CrowdStrike Detection Report "TheZoo"

ZUP Security Labs at Zup Innovation

Researcher Manager (s): Filipi Pires

Summary

1 Document Control

1.0.1 Version Control

WRITERS	DELIVERY DATA	PAG.	VERSION	STATUS
Filipi Pires	19/10/2020	18	1	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 performed in the execution of 33 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 32 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.

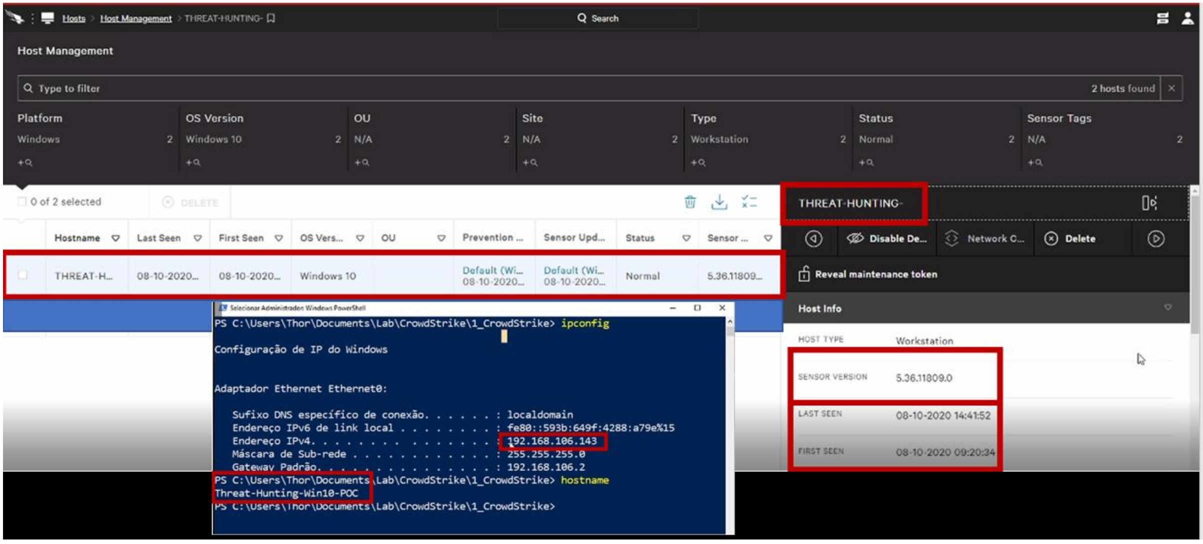
With the final product, the front responsible for the product will have an instrument capable of guiding a process of mitigation and / or correction, as well as optimized improvement, based on the criticality of risks.

2.0.1 Scope

The efficiency and detection analysis had as target the Cybereason Endpoint Protection application (`https://cloud.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:



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...	08-10-2020...	08-10-2020...	Windows 10		Default (Wi... 08-10-2020...	Default (Wi... 08-10-2020...	Normal	5.36.11809...

```
PS C:\Users\Thor\Documents\Lab\CrowdStrike\1_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. . . . . . . .  . . . . . . . : 192.168.106.143
   Máscara de Sub-rede . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . : 192.168.106.2
PS C:\Users\Thor\Documents\Lab\CrowdStrike\1_CrowdStrike> hostname
Threat-Hunting-Win10-POC
PS C:\Users\Thor\Documents\Lab\CrowdStrike\1_CrowdStrike>
```

HOST TYPE	Workstation
SENSOR VERSION	5.36.11809.0
LAST SEEN	08-10-2020 14:41:52
FIRST SEEN	08-10-2020 09:20:34

Image 1.1: Windows 10 Pro 2019 Virtual Machine

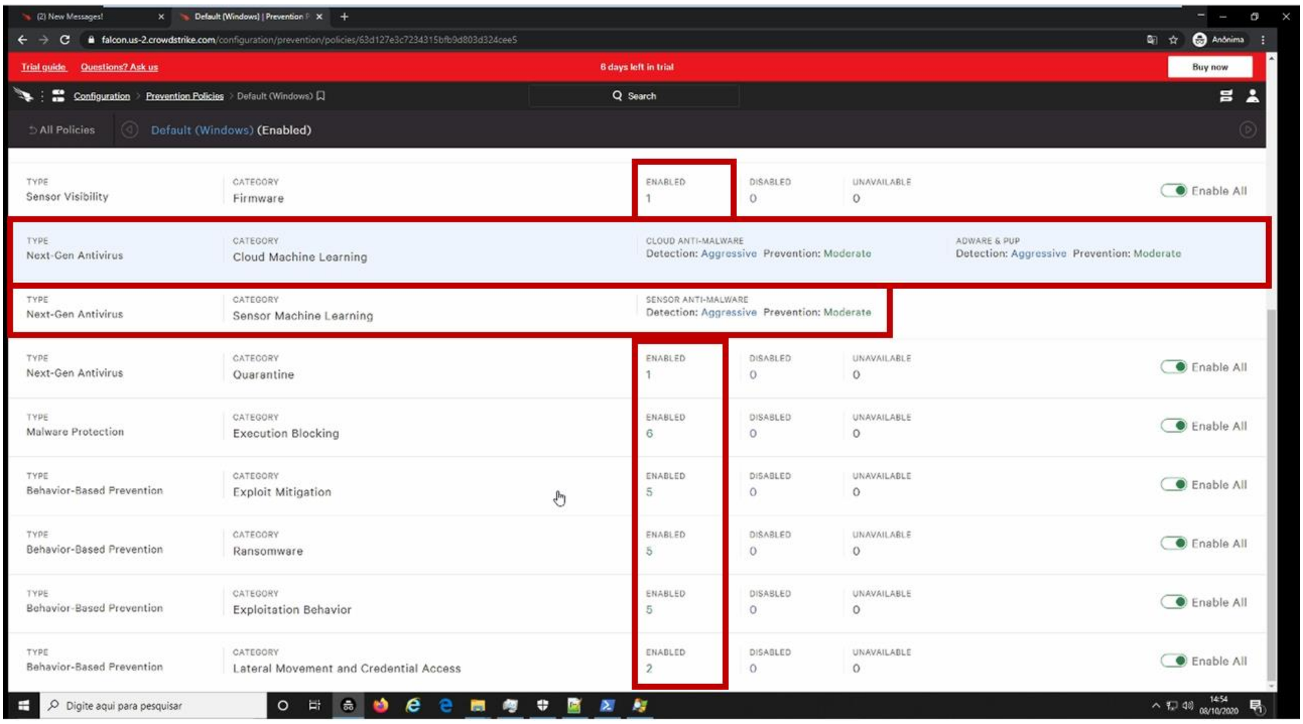
2.0.2 Project Summary

The execution of the security analysis tests of the Threat Hunting team it was carried out through the execution of 33 folders 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 19th** 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.

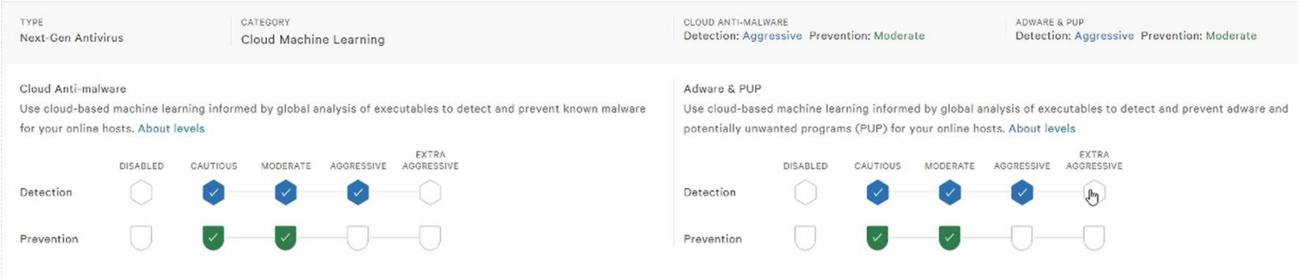


Default (Windows) (Enabled)

TYPE	CATEGORY	ENABLED	DISABLED	UNAVAILABLE	
Sensor Visibility	Firmware	1	0	0	Enable All
Next-Gen Antivirus	Cloud Machine Learning	CLOUD ANTI-MALWARE Detection: Aggressive Prevention: Moderate		ADWARE & PUP Detection: Aggressive Prevention: Moderate	
Next-Gen Antivirus	Sensor Machine Learning	SENSOR ANTI-MALWARE Detection: Aggressive Prevention: Moderate			
Next-Gen Antivirus	Quarantine	1	0	0	Enable All
Malware Protection	Execution Blocking	6	0	0	Enable All
Behavior-Based Prevention	Exploit Mitigation	5	0	0	Enable All
Behavior-Based Prevention	Ransomware	5	0	0	Enable All
Behavior-Based Prevention	Exploitation Behavior	5	0	0	Enable All
Behavior-Based Prevention	Lateral Movement and Credential Access	2	0	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: Moderate

ADWARE & PUP
Detection: Aggressive Prevention: Moderate

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

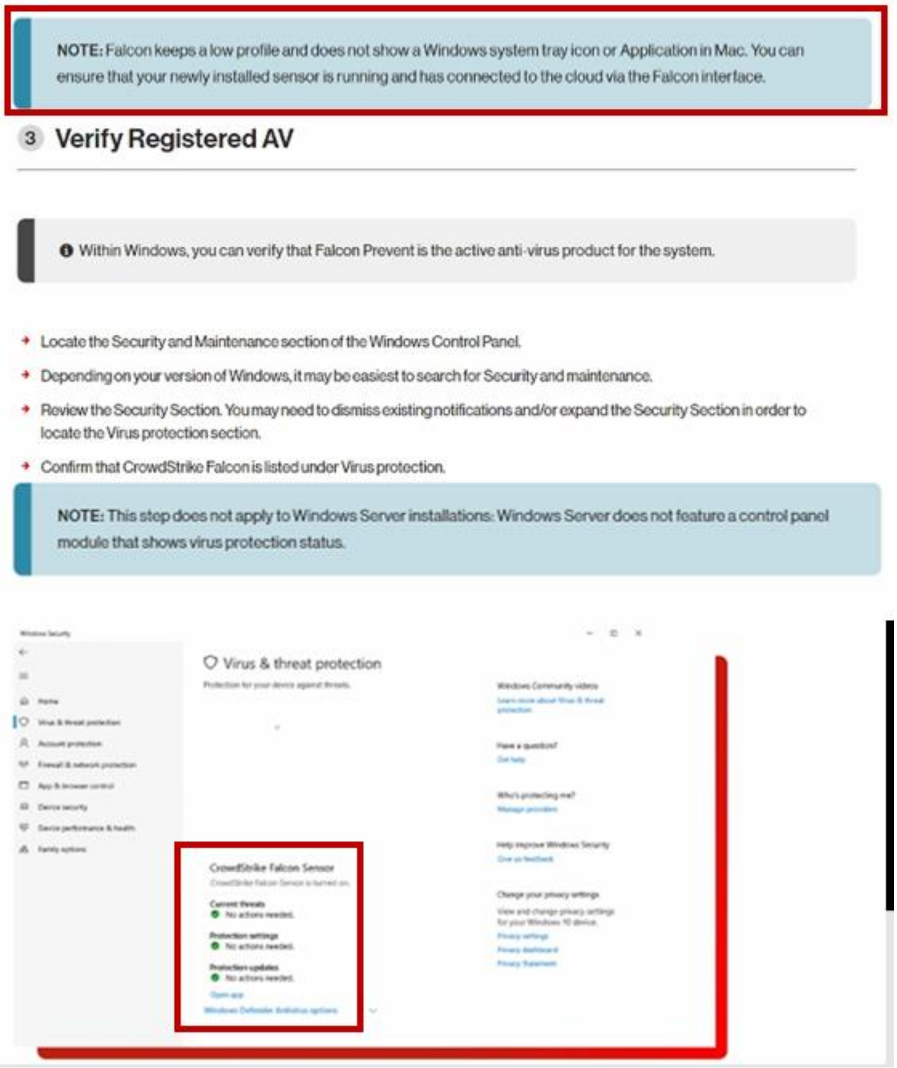
	DISABLED	CAUTIOUS	MODERATE	AGGRESSIVE	EXTRA AGGRESSIVE
Detection	○	✓	✓	✓	○
Prevention	□	✓	✓	□	□

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)

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.

Virus & threat protection
Protection for your device against threats.

CrowdStrike Falcon Sensor
CrowdStrike Falcon Sensor is turned on.

Current threats
● No actions needed.

Protection settings
● No actions needed.

Protection updates
● No actions needed.

Open app
Windows Defender Antivirus options

Windows Community videos
Learn more about Virus & threat protection

Have a question?
Get help

Who's protecting me?
Manage providers

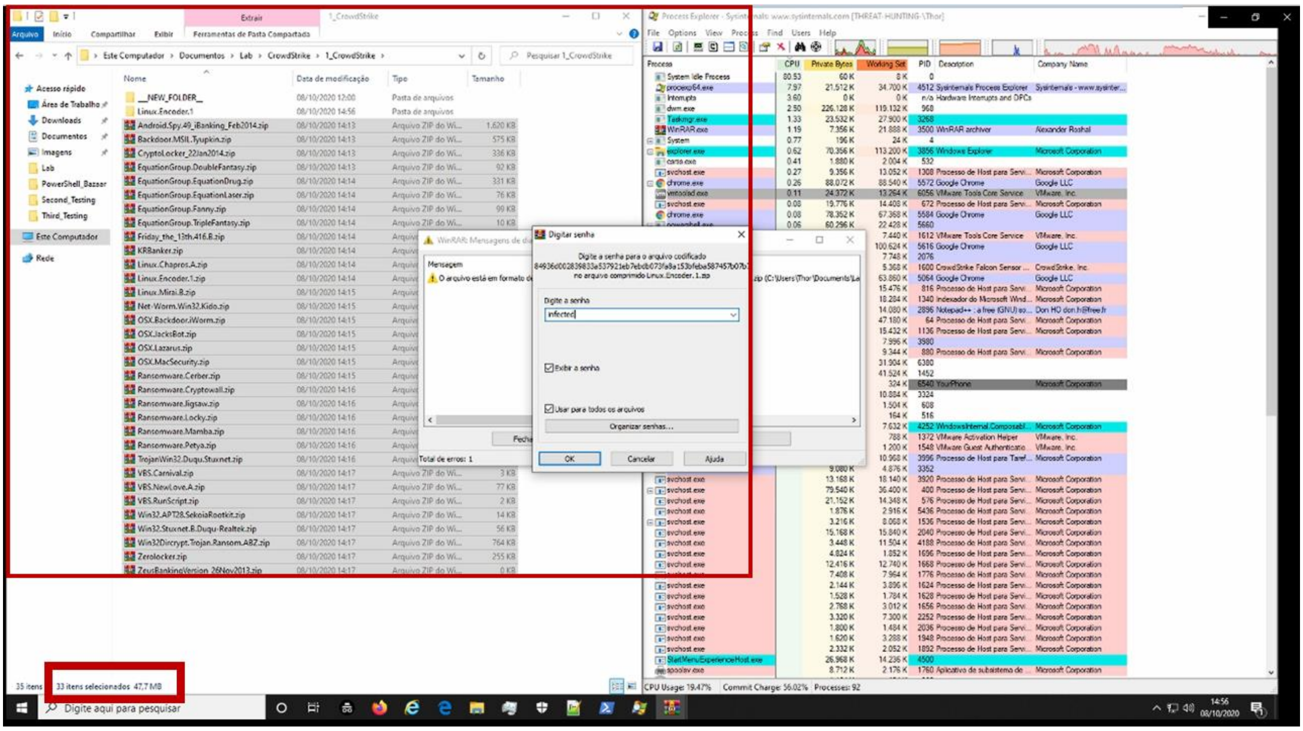
Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement

Image 1.4: Installation binary information

3.2 First Test

The first stage of the tests was through the download of 33 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`);



Este Computador › Documentos › Lab › CrowdStrike › 1_CrowdStrike ›

Nome	Data de modificação	Tipo	Tamanho
__NEW_FOLDER__	08/10/2020 12:00	Pasta de arquivos	
Linux.Encoder.1	08/10/2020 14:56	Pasta de arquivos	
Android.Spy.49_iBanking_Feb2014.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	1.620 KB
Backdoor.MSIL.Tyupkin.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	575 KB
CryptoLocker_22Jan2014.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	336 KB
EquationGroup.DoubleFantasy.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	92 KB
EquationGroup.EquationDrug.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	331 KB
EquationGroup.EquationLaser.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	76 KB
EquationGroup.Fanny.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	99 KB
EquationGroup.TripleFantasy.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	10 KB
Friday_the_13th.416.B.zip	08/10/2020 14:14	Arquiv	
KRBanker.zip	08/10/2020 14:14	Arquiv	
Linux.Chapros.A.zip	08/10/2020 14:14	Arquiv	
Linux.Encoder.1.zip	08/10/2020 14:14	Arquiv	
Linux.Mirai.B.zip	08/10/2020 14:15	Arquiv	
Net-Worm.Win32.Kido.zip	08/10/2020 14:15	Arquiv	
OSX.Backdoor.iWorm.zip	08/10/2020 14:15	Arquiv	
OSX.JacksBot.zip	08/10/2020 14:15	Arquiv	
OSX.Lazarus.zip	08/10/2020 14:15	Arquiv	
OSX.MacSecurity.zip	08/10/2020 14:15	Arquiv	
Ransomware.Cerber.zip	08/10/2020 14:15	Arquiv	
Ransomware.Cryptowall.zip	08/10/2020 14:16	Arquiv	
Ransomware.Jigsaw.zip	08/10/2020 14:16	Arquiv	
Ransomware.Locky.zip	08/10/2020 14:16	Arquiv	
Ransomware.Mamba.zip	08/10/2020 14:16	Arquiv	
Ransomware.Petya.zip	08/10/2020 14:16	Arquiv	
TrojanWin32.Duqu.Stuxnet.zip	08/10/2020 14:16	Arquiv	
VBS.Carnival.zip	08/10/2020 14:17	Arquivo ZIP do Wi...	3 KB
VBS.NewLove.A.zip	08/10/2020 14:17	Arquivo ZIP do Wi...	77 KB
VBS.RunScript.zip	08/10/2020 14:17	Arquivo ZIP do Wi...	2 KB
Win32.APT28.SekoiaRootkit.zip	08/10/2020 14:17	Arquivo ZIP do Wi...	14 KB
Win32.Stuxnet.B.Duqu-Realtek.zip	08/10/2020 14:17	Arquivo ZIP do Wi...	56 KB
Win32Dircrypt.Trojan.Ransom.ABZ.zip	08/10/2020 14:17	Arquivo ZIP do Wi...	764 KB
Zerolocker.zip	08/10/2020 14:17	Arquivo ZIP do Wi...	255 KB
ZeusBankingVersion_26Nov2013.zip	08/10/2020 14:17	Arquivo ZIP do Wi...	0 KB

35 itens | 33 itens selecionados 47,7 MB

WinRAR: Mensagens de di

Mensagem

O arquivo está em formato d

Total de erros: 1

Digitar senha

Digite a senha para o arquivo codificado
84936d002839833a537921eb7ebdb073fa8a153bfeba587457b07b
no arquivo comprimido Linux.Encoder.1.zip

Digite a senha

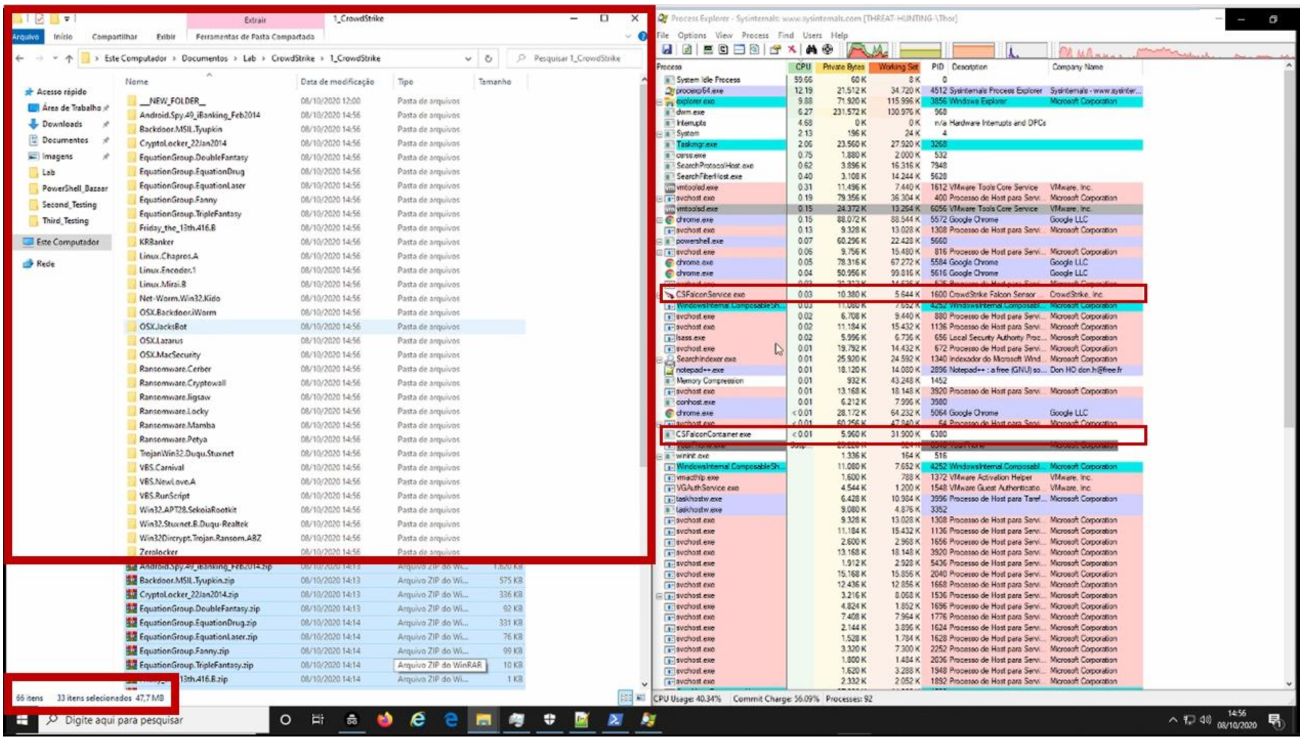
infected

☑ Exibir a senha

☑ Usar para todos os arquivos

Image 1.4: Download 33 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.



Nome	Data de modificação	Tipo	Tamanho
__NEW_FOLDER__	08/10/2020 12:00	Pasta de arquivos	
Android.Spy.49_iBanking_Feb2014	08/10/2020 14:56	Pasta de arquivos	
Backdoor.MSIL.Tyupkin	08/10/2020 14:56	Pasta de arquivos	
CryptoLocker_22Jan2014	08/10/2020 14:56	Pasta de arquivos	
EquationGroup.DoubleFantasy	08/10/2020 14:56	Pasta de arquivos	
EquationGroup.EquationDrug	08/10/2020 14:56	Pasta de arquivos	
EquationGroup.EquationLaser	08/10/2020 14:56	Pasta de arquivos	
EquationGroup.Fanny	08/10/2020 14:56	Pasta de arquivos	
EquationGroup.TripleFantasy	08/10/2020 14:56	Pasta de arquivos	
Friday_the_13th.416.B	08/10/2020 14:56	Pasta de arquivos	
KRBanker	08/10/2020 14:56	Pasta de arquivos	
Linux.Chapros.A	08/10/2020 14:56	Pasta de arquivos	
Linux.Encoder.1	08/10/2020 14:56	Pasta de arquivos	
Linux.Mirai.B	08/10/2020 14:56	Pasta de arquivos	
Net-Worm.Win32.Kido	08/10/2020 14:56	Pasta de arquivos	
OSX.Backdoor.iWorm	08/10/2020 14:56	Pasta de arquivos	
OSX.JacksBot	08/10/2020 14:56	Pasta de arquivos	
OSX.Lazarus	08/10/2020 14:56	Pasta de arquivos	
OSX.MacSecurity	08/10/2020 14:56	Pasta de arquivos	
Ransomware.Cerber	08/10/2020 14:56	Pasta de arquivos	
Ransomware.Cryptowall	08/10/2020 14:56	Pasta de arquivos	
Ransomware.Jigsaw	08/10/2020 14:56	Pasta de arquivos	
Ransomware.Locky	08/10/2020 14:56	Pasta de arquivos	
Ransomware.Mamba	08/10/2020 14:56	Pasta de arquivos	
Ransomware.Petya	08/10/2020 14:56	Pasta de arquivos	
TrojanWin32.Duqu.Stuxnet	08/10/2020 14:56	Pasta de arquivos	
VBS.Carnival	08/10/2020 14:56	Pasta de arquivos	
VBS.NewLove.A	08/10/2020 14:56	Pasta de arquivos	
VBS.RunScript	08/10/2020 14:56	Pasta de arquivos	
Win32.APT28.SekoiaRootkit	08/10/2020 14:56	Pasta de arquivos	
Win32.Stuxnet.B.Duqu-Realtek	08/10/2020 14:56	Pasta de arquivos	
Win32Dircrypt.Trojan.Ransom.ABZ	08/10/2020 14:56	Pasta de arquivos	
Zerolocker	08/10/2020 14:56	Pasta de arquivos	
Android.Spy.49_iBanking_Feb2014.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	1.620 KB
Backdoor.MSIL.Tyupkin.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	575 KB
CryptoLocker_22Jan2014.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	336 KB
EquationGroup.DoubleFantasy.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	92 KB
EquationGroup.EquationDrug.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	331 KB
EquationGroup.EquationLaser.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	76 KB
EquationGroup.Fanny.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	99 KB
EquationGroup.TripleFantasy.zip	08/10/2020 14:14	Arquivo ZIP do WinRAR	10 KB
13th.416.B.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	1 KB

66 itens 33 itens selecionados 47,7 MB

Digite aqui para pesquisar
Process Explorer - Sysinternals: www.sysinternals.com [THREAT-HUNTING-\Thor]
File
Options
View
Process
Find
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	59.66	60 K	8 K	0		
procexp64.exe	12.19	21.512 K	34.720 K	4512	Sysinternals Process Explorer	Sysinternals - www.sysinter...
explorer.exe	9.88	71.920 K	115.996 K	3856	Windows Explorer	Microsoft Corporation
dwm.exe	6.27	231.572 K	130.976 K	968		
Interrupts	4.68	0 K	0 K	n/a	Hardware Interrupts and DPCs	
System	2.13	196 K	24 K	4		
Taskmgr.exe	2.06	23.560 K	27.920 K	3268		
csrss.exe	0.75	1.880 K	2.000 K	532		
SearchProtocolHost.exe	0.62	3.896 K	16.316 K	7948		
SearchFilterHost.exe	0.40	3.108 K	14.244 K	5628		
vmtoolsd.exe	0.31	11.496 K	7.440 K	1612	VMware Tools Core Service	VMware, Inc.
svchost.exe	0.19	79.356 K	36.304 K	400	Processo de Host para Servi...	Microsoft Corporation
vmtoolsd.exe	0.15	24.372 K	13.264 K	6056	VMware Tools Core Service	VMware, Inc.
chrome.exe	0.15	88.072 K	88.544 K	5572	Google Chrome	Google LLC
svchost.exe	0.13	9.328 K	13.028 K	1308	Processo de Host para Servi...	Microsoft Corporation
powershell.exe	0.07	60.296 K	22.428 K	5660		
svchost.exe	0.06	9.756 K	15.480 K	816	Processo de Host para Servi...	Microsoft Corporation
chrome.exe	0.05	78.316 K	67.272 K	5584	Google Chrome	Google LLC
chrome.exe	0.04	50.956 K	99.816 K	5616	Google Chrome	Google LLC
[illegible]	0.03	31.312 K	14.536 K	636	Processo de Host para Servi...	Microsoft Corporation
CSFalconService.exe	0.03	10.380 K	5.644 K	1600	CrowdStrike Falcon Sensor ...	CrowdStrike, Inc.
WindowsInternal.ComposableSh...	0.03	11.080 K	7.652 K	4252	WindowsInternal.Composabl...	Microsoft Corporation
svchost.exe	0.02	6.708 K	9.440 K	880	Processo de Host para Servi...	Microsoft Corporation
svchost.exe	0.02	11.184 K	15.432 K	1136	Processo de Host para Servi...	Microsoft Corporation
lsass.exe	0.02	5.996 K	6.736 K	656	Local Security Authority Proc...	Microsoft Corporation
svchost.exe	0.01	19.792 K	14.432 K	672	Processo de Host para Servi...	Microsoft Corporation
SearchIndexer.exe	0.01	25.920 K	24.592 K	1340	Indexador do Microsoft Wind...	Microsoft Corporation
notepad++.exe	0.01	18.120 K	14.000 K	2896	Notepad++ : a free (GNU) so...	Don HO don.h@free.fr
Memory Compression	0.01	932 K	43.248 K	1452		
svchost.exe	0.01	13.168 K	18.148 K	3920	Processo de Host para Servi...	Microsoft Corporation
conhost.exe	0.01	6.212 K	7.996 K	3980		
chrome.exe	< 0.01	28.172 K	64.232 K	5064	Google Chrome	Google LLC
svchost.exe	< 0.01	60.256 K	47.840 K	64	Processo de Host para Servi...	Microsoft Corporation
CSFalconContainer.exe	< 0.01	5.960 K	31.900 K	6380		
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Microsoft Corporation
wininit.exe		1.336 K	164 K	516		
WindowsInternal.ComposableSh...		11.080 K	7.652 K	4252	WindowsInternal.Composabl...	Microsoft Corporation
vmacthlp.exe		1.600 K	788 K	1372	VMware Activation Helper	VMware, Inc.
VGAuthService.exe		4.544 K	1.200 K	1548	VMware Guest Authenticatio...	VMware, Inc.
taskhostw.exe		6.428 K	10.984 K	3996	Processo de Host para Taref...	Microsoft Corporation
taskhostw.exe		9.080 K	4.876 K	3352		
svchost.exe		9.328 K	13.028 K	1308	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		11.184 K	15.432 K	1136	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		2.600 K	2.968 K	1656	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		13.168 K	18.148 K	3920	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		1.912 K	2.928 K	5436	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		15.168 K	15.856 K	2040	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		12.436 K	12.856 K	1668	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		3.216 K	8.068 K	1536	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		4.824 K	1.852 K	1696	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		7.408 K	7.964 K	1776	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		2.144 K	3.896 K	1624	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		1.528 K	1.784 K	1628	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		3.320 K	7.300 K	2252	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		1.800 K	1.484 K	2036	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		1.620 K	3.288 K	1948	Processo de Host para Servi...	Microsoft Corporation
svchost.exe		2.332 K	2.052 K	1892	Processo de Host para Servi...	Microsoft Corporation

CPU Usage: 40.34% Commit Charge: 56.09% Processes: 92

Image 1.5: Extraction of 33 Folders with malicious files

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

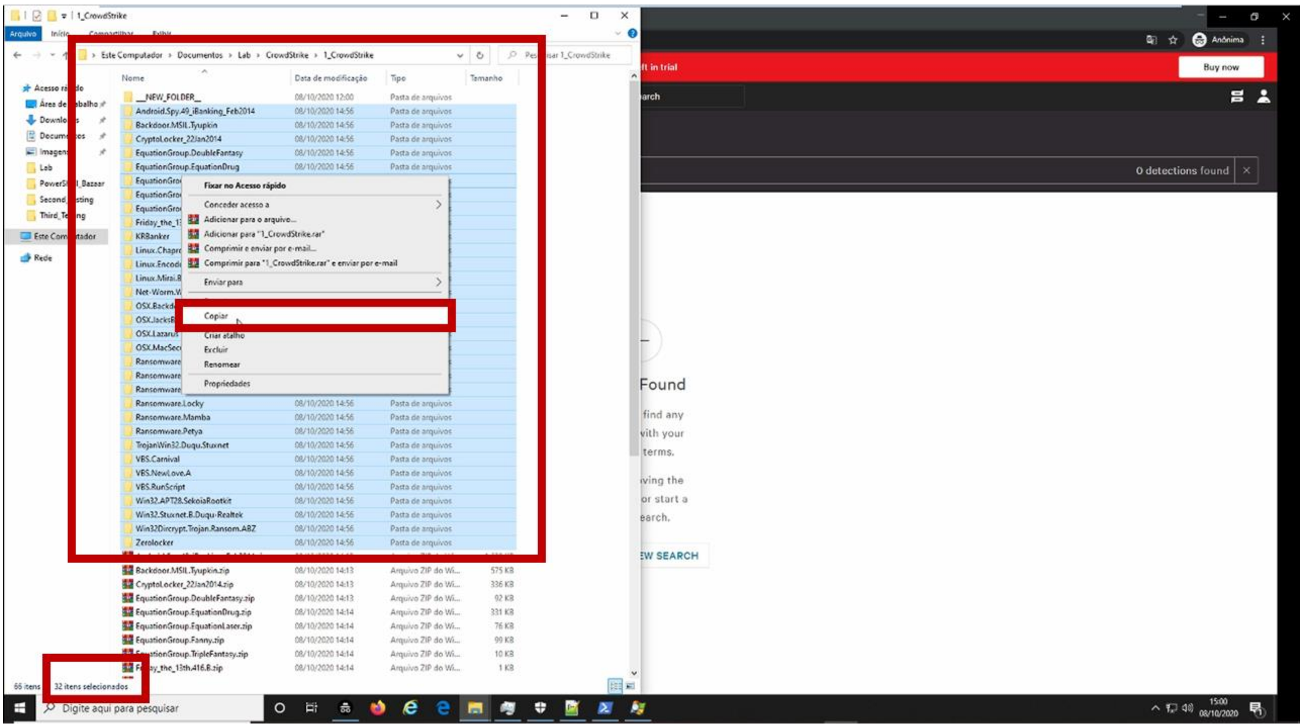
Machine learning (ML) is used for pre-execution prevention. Falcon Host employs sophisticated machine learning algorithms that can analyze millions of file characteristics to determine if a file is malicious. ***This signature-less technology enables Falcon Host to detect and block both known and unknown 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/

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.

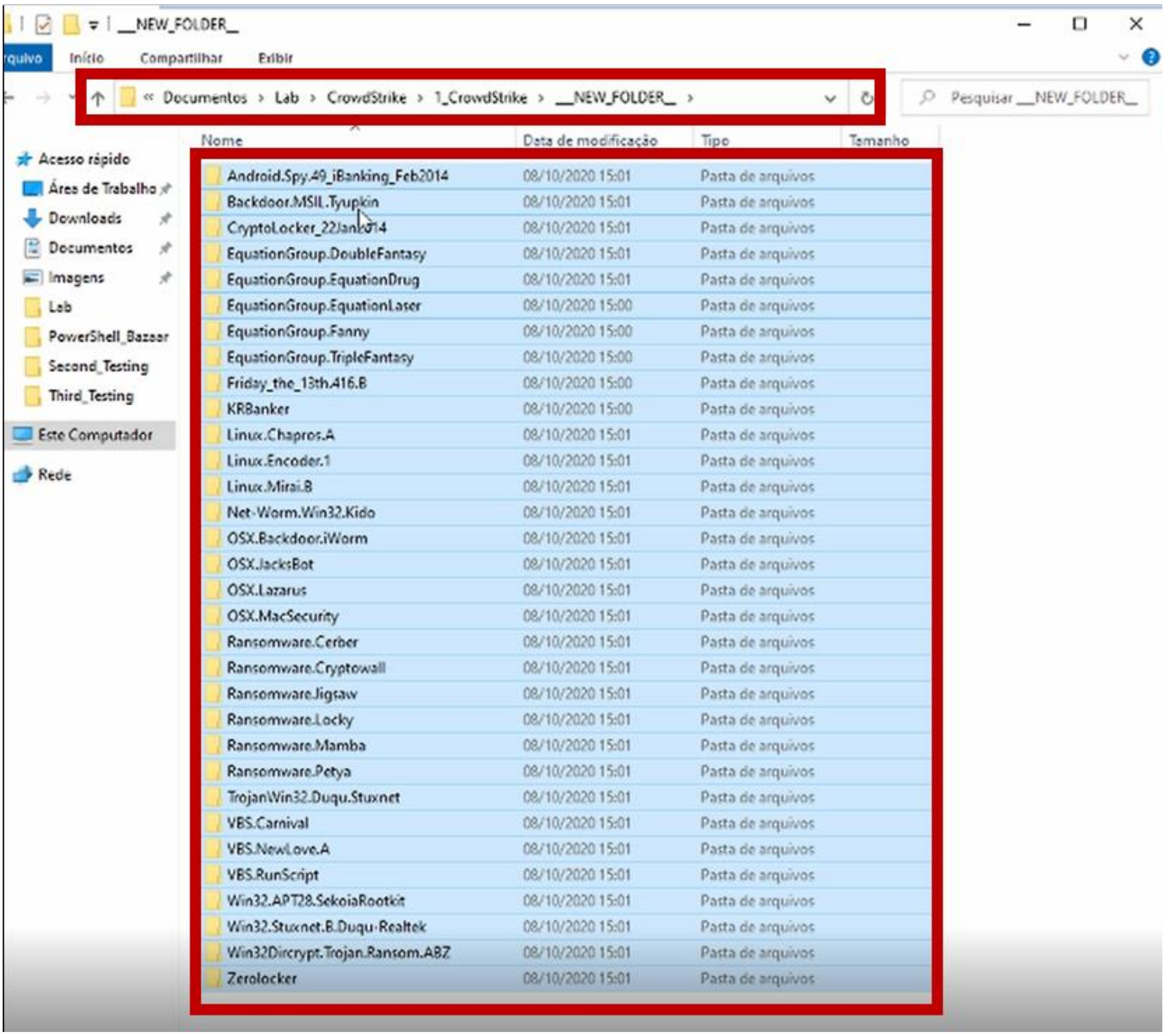


Nome	Data de modificação	Tipo	Tamanho
__NEW_FOLDER__	08/10/2020 12:00	Pasta de arquivos	
Android.Spy.49_iBanking_Feb2014	08/10/2020 14:56	Pasta de arquivos	
Backdoor.MSIL.Tyupkin	08/10/2020 14:56	Pasta de arquivos	
CryptoLocker_22Jan2014	08/10/2020 14:56	Pasta de arquivos	
EquationGroup.DoubleFantasy	08/10/2020 14:56	Pasta de arquivos	
EquationGroup.EquationDrug	08/10/2020 14:56	Pasta de arquivos	
EquationGro			
EquationGro			
EquationGro			
Friday_the_1			
KRBanker			
Linux.Chapro			
Linux.Encode			
Linux.Mirai.B			
Net-Worm.W			
OSX.Backd			
OSX.JacksR			
OSX.Lazarus			
OSX.MacSec			
Ransomware			
Ransomware			
Ransomware			
Ransomware.Locky	08/10/2020 14:56	Pasta de arquivos	
Ransomware.Mamba	08/10/2020 14:56	Pasta de arquivos	
Ransomware.Petya	08/10/2020 14:56	Pasta de arquivos	
TrojanWin32.Duqu.Stuxnet	08/10/2020 14:56	Pasta de arquivos	
VBS.Carnival	08/10/2020 14:56	Pasta de arquivos	
VBS.NewLove.A	08/10/2020 14:56	Pasta de arquivos	
VBS.RunScript	08/10/2020 14:56	Pasta de arquivos	
Win32.APT28.SekoiaRootkit	08/10/2020 14:56	Pasta de arquivos	
Win32.Stuxnet.B.Duqu-Realtek	08/10/2020 14:56	Pasta de arquivos	
Win32Dircrypt.Trojan.Ransom.ABZ	08/10/2020 14:56	Pasta de arquivos	
Zerolocker	08/10/2020 14:56	Pasta de arquivos	
Backdoor.MSIL.Tyupkin.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	575 KB
CryptoLocker_22Jan2014.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	336 KB
EquationGroup.DoubleFantasy.zip	08/10/2020 14:13	Arquivo ZIP do Wi...	92 KB
EquationGroup.EquationDrug.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	331 KB
EquationGroup.EquationLaser.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	76 KB
EquationGroup.Fanny.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	99 KB
EquationGroup.TripleFantasy.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	10 KB
Friday_the_13th.416.B.zip	08/10/2020 14:14	Arquivo ZIP do Wi...	1 KB

Image 1.7: __NEW_FOLDER__(CrowdStrike) – 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 32 folders 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`).



« Documentos › Lab › CrowdStrike › 1_CrowdStrike › __NEW_FOLDER__ ›

Nome	Data de modificação	Tipo	Tamanho
Android.Spy.49_iBanking_Feb2014	08/10/2020 15:01	Pasta de arquivos	
Backdoor.MSIL.Tyupkin	08/10/2020 15:01	Pasta de arquivos	
CryptoLocker_22Jan2014	08/10/2020 15:01	Pasta de arquivos	
EquationGroup.DoubleFantasy	08/10/2020 15:01	Pasta de arquivos	
EquationGroup.EquationDrug	08/10/2020 15:01	Pasta de arquivos	
EquationGroup.EquationLaser	08/10/2020 15:00	Pasta de arquivos	
EquationGroup.Fanny	08/10/2020 15:00	Pasta de arquivos	
EquationGroup.TripleFantasy	08/10/2020 15:00	Pasta de arquivos	
Friday_the_13th.416.B	08/10/2020 15:00	Pasta de arquivos	
KRBanker	08/10/2020 15:00	Pasta de arquivos	
Linux.Chapros.A	08/10/2020 15:01	Pasta de arquivos	
Linux.Encoder.1	08/10/2020 15:01	Pasta de arquivos	
Linux.Mirai.B	08/10/2020 15:01	Pasta de arquivos	
Net-Worm.Win32.Kido	08/10/2020 15:01	Pasta de arquivos	
OSX.Backdoor.iWorm	08/10/2020 15:01	Pasta de arquivos	
OSX.JacksBot	08/10/2020 15:01	Pasta de arquivos	
OSX.Lazarus	08/10/2020 15:01	Pasta de arquivos	
OSX.MacSecurity	08/10/2020 15:01	Pasta de arquivos	
Ransomware.Cerber	08/10/2020 15:01	Pasta de arquivos	
Ransomware.Cryptowall	08/10/2020 15:01	Pasta de arquivos	
Ransomware.Jigsaw	08/10/2020 15:01	Pasta de arquivos	
Ransomware.Locky	08/10/2020 15:01	Pasta de arquivos	
Ransomware.Mamba	08/10/2020 15:01	Pasta de arquivos	
Ransomware.Petya	08/10/2020 15:01	Pasta de arquivos	
TrojanWin32.Duqu.Stuxnet	08/10/2020 15:01	Pasta de arquivos	
VBS.Carnival	08/10/2020 15:01	Pasta de arquivos	
VBS.NewLove.A	08/10/2020 15:01	Pasta de arquivos	
VBS.RunScript	08/10/2020 15:01	Pasta de arquivos	
Win32.APT28.SekoiaRootkit	08/10/2020 15:01	Pasta de arquivos	
Win32.Stuxnet.B.Duqu-Realtek	08/10/2020 15:01	Pasta de arquivos	
Win32Dircrypt.Trojan.Ransom.ABZ	08/10/2020 15:01	Pasta de arquivos	
Zerolocker	08/10/2020 15:01	Pasta de arquivos	

Image 1.8: Malwares – Not Detected

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.

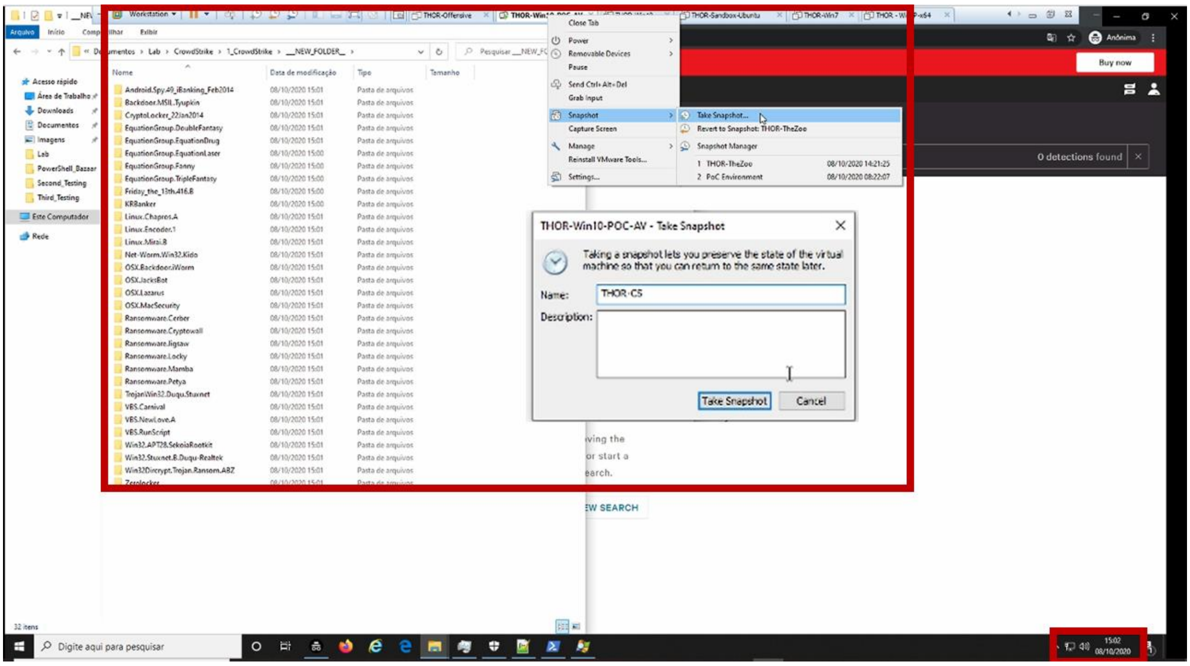
Reference: https://www.crowdstrike.com/endpoint-security-products/falcon-spotlight-vulnerability-management/

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.



Snapshot
Capture Screen
Manage
Reinstall VMware Tools...
Settings...
Take Snapshot...
Revert to Snapshot: THOR-TheZoo
Snapshot Manager
1 THOR-TheZoo 08/10/2020 14:21:25
2 PoC Environment 08/10/2020 08:22:07

THOR-Win10-POC-AV - Take Snapshot

Taking a snapshot lets you preserve the state of the virtual machine so that you can return to the same state later.

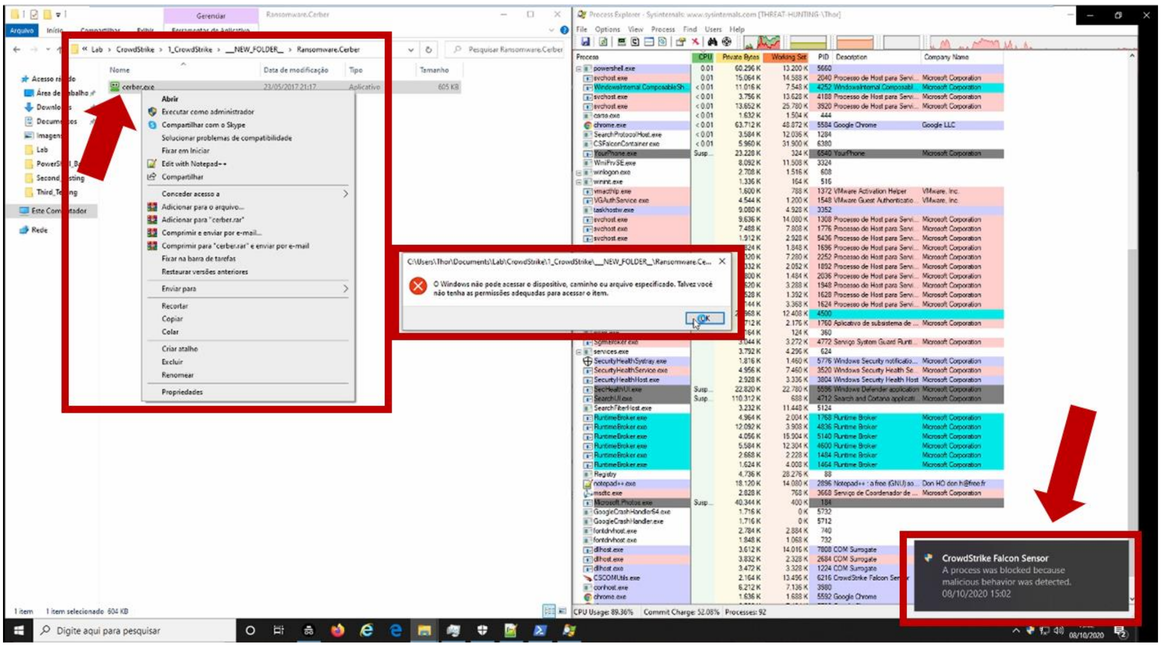
Name: THOR-CS

Description:

Take Snapshot | Cancel

Image 1.9: Snapshot

We started the manual execution of some malware chosen at random.
First malware chosen was Ransomware known as Cerber and It was BLOCKED



C:\Users\Thor\Documents\Lab\CrowdStrike\1_CrowdStrike\__NEW_FOLDER__\Ransomware.Ce...

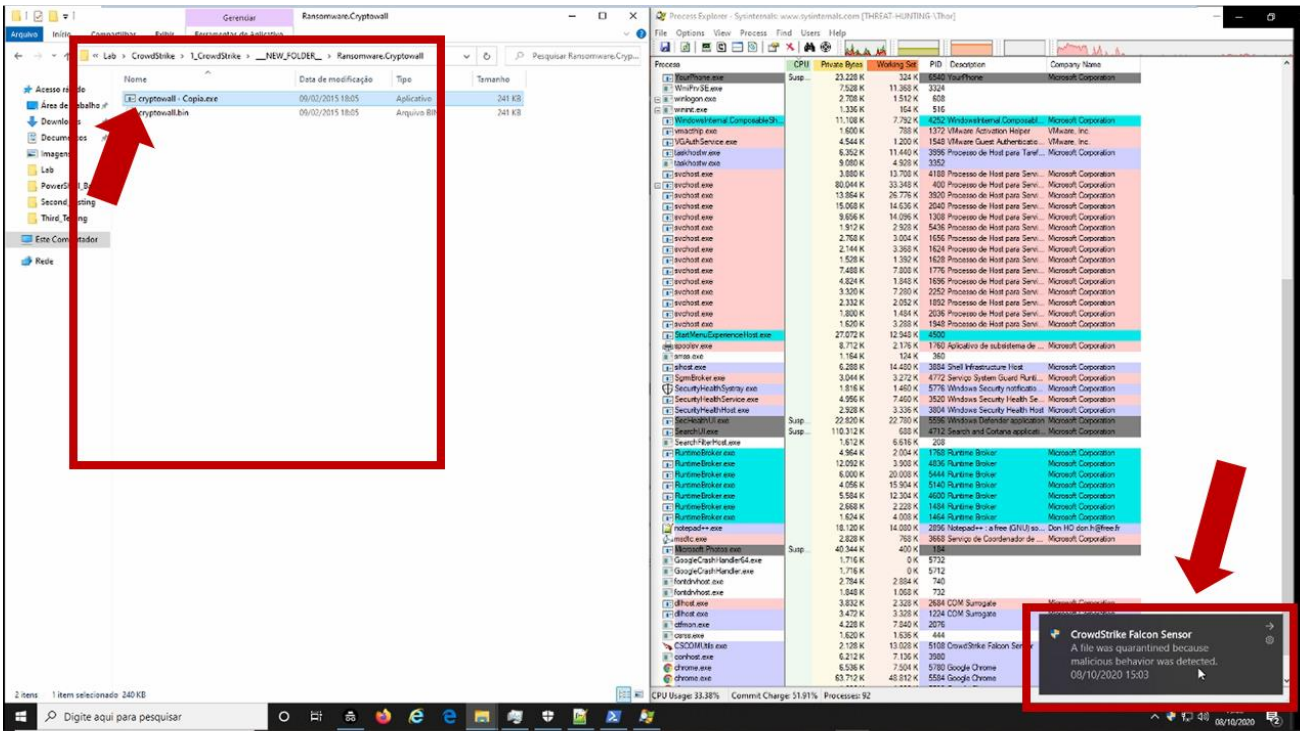
O Windows não pode acessar o dispositivo, caminho ou arquivo especificado. Talvez você não tenha as permissões adequadas para acessar o item.

OK

CrowdStrike Falcon Sensor
A process was blocked because malicious behavior was detected.
08/10/2020 15:02

Image 1.10: Ransomware Cerber - BLOCKED

Second malware chosen was Ransomware known as Cryptowall and It was BLOCKED



Nome	Data de modificação	Tipo	Tamanho
cryptowall - Cópia.exe	09/02/2015 18:05	Aplicativo	241 KB
cryptowall.bin	09/02/2015 18:05	Arquivo BIN	241 KB

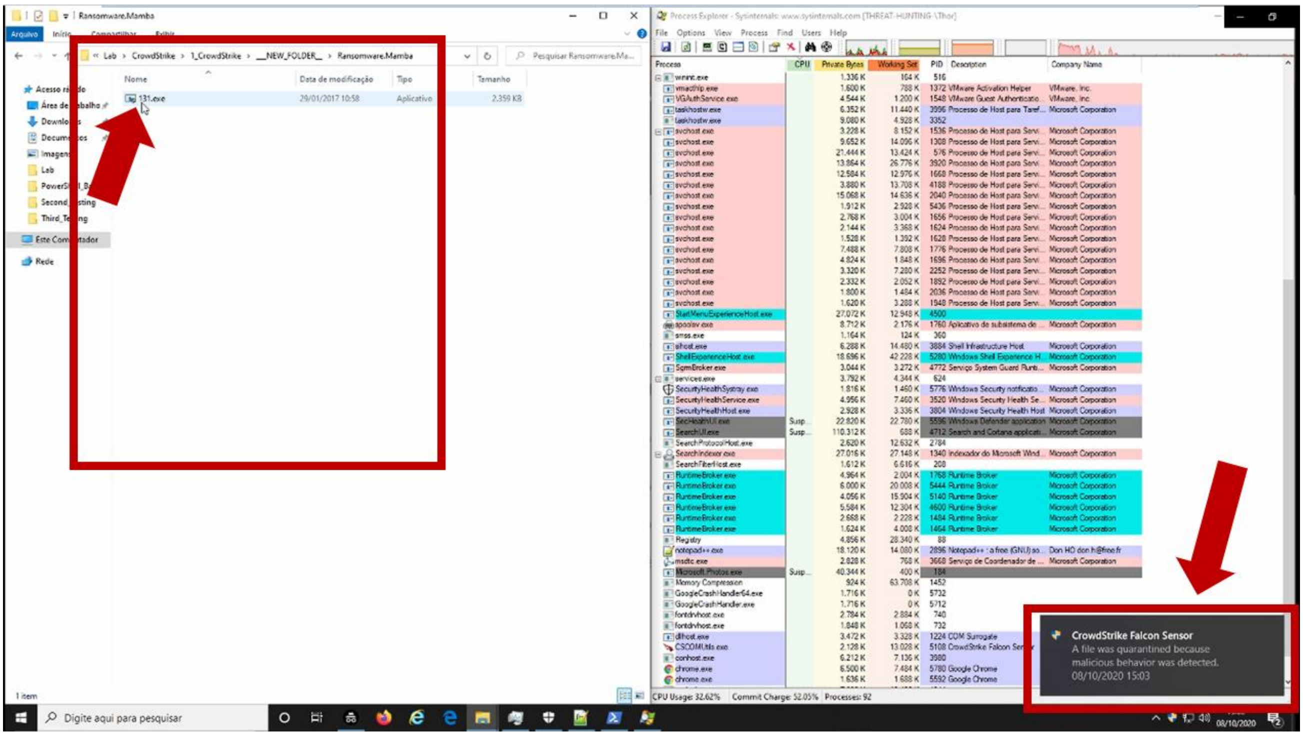
2 itens 1 item selecionado 240 KB

CPU Usage: 33.38% Commit Charge: 51.91% Processes: 92

CrowdStrike Falcon Sensor
A file was quarantined because malicious behavior was detected.
08/10/2020 15:03

Image 1.11: Ransomware Cryptowall - BLOCKED

Third malware chosen was Ransomware known as Mamba and It was BLOCKED



Nome	Data de modificação	Tipo	Tamanho
131.exe	29/01/2017 10:58	Aplicativo	2.359 KB

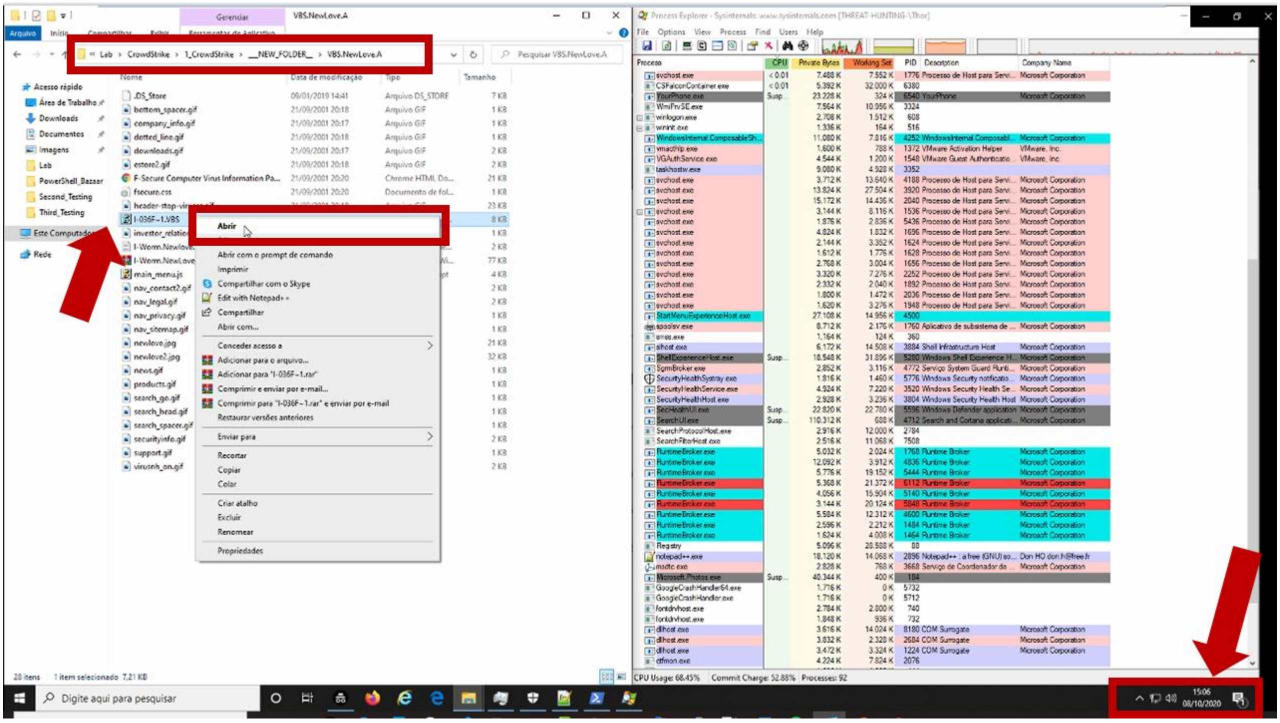
1 item

CPU Usage: 32.62% Commit Charge: 52.05% Processes: 92

CrowdStrike Falcon Sensor
A file was quarantined because malicious behavior was detected.
08/10/2020 15:03

Image 1.12: Ransomware Cryptowall - BLOCKED

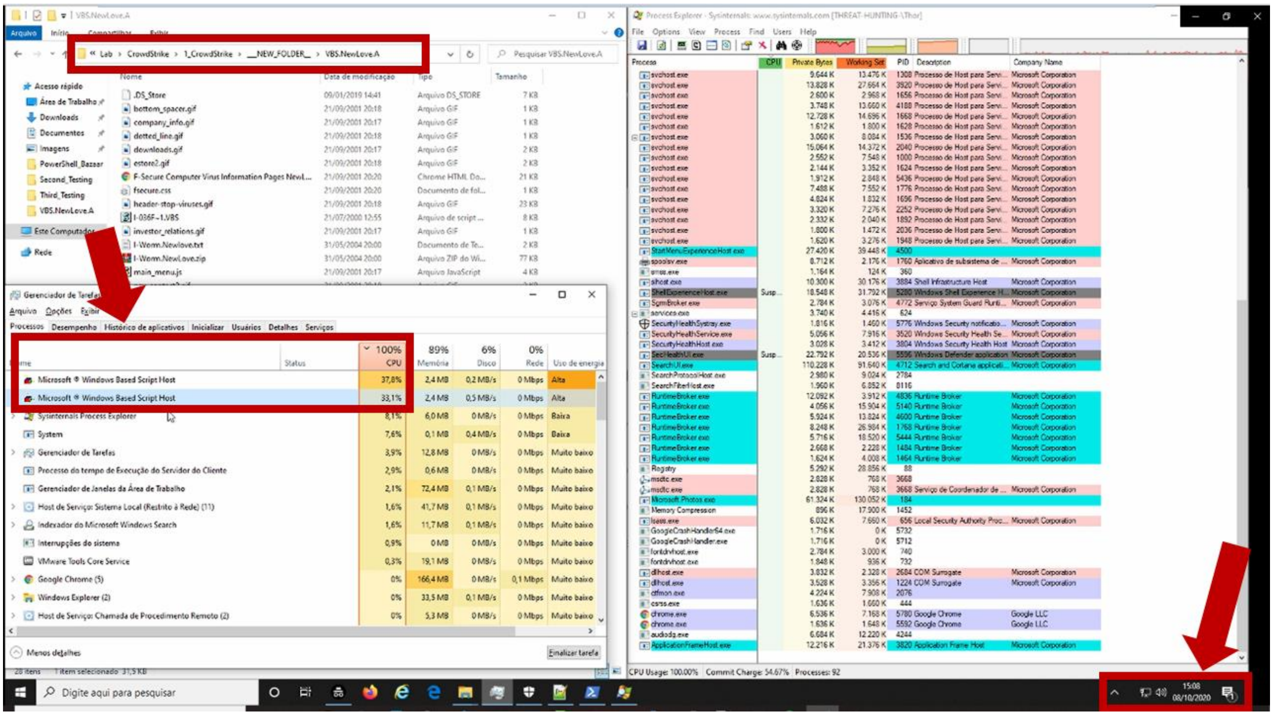
After two more test using PE (Portable Executable) file, and all those files were blocked, we tried to execute a VBS file, i.e, it's a **Virtual Basic script** written in the VBScript scripting language. It contains code that can be executed within Windows or Internet Explorer, via the Windows-based script host (Wscript.exe), to perform certain admin and processing functions.



Lab › CrowdStrike › 1_CrowdStrike › __NEW_FOLDER_ › VBS.NewLove.A
I-036F~1.VBS
Abrir
Abrir com o prompt de comando
Imprimir
Compartilhar com o Skype
Edit with Notepad++
Compartilhar
Abrir com...
Conceder acesso a
Adicionar para o arquivo...
Adicionar para "I-036F~1.rar"
Comprimir e enviar por e-mail...
Comprimir para "I-036F~1.rar" e enviar por e-mail
Restaurar versões anteriores
Enviar para
Recortar
Copiar
Colar
Criar atalho
Excluir
Renomear
Propriedades
Process Explorer - Sysinternals: www.sysinternals.com [THREAT-HUNTING\Thor]
CPU Usage: 68.45%   Commit Charge: 52.88%   Processes: 92
15:06
08/10/2020

Image 1.13: VBS Script Executed

After 2 minutes we can see that Windows-based script host (Wscript.exe) being executed in our machine, and not being blocked by CrowdStrike.



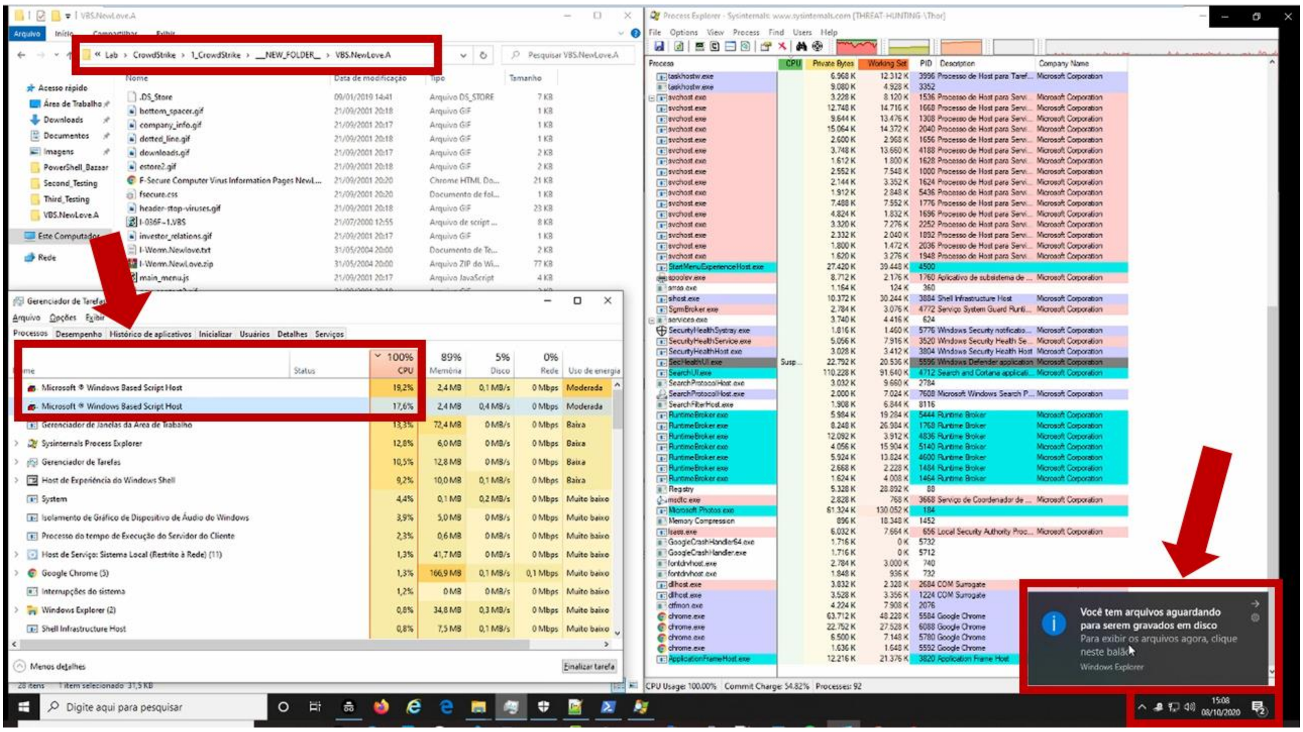
Lab › CrowdStrike › 1_CrowdStrike › __NEW_FOLDER_ › VBS.NewLove.A
Gerenciador de Tarefas
Arquivo Opções Exibir
Processos Desempenho Histórico de aplicativos Inicializar Usuários Detalhes Serviços
Menos detalhes
Finalizar tarefa
Process Explorer - Sysinternals: www.sysinternals.com [THREAT-HUNTING\Thor]
CPU Usage: 100.00%   Commit Charge: 54.67%   Processes: 92
15:08
08/10/2020

Nome	Status	100% CPU	89% Memória	6% Disco	0% Rede	Uso de energia
Microsoft ® Windows Based Script Host		37,8%	2,4 MB	0,2 MB/s	0 Mbps	Alta
Microsoft ® Windows Based Script Host		33,1%	2,4 MB	0,5 MB/s	0 Mbps	Alta
Sysinternals Process Explorer		8,1%	6,0 MB	0 MB/s	0 Mbps	Baixa
System		7,6%	0,1 MB	0,4 MB/s	0 Mbps	Baixa
Gerenciador de Tarefas		3,9%	12,8 MB	0 MB/s	0 Mbps	Muito baixo
Processo do tempo de Execução do Servidor do Cliente		2,9%	0,6 MB	0 MB/s	0 Mbps	Muito baixo
Gerenciador de Janelas da Área de Trabalho		2,1%	72,4 MB	0,1 MB/s	0 Mbps	Muito baixo
Host de Serviço: Sistema Local (Restrito à Rede) (11)		1,6%	41,7 MB	0,1 MB/s	0 Mbps	Muito baixo
Indexador do Microsoft Windows Search		1,6%	11,7 MB	0,1 MB/s	0 Mbps	Muito baixo
Interrupções do sistema		0,9%	0 MB	0 MB/s	0 Mbps	Muito baixo
VMware Tools Core Service		0,3%	19,1 MB	0 MB/s	0 Mbps	Muito baixo
Google Chrome (5)		0%	166,4 MB	0 MB/s	0,1 Mbps	Muito baixo
Windows Explorer (2)		0%	33,5 MB	0,1 MB/s	0 Mbps	Muito baixo
Host de Serviço: Chamada de Procedimento Remoto (2)		0%	5,3 MB	0 MB/s	0 Mbps	Muito baixo

Image 1.14: VBS Script executing wscript.exe process

After some seconds we can see an alert with the message in Portuguese:

“You have files waiting to be recorded to disc” as you can see below.



« Lab › CrowdStrike › 1_CrowdStrike › __NEW_FOLDER__ › VBS.NewLove.A

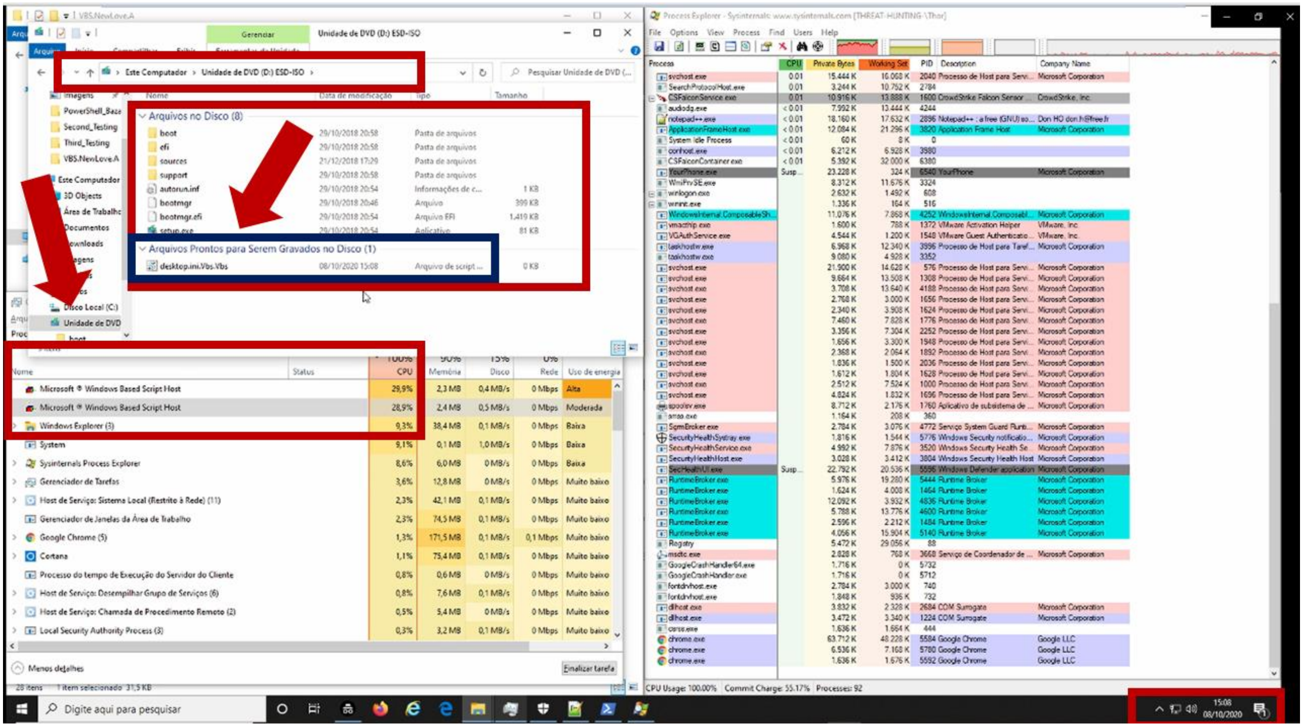
Nome	Status	CPU	Memória	Disco	Rede	Uso de energia
Microsoft ® Windows Based Script Host		19,2%	2,4 MB	0,1 MB/s	0 Mbps	Moderada
Microsoft ® Windows Based Script Host		17,6%	2,4 MB	0,4 MB/s	0 Mbps	Moderada

Você tem arquivos aguardando para serem gravados em disco
Para exibir os arquivos agora, clique neste balão
Windows Explorer

15:08
08/10/2020

Image 1.15: Alert box “You have files waiting to be recorded to disc”

When this alert it’s open, we can see that exist a ISO media on our machine, we see many files in this ISO to be performed, and we can find the *desktop.ini.Vbs.Vbs* as a file done to se executed.



Este Computador › Unidade de DVD (D:) ESD-ISO ›

Arquivos no Disco (8)

Nome	Data de modificação	Tipo	Tamanho
boot	29/10/2018 20:58	Pasta de arquivos	
efi	29/10/2018 20:58	Pasta de arquivos	
sources	21/12/2018 17:29	Pasta de arquivos	
support	29/10/2018 20:58	Pasta de arquivos	
autorun.inf	29/10/2018 20:54	Informações de c...	1 KB
bootmgr	29/10/2018 20:46	Arquivo	399 KB
bootmgr.efi	29/10/2018 20:54	Arquivo EFI	1.419 KB
setup.exe	29/10/2018 20:54	Aplicativo	81 KB

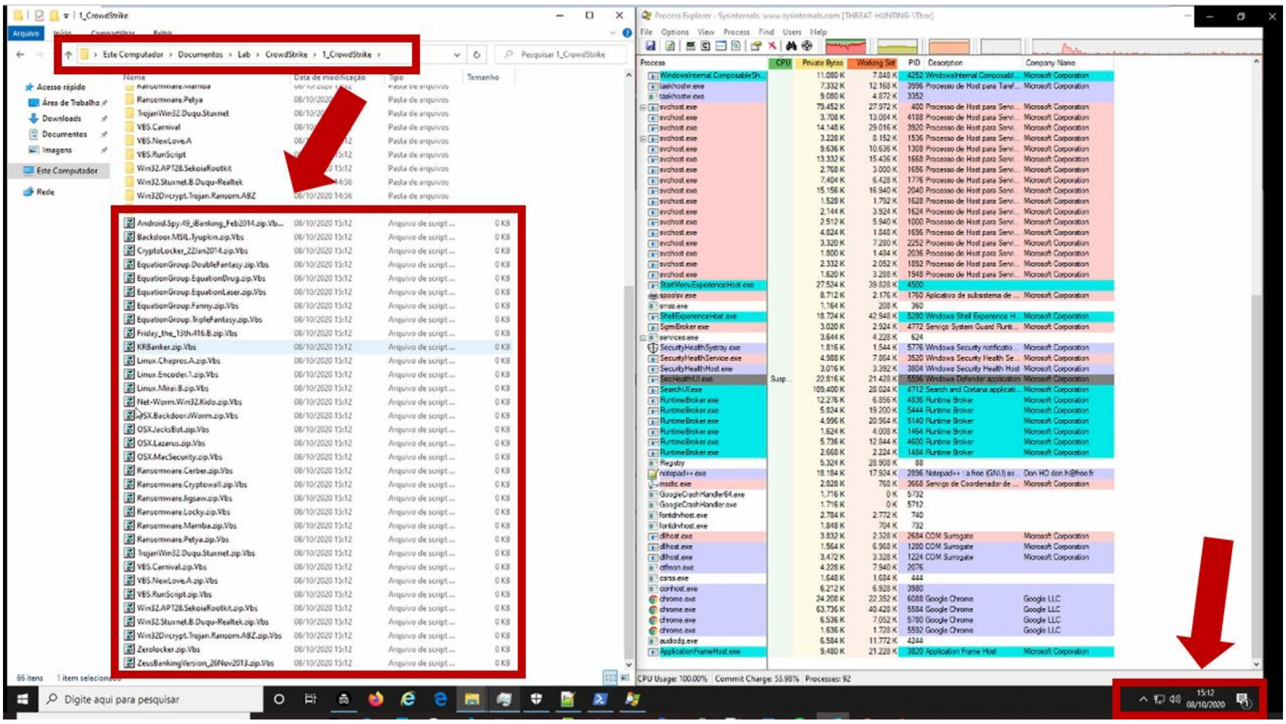
Arquivos Prontos para Serem Gravados no Disco (1)

Nome	Data de modificação	Tipo	Tamanho
desktop.ini.Vbs.Vbs	08/10/2020 15:08	Arquivo de script ...	0 KB

Nome	Status	CPU	Memória	Disco	Rede	Uso de energia
Microsoft ® Windows Based Script Host		29,9%	2,3 MB	0,4 MB/s	0 Mbps	Alta
Microsoft ® Windows Based Script Host		28,9%	2,4 MB	0,5 MB/s	0 Mbps	Moderada
Windows Explorer (3)		9,3%	38,4 MB	0,1 MB/s	0 Mbps	Baixa

Image 1.16: Alert box “You have files waiting to be recorded to disc”

After 4 min after it is possible to see an infection inside the our “victim” machine, all those file were change to extension *.Vbs* as we see in the ISO media.



› Este Computador › Documentos › Lab › CrowdStrike › 1_CrowdStrike ›

Nome	Data de modificação	Tipo	Tamanho
Ransomware.Petya	08/10/2020	Pasta de arquivos	
TrojanWin32.Duqu.Stuxnet	08/10/2020	Pasta de arquivos	
VBS.Carnival	08/10	Pasta de arquivos	
VBS.NewLove.A	08/	Pasta de arquivos	
VBS.RunScript	15:12	Pasta de arquivos	
Win32.APT28.SekoiaRootkit	15:12	Pasta de arquivos	
Win32.Stuxnet.B.Duqu-Realtek	14:56	Pasta de arquivos	
Win32Dircrypt.Trojan.Ransom.ABZ	08/10/2020 14:56	Pasta de arquivos	
Android.Spy.49_iBanking_Feb2014.zip.Vb...	08/10/2020 15:12	Arquivo de script ...	0 KB
Backdoor.MSIL.Tyupkin.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
CryptoLocker_22Jan2014.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
EquationGroup.DoubleFantasy.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
EquationGroup.EquationDrug.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
EquationGroup.EquationLaser.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
EquationGroup.Fanny.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
EquationGroup.TripleFantasy.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Friday_the_13th.416.B.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
KRBanker.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Linux.Chapros.A.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Linux.Encoder.1.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Linux.Mirai.B.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Net-Worm.Win32.Kido.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
OSX.Backdoor.iWorm.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
OSX.JacksBot.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
OSX.Lazarus.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
OSX.MacSecurity.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Ransomware.Cerber.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Ransomware.Cryptowall.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Ransomware.Jigsaw.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Ransomware.Locky.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Ransomware.Mamba.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Ransomware.Petya.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
TrojanWin32.Duqu.Stuxnet.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
VBS.Carnival.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
VBS.NewLove.A.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
VBS.RunScript.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Win32.APT28.SekoiaRootkit.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Win32.Stuxnet.B.Duqu-Realtek.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Win32Dircrypt.Trojan.Ransom.ABZ.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
Zerolocker.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB
ZeusBankingVersion_26Nov2013.zip.Vbs	08/10/2020 15:12	Arquivo de script ...	0 KB

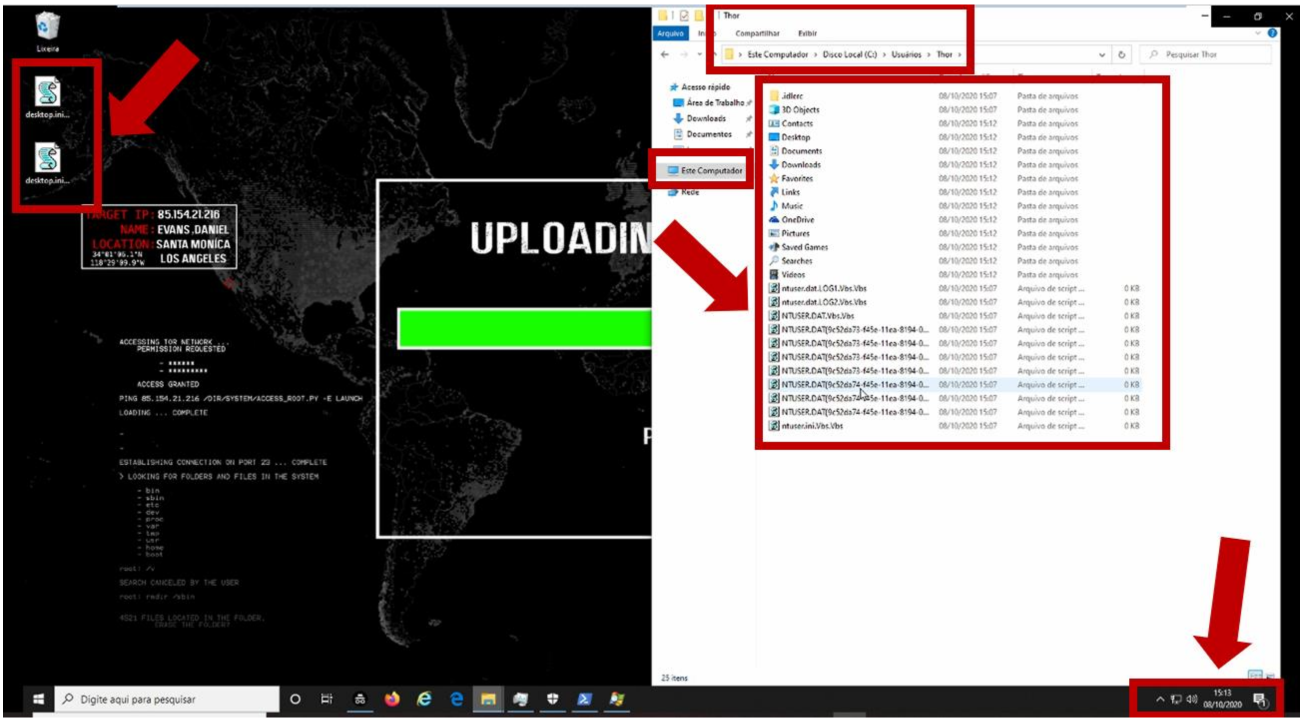
66 itens 1 item selecionado

CPU Usage: 100.00% Commit Charge: 53.98% Processes: 92

Process Explorer - Sysinternals: www.sysinternals.com [THREAT-HUNTING\Thor]
File Options View Process Find Users Help
Digite aqui para pesquisar
15:12
08/10/2020

Image 1.17: Infection Happening

As we can see below, this malware is associated with the execution of VBS - Visual Basic Script and he change all extension in the victim environment.



```
TARGET IP: 85.154.21.216
     NAME: EVANS,DANIEL
 LOCATION: SANTA MONICA
34°01'96.1"N    LOS ANGELES
118°29'99.9"W

ACCESSING TOR NETWORK ...
    PERMISSION REQUESTED

        - ******
        - *********

    ACCESS GRANTED

PING 85.154.21.216 /DIR/SYSTEM/ACCESS_ROOT.PY -E LAUNCH

LOADING ... COMPLETE

-

-

ESTABLISHING CONNECTION ON PORT 23 ... COMPLETE

> LOOKING FOR FOLDERS AND FILES IN THE SYSTEM

    - bin
    - sbin
    - etc
    - dev
    - proc
    - var
    - tmp
    - usr
    - home
    - boot

root: /v

SEARCH CANCELED BY THE USER

root: rmdir /sbin

4521 FILES LOCATED IN THE FOLDER.
        ERASE THE FOLDER?
```

UPLOADIN

› Este Computador › Disco Local (C:) › Usuários › Thor ›

.idlerc	08/10/2020 15:07	Pasta de arquivos	
3D Objects	08/10/2020 15:07	Pasta de arquivos	
Contacts	08/10/2020 15:12	Pasta de arquivos	
Desktop	08/10/2020 15:12	Pasta de arquivos	
Documents	08/10/2020 15:12	Pasta de arquivos	
Downloads	08/10/2020 15:12	Pasta de arquivos	
Favorites	08/10/2020 15:12	Pasta de arquivos	
Links	08/10/2020 15:12	Pasta de arquivos	
Music	08/10/2020 15:12	Pasta de arquivos	
OneDrive	08/10/2020 15:12	Pasta de arquivos	
Pictures	08/10/2020 15:12	Pasta de arquivos	
Saved Games	08/10/2020 15:12	Pasta de arquivos	
Searches	08/10/2020 15:12	Pasta de arquivos	
Videos	08/10/2020 15:12	Pasta de arquivos	
ntuser.dat.LOG1.Vbs.Vbs	08/10/2020 15:07	Arquivo de script ...	0 KB
ntuser.dat.LOG2.Vbs.Vbs	08/10/2020 15:07	Arquivo de script ...	0 KB
NTUSER.DAT.Vbs.Vbs	08/10/2020 15:07	Arquivo de script ...	0 KB
NTUSER.DAT{9c52da73-f45e-11ea-8194-0...	08/10/2020 15:07	Arquivo de script ...	0 KB
NTUSER.DAT{9c52da73-f45e-11ea-8194-0...	08/10/2020 15:07	Arquivo de script ...	0 KB
NTUSER.DAT{9c52da73-f45e-11ea-8194-0...	08/10/2020 15:07	Arquivo de script ...	0 KB
NTUSER.DAT{9c52da73-f45e-11ea-8194-0...	08/10/2020 15:07	Arquivo de script ...	0 KB
NTUSER.DAT{9c52da74-f45e-11ea-8194-0...	08/10/2020 15:07	Arquivo de script ...	0 KB
NTUSER.DAT{9c52da74-f45e-11ea-8194-0...	08/10/2020 15:07	Arquivo de script ...	0 KB
NTUSER.DAT{9c52da74-f45e-11ea-8194-0...	08/10/2020 15:07	Arquivo de script ...	0 KB
ntuser.ini.Vbs.Vbs	08/10/2020 15:07	Arquivo de script ...	0 KB

25 itens

Image 1.18: Infection complete.

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.
- **Infection based on VBS (Virtual Basic Script) – Known Malware**
  - This is the big surprise.

- **I-Worm.NewLove (Source)**

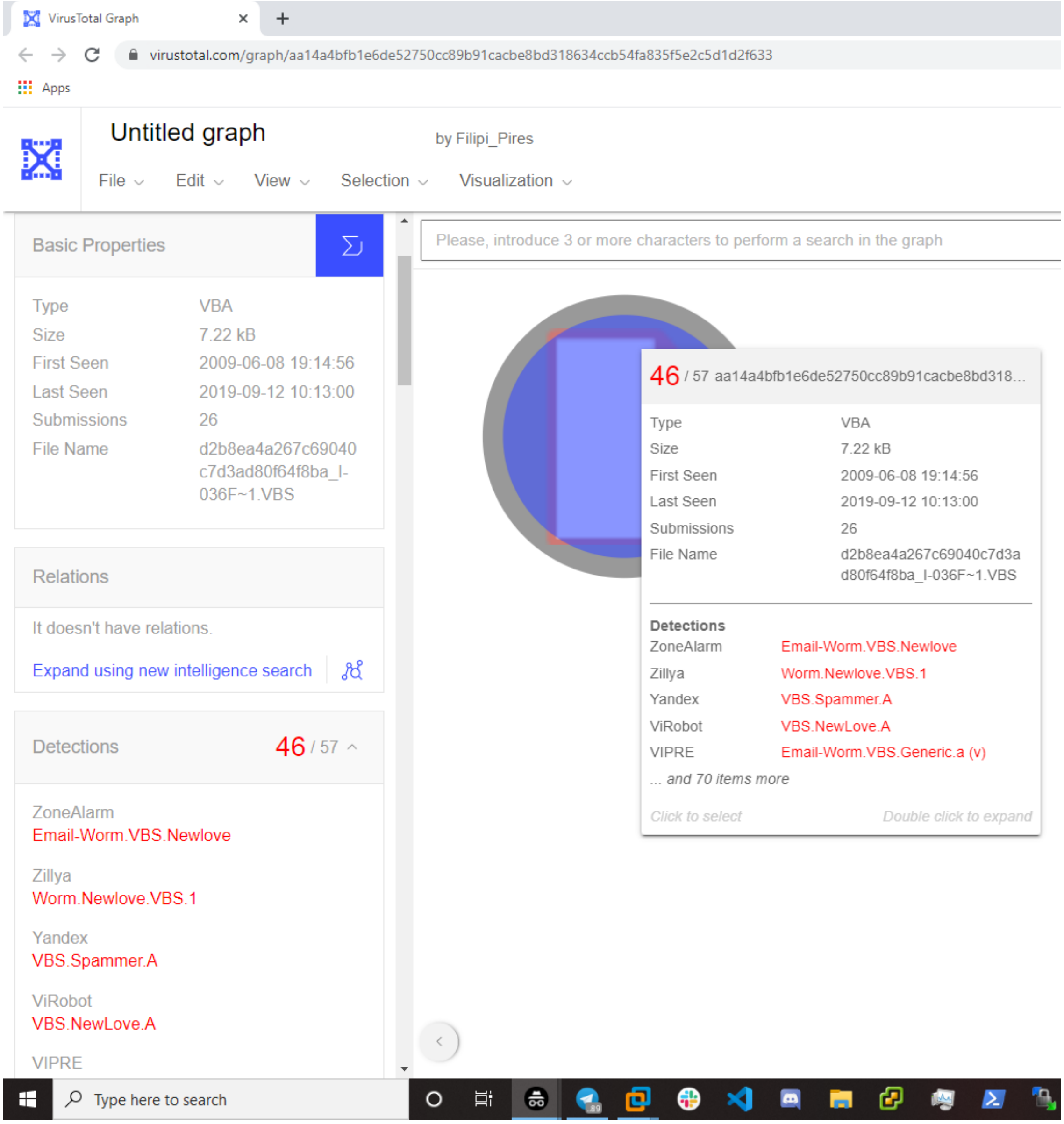
hxxps://github.com/ytisf/theZoo/tree/master/malwares/Binaries/VBS.NewLove.A

```
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.



VirusTotal Graph

virustotal.com/graph/aa14a4bfb1e6de52750cc89b91cacbe8bd318634ccb54fa835f5e2c5d1d2f633

Apps

Untitled graph

by Filipi_Pires

File Edit View Selection Visualization

Basic Properties

Type	VBA
Size	7.22 kB
First Seen	2009-06-08 19:14:56
Last Seen	2019-09-12 10:13:00
Submissions	26
File Name	d2b8ea4a267c69040c7d3ad80f64f8ba_I-036F~1.VBS

Relations

It doesn't have relations.

Expand using new intelligence search

Detections 46 / 57

ZoneAlarm
Email-Worm.VBS.Newlove

Zillya
Worm.Newlove.VBS.1

Yandex
VBS.Spammer.A

ViRobot
VBS.NewLove.A

VIPRE

Please, introduce 3 or more characters to perform a search in the graph

46 / 57 aa14a4bfb1e6de52750cc89b91cacbe8bd318...

Type	VBA
Size	7.22 kB
First Seen	2009-06-08 19:14:56
Last Seen	2019-09-12 10:13:00
Submissions	26
File Name	d2b8ea4a267c69040c7d3ad80f64f8ba_I-036F~1.VBS

Detections

ZoneAlarm	Email-Worm.VBS.Newlove
Zillya	Worm.Newlove.VBS.1
Yandex	VBS.Spammer.A
ViRobot	VBS.NewLove.A
VIPRE	Email-Worm.VBS.Generic.a (v)

... and 70 items more

Click to select Double click to expand

Type here to search

Image 1.19: I-Worm.NewLove – VirusTotal

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 will be sent to CrowdStrike Team to validate with them how the detection flow for known malware works, and why this **VBS/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;