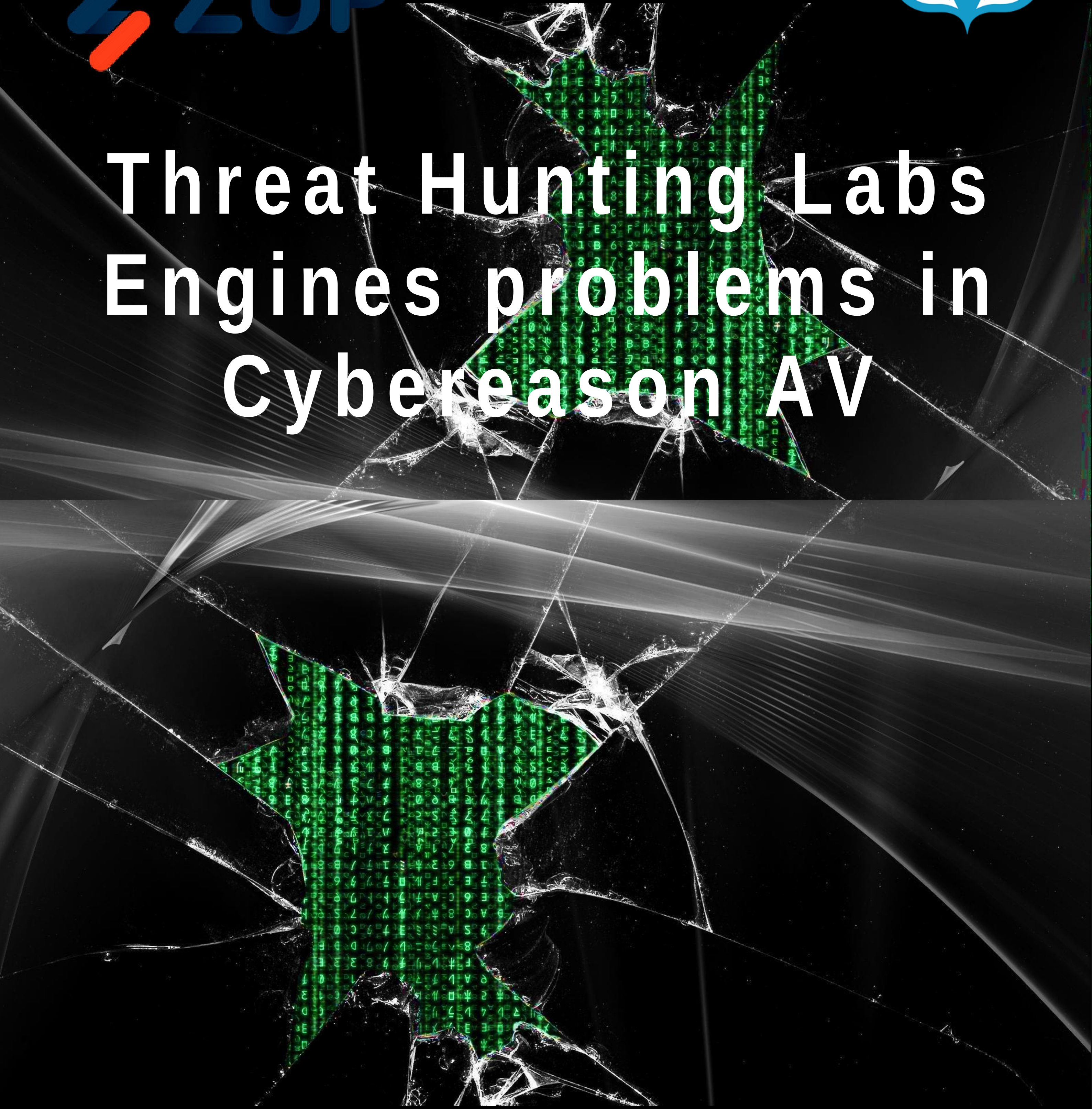
Threat Hunting Labs Engines problems in Cybereason AV



ZUP Security Labs at Zup Innovation

Researcher & CyberSecurity Manager: Filipi Pires

Abstract

There are a large number of cyber threats today, many of these cyber threats can be based on malicious code, one of this code is known as Malware (Malicious Software or Maldoc - Malicious Document) to refer these kinds of threats. The term Malware, is a generic term that covers all types of programs specifically developed to perform malicious actions on a computer, thus the term malware has become the name for any type of program specifically developed to perform harmful actions and malicious activities on a compromised system. This paper presents how it is possible to execute several efficiency and detection tests in endpoint solution, provided by Cybereason, this document brings the result of the defensive security analysis with an offensive mindset performed in the execution of 42 different Malwares in controlled environment, using three different techniques simulating a real-attack, with the final result, 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..

Keywords: MalwareAnalysis, Anti-Virus, ThreatHunting,Security.

1 Introduction

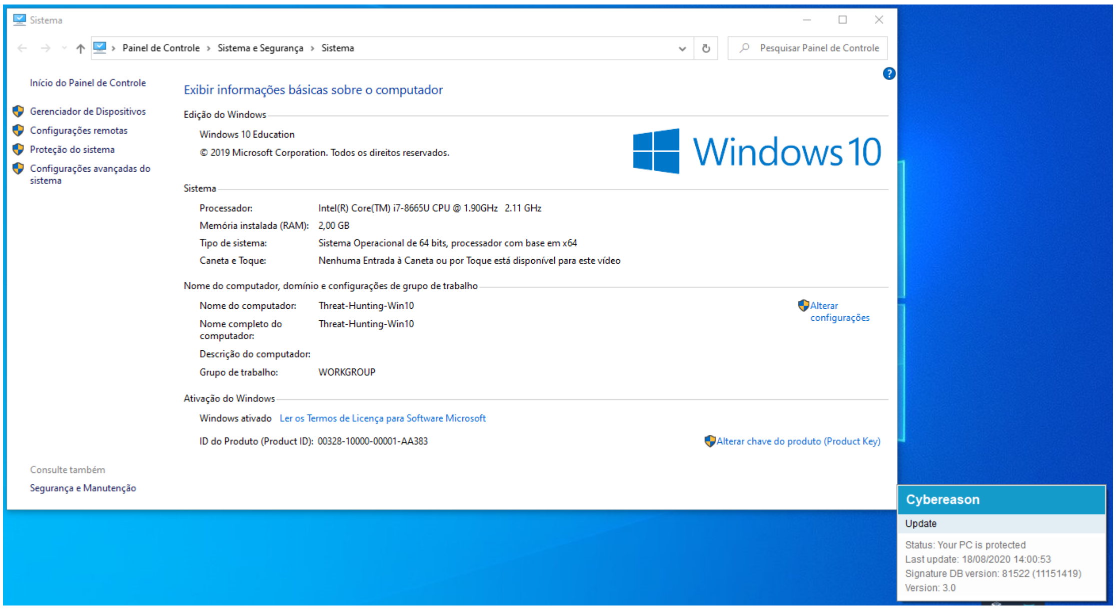
The purpose of this document, it was to execute several efficiency and detection tests in our endpoint solution, provided by Cybereason, this document brings the result of the defensive security analysis with an offensive mindset performed in the execution of 42 different Malwares in our environment.

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 42 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 *fullscan* 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 (`Cybereason Cloud Solution`) in **Version 20.1.261.0;**
Installed in the windows machine `Windows 10 Education 2019`;
Hostname - `Threat-Hunting-win10`, as you can see in the picture below:


Sistema
Painel de Controle › Sistema e Segurança › Sistema
Pesquisar Painel de Controle
Início do Painel de Controle
Gerenciador de Dispositivos
Configurações remotas
Proteção do sistema
Configurações avançadas do sistema
Windows 10
Alterar configurações
Alterar chave do produto (Product Key)
Consulte também
Segurança e Manutenção

Exibir informações básicas sobre o computador

Edição do Windows

Windows 10 Education
© 2019 Microsoft Corporation. Todos os direitos reservados.

Sistema

Processador:	Intel(R) Core(TM) i7-8665U CPU @ 1.90GHz 2.11 GHz
Memória instalada (RAM):	2,00 GB
Tipo de sistema:	Sistema Operacional de 64 bits, processador com base em x64
Caneta e Toque:	Nenhuma Entrada à Caneta ou por Toque está disponível para este vídeo

Nome do computador, domínio e configurações de grupo de trabalho

Nome do computador:	Threat-Hunting-Win10
Nome completo do computador:	Threat-Hunting-Win10
Descrição do computador:	
Grupo de trabalho:	WORKGROUP

Ativação do Windows

Windows ativado Ler os Termos de Licença para Software Microsoft

ID do Produto (Product ID): 00328-10000-00001-AA383

Cybereason
Update
Status: Your PC is protected
Last update: 18/08/2020 14:00:53
Signature DB version: 81522 (11151419)
Version: 3.0

Image 1.1: Windows 10 Education 2019 Virtual Machine

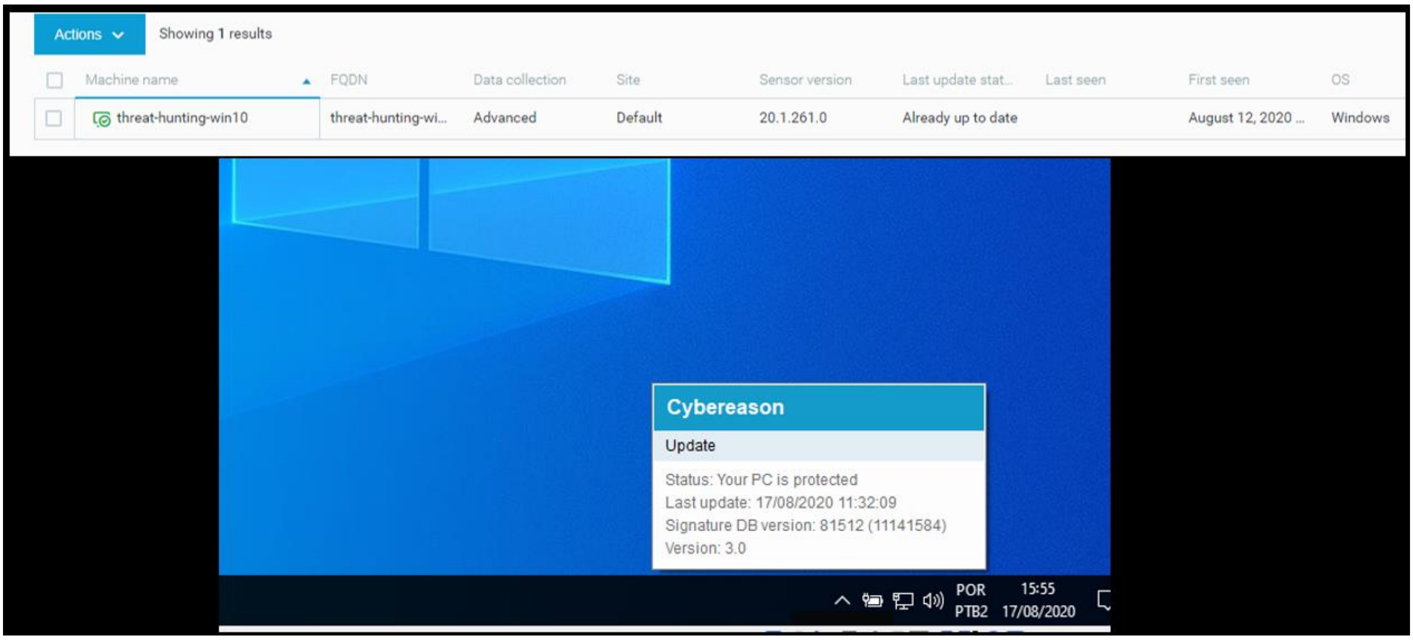
2.0.2 Project Summary

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 **4 days**, without count the weekend, along with the making of this document. The intrusion test started on the **12th of August** of the year 2020 and it was completed on the **18th of August** 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 (`ZUP - Threat Hunting – Policy`) e and applied to due device.



Showing 1 results

□	Machine name	FQDN	Data collection	Site	Sensor version	Last update stat...	Last seen	First seen	OS
□	threat-hunting-win10	threat-hunting-wi...	Advanced	Default	20.1.261.0	Already up to date		August 12, 2020 ...	Windows

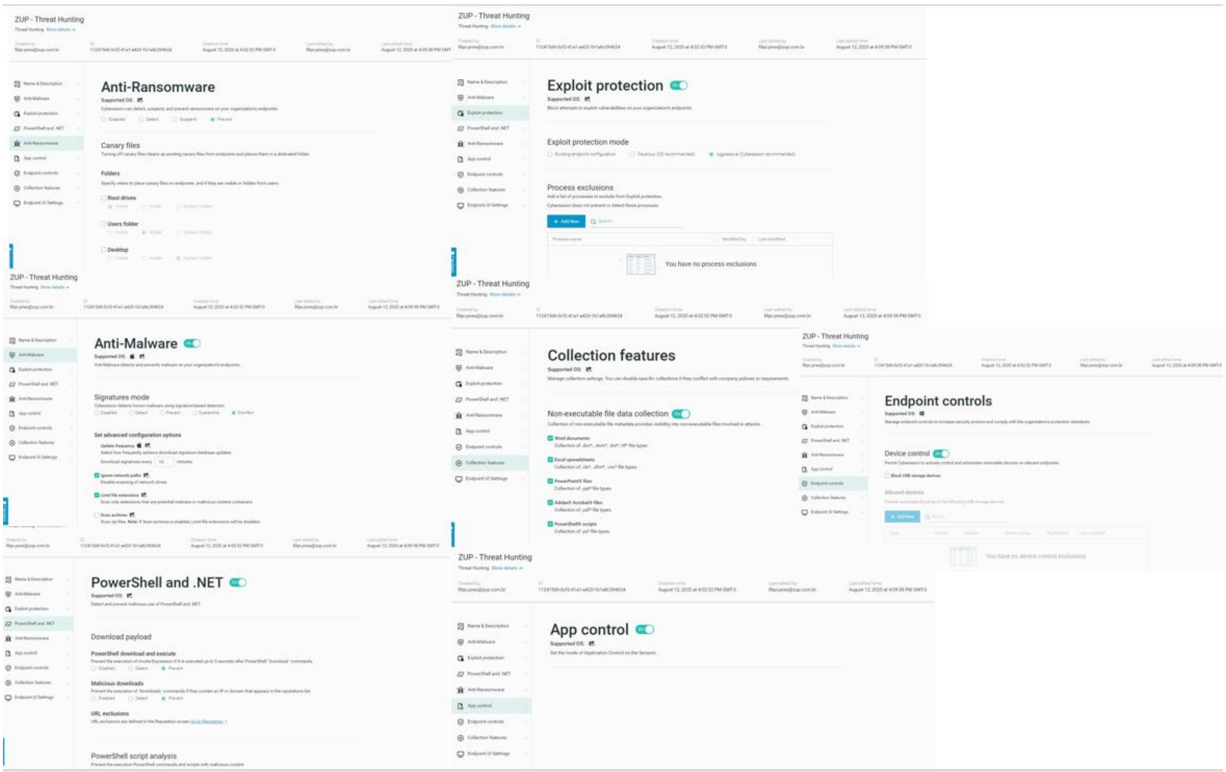
Cybereason

Update

Status: Your PC is protected
Last update: 17/08/2020 11:32:09
Signature DB version: 81512 (11141584)
Version: 3.0

Image 1.2: Virtual Machine with Policy applied

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



ZUP - Threat Hunting

Anti-Ransomware

Canary files

Folders

□ Root drives

□ Users folder

□ Desktop

ZUP - Threat Hunting

Exploit protection

Exploit protection mode

Process exclusions

You have no process exclusions

ZUP - Threat Hunting

Anti-Malware

Signatures mode

Set advanced configuration options

ZUP - Threat Hunting

Collection features

Non-executable file data collection

ZUP - Threat Hunting

Endpoint controls

Device control

ZUP - Threat Hunting

PowerShell and .NET

Download payload

PowerShell script analysis

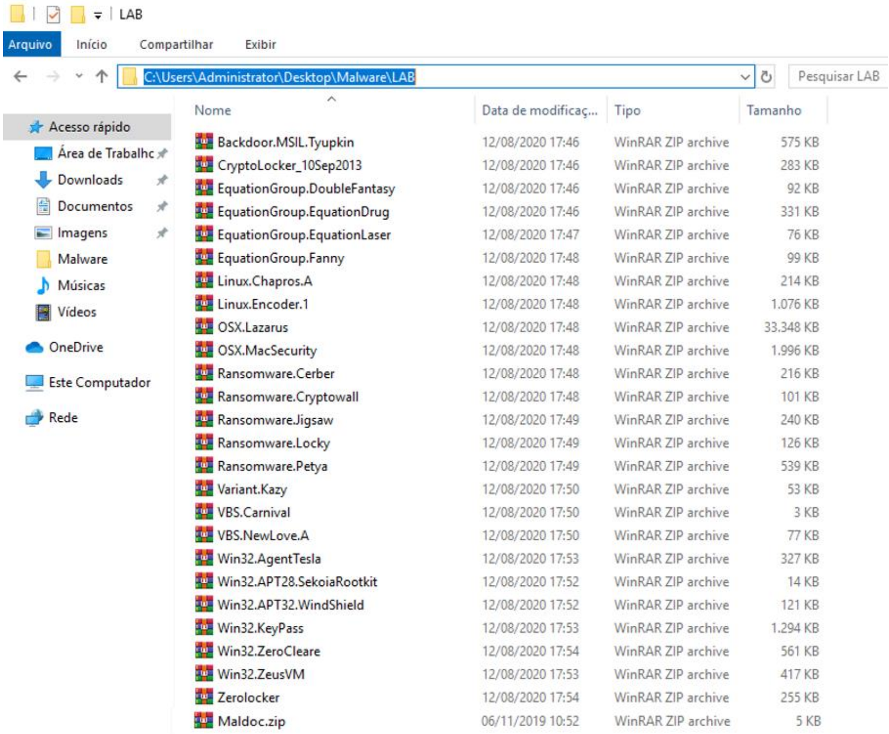
ZUP - Threat Hunting

App control

Image 1.3: Policy cretead by Cybereason Manager

3.2 First Test

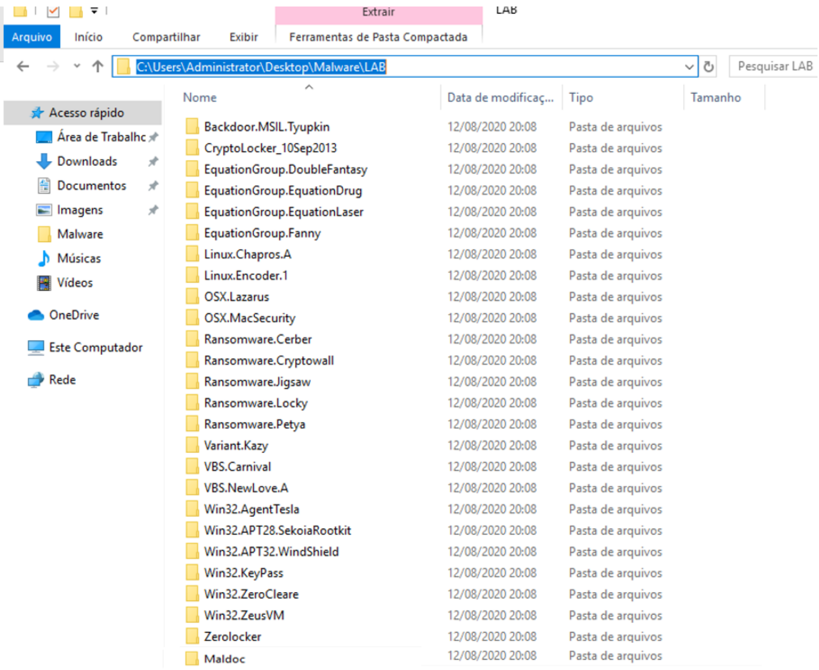
The first stage of the tests was through the download of 26 folders containing a total of 42 malware, all of which are already known to be older, all of them are in the public repository known and maintained by the security community called **The Zoo** (`https://github.com/ytisf/theZoo/tree/master/malwares/Binaries`);



Nome	Data de modificaç...	Tipo	Tamanho
Backdoor.MSIL.Tyupkin	12/08/2020 17:46	WinRAR ZIP archive	575 KB
CryptoLocker_10Sep2013	12/08/2020 17:46	WinRAR ZIP archive	283 KB
EquationGroup.DoubleFantasy	12/08/2020 17:46	WinRAR ZIP archive	92 KB
EquationGroup.EquationDrug	12/08/2020 17:46	WinRAR ZIP archive	331 KB
EquationGroup.EquationLaser	12/08/2020 17:47	WinRAR ZIP archive	76 KB
EquationGroup.Fanny	12/08/2020 17:48	WinRAR ZIP archive	99 KB
Linux.Chapros.A	12/08/2020 17:48	WinRAR ZIP archive	214 KB
Linux.Encoder.1	12/08/2020 17:48	WinRAR ZIP archive	1.076 KB
OSX.Lazarus	12/08/2020 17:48	WinRAR ZIP archive	33.348 KB
OSX.MacSecurity	12/08/2020 17:48	WinRAR ZIP archive	1.996 KB
Ransomware.Cerber	12/08/2020 17:48	WinRAR ZIP archive	216 KB
Ransomware.Cryptowall	12/08/2020 17:48	WinRAR ZIP archive	101 KB
Ransomware.Jigsaw	12/08/2020 17:49	WinRAR ZIP archive	240 KB
Ransomware.Locky	12/08/2020 17:49	WinRAR ZIP archive	126 KB
Ransomware.Petya	12/08/2020 17:49	WinRAR ZIP archive	539 KB
Variant.Kazy	12/08/2020 17:50	WinRAR ZIP archive	53 KB
VBS.Carnival	12/08/2020 17:50	WinRAR ZIP archive	3 KB
VBS.NewLove.A	12/08/2020 17:50	WinRAR ZIP archive	77 KB
Win32.AgentTesla	12/08/2020 17:53	WinRAR ZIP archive	327 KB
Win32.APT28.SekoiaRootkit	12/08/2020 17:52	WinRAR ZIP archive	14 KB
Win32.APT32.WindShield	12/08/2020 17:52	WinRAR ZIP archive	121 KB
Win32.KeyPass	12/08/2020 17:53	WinRAR ZIP archive	1.294 KB
Win32.ZeroCleare	12/08/2020 17:54	WinRAR ZIP archive	561 KB
Win32.ZeusVM	12/08/2020 17:53	WinRAR ZIP archive	417 KB
Zerolocker	12/08/2020 17:54	WinRAR ZIP archive	255 KB
Maldoc.zip	06/11/2019 10:52	WinRAR ZIP archive	5 KB

Image 1.4: Download 26 Folders with malicious files

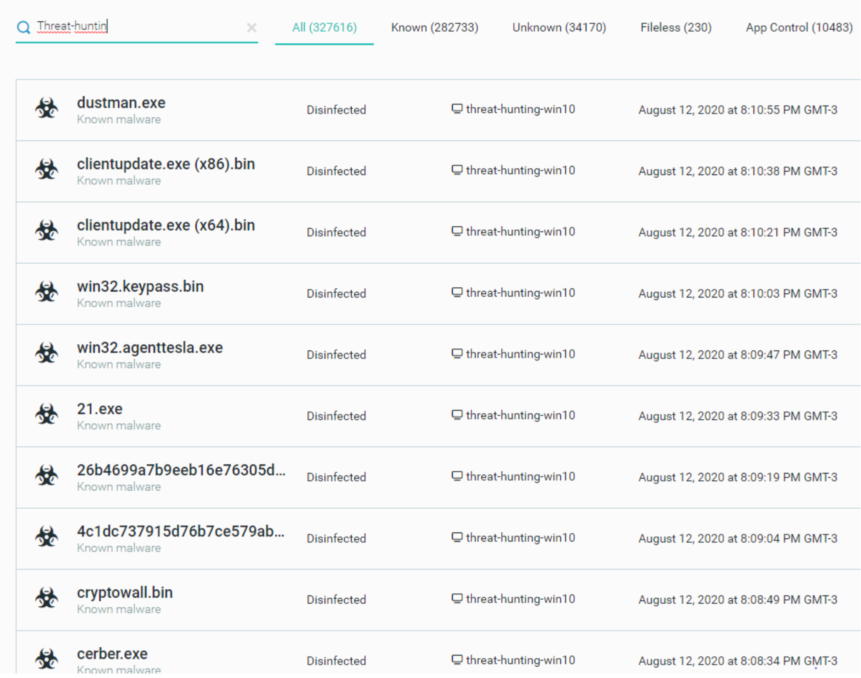
The purpose of this test was to simulate the same process as a user receiving a zipped file (`.zip`) and performing the extraction of these artifacts in their own environment.



Nome	Data de modificaç...	Tipo	Tamanho
Backdoor.MSIL.Tyupkin	12/08/2020 20:08	Pasta de arquivos	
CryptoLocker_10Sep2013	12/08/2020 20:08	Pasta de arquivos	
EquationGroup.DoubleFantasy	12/08/2020 20:08	Pasta de arquivos	
EquationGroup.EquationDrug	12/08/2020 20:08	Pasta de arquivos	
EquationGroup.EquationLaser	12/08/2020 20:08	Pasta de arquivos	
EquationGroup.Fanny	12/08/2020 20:08	Pasta de arquivos	
Linux.Chapros.A	12/08/2020 20:08	Pasta de arquivos	
Linux.Encoder.1	12/08/2020 20:08	Pasta de arquivos	
OSX.Lazarus	12/08/2020 20:08	Pasta de arquivos	
OSX.MacSecurity	12/08/2020 20:08	Pasta de arquivos	
Ransomware.Cerber	12/08/2020 20:08	Pasta de arquivos	
Ransomware.Cryptowall	12/08/2020 20:08	Pasta de arquivos	
Ransomware.Jigsaw	12/08/2020 20:08	Pasta de arquivos	
Ransomware.Locky	12/08/2020 20:08	Pasta de arquivos	
Ransomware.Petya	12/08/2020 20:08	Pasta de arquivos	
Variant.Kazy	12/08/2020 20:08	Pasta de arquivos	
VBS.Carnival	12/08/2020 20:08	Pasta de arquivos	
VBS.NewLove.A	12/08/2020 20:08	Pasta de arquivos	
Win32.AgentTesla	12/08/2020 20:08	Pasta de arquivos	
Win32.APT28.SekoiaRootkit	12/08/2020 20:08	Pasta de arquivos	
Win32.APT32.WindShield	12/08/2020 20:08	Pasta de arquivos	
Win32.KeyPass	12/08/2020 20:08	Pasta de arquivos	
Win32.ZeroCleare	12/08/2020 20:08	Pasta de arquivos	
Win32.ZeusVM	12/08/2020 20:08	Pasta de arquivos	
Zerolocker	12/08/2020 20:08	Pasta de arquivos	
Maldoc	12/08/2020 20:08	Pasta de arquivos	

Image 1.5: Extraction of 26 Folders with malicious files

After performing the action of extracting the files, it was possible to verify in the cybereason "***`Malware Alerts`***" logs that only 12 malwares were detected.



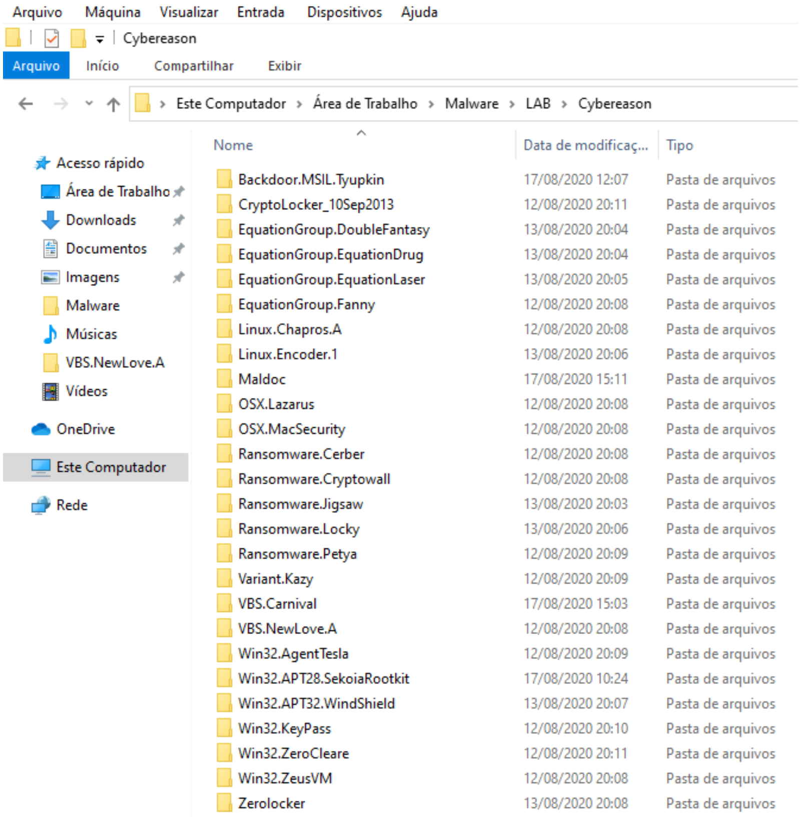
Threat-huntin | All (327616) | Known (282733) | Unknown (34170) | Fileless (230) | App Control (10483)

dustman.exe Known malware	Disinfected	threat-hunting-win10	August 12, 2020 at 8:10:55 PM GMT-3
clientupdate.exe (x86).bin Known malware	Disinfected	threat-hunting-win10	August 12, 2020 at 8:10:38 PM GMT-3
clientupdate.exe (x64).bin Known malware	Disinfected	threat-hunting-win10	August 12, 2020 at 8:10:21 PM GMT-3
win32.keypass.bin Known malware	Disinfected	threat-hunting-win10	August 12, 2020 at 8:10:03 PM GMT-3
win32.agenttesla.exe Known malware	Disinfected	threat-hunting-win10	August 12, 2020 at 8:09:47 PM GMT-3
21.exe Known malware	Disinfected	threat-hunting-win10	August 12, 2020 at 8:09:33 PM GMT-3
26b4699a7b9eeb16e76305d... Known malware	Disinfected	threat-hunting-win10	August 12, 2020 at 8:09:19 PM GMT-3
4c1dc737915d76b7ce579ab... Known malware	Disinfected	threat-hunting-win10	August 12, 2020 at 8:09:04 PM GMT-3
cryptowall.bin Known malware	Disinfected	threat-hunting-win10	August 12, 2020 at 8:08:49 PM GMT-3
cerber.exe Known malware	Disinfected	threat-hunting-win10	August 12, 2020 at 8:08:34 PM GMT-3

Image 1.6: Malware Alerts Detection Cybereason

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.

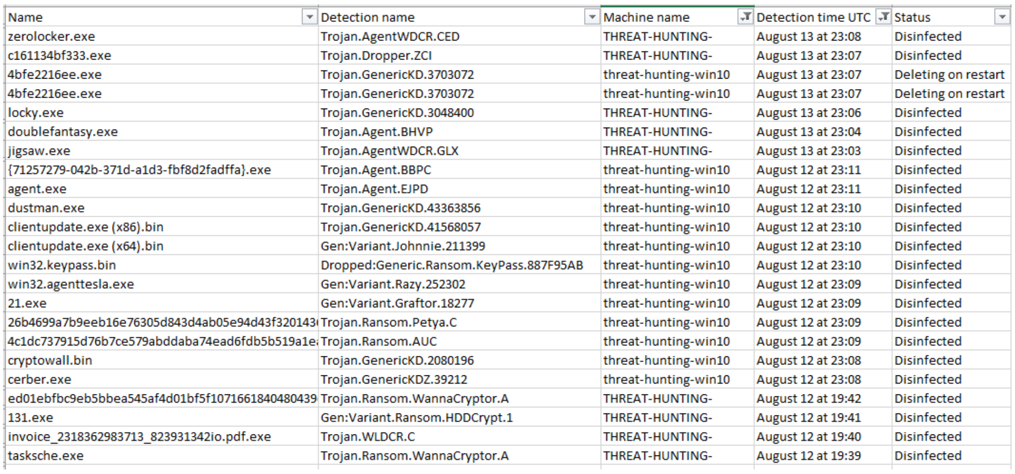


Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
Cybereason
Arquivo Início Compartilhar Exibir
Este Computador › Área de Trabalho › Malware › LAB › Cybereason
Acesso rápido
Área de Trabalho
Downloads
Documentos
Imagens
Malware
Músicas
VBS.NewLove.A
Vídeos
OneDrive
Este Computador
Rede

Nome	Data de modificaç...	Tipo
Backdoor.MSIL.Tyupkin	17/08/2020 12:07	Pasta de arquivos
CryptoLocker_10Sep2013	12/08/2020 20:11	Pasta de arquivos
EquationGroup.DoubleFantasy	13/08/2020 20:04	Pasta de arquivos
EquationGroup.EquationDrug	13/08/2020 20:04	Pasta de arquivos
EquationGroup.EquationLaser	13/08/2020 20:05	Pasta de arquivos
EquationGroup.Fanny	12/08/2020 20:08	Pasta de arquivos
Linux.Chapros.A	12/08/2020 20:08	Pasta de arquivos
Linux.Encoder.1	13/08/2020 20:06	Pasta de arquivos
Maldoc	17/08/2020 15:11	Pasta de arquivos
OSX.Lazarus	12/08/2020 20:08	Pasta de arquivos
OSX.MacSecurity	12/08/2020 20:08	Pasta de arquivos
Ransomware.Cerber	12/08/2020 20:08	Pasta de arquivos
Ransomware.Cryptowall	12/08/2020 20:08	Pasta de arquivos
Ransomware.Jigsaw	13/08/2020 20:03	Pasta de arquivos
Ransomware.Locky	13/08/2020 20:06	Pasta de arquivos
Ransomware.Petya	12/08/2020 20:09	Pasta de arquivos
Variant.Kazy	12/08/2020 20:09	Pasta de arquivos
VBS.Carnival	17/08/2020 15:03	Pasta de arquivos
VBS.NewLove.A	12/08/2020 20:08	Pasta de arquivos
Win32.AgentTesla	12/08/2020 20:09	Pasta de arquivos
Win32.APT28.SekoiaRootkit	17/08/2020 10:24	Pasta de arquivos
Win32.APT32.WindShield	13/08/2020 20:07	Pasta de arquivos
Win32.KeyPass	12/08/2020 20:10	Pasta de arquivos
Win32.ZeroCleare	12/08/2020 20:11	Pasta de arquivos
Win32.ZeusVM	12/08/2020 20:08	Pasta de arquivos
Zerolocker	13/08/2020 20:08	Pasta de arquivos

Image 1.7: New Folder (Cybereason Folder) – Malware manipulation

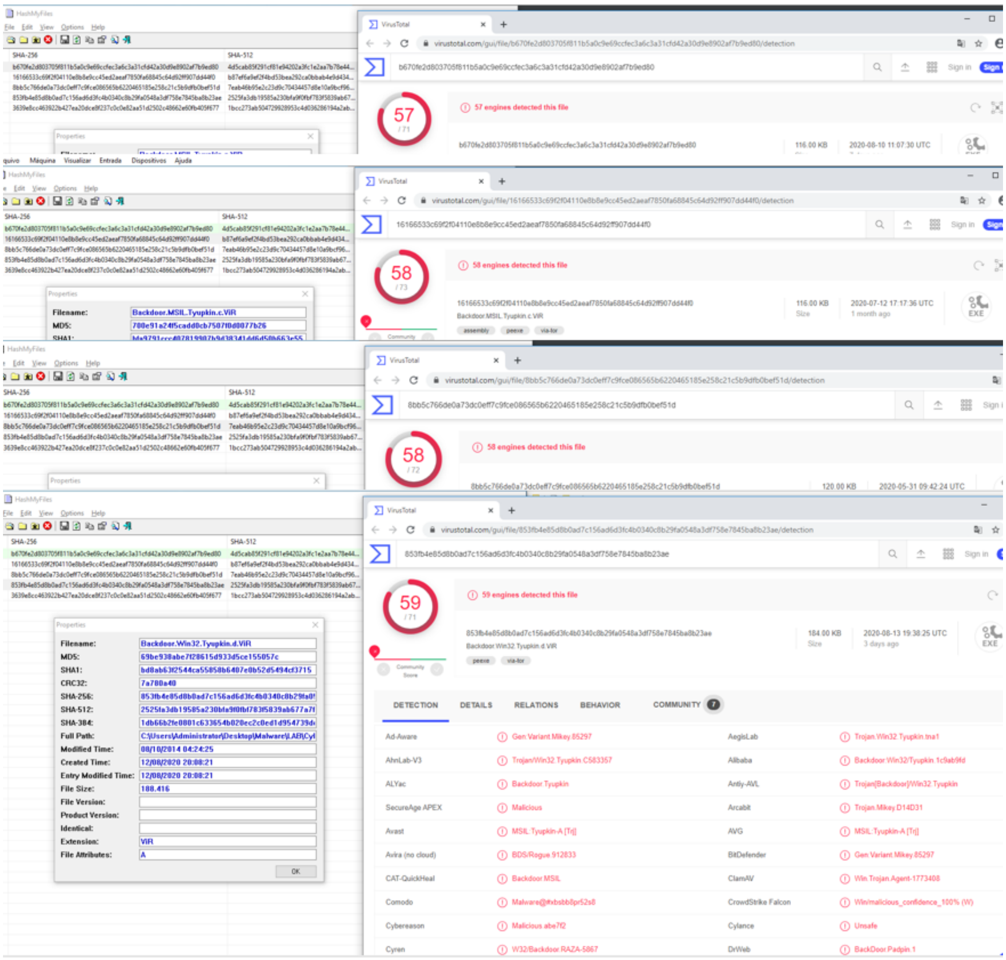
When a new file is generated on the disk, soon we should have a new entry in a block of that disk and in theory the antivirus should take some action (considering that it has the real time enabled), we could define it as a file manipulation (still not running) where the endpoint protection is already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



Name	Detection name	Machine name	Detection time UTC	Status
zerolocker.exe	Trojan.AgentWDCR.CED	THREAT-HUNTING-	August 13 at 23:08	Disinfected
c161134bf333.exe	Trojan.Dropper.ZCI	THREAT-HUNTING-	August 13 at 23:07	Disinfected
4bfe2216ee.exe	Trojan.GenericKD.3703072	threat-hunting-win10	August 13 at 23:07	Deleting on restart
4bfe2216ee.exe	Trojan.GenericKD.3703072	threat-hunting-win10	August 13 at 23:07	Deleting on restart
locky.exe	Trojan.GenericKD.3048400	THREAT-HUNTING-	August 13 at 23:06	Disinfected
doublefantasy.exe	Trojan.Agent.BHVP	THREAT-HUNTING-	August 13 at 23:04	Disinfected
jigsaw.exe	Trojan.AgentWDCR.GLX	THREAT-HUNTING-	August 13 at 23:03	Disinfected
{71257279-042b-371d-a1d3-fbf8d2fadffa}.exe	Trojan.Agent.BBPC	threat-hunting-win10	August 12 at 23:11	Disinfected
agent.exe	Trojan.Agent.EJPD	threat-hunting-win10	August 12 at 23:11	Disinfected
dustman.exe	Trojan.GenericKD.43363856	threat-hunting-win10	August 12 at 23:10	Disinfected
clientupdate.exe (x86).bin	Trojan.GenericKD.41568057	threat-hunting-win10	August 12 at 23:10	Disinfected
clientupdate.exe (x64).bin	Gen:Variant.Johnnie.211399	threat-hunting-win10	August 12 at 23:10	Disinfected
win32.keypass.bin	Dropped:Generic.Ransom.KeyPass.887F95AB	threat-hunting-win10	August 12 at 23:10	Disinfected
win32.agenttesla.exe	Gen:Variant.Razy.252302	threat-hunting-win10	August 12 at 23:09	Disinfected
21.exe	Gen:Variant.Graftor.18277	threat-hunting-win10	August 12 at 23:09	Disinfected
26b4699a7b9eeb16e76305d843d4ab05e94d43f320143	Trojan.Ransom.Petya.C	threat-hunting-win10	August 12 at 23:09	Disinfected
4c1dc737915d76b7ce579abddaba74ead6fdb5b519a1e	Trojan.Ransom.AUC	threat-hunting-win10	August 12 at 23:09	Disinfected
cryptowall.bin	Trojan.GenericKD.2080196	threat-hunting-win10	August 12 at 23:08	Disinfected
cerber.exe	Trojan.GenericKDZ.39212	threat-hunting-win10	August 12 at 23:08	Disinfected
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439	Trojan.Ransom.WannaCryptor.A	THREAT-HUNTING-	August 12 at 19:42	Disinfected
131.exe	Gen:Variant.Ransom.HDDCrypt.1	THREAT-HUNTING-	August 12 at 19:41	Disinfected
invoice_2318362983713_823931342io.pdf.exe	Trojan.WLDCR.C	THREAT-HUNTING-	August 12 at 19:40	Disinfected
tasksche.exe	Trojan.Ransom.WannaCryptor.A	THREAT-HUNTING-	August 12 at 19:39	Disinfected

Image 1.8: Detection logs about Manipulations files (without execution)

After performing this second test, we noticed that only 2 more threats were detected, but there were still many malware that had not been detected, as we can see below, as 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`).



SHA-256	SHA-512
b670fe2d803705f811b5a0c9e69ccfec3a6c3a31cfd42a30d9e8902af7b9ed80	4d5cab85f291cf81e94202a3fc1e2aa7b78e44...
16166533c69f2f04110e8b8e9cc45ed2aeaf7850fa68845c64d92ff907dd44f0	b87ef6a9ef2f4bd53bea292ca0bbab4e9d434...
8bb5c766de0a73dc0eff7c9fce086565b6220465185e258c21c5b9dfb0bef51d	7eab46b95e2c23d9c70434457d8e10a9bcf96...
853fb4e85d8b0ad7c156ad6d3fc4b0340c8b29fa0548a3df758e7845ba8b23ae	2525fa3db19585a230bfa9f0fbf783f5839ab67...
3639e8cc463922b427ea20dce8f237c0c0e82aa51d2502c48662e60fb405f677	1bcc273ab504729928953c4d036286194a2ab...

Filename: Backdoor.MSIL.Tyupkin.c.ViR
MD5: 700e91a24f5cadd0cb7507f0d0077b26

Filename: Backdoor.Win32.Tyupkin.d.ViR
MD5: 69be938abe7f28615d933d5ce155057c
SHA1: bd8ab63f2544ca55858b6407e0b52d5494cf3715
CRC32: 7a780a40
SHA-256: 853fb4e85d8b0ad7c156ad6d3fc4b0340c8b29fa0!
SHA-512: 2525fa3db19585a230bfa9f0fbf783f5839ab677a7f
SHA-384: 1db66b2fe0801c633654b020ec2c0ed1d954739d
Full Path: C:\Users\Administrator\Desktop\Malware\LAB\Cyl
Modified Time: 08/10/2014 04:24:25
Created Time: 12/08/2020 20:08:21
Entry Modified Time: 12/08/2020 20:08:21
File Size: 188.416
File Version:
Product Version:
Identical:
Extension: ViR
File Attributes: A

virustotal.com/gui/file/b670fe2d803705f811b5a0c9e69ccfec3a6c3a31cfd42a30d9e8902af7b9ed80/detection

57 / 71 — 57 engines detected this file

b670fe2d803705f811b5a0c9e69ccfec3a6c3a31cfd42a30d9e8902af7b9ed80 — 116.00 KB — 2020-08-10 11:07:30 UTC

virustotal.com/gui/file/16166533c69f2f04110e8b8e9cc45ed2aeaf7850fa68845c64d92ff907dd44f0/detection

58 / 73 — 58 engines detected this file

16166533c69f2f04110e8b8e9cc45ed2aeaf7850fa68845c64d92ff907dd44f0 — Backdoor.MSIL.Tyupkin.c.VIR — 116.00 KB Size — 2020-07-12 17:17:36 UTC 1 month ago

virustotal.com/gui/file/8bb5c766de0a73dc0eff7c9fce086565b6220465185e258c21c5b9dfb0bef51d/detection

58 / 72 — 58 engines detected this file

8bb5c766de0a73dc0eff7c9fce086565b6220465185e258c21c5b9dfb0bef51d — 120.00 KB — 2020-05-31 09:42:24 UTC

virustotal.com/gui/file/853fb4e85d8b0ad7c156ad6d3fc4b0340c8b29fa0548a3df758e7845ba8b23ae/detection

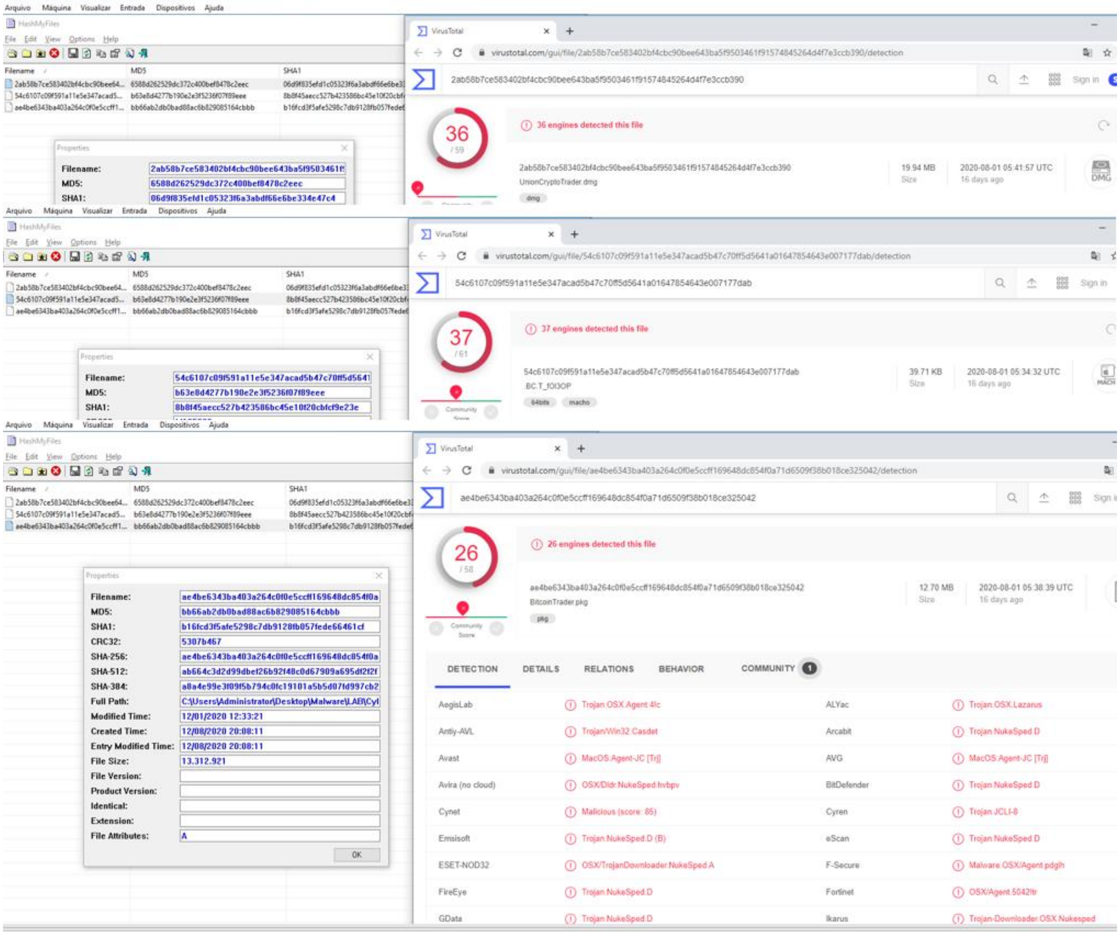
59 / 71 — 59 engines detected this file

853fb4e85d8b0ad7c156ad6d3fc4b0340c8b29fa0548a3df758e7845ba8b23ae — Backdoor.Win32.Tyupkin.d.VIR — 184.00 KB Size — 2020-08-13 19:38:25 UTC 3 days ago

Ad-Aware	Gen:Variant.Mikey.85297	AegisLab	Trojan.Win32.Tyupkin.tna1
AhnLab-V3	Trojan/Win32.Tyupkin.C583357	Alibaba	Backdoor:Win32/Tyupkin.1c9ab9fd
ALYac	Backdoor.Tyupkin	Antiy-AVL	Trojan[Backdoor]/Win32.Tyupkin
SecureAge APEX	Malicious	Arcabit	Trojan.Mikey.D14D31
Avast	MSIL:Tyupkin-A [Trj]	AVG	MSIL:Tyupkin-A [Trj]
Avira (no cloud)	BDS/Rogue.912833	BitDefender	Gen:Variant.Mikey.85297
CAT-QuickHeal	Backdoor.MSIL	ClamAV	Win.Trojan.Agent-1773408
Comodo	Malware@#xbsbb8pr52s8	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.abe7f2	Cylance	Unsafe
Cyren	W32/Backdoor.RAZA-5867	DrWeb	BackDoor.Padpin.1

Image 1.9: Backdoor Known – Not Detected

Other threats that were created by APT (Advanced Persistent Threats) groups like Lazarus Groups in other more.


Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
HashMyFiles
File Edit View Options Help
VirusTotal
Sign in

Filename	MD5	SHA1
2ab58b7ce583402bf4cbc90bee64...	6588d262529dc372c400bef8478c2eec	06d9f835efd1c05323f6a3abdf66e6be3
54c6107c09f591a11e5e347acad5...	b63e8d4277b190e2e3f5236f07f89eee	8b8f45aecc527b423586bc45e10f20cbf
ae4be6343ba403a264c0f0e5ccff1...	bb66ab2db0bad88ac6b829085164cbbb	b16fcd3f5afe5298c7db9128fb057fede6

Properties

Filename: 2ab58b7ce583402bf4cbc90bee643ba5f9503461f
MD5: 6588d262529dc372c400bef8478c2eec
SHA1: 06d9f835efd1c05323f6a3abdf66e6be334e47c4

virustotal.com/gui/file/2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390/detection

2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390

36 / 59

36 engines detected this file

2ab58b7ce583402bf4cbc90bee643ba5f9503461f91574845264d4f7e3ccb390
UnionCryptoTrader.dmg
dmg

19.94 MB Size

2020-08-01 05:41:57 UTC 16 days ago

DMG

Properties

Filename: 54c6107c09f591a11e5e347acad5b47c70ff5d5641
MD5: b63e8d4277b190e2e3f5236f07f89eee
SHA1: 8b8f45aecc527b423586bc45e10f20cbfcf9e23e

virustotal.com/gui/file/54c6107c09f591a11e5e347acad5b47c70ff5d5641a01647854643e007177dab/detection

54c6107c09f591a11e5e347acad5b47c70ff5d5641a01647854643e007177dab

37 / 61

37 engines detected this file

54c6107c09f591a11e5e347acad5b47c70ff5d5641a01647854643e007177dab
.BC.T_f0l3OP
64bits macho

39.71 KB Size

2020-08-01 05:34:32 UTC 16 days ago

MACH

Community Score

Properties

Filename: ae4be6343ba403a264c0f0e5ccff169648dc854f0a
MD5: bb66ab2db0bad88ac6b829085164cbbb
SHA1: b16fcd3f5afe5298c7db9128fb057fede66461cf
CRC32: 5307b467
SHA-256: ae4be6343ba403a264c0f0e5ccff169648dc854f0a
SHA-512: ab664c3d2d99dbef26b92f48c0d67909a695df2f2f
SHA-384: a8a4e99e3f09f5b794c0fc19101a5b5d07fd997cb2
Full Path: C:\Users\Administrator\Desktop\Malware\LAB\Cyl
Modified Time: 12/01/2020 12:33:21
Created Time: 12/08/2020 20:08:11
Entry Modified Time: 12/08/2020 20:08:11
File Size: 13.312.921
File Version:
Product Version:
Identical:
Extension:
File Attributes: A

virustotal.com/gui/file/ae4be6343ba403a264c0f0e5ccff169648dc854f0a71d6509f38b018ce325042/detection

ae4be6343ba403a264c0f0e5ccff169648dc854f0a71d6509f38b018ce325042

26 / 58

26 engines detected this file

ae4be6343ba403a264c0f0e5ccff169648dc854f0a71d6509f38b018ce325042
BitcoinTrader.pkg
pkg

12.70 MB Size

2020-08-01 05:38:39 UTC 16 days ago

Community Score

AegisLab	Trojan.OSX.Agent.4!c	ALYac	Trojan.OSX.Lazarus
Antiy-AVL	Trojan/Win32.Casdet	Arcabit	Trojan.NukeSped.D
Avast	MacOS:Agent-JC [Trj]	AVG	MacOS:Agent-JC [Trj]
Avira (no cloud)	OSX/Dldr.NukeSped.hvbpv	BitDefender	Trojan.NukeSped.D
Cynet	Malicious (score: 85)	Cyren	Trojan.JCLI-8
Emsisoft	Trojan.NukeSped.D (B)	eScan	Trojan.NukeSped.D
ESET-NOD32	OSX/TrojanDownloader.NukeSped.A	F-Secure	Malware.OSX/Agent.pdgln
FireEye	Trojan.NukeSped.D	Fortinet	OSX/Agent.5042!tr
GData	Trojan.NukeSped.D	Ikarus	Trojan-Downloader.OSX.Nukesped

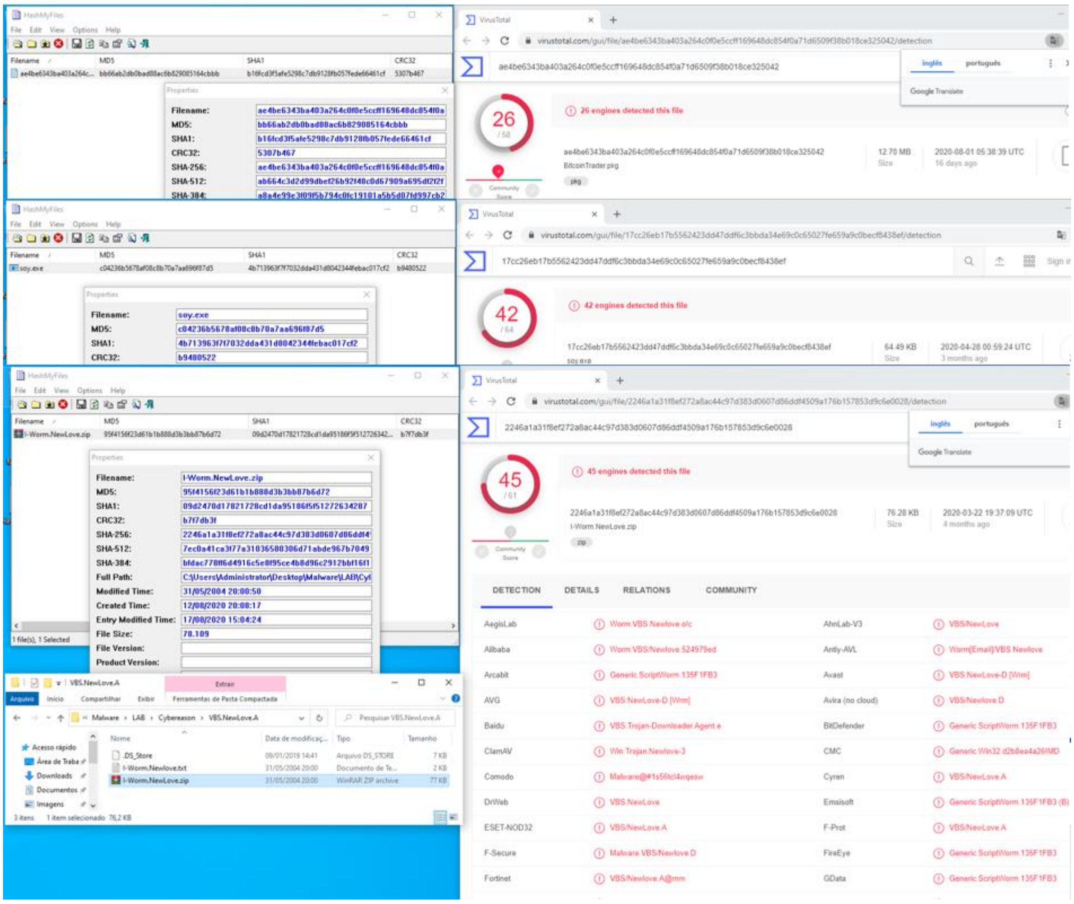
Image 1.10: Lazarus Malwares – Not Detected

In addition to this evidence, there are other types of better-known malware associated with organizations that run APTS, such as:

- EquationGroup (Malicious PE)
- Linux Chapro (Malicious ELF)
- Linux Enconder (Malicious ELF)
- MacOS – Lazarus (Malicous Mach-o)
- Malware in PDF (Maldoc Sample)

3.4 Third Test

The third stage of the tests was through the use of the *fullscan* function by Cybereason Manager, to perform a complete scan of the entire disk, manually, in this way, all malware should be eliminated, as they are already known malware as mentioned earlier.



HashMyFiles

Filename	MD5	SHA1	CRC32
ae4be6343ba403a264c...	bb66ab2db0bad88ac6b829085164cbbb	b16fcd3f5afe5298c7db9128fb057fede66461cf	5307b467

Properties

Filename: ae4be6343ba403a264c0f0e5ccff169648dc854f0a
MD5: bb66ab2db0bad88ac6b829085164cbbb
SHA1: b16fcd3f5afe5298c7db9128fb057fede66461cf
CRC32: 5307b467
SHA-256: ae4be6343ba403a264c0f0e5ccff169648dc854f0a
SHA-512: ab664c3d2d99dbef26b92f48c0d67909a695df2f2f
SHA-384: a8a4e99e3f09f5b794c0fc19101a5b5d07fd997cb2

VirusTotal
virustotal.com/gui/file/ae4be6343ba403a264c0f0e5ccff169648dc854f0a71d6509f38b018ce325042/detection
ae4be6343ba403a264c0f0e5ccff169648dc854f0a71d6509f38b018ce325042

26 / 58
26 engines detected this file
ae4be6343ba403a264c0f0e5ccff169648dc854f0a71d6509f38b018ce325042
BitcoinTrader.pkg
pkg
12.70 MB Size
2020-08-01 05:38:39 UTC 16 days ago

HashMyFiles

Filename	MD5	SHA1	CRC32
soy.exe	c04236b5678af08c8b70a7aa696f87d5	4b713963f7f7032dda431d8042344febac017cf2	b9480522

Properties

Filename: soy.exe
MD5: c04236b5678af08c8b70a7aa696f87d5
SHA1: 4b713963f7f7032dda431d8042344febac017cf2
CRC32: b9480522

VirusTotal
virustotal.com/gui/file/17cc26eb17b5562423dd47ddf6c3bbda34e69c0c65027fe659a9c0becf8438ef/detection
17cc26eb17b5562423dd47ddf6c3bbda34e69c0c65027fe659a9c0becf8438ef

42 / 64
42 engines detected this file
17cc26eb17b5562423dd47ddf6c3bbda34e69c0c65027fe659a9c0becf8438ef
soy.exe
64.49 KB Size
2020-04-28 00:59:24 UTC 3 months ago

HashMyFiles

Filename	MD5	SHA1	CRC32
I-Worm.NewLove.zip	95f4156f23d61b1b888d3b3bb87b6d72	09d2470d17821728cd1da95186f5f512726342...	b7f7db3f

1 file(s), 1 Selected

Properties

Filename: I-Worm.NewLove.zip
MD5: 95f4156f23d61b1b888d3b3bb87b6d72
SHA1: 09d2470d17821728cd1da95186f5f51272634287
CRC32: b7f7db3f
SHA-256: 2246a1a31f8ef272a8ac44c97d383d0607d86ddf4
SHA-512: 7ec0a41ca3f77a31036580306d71abde967b7049
SHA-384: bfdac778ff6d4916c5e8f95ce4b8d96c2912bbf16f1
Full Path: C:\Users\Administrator\Desktop\Malware\LAB\Cyb
Modified Time: 31/05/2004 20:00:50
Created Time: 12/08/2020 20:08:17
Entry Modified Time: 17/08/2020 15:04:24
File Size: 78.109
File Version:
Product Version:

VBS.NewLove.A
Malware › LAB › Cybereason › VBS.NewLove.A

Nome	Data de modificaç...	Tipo	Tamanho
.DS_Store	09/01/2019 14:41	Arquivo DS_STORE	7 KB
I-Worm.Newlove.txt	31/05/2004 20:00	Documento de Te...	2 KB
I-Worm.NewLove.zip	31/05/2004 20:00	WinRAR ZIP archive	77 KB

3 itens 1 item selecionado 76,2 KB

VirusTotal
virustotal.com/gui/file/2246a1a31f8ef272a8ac44c97d383d0607d86ddf4509a176b157853d9c6e0028/detection
2246a1a31f8ef272a8ac44c97d383d0607d86ddf4509a176b157853d9c6e0028

45 / 61
45 engines detected this file
2246a1a31f8ef272a8ac44c97d383d0607d86ddf4509a176b157853d9c6e0028
I-Worm.NewLove.zip
zip
76.28 KB Size
2020-03-22 19:37:09 UTC 4 months ago

DETECTION DETAILS RELATIONS COMMUNITY

AegisLab	Worm.VBS.Newlove.o!c	AhnLab-V3	VBS/NewLove
Alibaba	Worm:VBS/Newlove.524979ed	Antiy-AVL	Worm[Email]/VBS.Newlove
Arcabit	Generic.ScriptWorm.135F1FB3	Avast	VBS:NewLove-D [Wrm]
AVG	VBS:NewLove-D [Wrm]	Avira (no cloud)	VBS/Newlove.D
Baidu	VBS.Trojan-Downloader.Agent.e	BitDefender	Generic.ScriptWorm.135F1FB3
ClamAV	Win.Trojan.Newlove-3	CMC	Generic.Win32.d2b8ea4a26!MD
Comodo	Malware@#1s56tcl4vqesw	Cyren	VBS/NewLove.A
DrWeb	VBS.NewLove	Emsisoft	Generic.ScriptWorm.135F1FB3 (B)
ESET-NOD32	VBS/NewLove.A	F-Prot	VBS/NewLove.A
F-Secure	Malware.VBS/Newlove.D	FireEye	Generic.ScriptWorm.135F1FB3
Fortinet	VBS/Newlove.A@mm	GData	Generic.ScriptWorm.135F1FB3

Image 1.11: Malwares – Not Detected after *FullScan*

3 Impact and Risk

At the end of this test, it was possible to verify that there are currently 3 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 Cybereason 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 EXE files Not Detected in the second test.**
  - PE files not detected even though malicious; it was not detected.
- **Malicious PDF file Not Detected in the second test.**
  - *DLL* files not detected even though malicious; it was not detected.
- **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 *fullscan*.**
  - *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 INFORMATION NOT BLOCKED

- **I-Worm.NewLove**

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

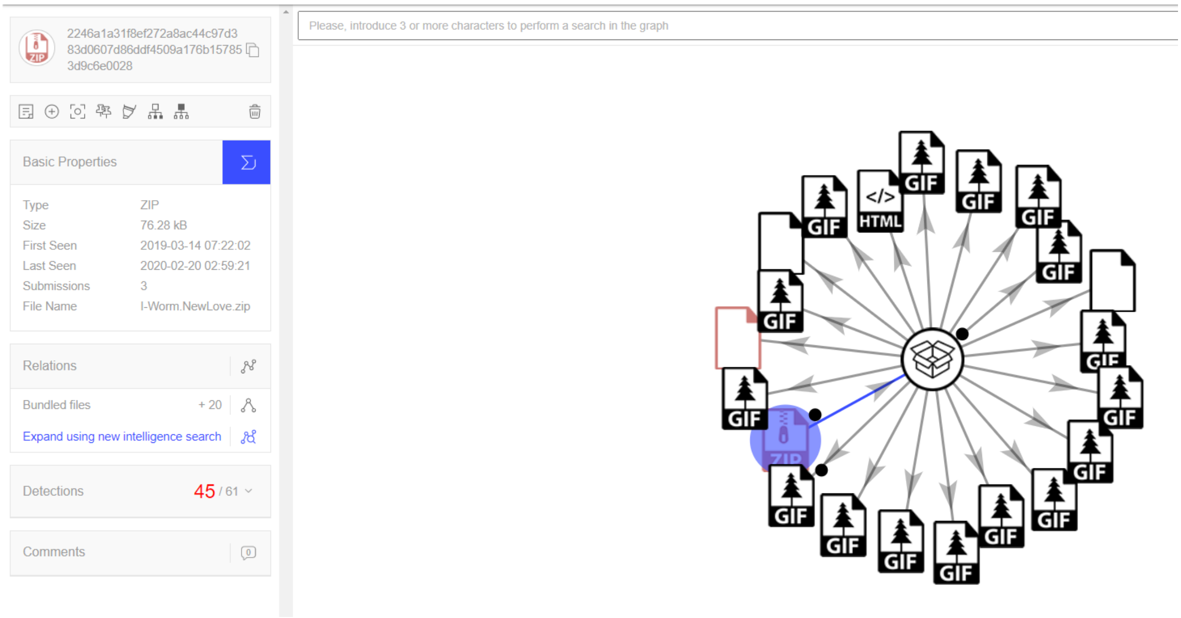
Worm-type malware, with high criticality, associated with the execution of VBS - Visual Basic Script, we have as a characteristic high propagation within the environment in which it is executed.

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

File type    ZIP
Magic  Zip archive data, at least v2.0 to extract

History
First Submission   2019-03-14 07:22:02
Last Submission    2020-02-20 02:59:21
Last Analysis      2020-03-22 19:37:09
Earliest Contents Modification 2000-07-21 12:55:20
Latest Contents Modification   2001-09-21 20:20:26

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



2246a1a31f8ef272a8ac44c97d383d0607d86ddf4509a176b157853d9c6e0028

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

Basic Properties

Type	ZIP
Size	76.28 kB
First Seen	2019-03-14 07:22:02
Last Seen	2020-02-20 02:59:21
Submissions	3
File Name	I-Worm.NewLove.zip

Relations

Bundled files + 20

Expand using new intelligence search

Detections 45 / 61

Comments 0

Image 1.12: • I-Worm.NewLove.zip – VirusTotal

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

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

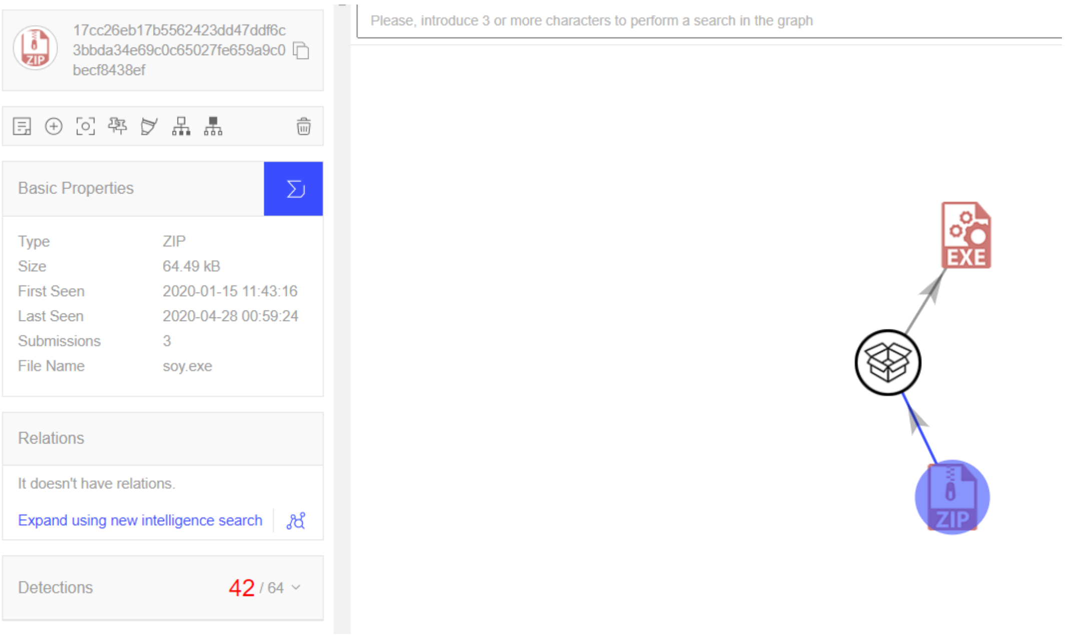
Trojan-type malware, which has a dropper behavior, and is responsible for downloading other malware within the victim's environment, developed for Windows 7, Windows 8, Windows 8.1 and Windows 10 operating systems.

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

File type    ZIP
Magic  Zip archive data, at least v2.0 to extract

History
First Submission   2020-01-15 11:43:16
Last Submission    2020-04-28 00:59:24
Last Analysis      2020-04-28 00:59:24
Earliest Contents Modification  2019-12-09 12:36:08
Latest Contents Modification    2019-12-09 12:36:08

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



17cc26eb17b5562423dd47ddf6c3bbda34e69c0c65027fe659a9c0becf8438ef

Basic Properties

Type	ZIP
Size	64.49 kB
First Seen	2020-01-15 11:43:16
Last Seen	2020-04-28 00:59:24
Submissions	3
File Name	soy.exe

Relations

It doesn't have relations.

Expand using new intelligence search

Detections 42 / 64

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

Image 1.13: Win32.ZeroCleare (soy.exe) - VirusTotal

- **OSX.Lazarus**

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

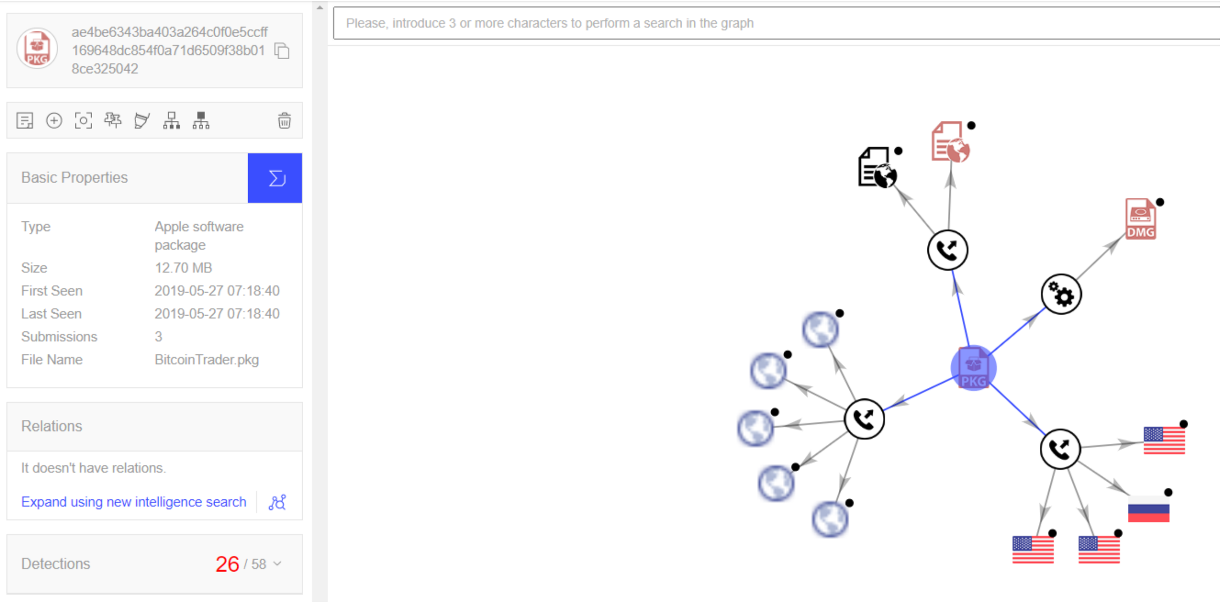
Malware developed for MacOS environments, focusing on cryptocurrency developed by Lazarus Group (APT group).

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

File type    Apple software package
Magic  xar archive version 1, SHA-1 checksum

History
First Submission   2019-05-27 07:18:40
Last Submission    2019-05-27 07:18:40
Last Analysis      2020-08-01 05:38:39

Names
BitcoinTrader.pkg
```



ae4be6343ba403a264c0f0e5ccff169648dc854f0a71d6509f38b018ce325042

Basic Properties

Type	Apple software package
Size	12.70 MB
First Seen	2019-05-27 07:18:40
Last Seen	2019-05-27 07:18:40
Submissions	3
File Name	BitcoinTrader.pkg

Relations

It doesn't have relations.

Expand using new intelligence search

Detections 26 / 58

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

Image 1.14: OSX.Lazarus - VirusTotal

4 Recommendation Actions

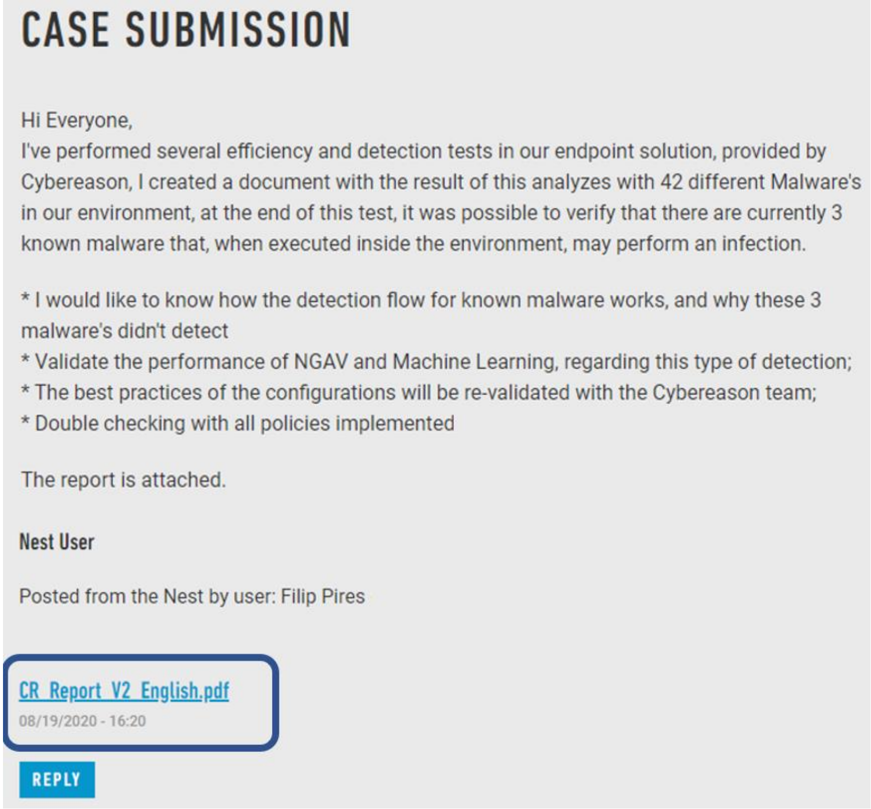
As we mentioned before, the idea it was execute test in many malwares, and this case, for this reason to be totally known the following actions will be taken to improve the protection environment of our assets:

- This report it was sent to Cybereason to validate with them how the detection flow for known malware works, and why these 3 malwares didn't detect;
- Validate the performance of NGAV and Machine Learning, regarding this type of detection;
- The best practices of the configurations should be revalidated with the Cybereason team;
- Double checking with all policies implemented at the customer that bought the solution;

5 Answers from Cybereason 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 42 different Malwares in our environment.

We opened a support case with the Cybereason support team on **August 19th** as you can see below



CASE SUBMISSION

Hi Everyone,
I've performed several efficiency and detection tests in our endpoint solution, provided by Cybereason, I created a document with the result of this analyzes with 42 different Malware's in our environment, at the end of this test, it was possible to verify that there are currently 3 known malware that, when executed inside the environment, may perform an infection.

* I would like to know how the detection flow for known malware works, and why these 3 malware's didn't detect
* Validate the performance of NGAV and Machine Learning, regarding this type of detection;
* The best practices of the configurations will be re-validated with the Cybereason team;
* Double checking with all policies implemented

The report is attached.

Nest User

Posted from the Nest by user: Filip Pires

CR_Report_V2_English.pdf
08/19/2020 - 16:20

Image 1.15: Support Case issue

We just receive a generic information by support:

- **20/08 | 25/08 | 26/08 | 27/08 | 31/08 | 04/09 | 10/09 | 11/09**
  - Remember that we are talk about **Critical** problem here.

After many times, I escalate this problem with many Customer Success Managers, Support Managers, Director Customers and VP from Cybereason, but we still waiting any resolution of this Detection problem.

By the end, a simple question that we need to do in those cases is:

Why didn't Cybereason detect them? ...What engine didn't work well? Or maybe, Which flow failed? Detection by pattern? Signature? NGAV? ML? We need to have (If possible) answers for these questions.