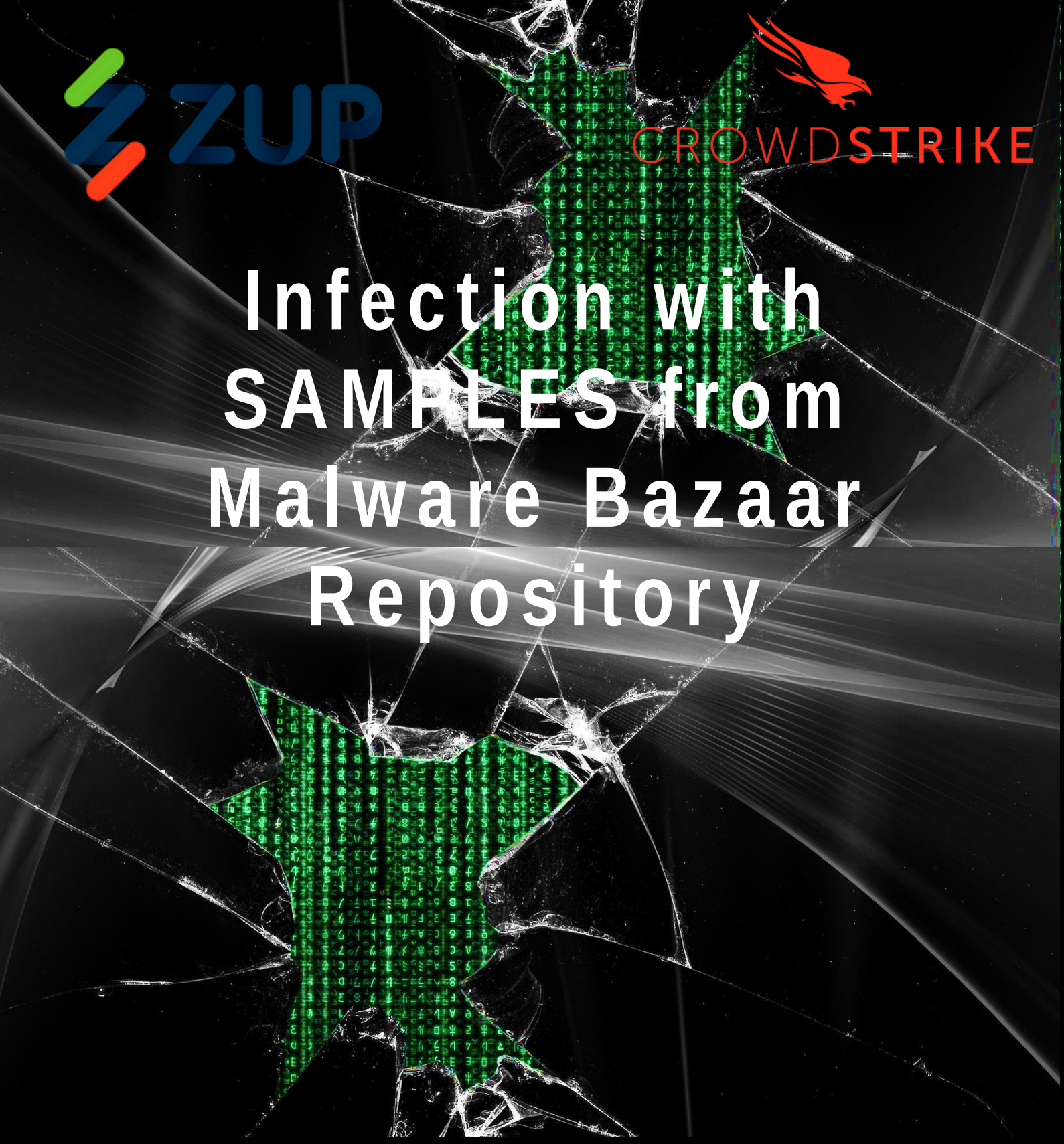

Infection with SAMPLES from Malware Bazaar Repository

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 lab environment protected with an endpoint solution, provided by **CrowdStrike**, 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.crowdstrike.com`) in **Version:**

- **Sensor Version = 5.36.11809.0**

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

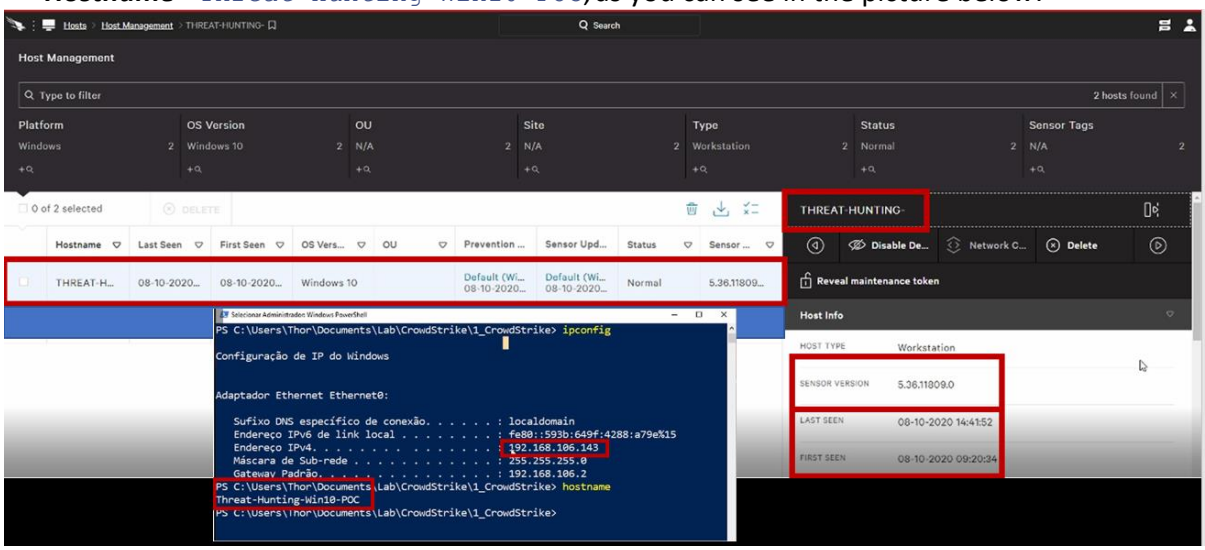

Image 1.1: Windows 10 Pro 2019 Virtual Machine

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 586 kind of files with many 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 **October 08th** of the year 2020 and it was completed on **October 20th** 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.

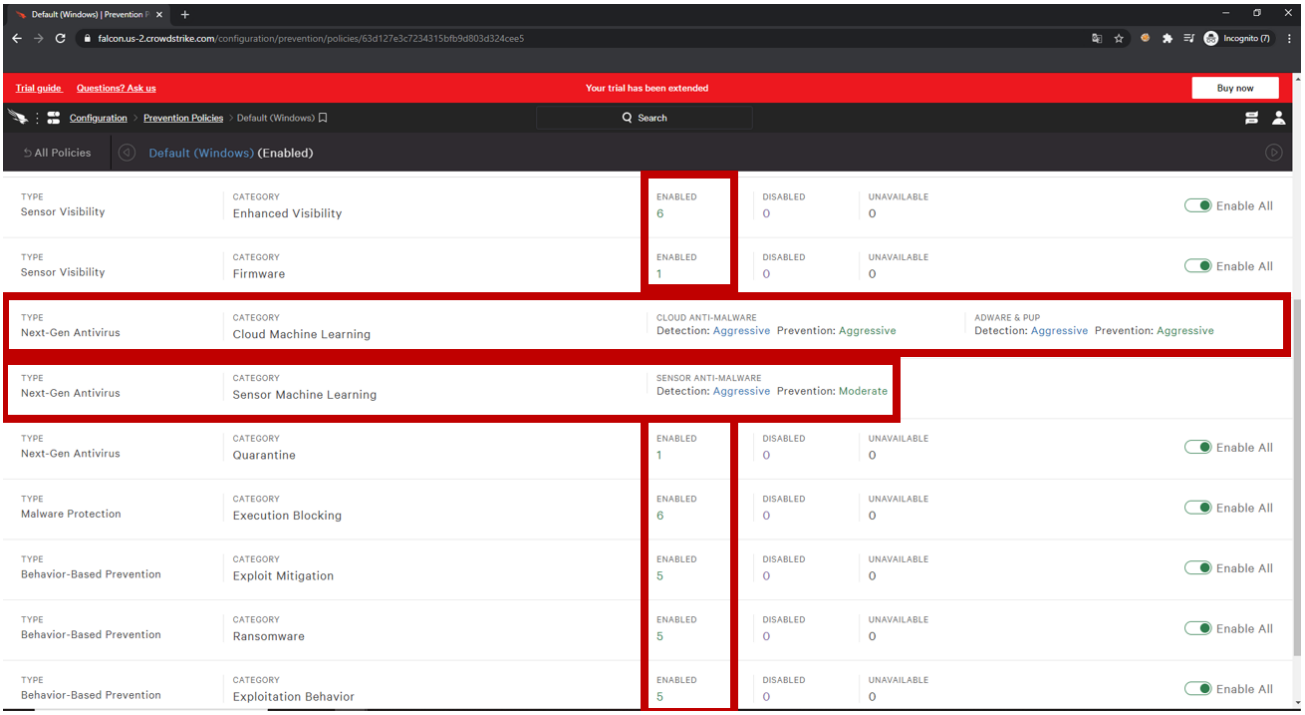

Image 1.2: Virtual Machine with Policy applied

The policy used was named **`Default (Windows)`**, following the best practices recommended by the manufacturer, and, for testing purposes, all due actions were based on an aggressive detection method.

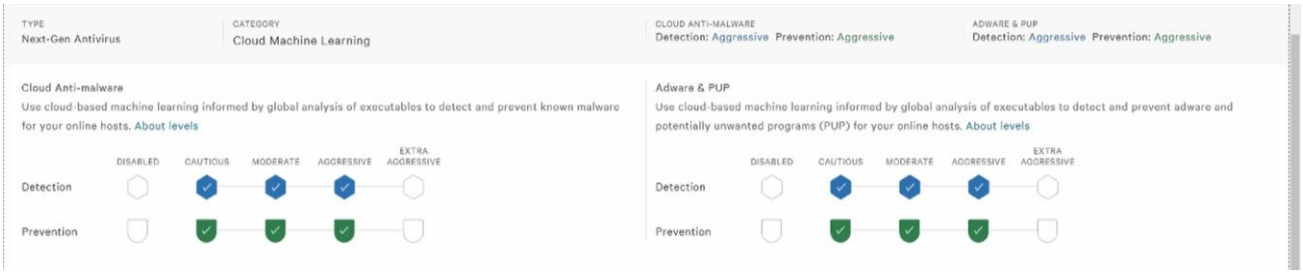

Image 1.3: Policy Next-Gen Antivirus (Default Policy)

Take look in this example, because we changed the CLOUD ANTI-MALWARE and ADWARE & PUP to AGGRESSIVE MODE.

One of the differences that we see with CrowdStrike is the non-use of Icon related of the binary.

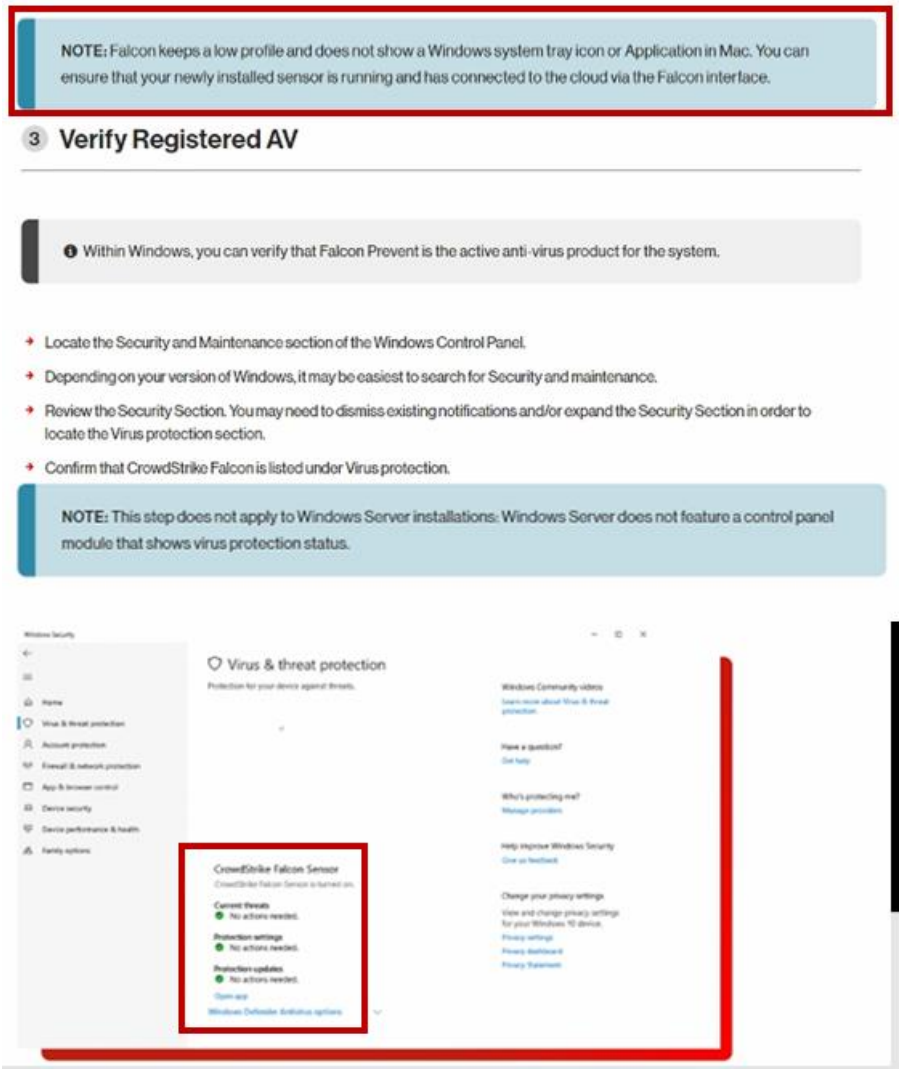

Image 1.4: Installation binary information

3.2 First Test

The first stage of the tests was through the download of the **586 kind of files** with many 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 2020-10-01

(https://mb-api.abuse.ch/downloads/2020-10-01.zip);

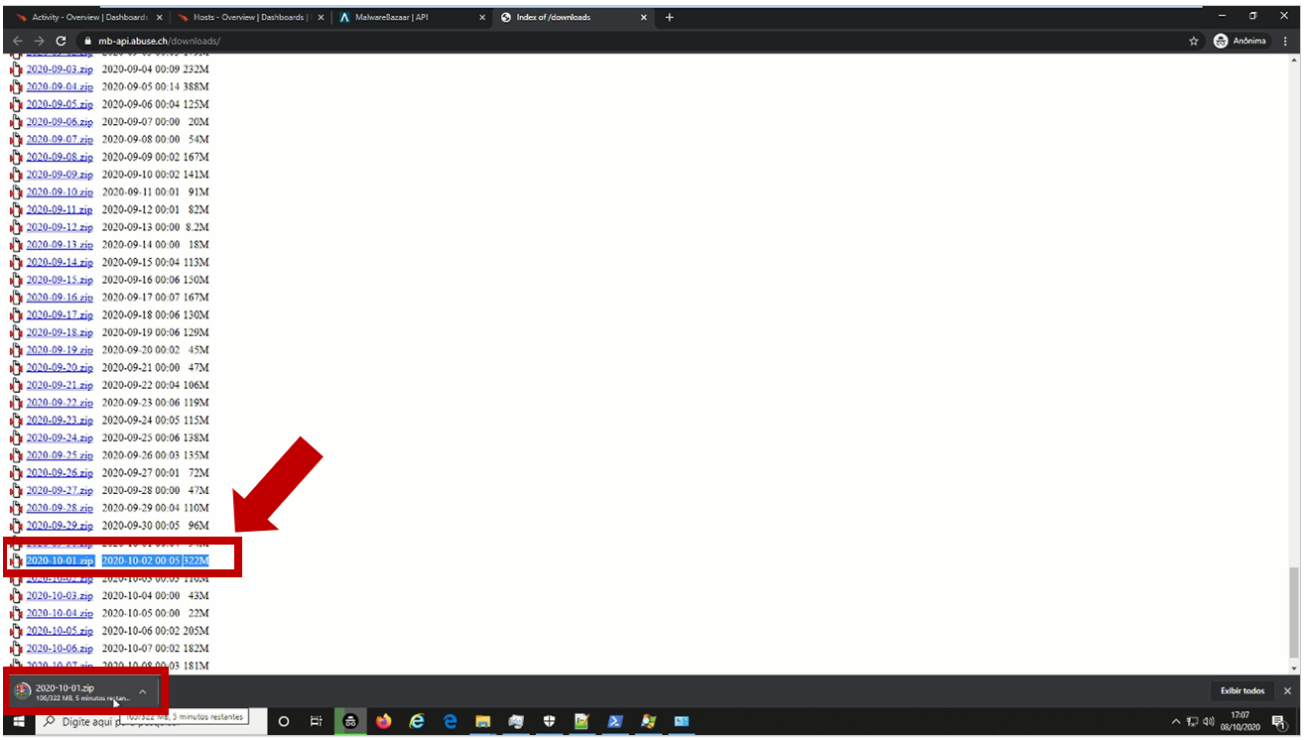

Image 1.5: Daily baches in Malware Bazaar

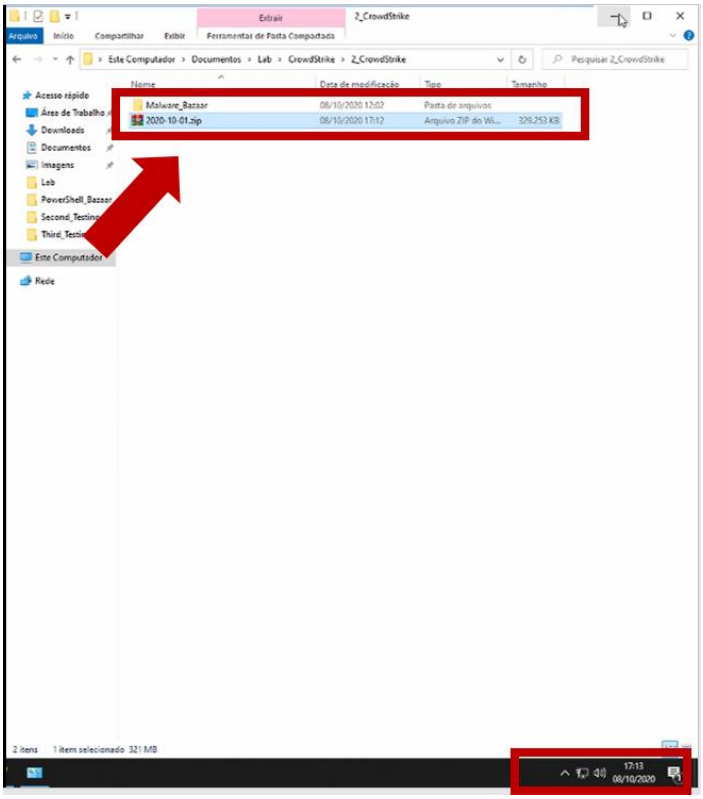

Image 1.6: Download more than 586 Files inside this Folder

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.

After performing the action of extracting the files, it was possible to verify that CrowdStrike Security Endpoint there were **didn't detect any malware** when it was downloaded to the victim machine, that if executed inside the environment, could perform an infection.

All those malwares are known and should be detected by signature, but they didn't.

Regarding some with the vendor CrowdStrike doesn't work based on signature, this is one of the reasons, low consumption of computational resources

Machine learning (ML) is used for pre-execution prevention. Falcon Host employs sophisticated machine learning algorithms that can analyze millions of file characteristics to determine if a file is malicious. ***This signature-less technology enables Falcon Host to detect and block both known and unknown malware****. CrowdStrike ML technology has been independently tested and furthermore, it was provided to VirusTotal to contribute to the security community for the benefit of all. For more information about CrowdStrike ML, read the blog, "CrowdStrike Machine Learning and VirusTotal."*

Reference: https://www.crowdstrike.com/resources/data-sheets/preventing-malware-beyond/

Other References: https://www.crowdstrike.com/press-releases/crowdstrikes-machine-learning-engine-becomes-first-signature-less-engine-integrated-virustotal/

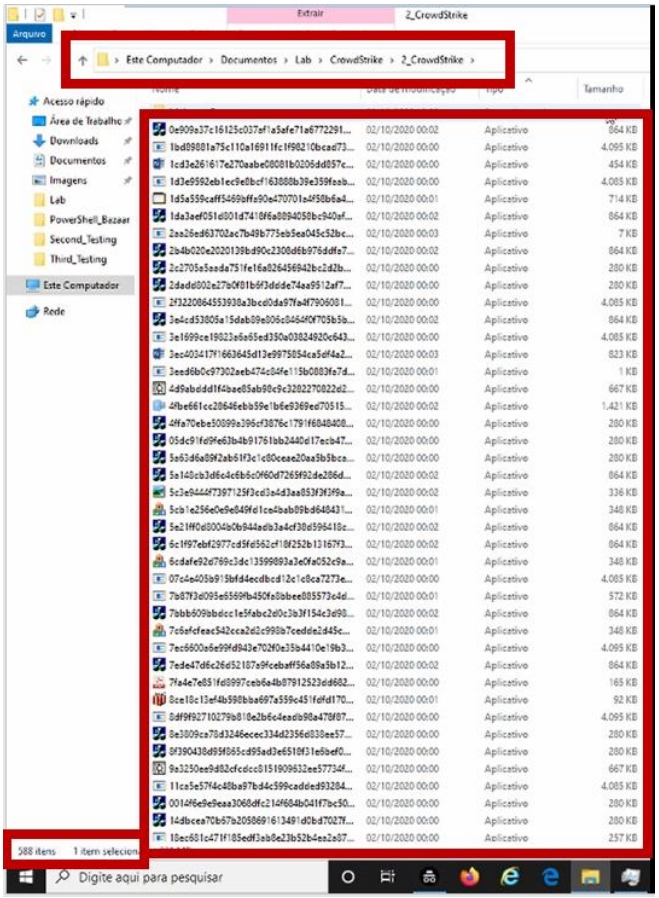

Image 1.7: Extraction of the files from daily batches

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.

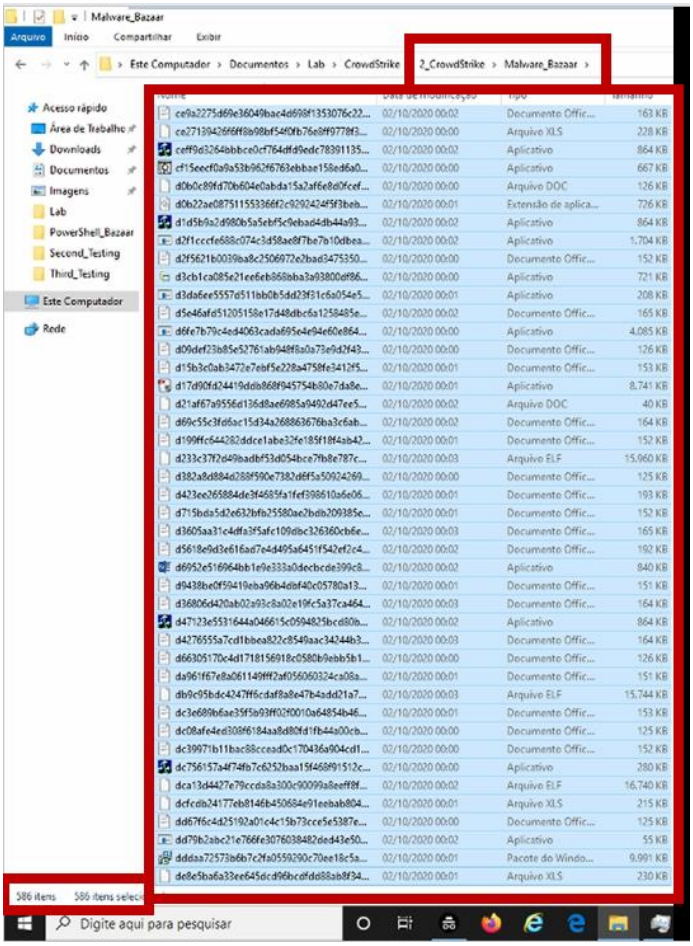

Image 1.8: _Malware_Bazaar (New_Folder) – Coping another folder.

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.

After performing this second test, we saw that the same **586 kind of files** with 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`).

3.4 Third Test

The third stage of the tests was through the use of the ***FULLSCAN*** action by **Cloud CrowdStrike**, 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, but in this case, we can't do this test, i.e, *CrowdStrike has a scanless technology*.

Spotlight utilizes scanless technology, delivering an always-on, automated vulnerability management solution with prioritized data in real time. It eliminates bulky, dated reports with its fast, intuitive dashboard.

Reference: https://www.crowdstrike.com/endpoint-security-products/falcon-spotlight-vulnerability-management/

All surprises forced us to perform an unscheduled test for this stage.

3.4 Fourth Test

The fourth stage of the tests (**unscheduled**) using "*Malware Execution*" manually, in this way, we can look the behavior of these detection engine works in real-time and all malware should be eliminated, as they are already known malware as mentioned earlier.

First of all, we executed the snapshot in our lab machine.

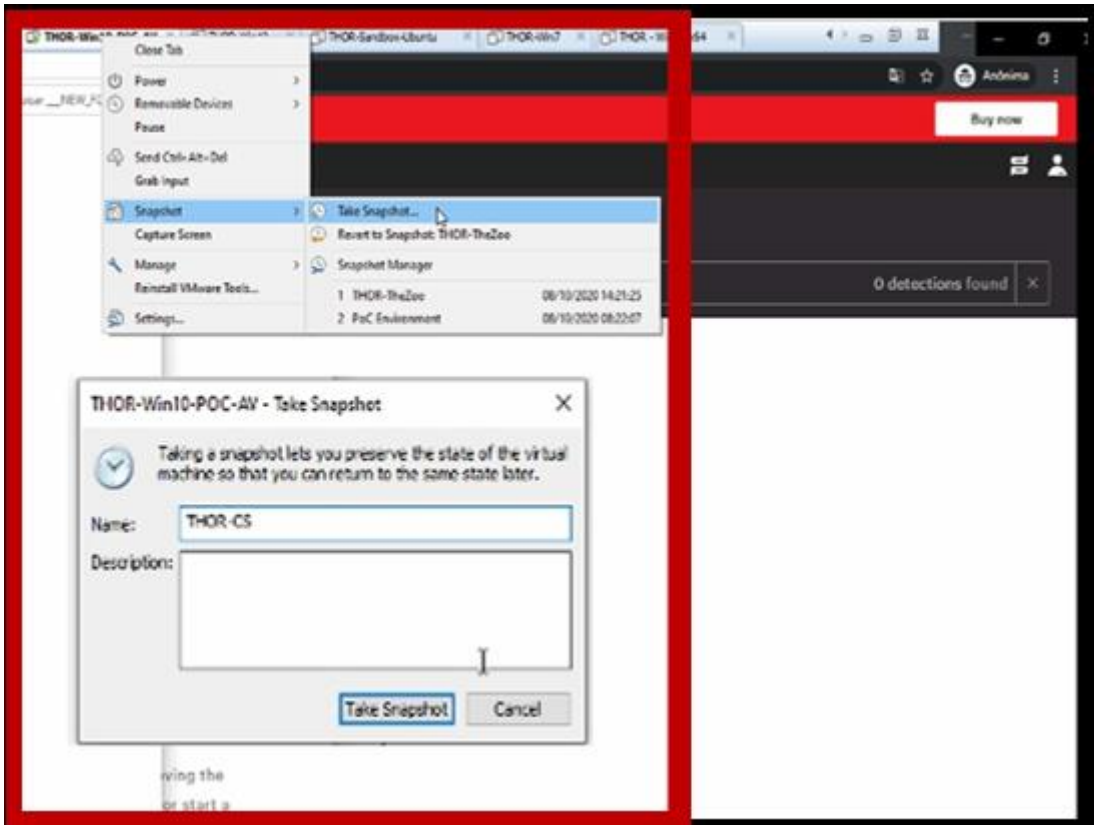

Image 1.9: SnapShot

We started the manual execution of some malware chosen at random.

First malware chosen was EMOTED variable and It was BLOCKED

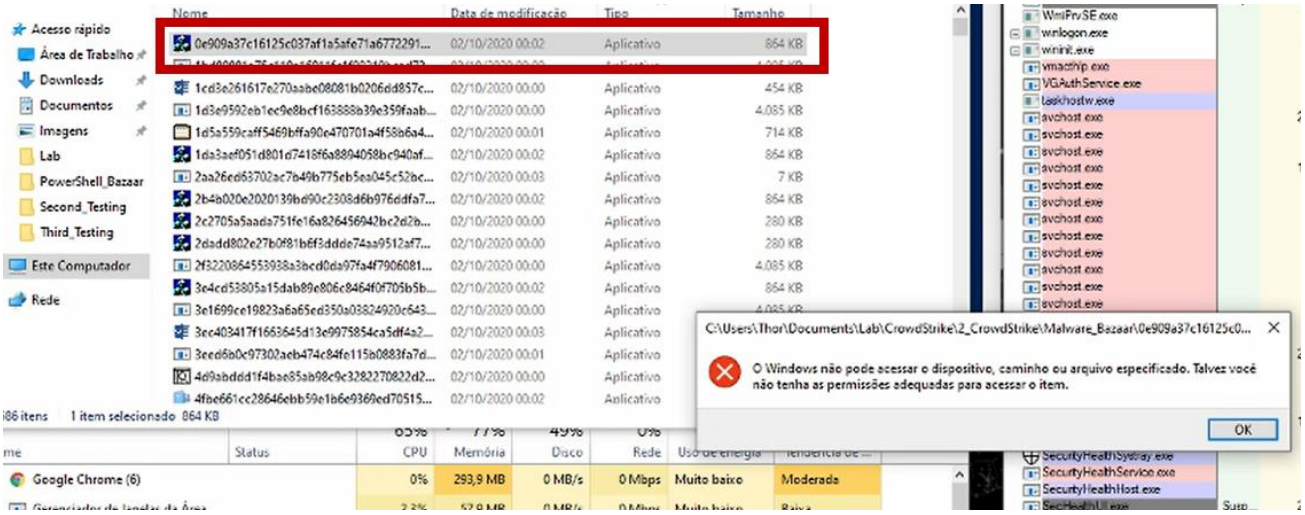

Image 1.10: Emoted Variable - BLOCKED

Second malware chosen was Generic Trojan and It was BLOCKED

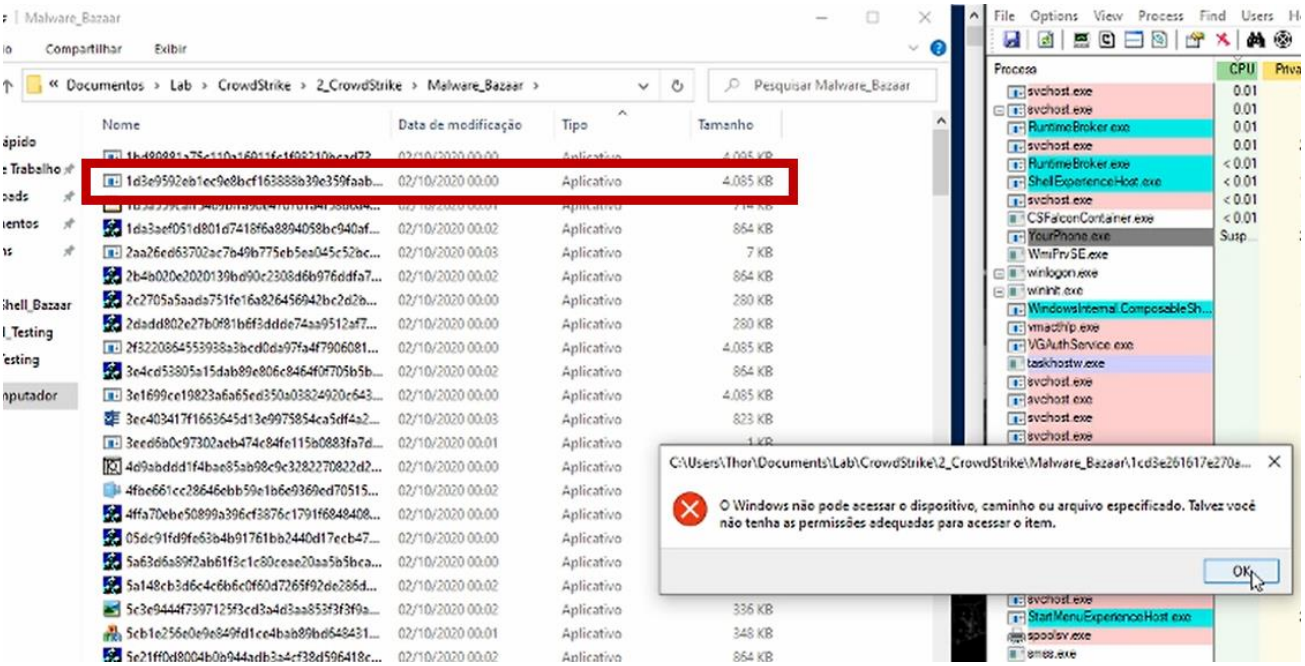

Image 1.11: Generic Trojan - BLOCKED

Third malware chosen was another Trojan Generic Variable and It was BLOCKED

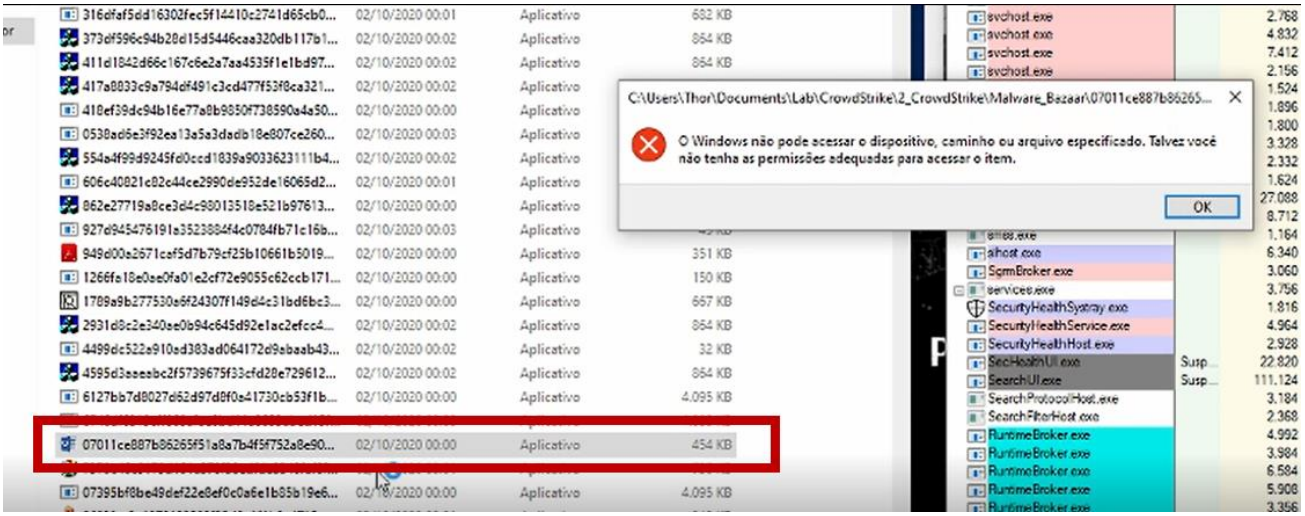

Image 1.12: Another Generic Trojan - BLOCKED

After many more test using PE (Portable Executable) file, and all those files were blocked, we tried to execute a MSI file, i.e, MSI is an installer package file format used by Windows. Its name comes from the program's original title, Microsoft Installer, which has since changed to Windows Installer. MSI files are used for installation, storage, and removal of programs.

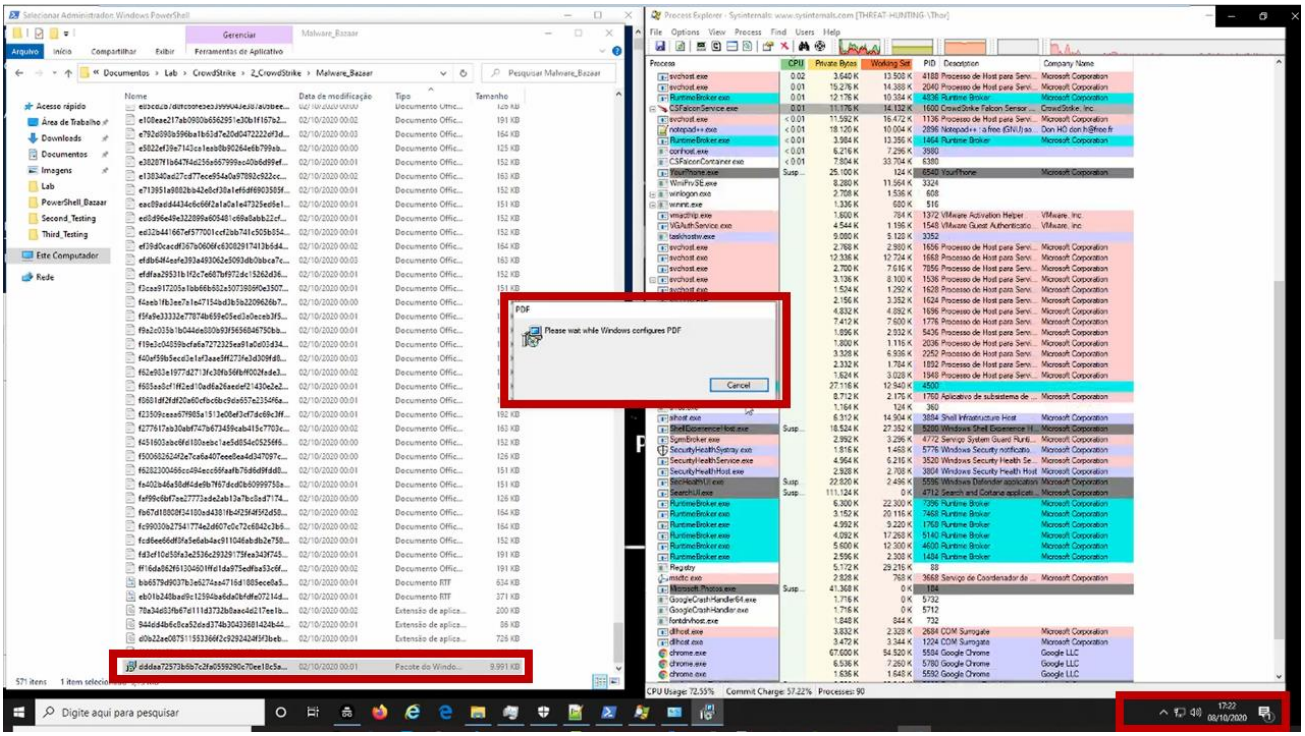

Image 1.13 MSI Executed

After to execute this binary, it seems that a "**to PDF program Installation process**" being executed in our machine, and not being blocked by CrowdStrike.

This malware executed in our environment it's known as: **Zusy Malware**

Zusy malware is a banking Trojan that uses man-in-the-middle attacks to steal bank information. It is a spin-off of the well-known Zeus banking Trojan and is where Zusy takes its name, although Zusy is also known as TinyBanker, Tinba, and Zegost. But 'what's in a name', right? Especially when you're referring to a malware that packs a powerful punch no matter what it's called. And that's exactly what Zusy malware does. Its goal is to steal money from online bank accounts and gather personal information from its victims such as their passwords, banking credentials, and social security numbers

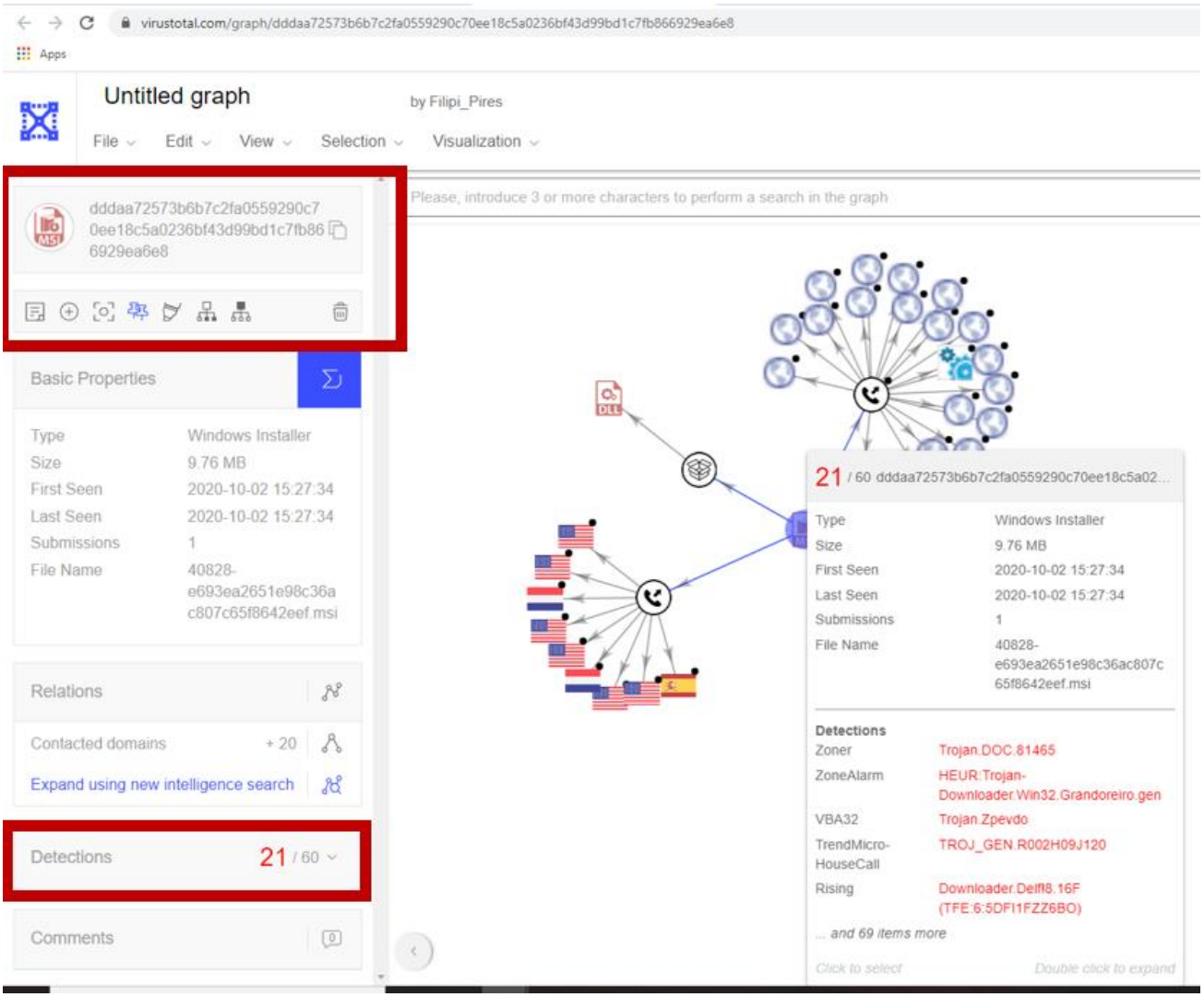

Image 1.14 Virus Total Detection

3 Impact

At the end of this test, it was possible to verify that there many malwares that, when executed inside the environment, may perform an infection.

- **CrowdStrike didn't work with Signature based;**
    - Which makes our environment very vulnerable;
- **Dependency of the real time engines;**
    - Which may be a risk as noted in our test;
- **After the first extraction, no one know malware 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.
- **Malicious EXE files Not Detected**
    - PE files not detected even though malicious; it was not detected.
- **Malicious ELF files Not Detected**
    - *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.
- **After second test no one know malware were detected;**
    - After this moviment, no one malware it was detected.
- **Infection based on MSI (Microsoft Installer – Known Malware**
    - This is the big surprise.

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 **CrowdStrike Team** to validate with them how the detection flow for known malware works, and why all those malwares didn't were detected;
- This report will be sent to CrowdStrike Team to validate with them how the detection flow for known malware works, and why this **MSI Malware didn't was 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 CrowdStrike team;