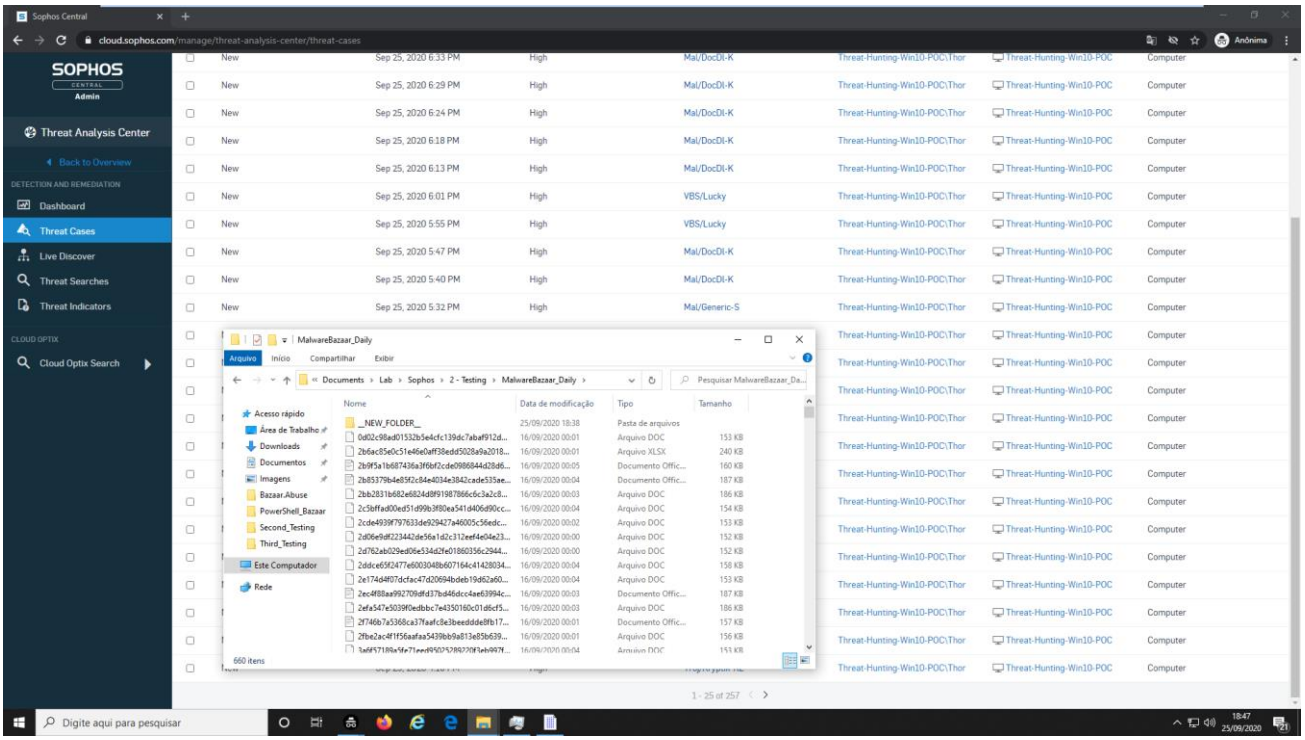


Image 1.5: Extraction of the files from daily batches

After performing the action of extracting the files, it was possible to verify that Sophos Security Endpoint starts the block process, following the best practices a function named **Outbreak Detected is called,** this feature enables when any device has experienced 100 detections in a minus 24-hour period. This is to avoid flooding an admin with similar or repeated detection events during a malware outbreak.

During an outbreak the priority should be dealing with the detections on the device, so you may want to take this machine off your network while it is being investigated.

The important point here is:

We had more than **1150 malware**, and after outbreak detection to be started, we can see just 100 malwares blocked, even though our virtual machine had more than 1000 we can see that the behavior detection process happens this way, first Sophos endpoint detect after that clean, but for us, this process it was very slowly.

If you are a Sophos Intercept X customer and would like more information on what led up to the detection, use the Threat Cases feature in the Sophos Central Admin console to see what was happening on the computer at the time. (Information provide by Sophos Support)

Source: https://support.sophos.com/support/s/article/KB-000037174?language=en_US

If you are unsure how to deal with the outbreak please contact Sophos Support

If you believe the detections that led to the malware outbreak event being reported are incorrect (false positive) please see article: How to investigate and resolve a potential False Positive / Incorrect Detection

Once you have resolved the cause of the outbreak and the threat (or PUA) has been removed, **you need to mark the Outbreak event as resolved in the Sophos Central Console**.

So, after to mark the machine as solved, we following wait for the detection process, and for our surprise, just **232 malwares** blocked as you can see below

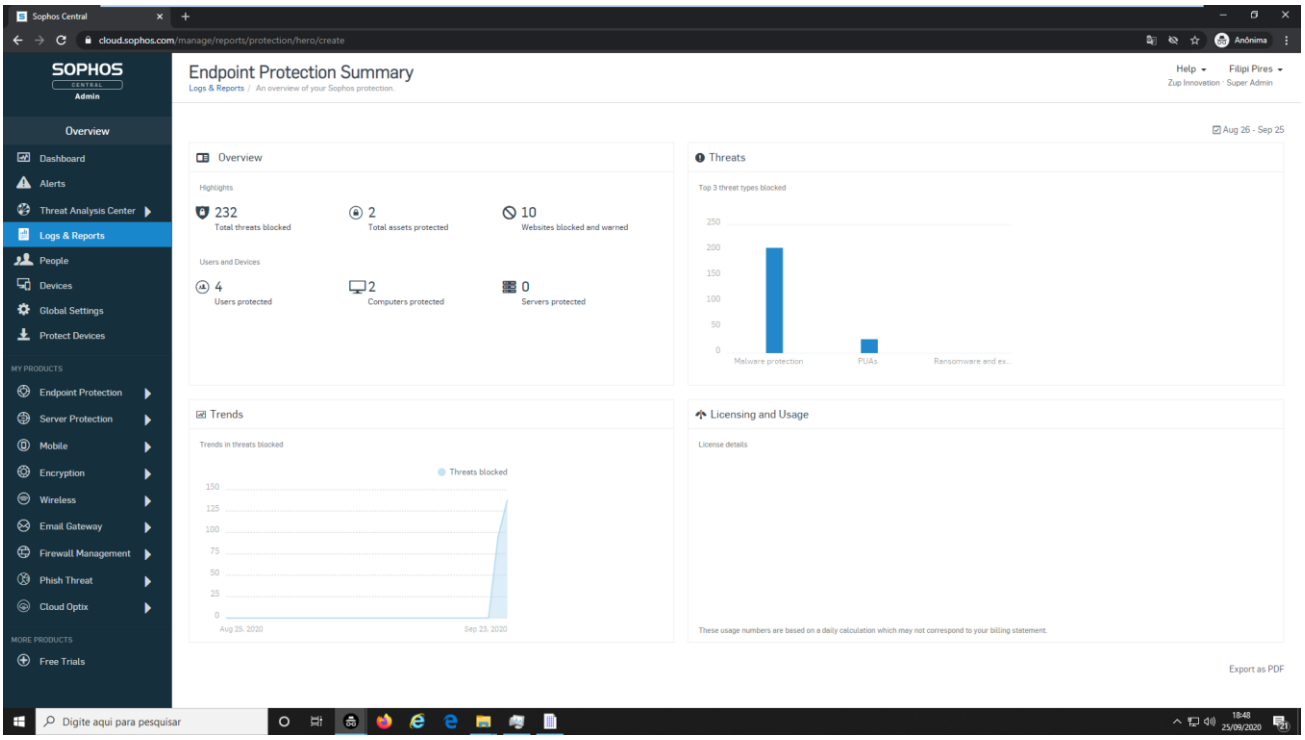


Image 1.6: Malwares Detection first stage by Sophos

3.3 Second Test

The second stage of the tests was through the transfer of folders to another directory within the same machine, the purpose of this test was to simulate a transfer of files within the same environment.

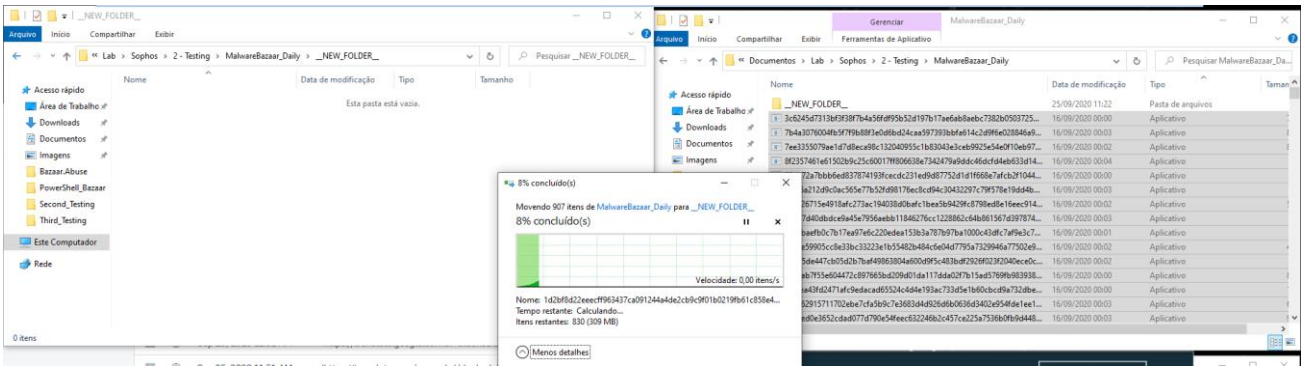


Image 1.7: __NEW_FOLDER__(Sophos) – Coping another folder.

When a new file is generated on the disk, soon we should have a new entry in a block of that disk and in theory the antivirus should take some action (considering that it has the real time enabled), we could define it as a file manipulation (still not running) where the endpoint protection is already necessary, considering that a new directory was created, soon we would have a new repository with several hashes inside to be examined.

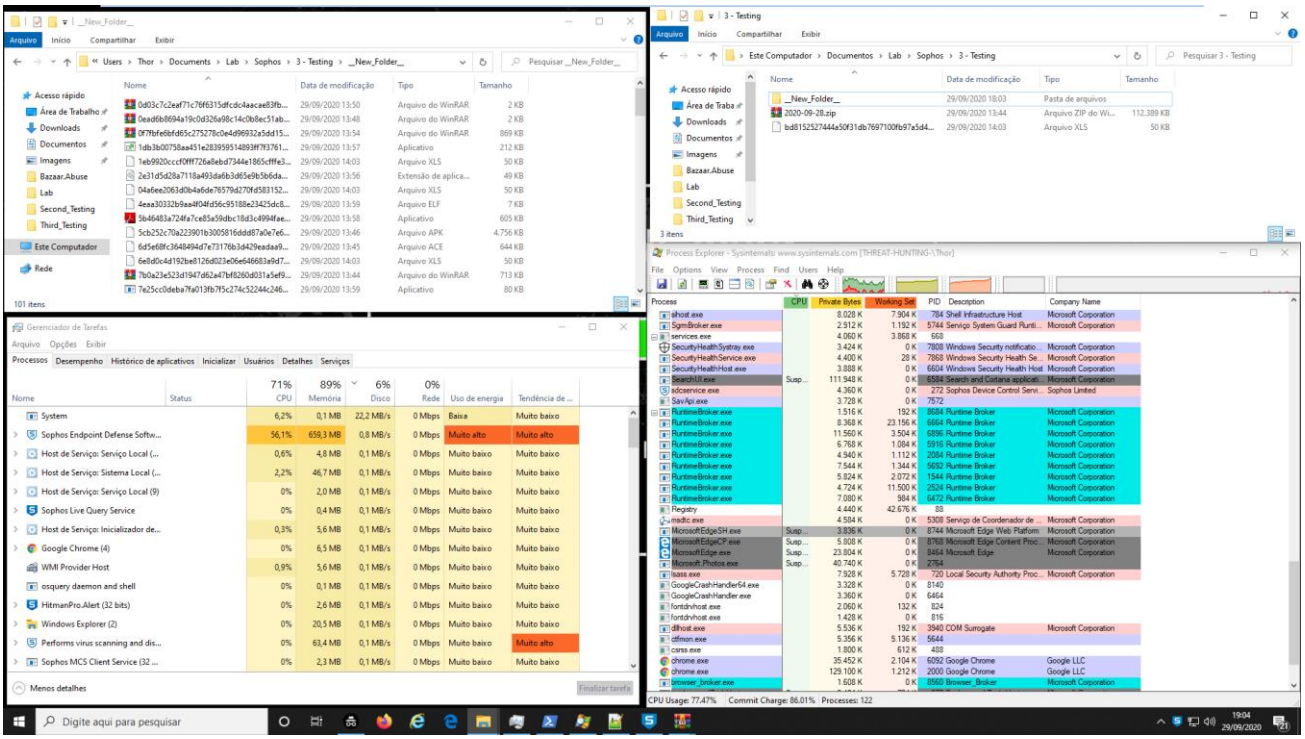


Image 1.8: __NEW_FOLDER__(Sophos) – Malware manipulation

During this stage a very strange situation caught our attention, only 86 malwares were moved to new folder, many information's about **Detection process** and/or **Detection flow** aren't clear how works, after that we saw many alerts about possible blocks and detections, but we didn't get to find any information clear about blocks.

The victim machine stayed with many alerts during this test, and CPU and Memory had a very high consumption in the machine, during this test, for our perspective looks like the detection engines got lost in all detection process, after that we need to execute the reboot of this machine, to try understand with the alerts will be finished or may some malwares will be detected.

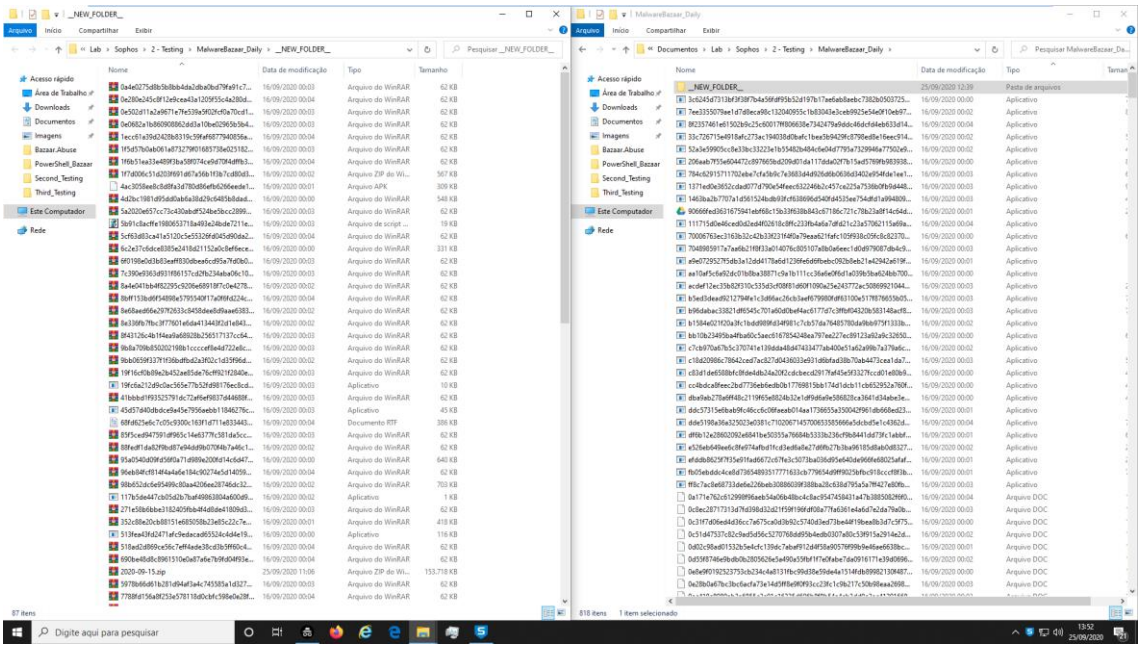


Image 1.9: _NEW_FOLDER_ – After Reboot.

Our expectation it was that there would be many detections, but after almost one hour there was no new detection by Sophos Endpoint Protection, so, remained 787 malwares from the first folder not detected and 86 malwares from the second folder not detected as well.

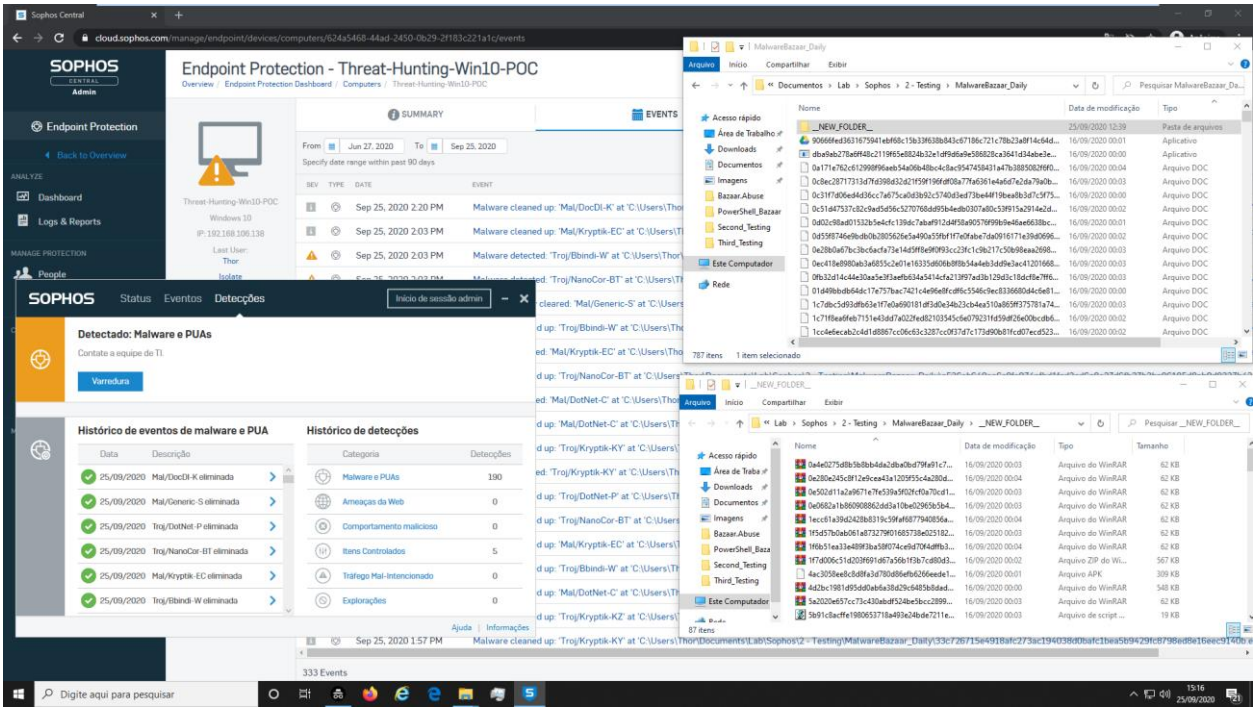


Image 1.8: Second Test finished

3.4 Third Test

The third stage of the tests was through the use of the *ScanNow* action by Cloud Sophos, to perform a complete scan on the machine, manually, in this way, all malware should be eliminated, as they are already known malware as mentioned earlier.

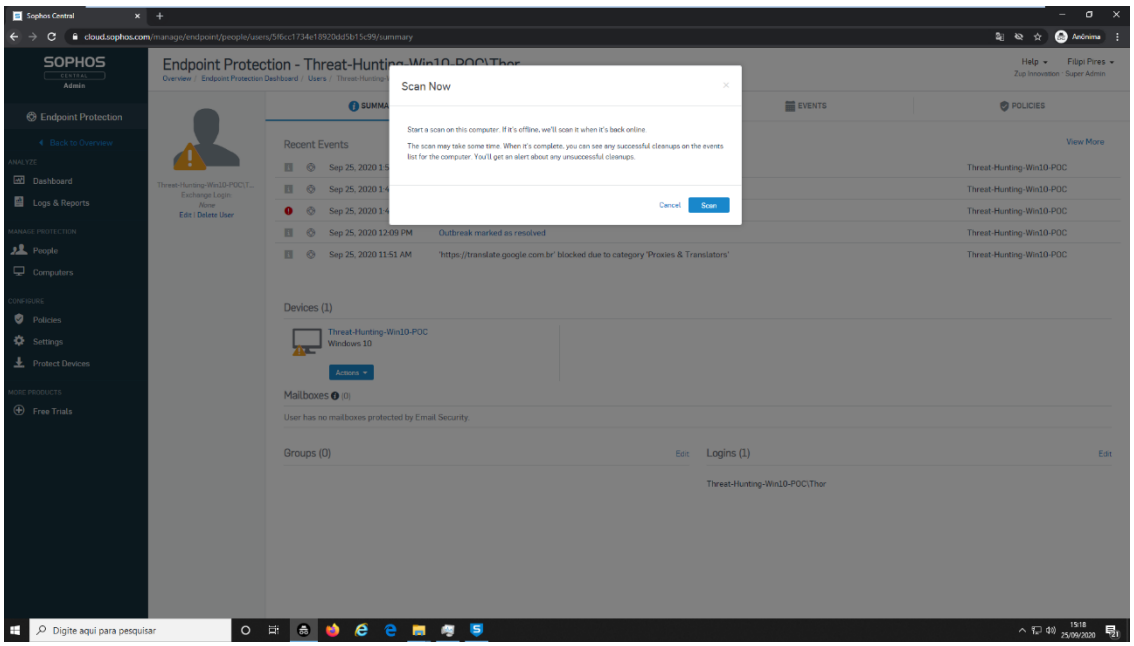


Image 1.9: *ScanNow By Sophos Central*

After performing this third test and the execution of the *ScanNow* feature, we saw the same behavior in our environment, the Windows 10 machine stayed with many alerts during this test, and CPU and Memory had a very high consumption in the machine, during this test, for our perspective looks like the detection engines got lost in all detection process, after that we need to execute the reboot of this.

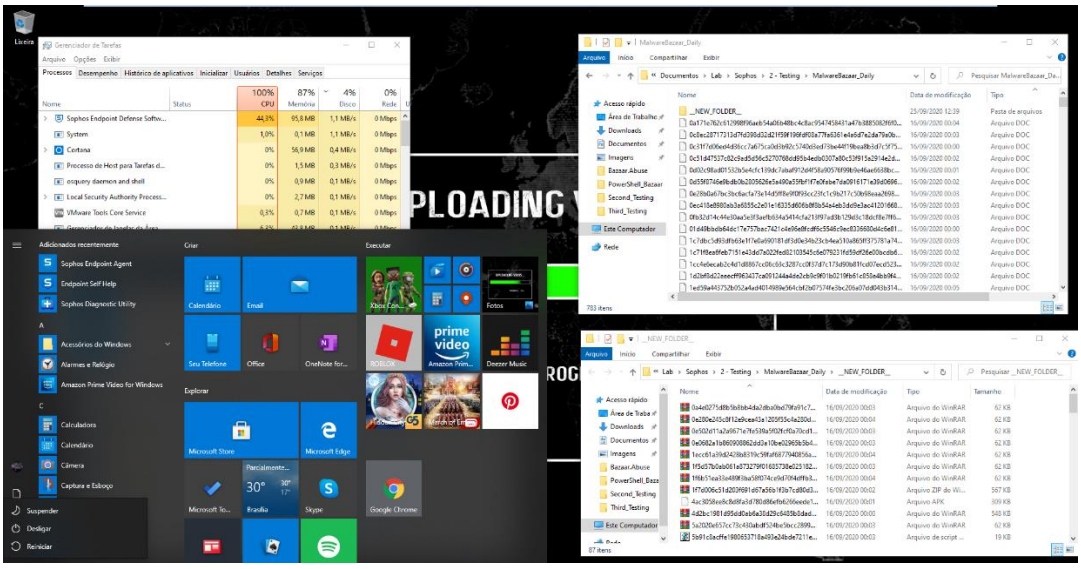


Image 1.10: Malwares – Not Detected after *ScanNow*

We tried to execute another test not pretending in the begin, as we have many malwares not detected by Sophos Endpoint Security, we ran a Scan provide by Agent installed in Windows

10 Machine.

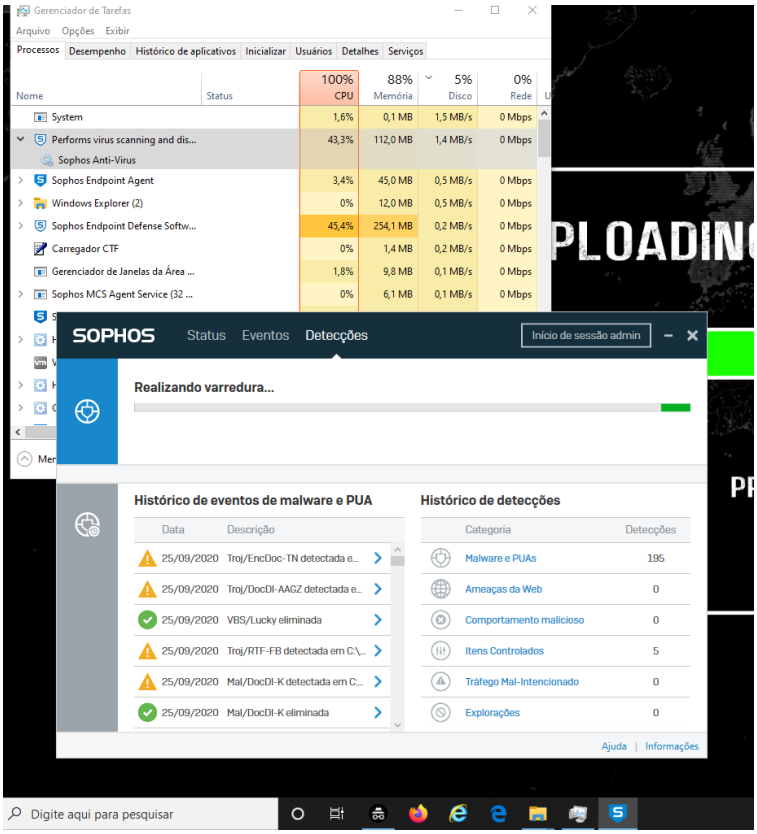


Image 1.11: Malwares –*ScanNow* provide by Agent

However, in the end of this test, unfortunately it was not clear something about the product, like a detection time, flow of detection engines, machine performance and mainly inefficient of detection, when we open the **Sophos Central today (28/09/2020)** in the Windows 10 Machine, we found that the console was very alert with detections but that depended on an individual action by the support team, this team needs to applied **"Marked as Resolved"**

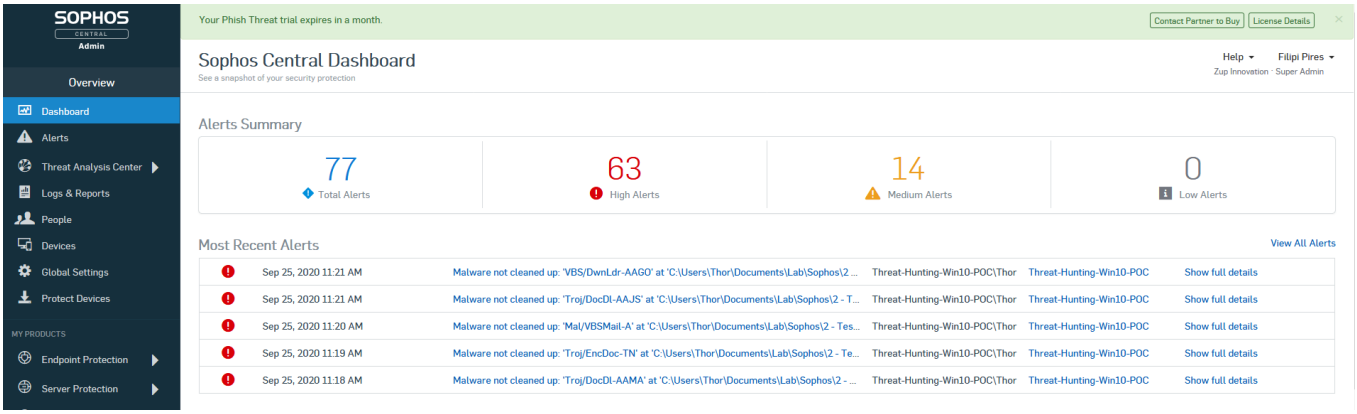


Image 1.12: Sophos Central –*Many Alerts*

Before the perform the task (Mark as Resolved), we access the Windows 10 Machine again and we see another time many alert pop-ups in the user machine as you can see below.

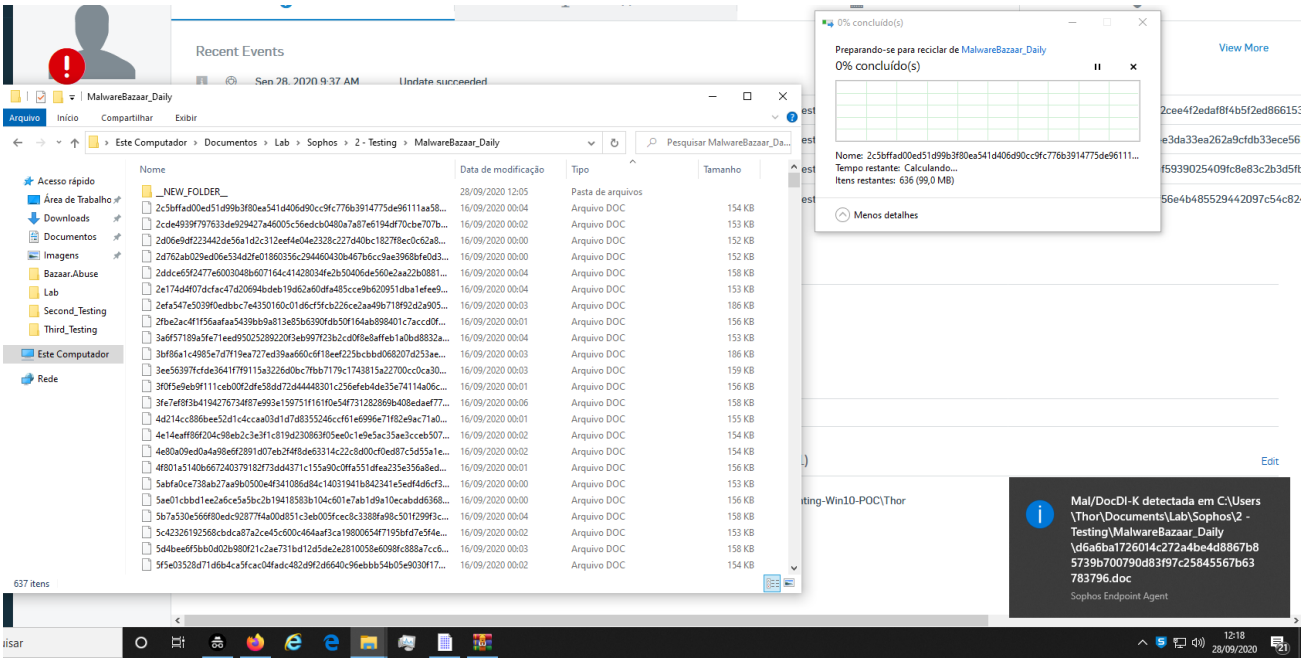


Image 1.13: Sophos Central –*Many Alerts*

So, to finalize this test **we deleted all files manually**, because the Sophos Endpoint Security didn't detect more than 600 malwares, and we performed the task of the **MARK AS RESOLVED**.

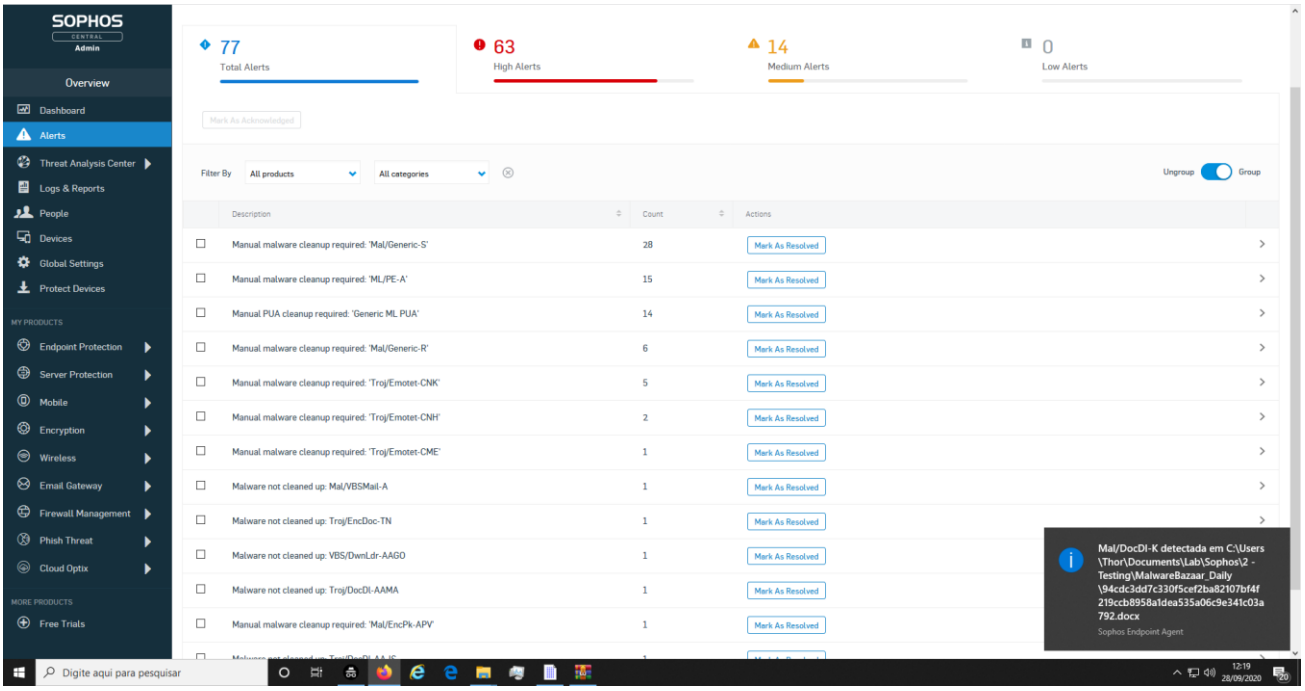


Image 1.14: Sophos Central – *Marked as Resolved*

3 Impact and Risk

At the end of this test, it was possible to verify that this solution can bring many risks in our environment, even when it comes to a known malware, whether executed inside the any environment, may perform an infection.

- **After the first extraction, just few samples were detected;**
    - When it comes a major malware infection we can have several types of attack vectors, so it is very important we have an efficient detection.
- **Endpoint went into Outbreak Prevent mode;**
    - Very interesting feature, but the risk is, we can stop an user or machine, just because received many malware in 24 hours, it doesn't mean that is a outbreak, like a pandemic, and it's not clear, how the engines works after this break.
- **High CPU and memory consumption during the detection process;**
    - Very high load on CPU and Memory used by many processes requested by AV, which directly impacts the user experience.
- **Necessity to reboot the machines more than once, due to alerts and Outbreak Prevent mode;**
    - Due the high load on CPU and Memory, it was impossible the machine continue work well, there as necessity of the machine reboot..
- **After second test more than 80 Malwares not detected when moved to another folder;**
    - Due the high load on CPU and Memory, high alert pop-ups and maybe the outbreak prevent feature, It was not clear how the engines would work when any sample have bee writen in a new block part of the disk.
- **After the ScanNow and the end of this teste, we havbe more than 600 Malwares not Detection, that is, just 54% in success detection**
    - More than 600 Malwares inside on Windows 10 machine, note detected by Sophos Endpoint Solution, totally dangerous, if you see in the Sophos Central, you'll find almost 600 Detection logs "Events reports", that is, we had 1159 malwares, many there were not detected that whether executed could take a big infection on this machine.

4 Recommendation Actions

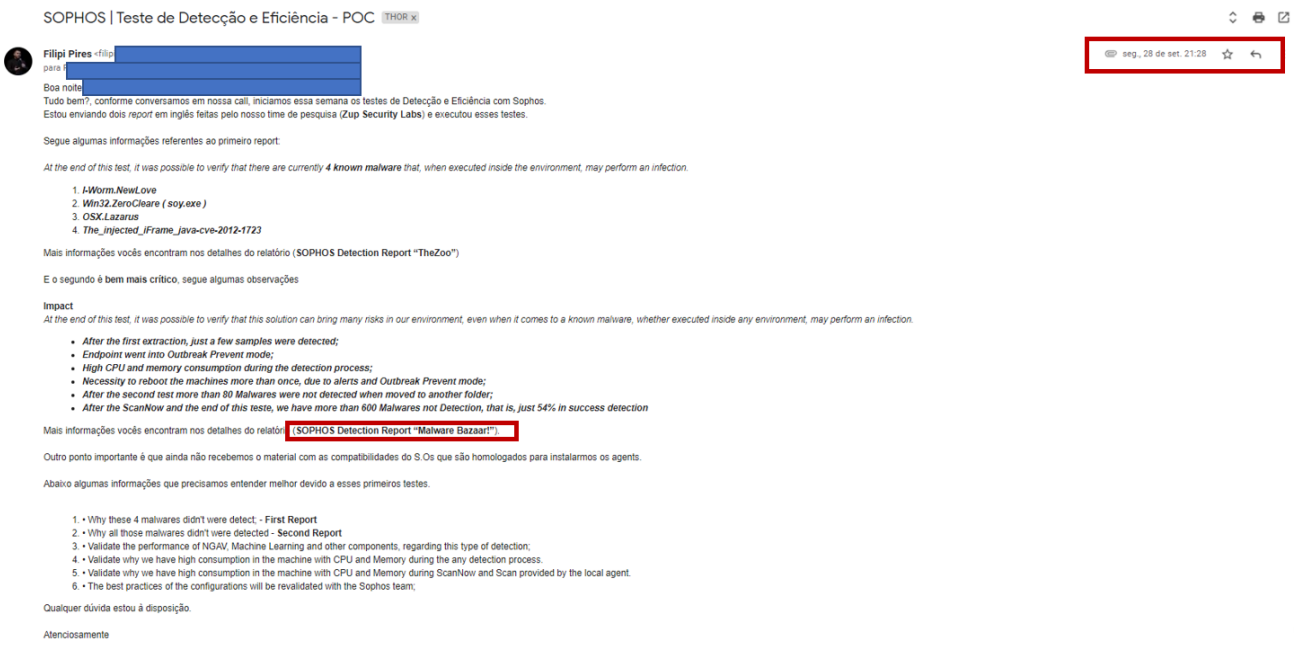
As we mentioned before, the idea it was execute test in many malwares, and this case, for this reason to be totally known the following actions will be taken to improve the protection environment of our assets:

- This report should be sent to **Sophos Security Team** to validate with them how the detection flow for known malware works, and why all those malwares didn't were detected;
- Validate the performance of NGAV, Machine Learning and other components, regarding this type of detection;
- Validate why we have high consumption in the machine with CPU and Memory during the any detection process.
- Validate why we have high consumption in the machine with CPU and Memory during *ScanNow* and Scan provide by local agent.
- The best practices of the configurations will be revalidated with the Sophos team;

5 Answers from Sophos Company

As we mentioned before, the idea it was execute test in many malwares, and this case to bring the result of the defensive security analysis with an offensive mindset a download manually and executing of daily batches of malware sample created by **MalwareBazaar** in our test environment.

We sent this email request information's with the Sophos Support team on **September 28th** as you can see below



SOPHOS | Teste de Detecção e Eficiência - POC THOR x

seg., 28 de set. 21:28

Filipi Pires <filip
para

Boa noite
Tudo bem?, conforme conversamos em nossa call, iniciamos essa semana os testes de Detecção e Eficiência com Sophos.
Estou enviando dois *report* em inglês feitas pelo nosso time de pesquisa (**Zup Security Labs**) e executou esses testes.

Segue algumas informações referentes ao primeiro report:

*At the end of this test, it was possible to verify that there are currently **4 known malware** that, when executed inside the environment, may perform an infection.*

1. ***I-Worm.NewLove***
2. ***Win32.ZeroCleare (soy.exe)***
3. ***OSX.Lazarus***
4. ***The_injected_iFrame_java-cve-2012-1723***

Mais informações vocês encontram nos detalhes do relatório (**SOPHOS Detection Report "TheZoo"**)

E o segundo é **bem mais crítico**, segue algumas observações

Impact
At the end of this test, it was possible to verify that this solution can bring many risks in our environment, even when it comes to a known malware, whether executed inside any environment, may perform an infection.

- ***After the first extraction, just a few samples were detected;***
- ***Endpoint went into Outbreak Prevent mode;***
- ***High CPU and memory consumption during the detection process;***
- ***Necessity to reboot the machines more than once, due to alerts and Outbreak Prevent mode;***
- ***After the second test more than 80 Malwares were not detected when moved to another folder;***
- ***After the ScanNow and the end of this teste, we have more than 600 Malwares not Detection, that is, just 54% in success detection***

Mais informações vocês encontram nos detalhes do relatório (**SOPHOS Detection Report "Malware Bazaar!"**).

Outro ponto importante é que ainda não recebemos o material com as compatibilidades do S.Os que são homologados para instalarmos os agents.

Abaixo algumas informações que precisamos entender melhor devido a esses primeiros testes.

1. • Why these 4 malwares didn't were detect; - **First Report**
2. • Why all those malwares didn't were detected - **Second Report**
3. • Validate the performance of NGAV, Machine Learning and other components, regarding this type of detection;
4. • Validate why we have high consumption in the machine with CPU and Memory during the any detection process.
5. • Validate why we have high consumption in the machine with CPU and Memory during ScanNow and Scan provided by the local agent.
6. • The best practices of the configurations will be revalidated with the Sophos team;

Qualquer dúvida estou à disposição.

Atenciosamente

I sent other email on **October 06th** and another email on **October 09th**, all of than with Reports showing many testes that we did in Sophos Endpoint Solution.

After almost 15 days, I received I generic answer to the Vendor as you can see below:

"*We've similar things like this before. To be honest, this is an unrealistic test. It does not represent what happens in the real world. An attacker is unlikely to drop that many new and unique pieces of malware - they would likely cause their attack to become unstable.*
When reputable security test operations conduct testing, they deliver the threats in sequence, just like what would happen in the real world.

Looking at how this report was done, i can think back to when Cylance and Deep Instinct run tests like this with malware from Virus Total, Malware Bazaar and other corpus of malicious code

Direct them to places that test anti malware tools and how they've devised the right methods when testing.

NSS Labs: https://www.nsslabs.com/reports/endpoint-security-test-methodology-v5-0/
SELabs: https://selabs.uk/wp-content/uploads/2020/04/04-predictive-malware-response-testing-methodology.pdf

The method of 'dumping a bunch of PEs onto disk' is NOT representative of the real world and doing so one should expect system resources to peak whilst the realtime protection attempts to deal with the massive influx of malicious entities. Simple facts, nothing surprising here."