Hunting the Hunters: Detection and Efficiency Testing of Endpoint Security Sensors

ZUP Security Labs at Zup Innovation

Principal Security Engineer: 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 performed in the execution of 27 folders download with **Malwares by The Zoo** repository 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, downloading these artifacts directly on the victim's machine. The second objective consisted of analyzing the detection of those same 27 folders download with Malwares (or those not detected yet) when they were changed directories, the idea here is to work with manipulation of samples (without execution), and the third focal objective it was the execution of a *ScanNow* inside victim's machines for effectiveness analysis.

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:

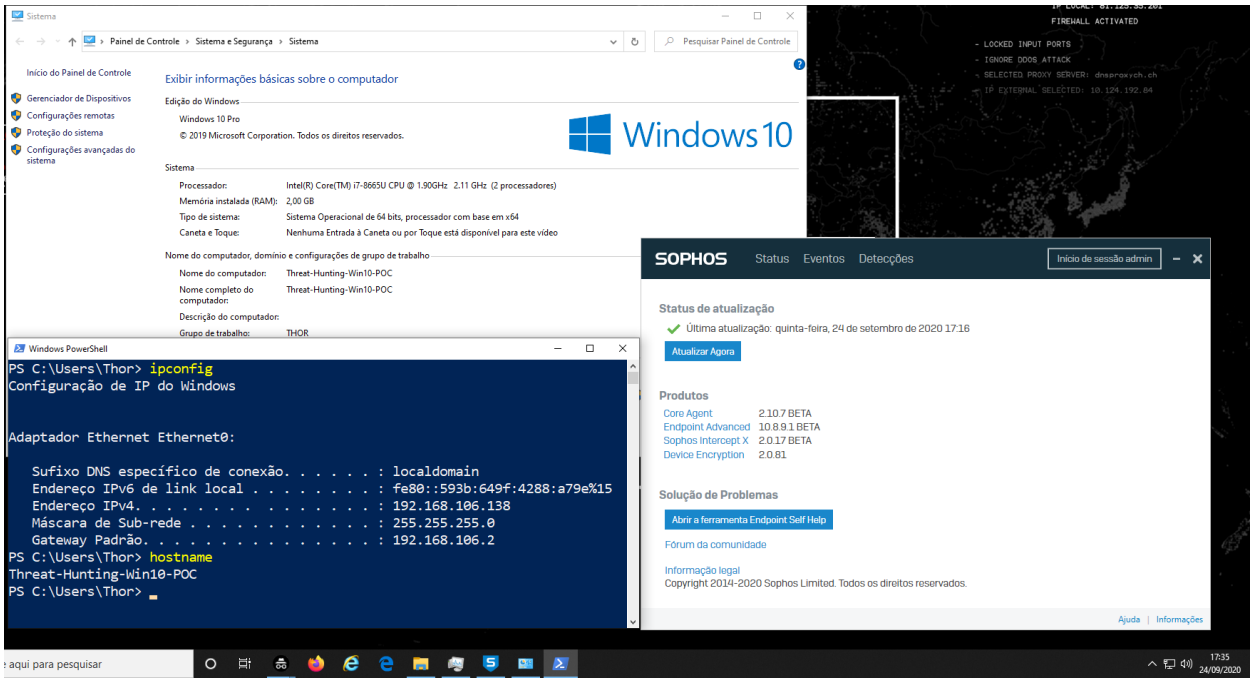


Image 1.1: Windows 10 Pro 2019 Virtual Machine

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 42 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 days**, 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.

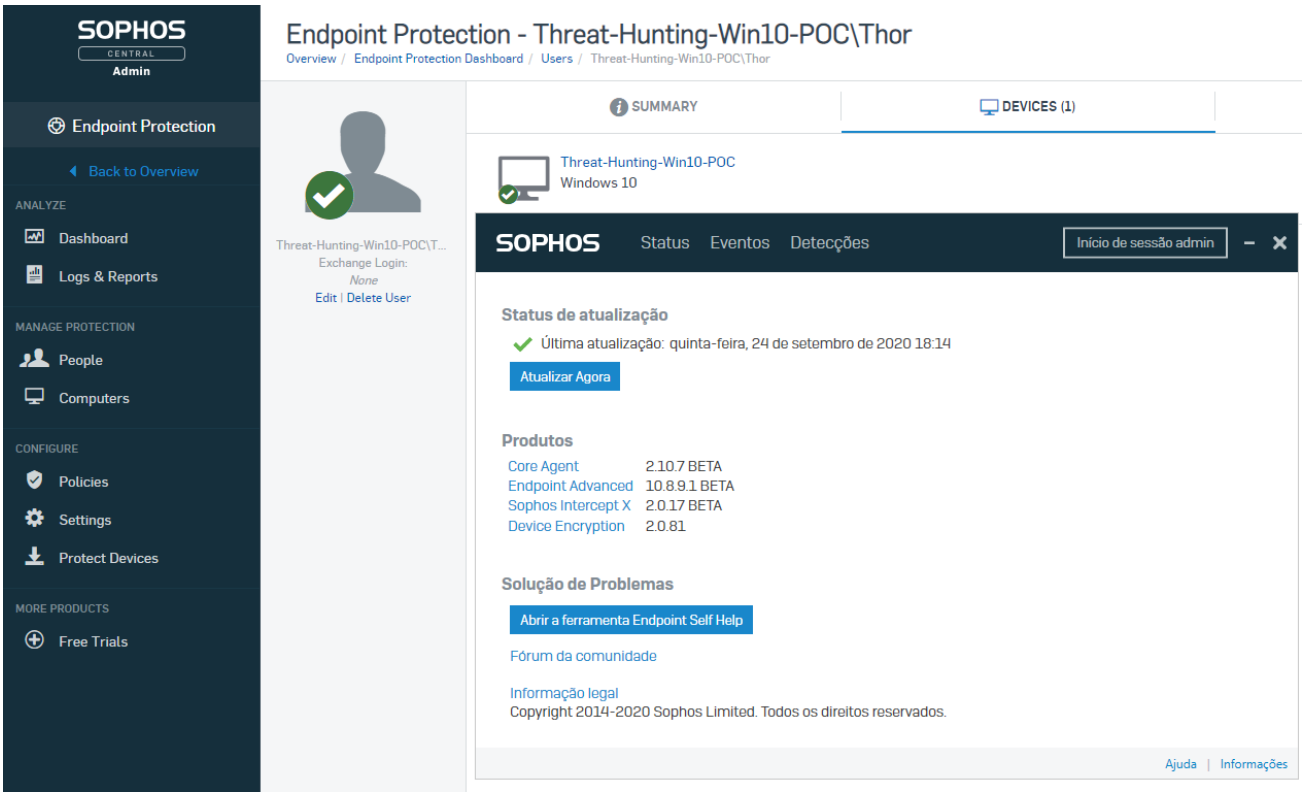


Image 1.2: Virtual Machine with Policy applied

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.

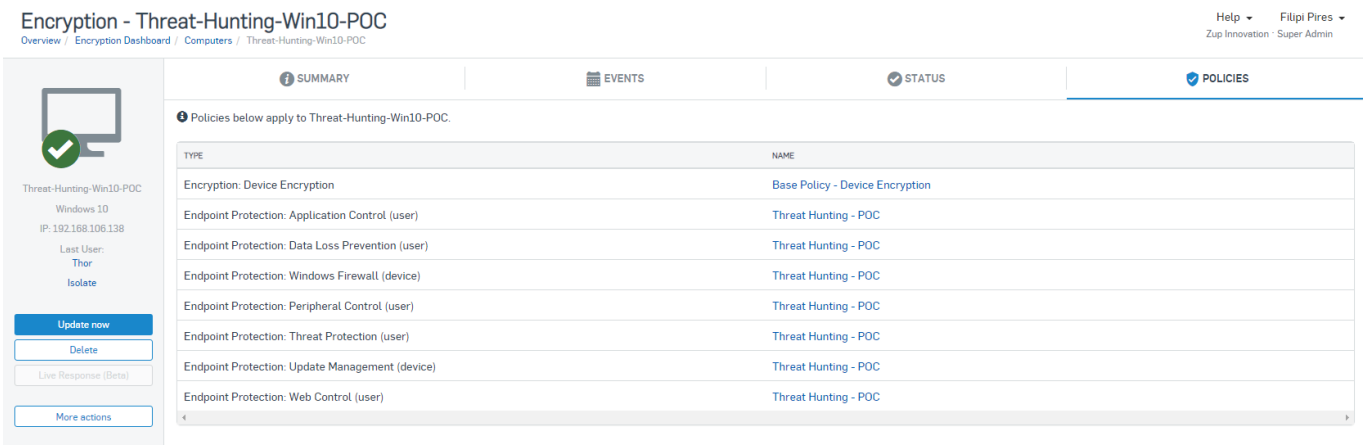


Image 1.3: Policy created by Sophos Central

3.2 First Test

The first stage of the tests was through the download of 27 folders with many different kind of malwares, all of which are already known to be older, all of them are in the public repository known and maintained by the security community called **The Zoo** (`https://github.com/ytisf/theZoo/tree/master/malwares/Binaries`);

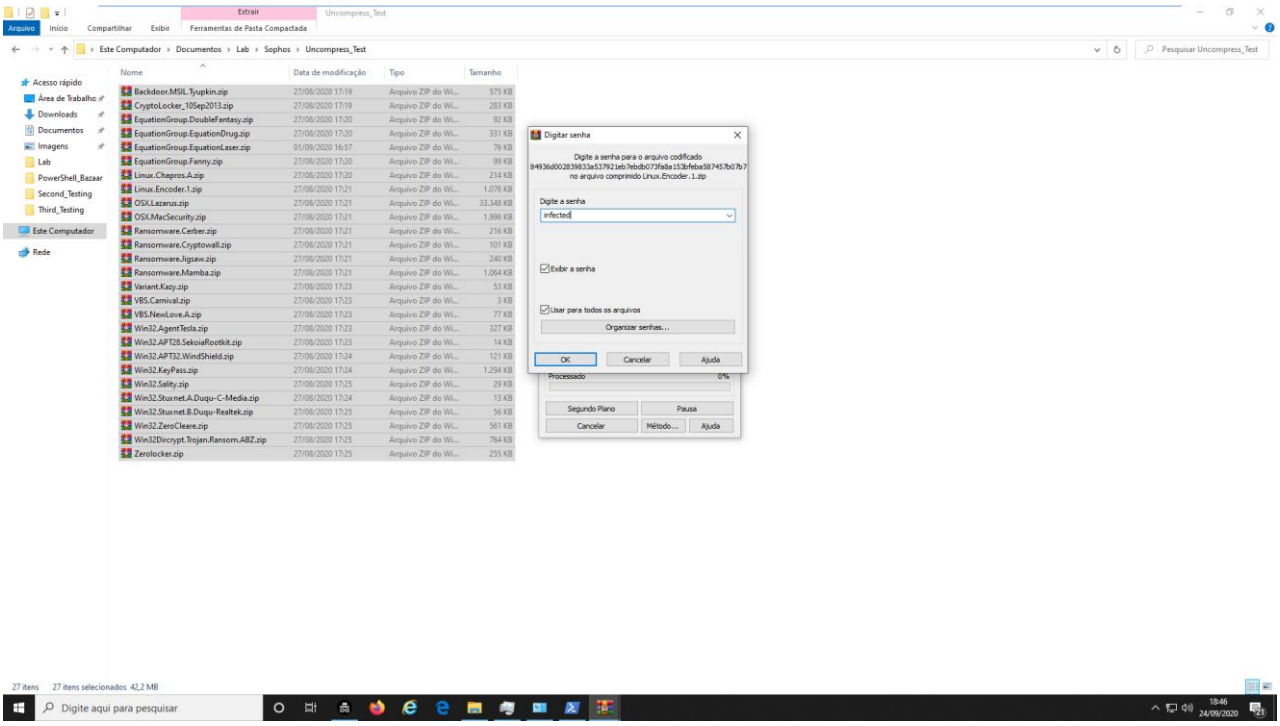


Image 1.4: Download 27 Folders with malicious files

The purpose of this test 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.

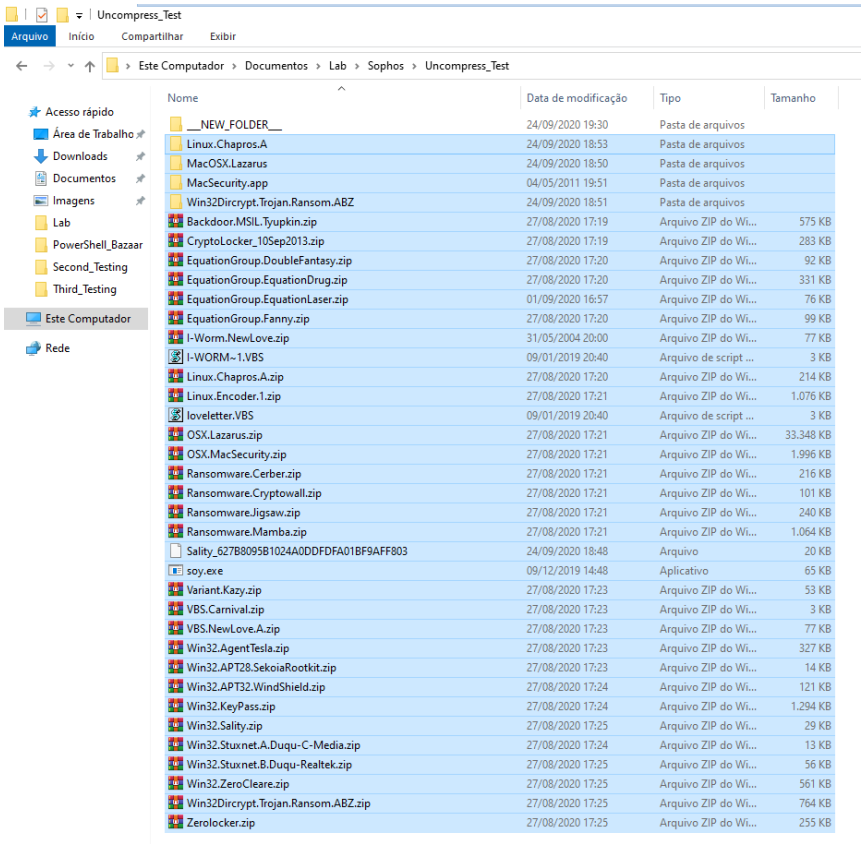


Image 1.5: Extraction of 26 Folders with malicious files

After performing the action of extracting the files, it was possible to verify that Sophos Security Endpoint there were currently **4 (four) Malwares** that, when executed inside the environment, could perform an infection.

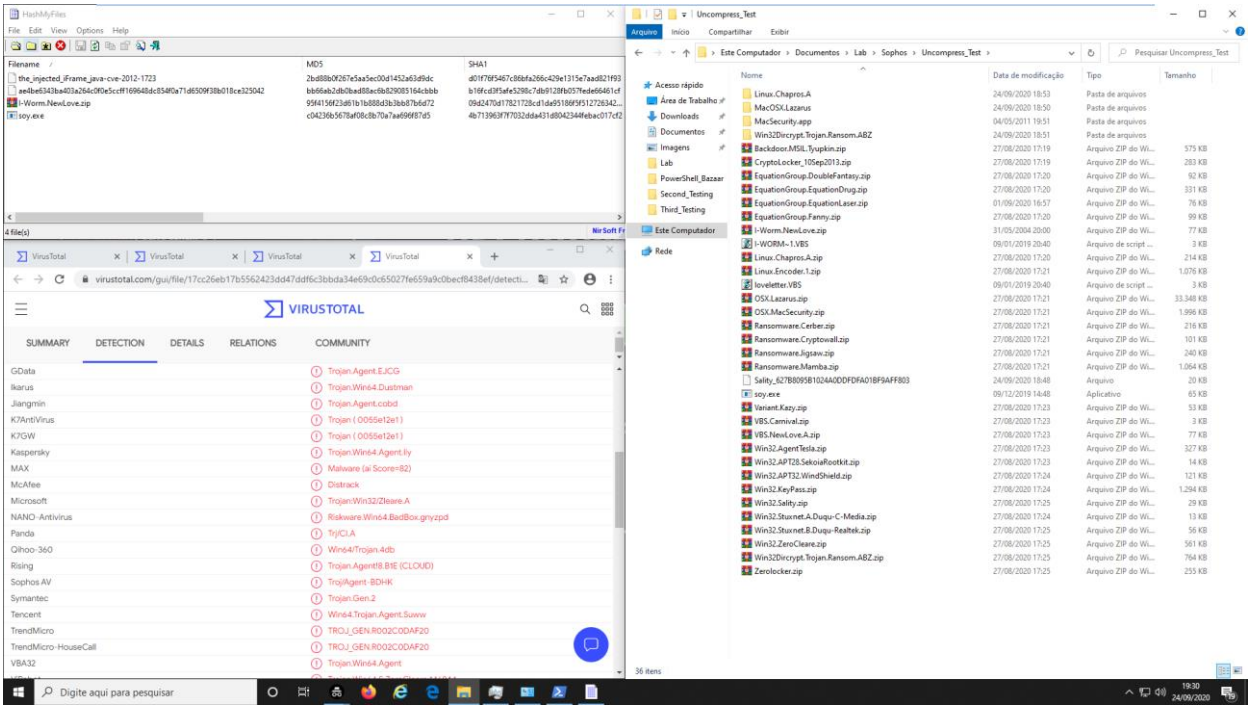


Image 1.6: Malwares Not Detection by Sophos

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.

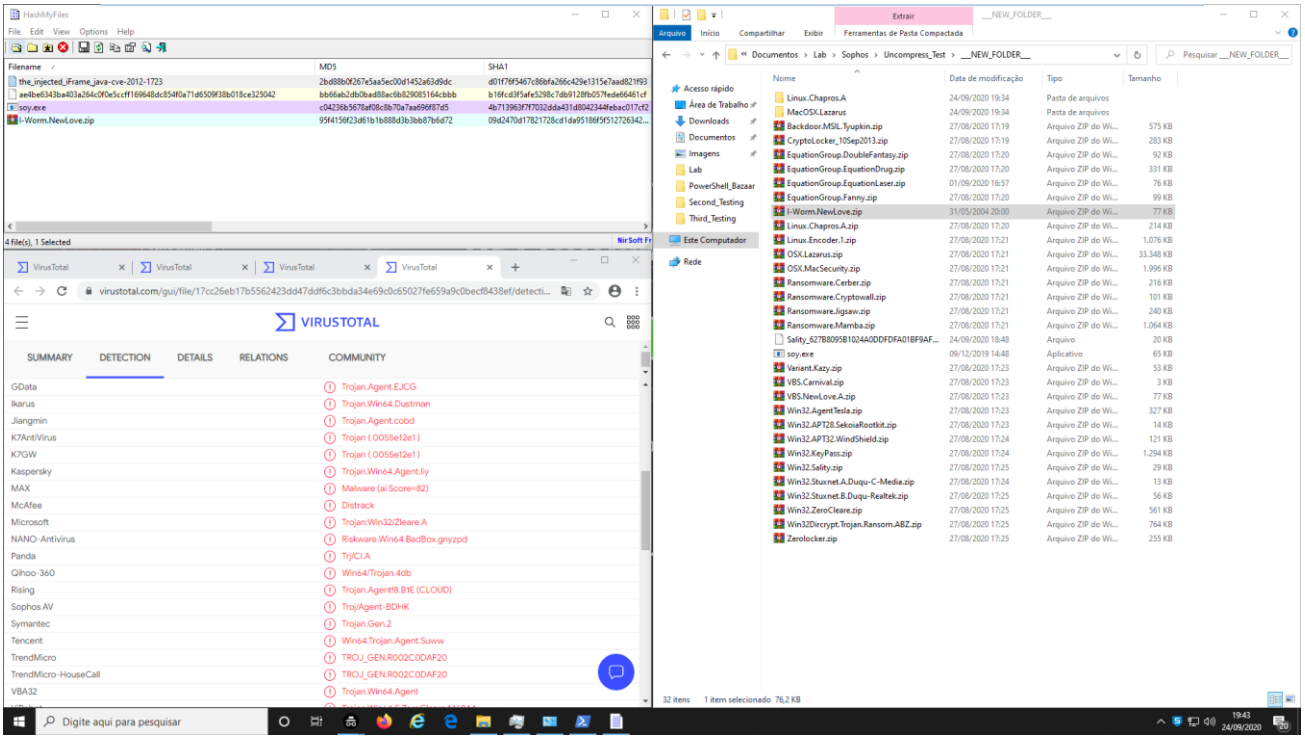


Image 1.7: __NEW_FOLDER__(Sophoo) – Malware manipulation

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..

After performing this second test, we saw that the same 4 malwares there were detected yet, as we can see below and mentioned earlier, all these malware were already known and validated even in the tool about antivirus scanning known as a Virus Total (https://virustotal.com).

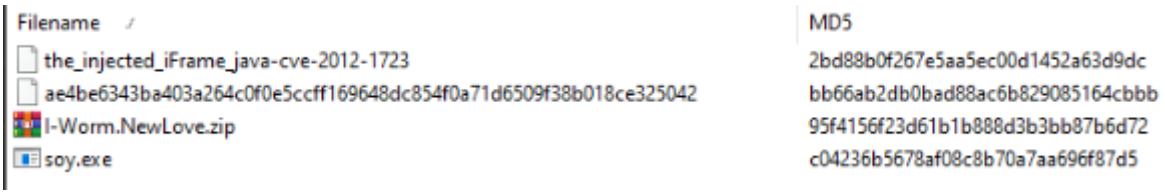


Image 1.8: Malwares – Not Detected

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.

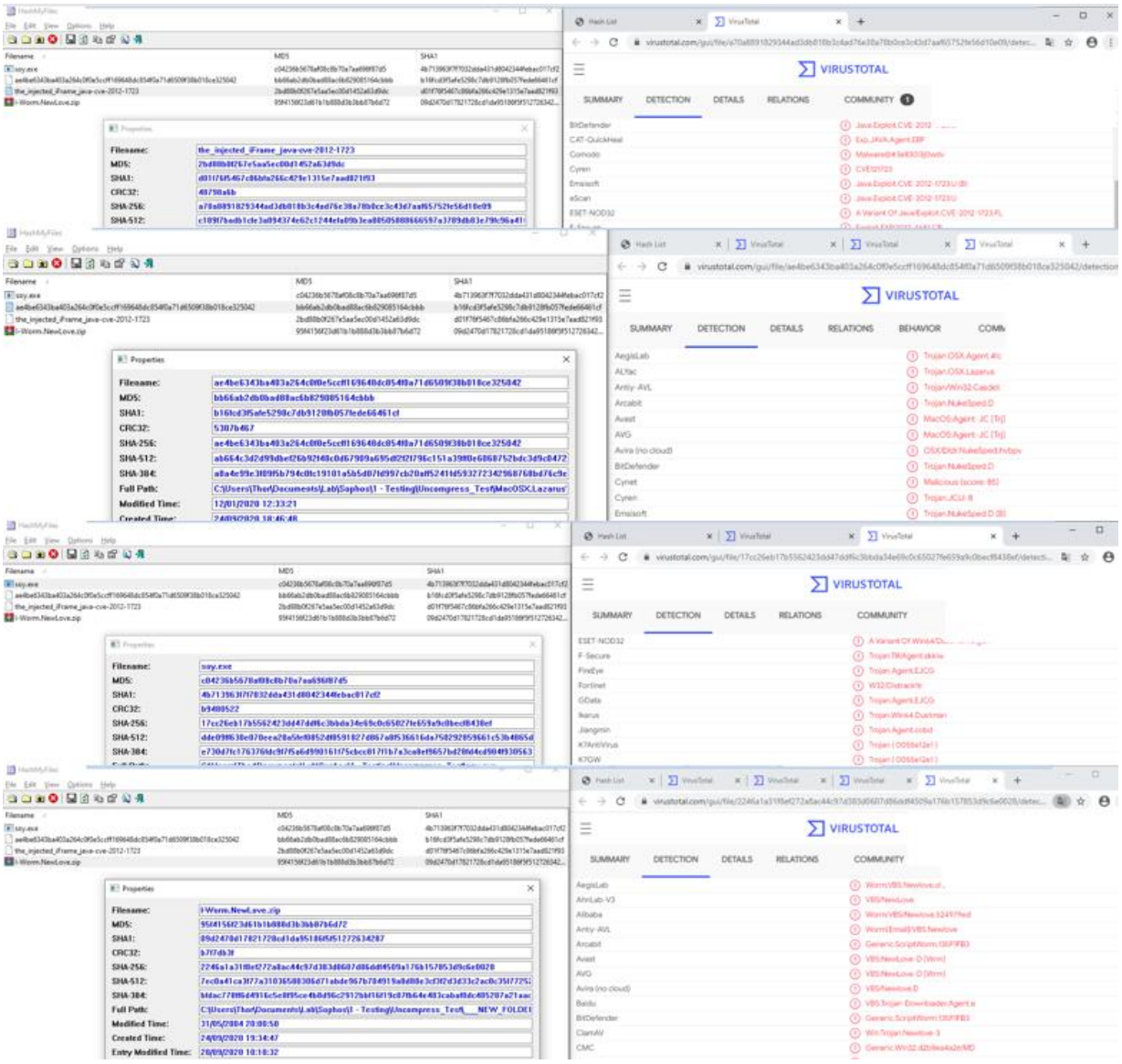


Image 1.9: Malwares – Not Detected after *ScanNow*

After performing this third test and the execution of the ScanNow feature, we saw that the same 4 malwares there were detected yet, as we can see below and mentioned earlier, even all these malwares were already known.

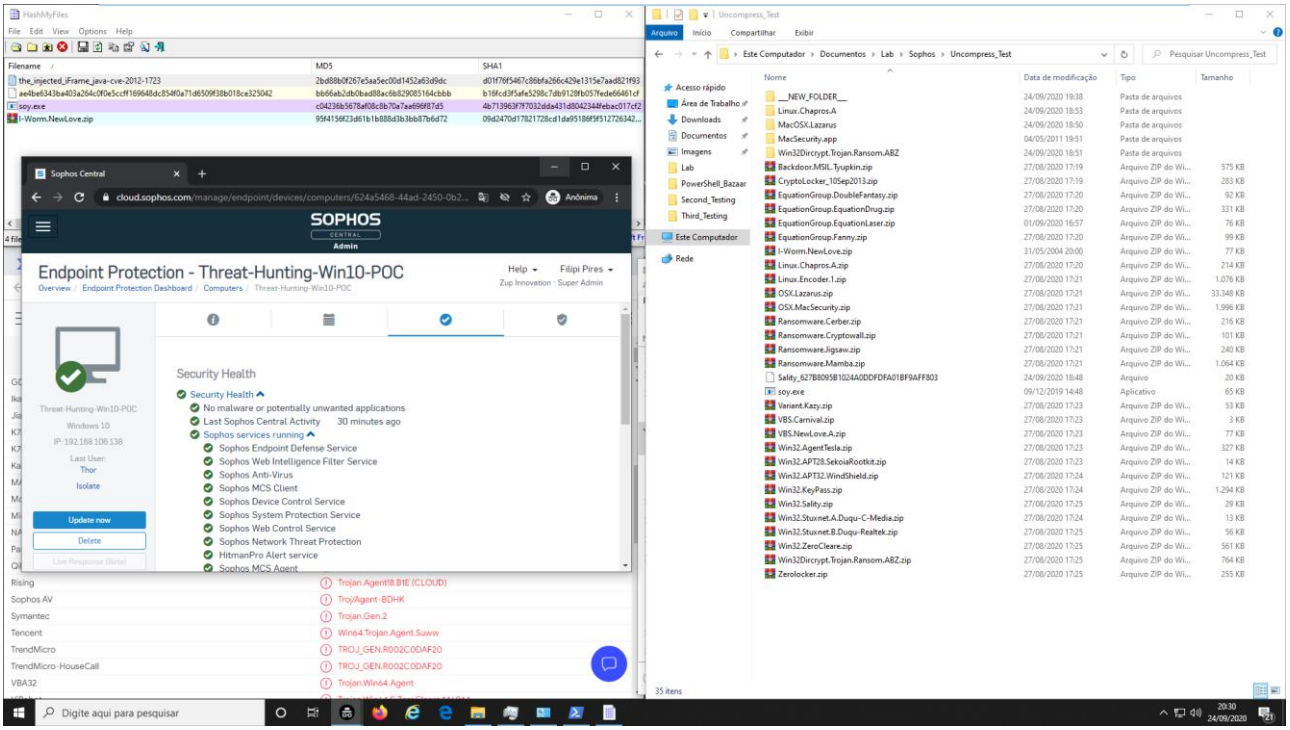


Image 1.10: Malwares – Not Detected after *ScanNow*

3 Impact and Risk

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.

- **Problem during the first test - unzipping ZIP file (Not Blocked)**
  - During this test it was possible to see that the Sophos Endpoint Solution didn't block many ZIP files, all of them known as a malicious file, if the attack happened in the same time in the victim, this user could click in anyone of the samples and could be infected, because it's not clear how works the prevalence, maybe priority of the engine in the detection flow.
- **Malicious .Zip files NOT Detected**
  - As we can see the sample (`I-Worm.NewLove.zip | hash-2246a1a31f8ef272a8ac44c97d383d0607d86ddf4509a176b157853d9c6e0028`) it's not detected like a Malicious.
- **Malicious ELF files Not Detected in the second test.**
  - *ELF* file not detected even though malicious; In our test environment, wouldn't be dangerous, because our environment it was Windows, but

should be block but it was not detected.

- **Malicious files Not Detected in the third test after *ScanNow*.**
    - *ELF* file not detected even though malicious; In our test environment, wouldn't be dangerous, because our environment it was Windows, but should be block but it was not detected.

MALWARES NOT BLOCKED / ATTACK VECTOR

- **I-Worm.NewLove**

hxxps://github.com/ytisf/theZoo/tree/master/malwares/Binaries/VBS.NewLove.A

```
Basic Properties
MD5   95f4156f23d61b1b888d3b3bb87b6d72
SHA-1 09d2470d17821728cd1da95186f5f51272634287
SHA-256     2246a1a31f8ef272a8ac44c97d383d0607d86ddf4509a176b157853d9c6e0028
Vhash 773a411c5a56087d4d7c5cc36bbf2901
SSDEEP
      1536:cfY1wBDtr94PLDcwZANv1pG1ZuQK10Oksk/L1xVCXJW5C6U7EjSRVveO:R1wBJoL4F1w6QK1
qFnVCXJYCF7aO

Names
I-Worm.NewLove.zip
output.149790737.txt;
```

Worm-type malware, with high criticality, associated with the execution of VBS - Visual Basic Script, we have as a characteristic high propagation within the environment in which it is executed.

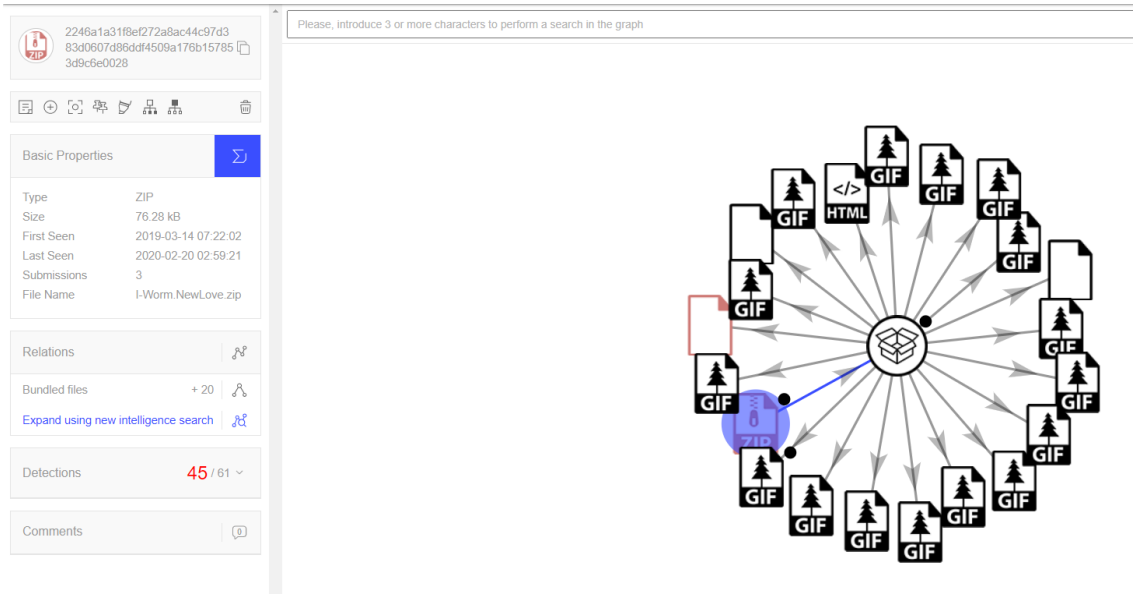


Image 1.10: • I-Worm.NewLove.zip – VirusTotal

- **Win32.ZeroCleare (soy.exe)**

hxxps://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Win32.ZeroCleare

Trojan-type malware, which has a dropper behavior, and is responsible for downloading other malware within the victim's environment, developed for Windows 7, Windows 8, Windows 8.1 and Windows 10 operating systems.

```
Basic Properties
MD5    c04236b5678af08c8b70a7aa696f87d5
SHA-1  4b713963f7f7032dda431d8042344febac017cf2
SHA-256      17cc26eb17b5562423dd47ddf6c3bbda34e69c0c65027fe659a9c0becf8438ef
Vhash  cbfe429774b42621c19bbecbf0681ac1
SSDEEP
       1536:wYFJsIiHyVaM2frJe31Uod74Fru71mTUscFDoRZe6m/fqhuFOnto7:wcWIiHmM8lkFyJmTvc
Boze6m3qT2

Names
soy.exe
output.149792855.txt;
```

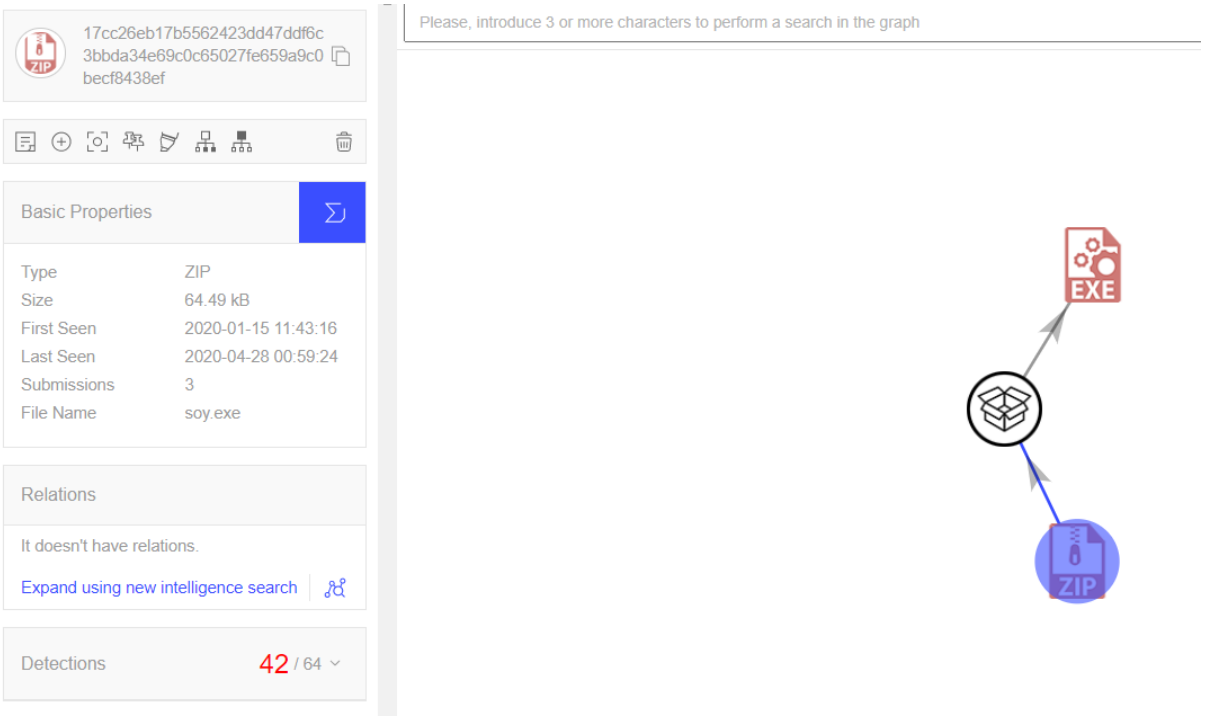


Image 1.11: Win32.ZeroCleare (soy.exe) - VirusTotal

- **OSX.Lazarus**

hxxps://github.com/ytisf/theZoo/blob/master/malwares/Binaries/OSX.Lazarus/

```
Basic Properties
MD5    bb66ab2db0bad88ac6b829085164cbbb
SHA-1  b16fcd3f5afe5298c7db9128fb057fede66461cf
SHA-256      ae4be6343ba403a264c0f0e5ccff169648dc854f0a71d6509f38b018ce325042
SSDEEP 393216:PB1L7fxLRsW73YjCet0N10FHuFQdpEMcKY66o:b7f5Rswoj4CJuGdpc66o

Names
BitcoinTrader.pkg;
```

Malware developed for MacOS environments, focusing on cryptocurrency developed by Lazarus Group (APT group).

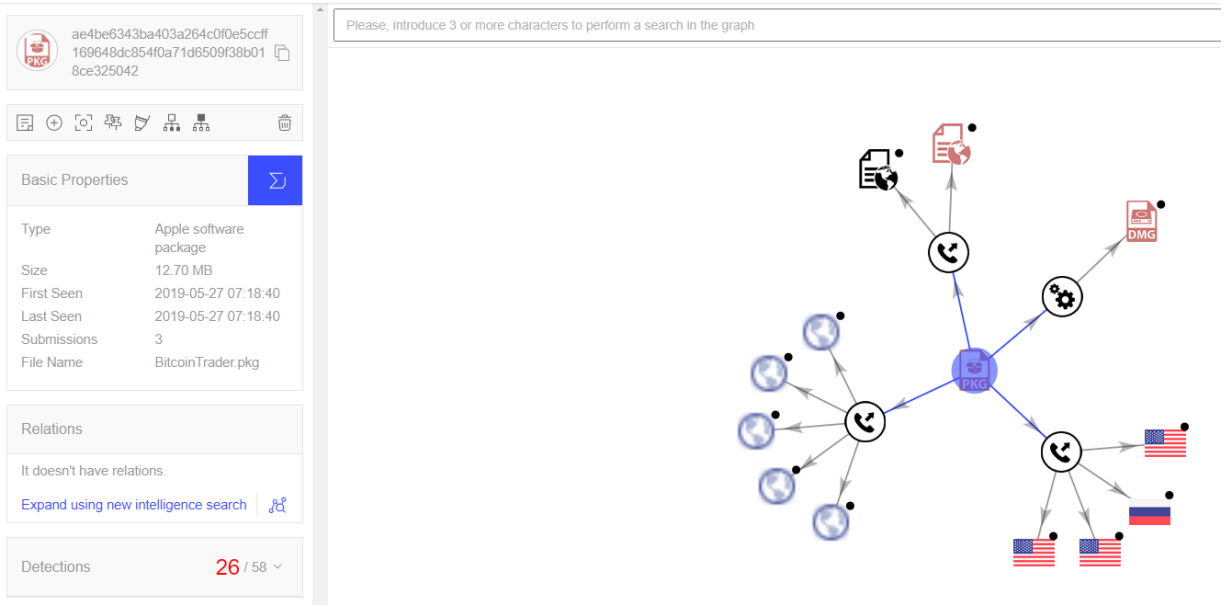


Image 1.12: OSX.Lazarus - VirusTotal

- **The_injected_iFrame_java-cve-2012-1723**

hxxps://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Linux.Chapros.A

```
Basic Properties

MD5    2bd88b0f267e5aa5ec00d1452a63d9dc
SHA-1  d01f76f5467c86bfa266c429e1315e7aad821f93
SHA-256      a70a8891829344ad3db818b3c4ad76e38a78b0ce3c43d7aaf65752fe56d10e09
Vhash  03fc64a044d19b92f3ce659f6ee3b940
SSDEEP 768:+8YnvovLx9vqu8UvRRToT2Sv4LoM0kit/la0cO:+8YWF1XMAF0kjO


Names
2bd88b0f267e5aa5ec00d1452a63d9dc_the_injected_iFrame_java-cve-2012-1723
the_injected_iFrame_java-cve-2012-1723
java-cve-2012-1723
a70a8891829344ad3db818b3c4ad76e38a78b0ce3c43d7aaf65752fe56d10e09.bin
d01f76f5467c86bfa266c429e1315e7aad821f93_jar.jar
2BD88B0F267E5AA5EC00D1452A63D9DC
jar.jar
nYCND
the_injected_iFrame_java-cve-2012-1723.infected;
```

Java Exploit

Unspecified vulnerability in the ***Java Runtime Environment (JRE)*** component in Oracle Java SE 7 update 4 and earlier, 6 update 32 and earlier, 5 update 35 and earlier, and 1.4.2_37 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.

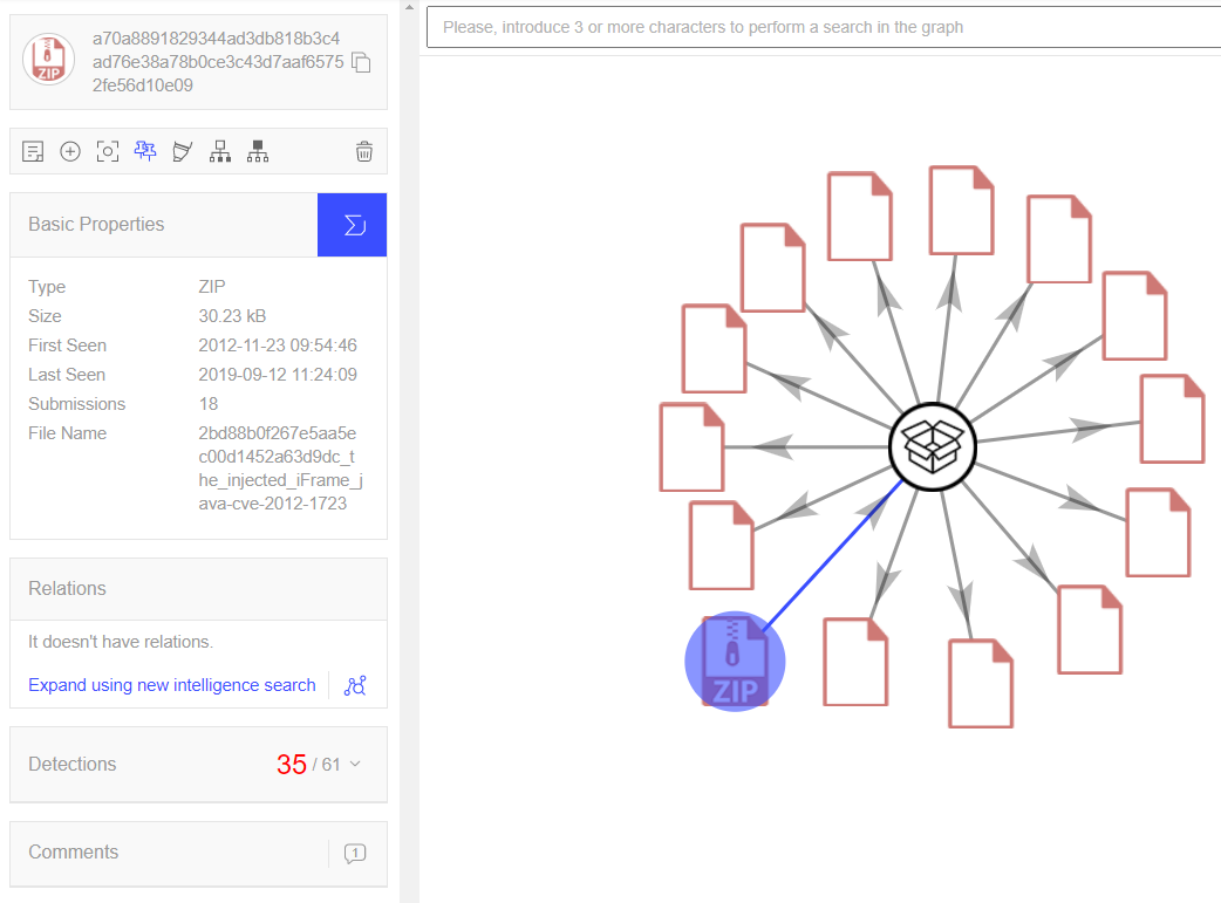


Image 1.13: The_injected_iFrame_java-cve-2012-1723 - VirusTotal

4 Recommendation Actions

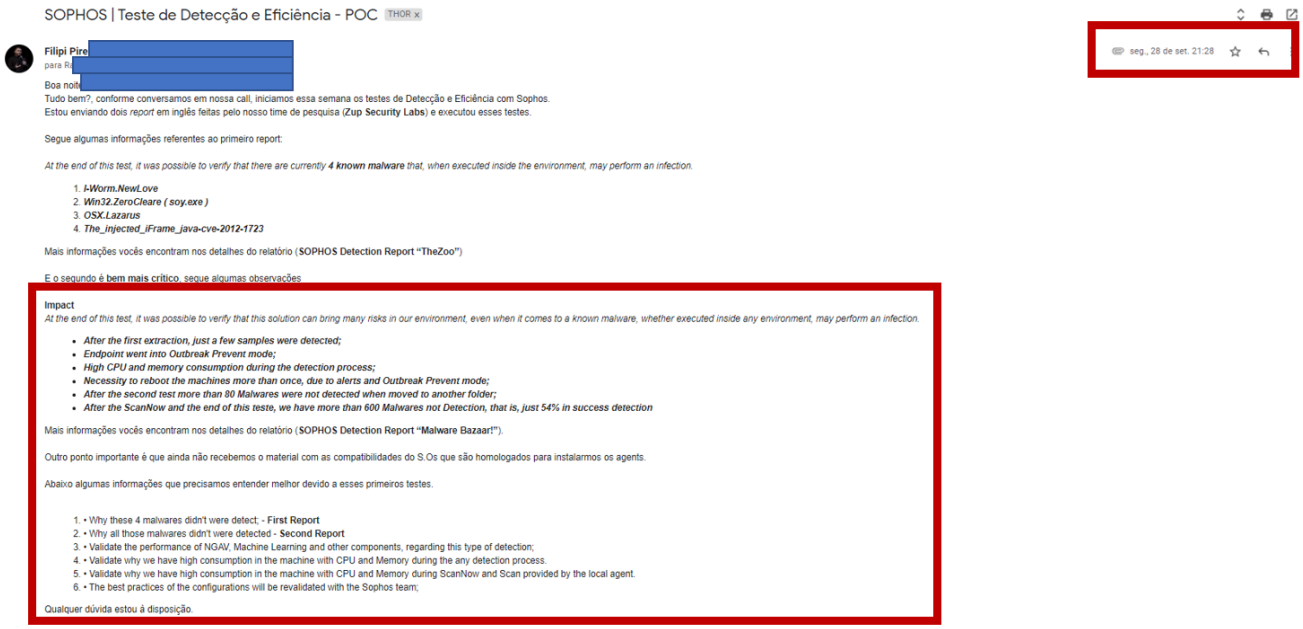
As we mentioned before, the idea it was execute test in many malwares, and this case, for this reason to be totally known the following actions will be taken to improve the protection environment of our assets:

- This report was sent to Sophos Security Team to validate with them how the detection flow for known malware works, and why these 4 malwares didn't detect;
- Validate the performance of NGAV, Machine Learning and other components, regarding this type of detection;
- 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 performed in the execution of 27 folders different Malwares in our 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 Pire [redacted]
para R[redacted]

Boa noit[redacted]
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!"**).

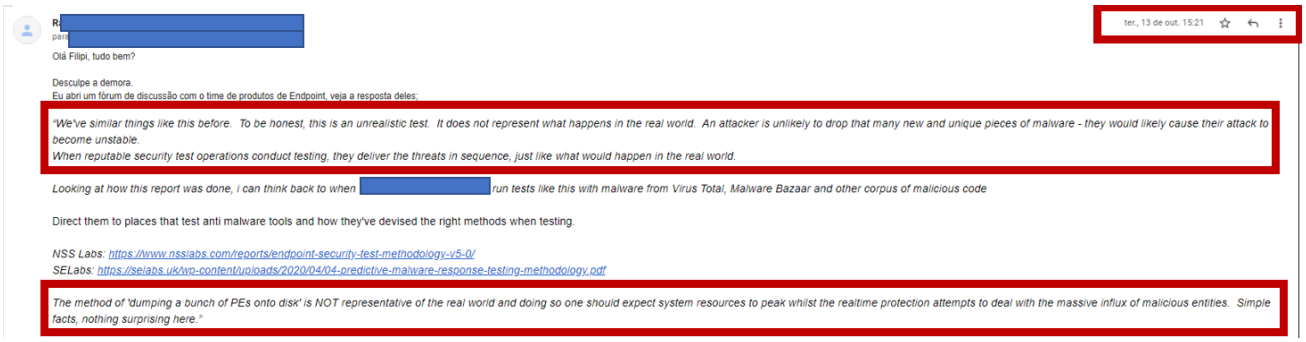
Outro ponto importante é que ainda não recebemos o material com as compatibilidades do S.Os que são homologados para instalarmos os agents.

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.

But for my surprise, after fifteen days (on **October 13th**), we received an unbelievable and generic answer about the test.



R[redacted]
para [redacted]

ter., 13 de out. 15:21

Olá Filipi, tudo bem?

Desculpe a demora.
Eu abri um fórum de discussão com o time de produtos de Endpoint, veja a resposta deles;

"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 [redacted] *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."