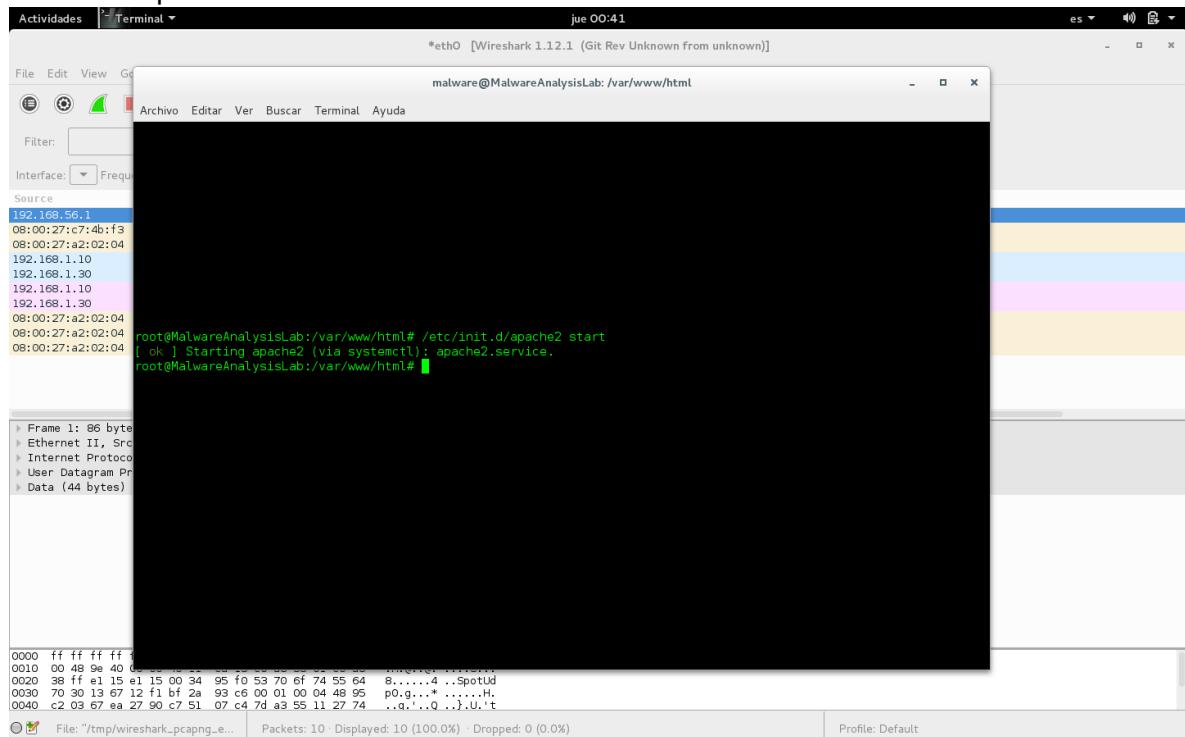

MANUAL DE USUARIO

Proyecto01 – Análisis de Software Malicioso.

Alumno: José Ricardo Rodríguez Abreu

Para ejecutar correctamente su pieza de malware debe seguir correctamente los siguientes pasos:

1. Deberá tener un servidor corriendo capturando el tráfico de red en el cual pueda proporcionar respuesta a peticiones http. En este caso usamos el servidor Apache en una máquina Linux Debian.



2. Iniciar el servidor apache con el siguiente comando

```
$sudo /etc/init.d/apache2 start
```

o lo que es equivalente a estar en una sesión de usuario root y escribir:

```
#/etc/init.d/apache2 start
```

3. Después de iniciar el servidor nos movemos al directorio en la ruta

/var/www/html ("var/www/" para algunas versiones) y creamos un archivo (como usuario root) llamado comando.txt con el siguiente comando

```
#touch comando.txt
```

Actividades Terminal jue 00:38

*eth0 [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

```
File Edit View Go
Archivo Editar Ver Buscar Terminal Ayuda
Interface: /var/www/html
Source
192.168.56.1
08:00:27:c7:4b:f3
08:00:27:a2:02:04
192.168.1.10
192.168.1.30
192.168.1.10
192.168.1.30
08:00:27:a2:02:04
08:00:27:a2:02:04
08:00:27:a2:02:04

total 12
-rw-r--r-- 1 malware malware 206 sep 21 23:42 comando.txt
-rw-r--r-- 1 root      root    177 sep 11 19:52 index.html
-rw-r--r-- 1 root      root    14 sep 11 19:57 Key.txt
root@MalwareAnalysisLab:/var/www/html# ls -l

Frame 1: 86 byte
Ethernet II, Src: (08:00:27:c7:4b:f3), Dst: (192.168.56.1)
User Datagram Protocol, Src Port: 49152, Dst Port: 80
Data (44 bytes)

0000 ff ff ff ff ff 00 48 9e 40 00 00 15 e1 15 00 34 95 f0 53 70 6f 74 55 64 8.....4 .Sputd
0020 38 ff e1 15 e1 15 00 34 95 f0 53 70 6f 74 55 64 p0.g...* .....H.
0030 70 30 13 67 12 f1 bf 2a 93 c6 00 01 00 04 48 95 ..g'..Q ..J.U.'t
0040 c2 03 67 ea 27 90 c7 51 07 c4 7d a3 55 11 27 74

File: "/tmp/wireshark.pcapng.e..." Packets: 10 Displayed: 10 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
```

- El archivo llamado comando.txt debe incluir en su primera línea un número del 1 al 7 o un comando especificado. En la siguiente imagen se muestran el contenido que puede tomar el malware como parámetros. **Cabe decir que si el parámetro es diferente el malware toma uno de los comandos anteriores aleatoriamente (excluyendo al 1729).**

Actividades Terminal jue 00:56

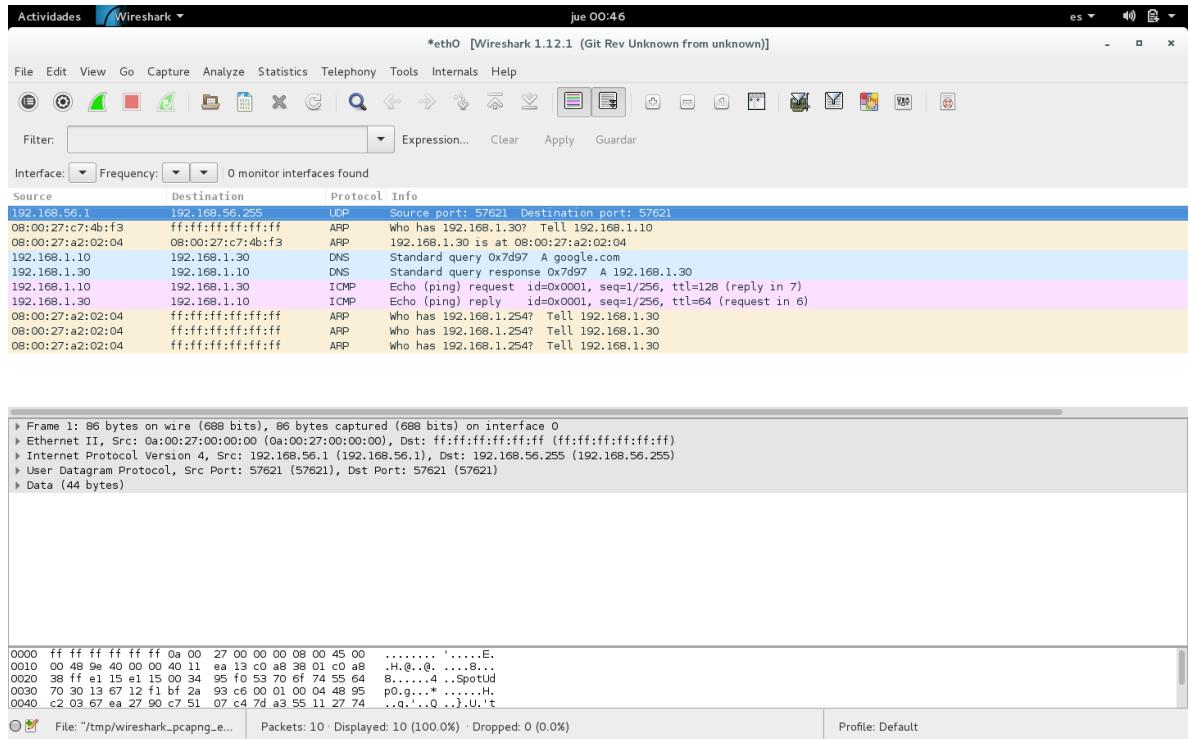
malware@MalwareAnalysisLab: /var/www/html

```
Archivo Editar Ver Buscar Terminal Ayuda
File Edit Options Buffers Tools Text Help
1729
#Colocar el numero que se desee o el puro nombre en la primera linea.
1 APAGAR
2 REINICIAR
3 SUSPENDER
4 CERRAR SESION
5 CALCULADORA
6 EXPLORER
7 IEXPLORER
1729 RODAB (Este es especial y realiza NADA)
```

-:U:-:--:P1 comando.txt All (1) (Text) --

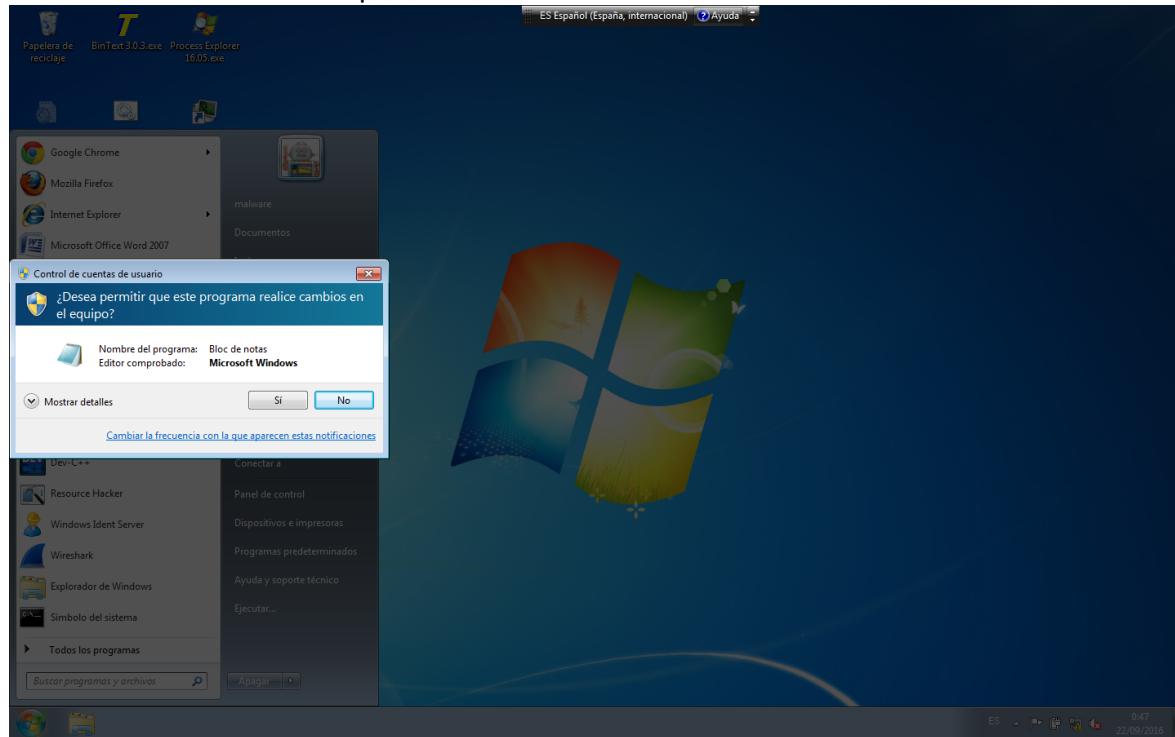
End of buffer

5. (Opcional) Como paso opcional y para poder observar el tráfico del malware abrimos Wireshark y empezamos a capturar el tráfico de red.

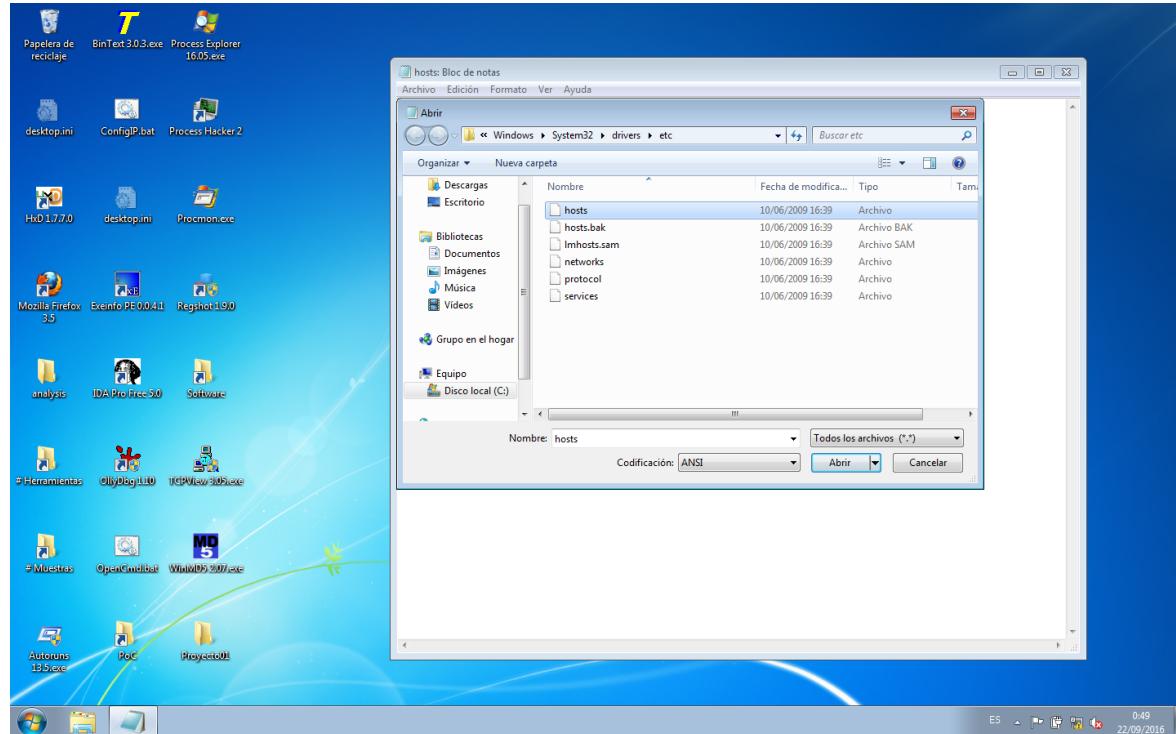


6. En su máquina Windows (Windows 7) deberá:

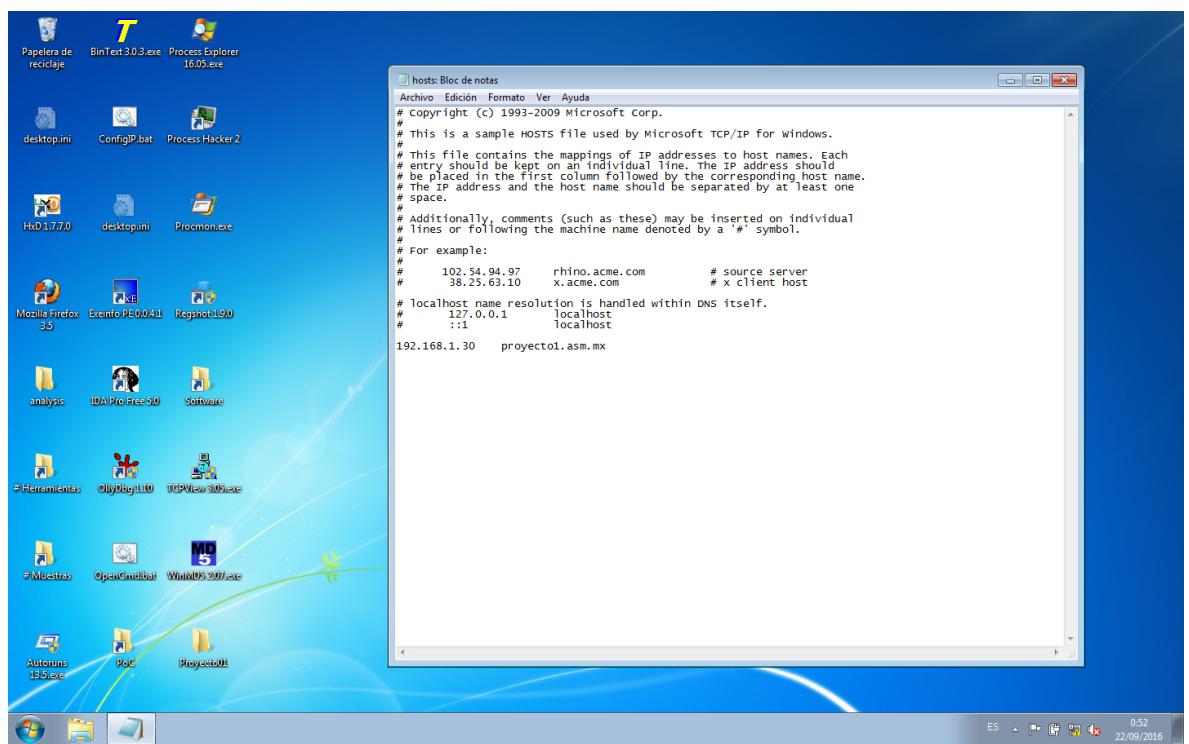
a. Abrir un Bloc de notas con permisos de administrador.



- b. Abrir el archivo llamado hosts que se encuentra en
C:\Windows\System32\drivers\etc

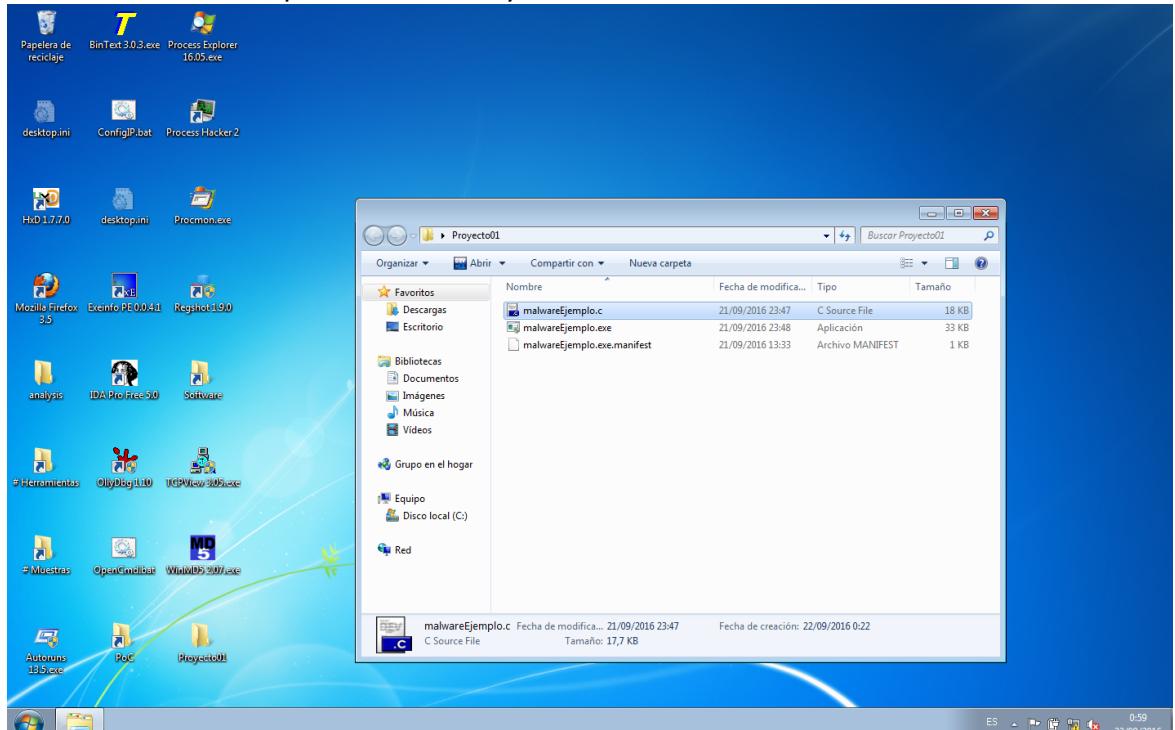


- c. Agregar la siguiente línea al final del documento:
192.168.1.30 proyecto1.asm.mx

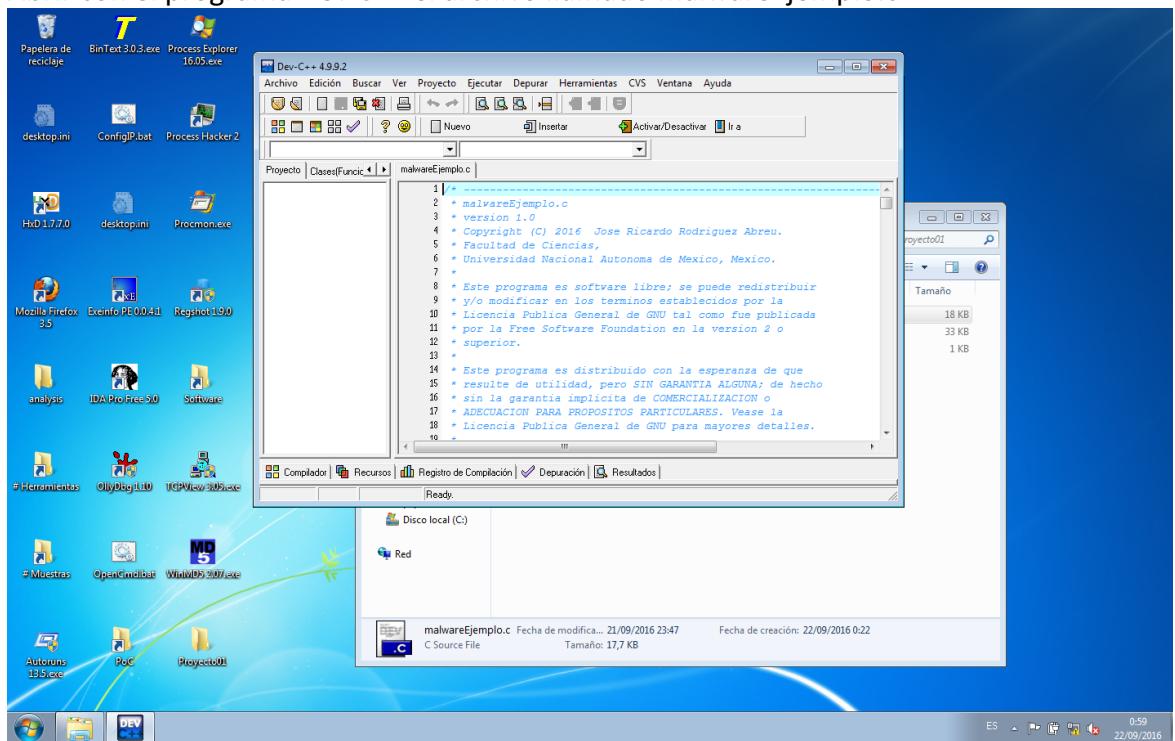


7. (Opcional) Compilar: El malware incluye por default un archivo .exe pero si se desea compilar de deberán seguir los siguientes pasos:

- Se deberá abrir la carpeta llamada Proyecto01



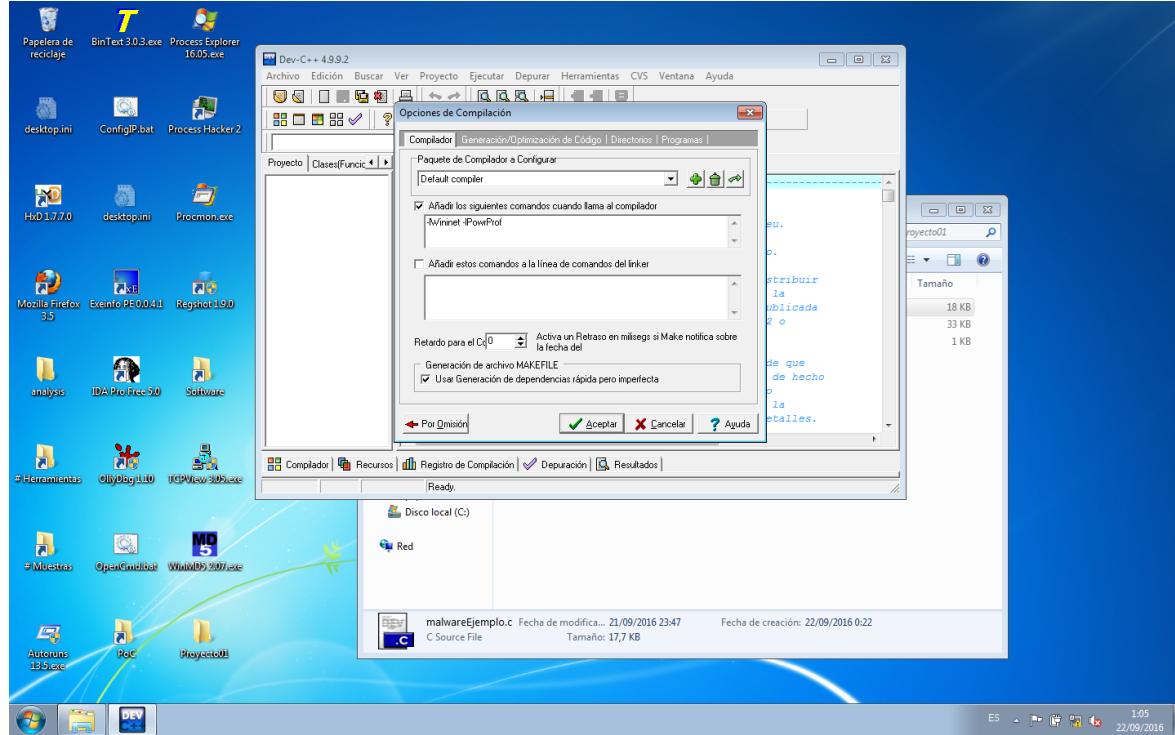
- Abrir con el programa Dev C++ el archivo llamado malwareEjemplo.c



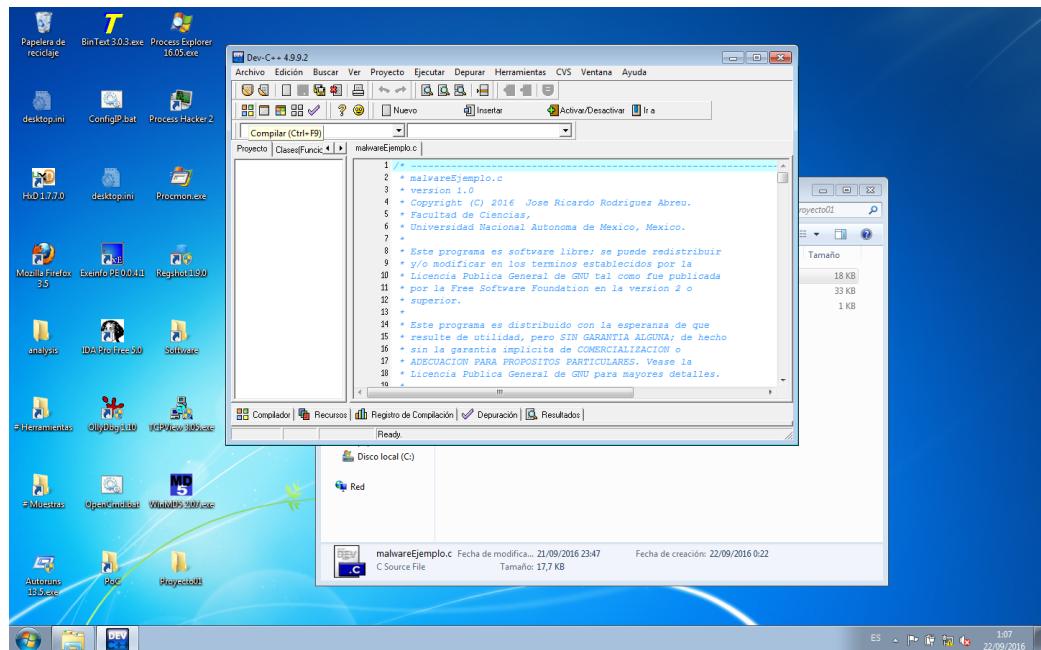
- c. Damos click en Herramientas -> Opciones de compilador y activamos la casilla que dice “Añadir los siguientes comandos cuando se llama al compilador” y dentro del cuadro de texto agregamos la siguiente línea:

```
-lWininet -lPowrProf
```

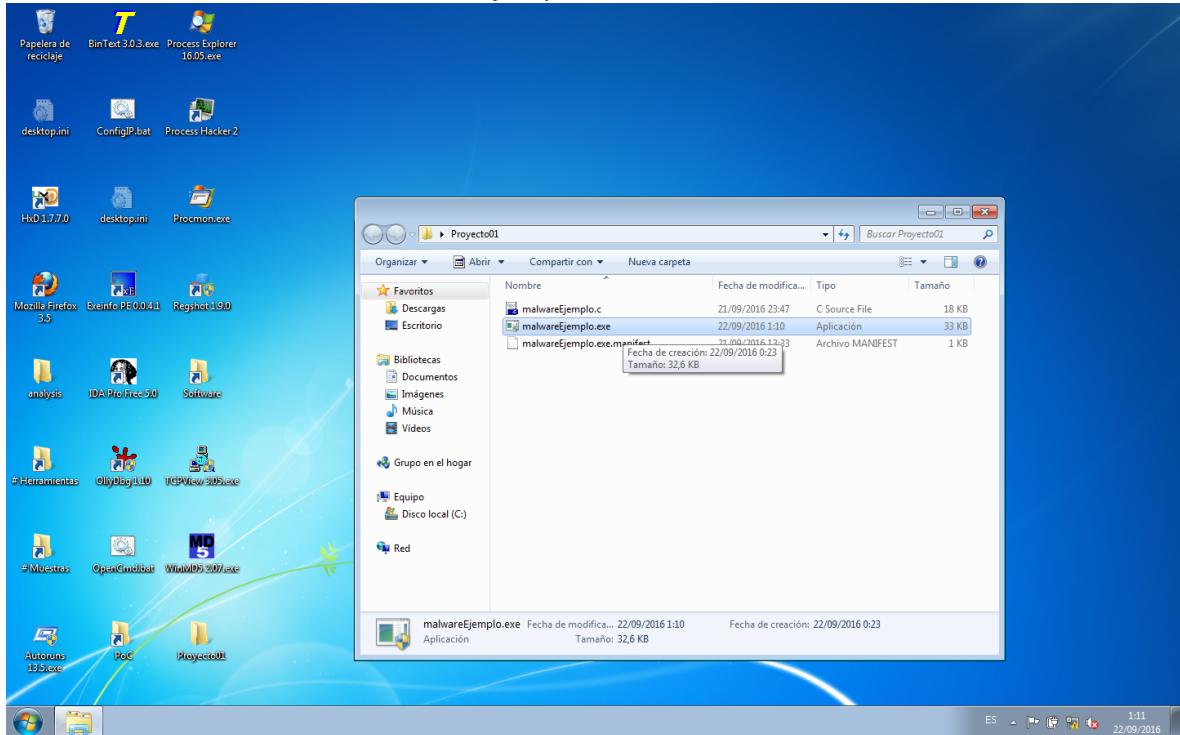
Después damos click en aceptar.



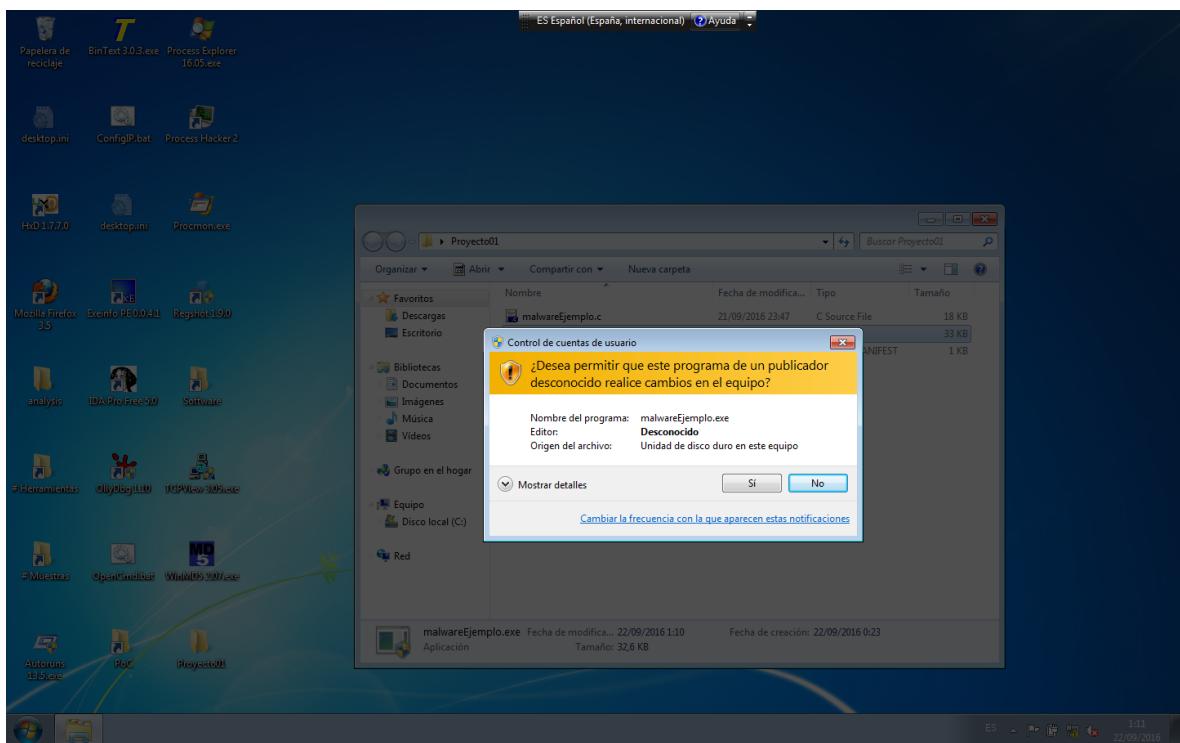
- d. Damos click en Ejecutar->Compilar ó Ctrl+F9 ó directamente sobre el botón del lado izquierdo y esto nos debe generar un archivo llamado malwareEjemplo.exe en la misma ubicación donde se encuentra nuestro archivo fuente.



8. Nos ubicamos en la carpeta del proyecto nombrada como Proyecto01 y damos doble click sobre el archivo malwareEjemplo.exe

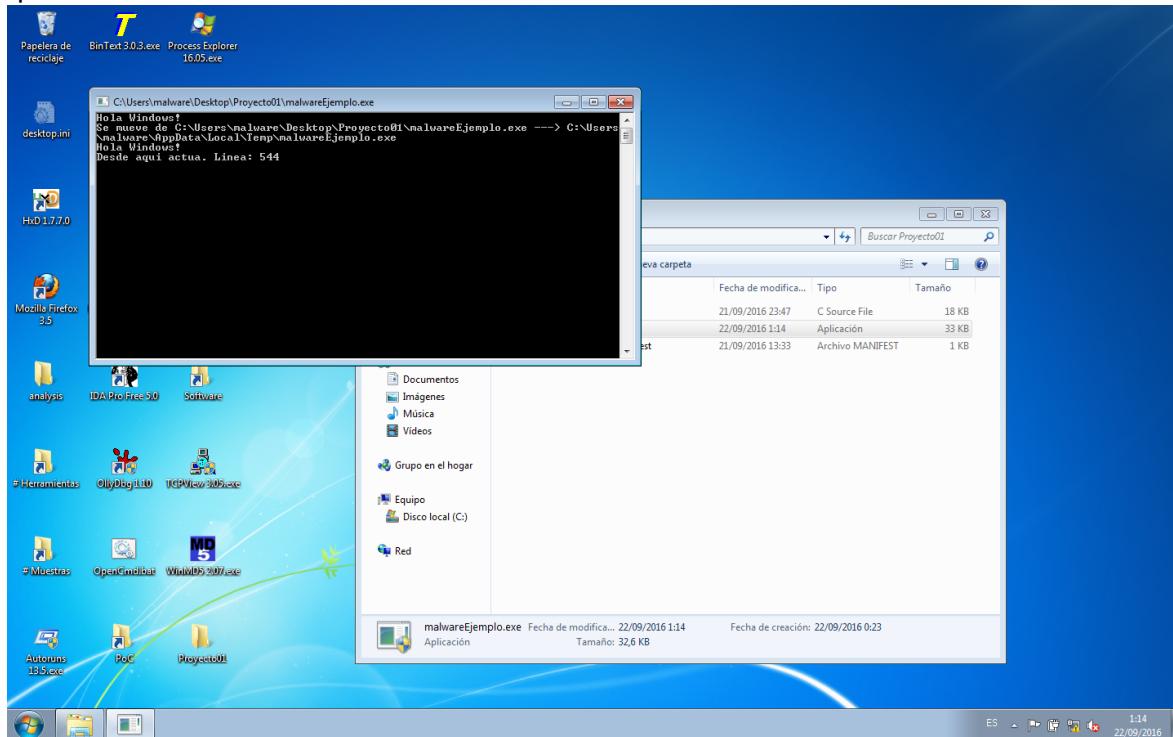


9. El malware pedirá automáticamente permisos de administrador (para generar la persistencia en el sistema) sin embargo, puede ser ejecutado sin permisos de administrador y generar las acciones maliciosas, aunque sin efecto persistente.

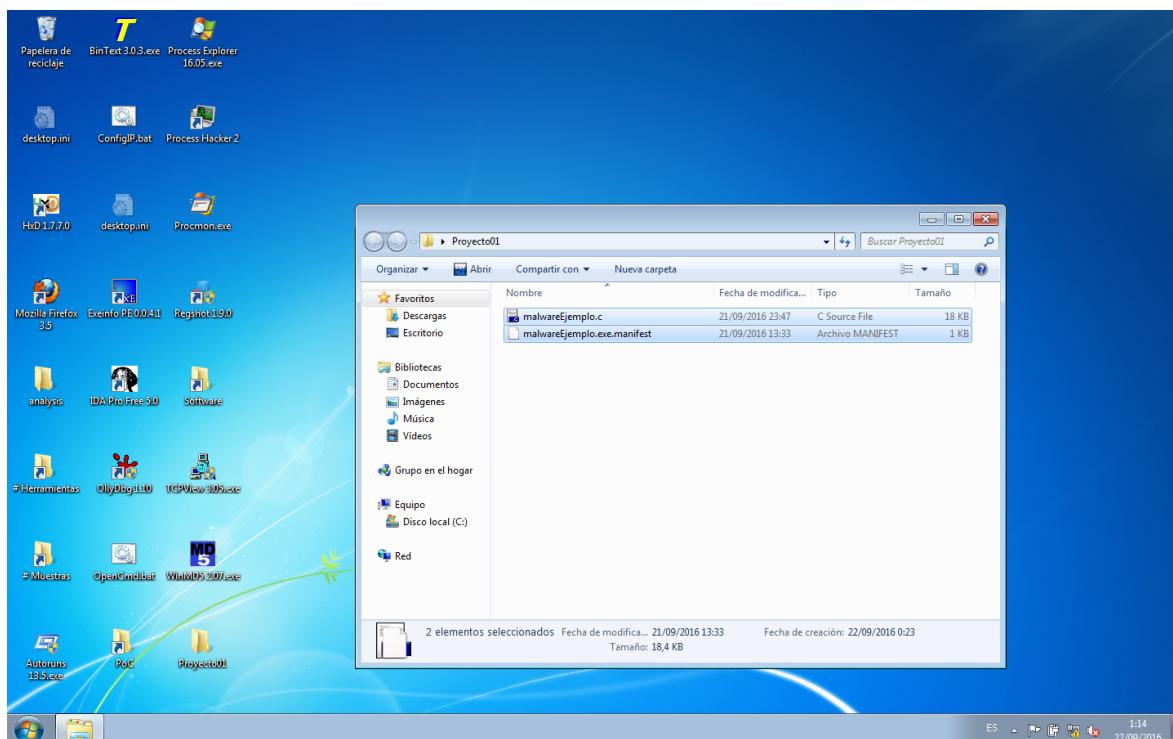


10. A continuación, se presenta un pequeño resumen de lo que el malware hace paso a paso en el sistema:

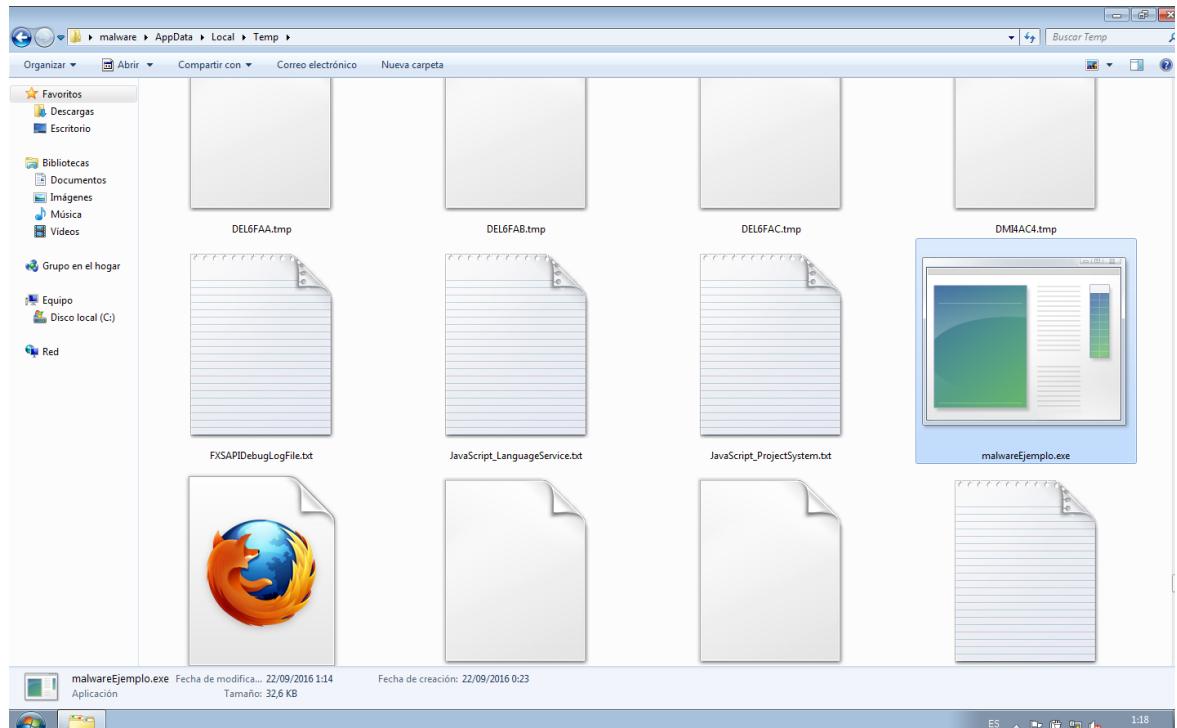
- El malware inmediatamente abrirá una pantalla de la línea de comandos que será cerrada automáticamente casi de inmediato.



- Podremos ver que el archivo con extensión .exe ha desaparecido.

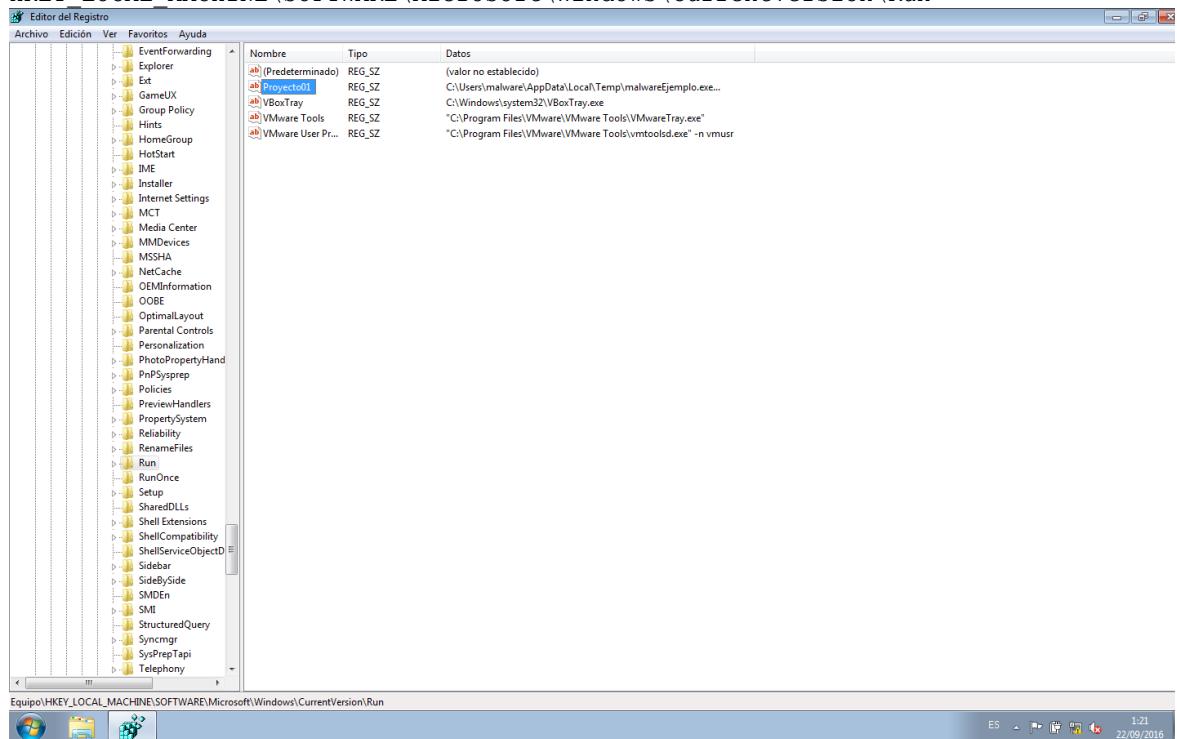


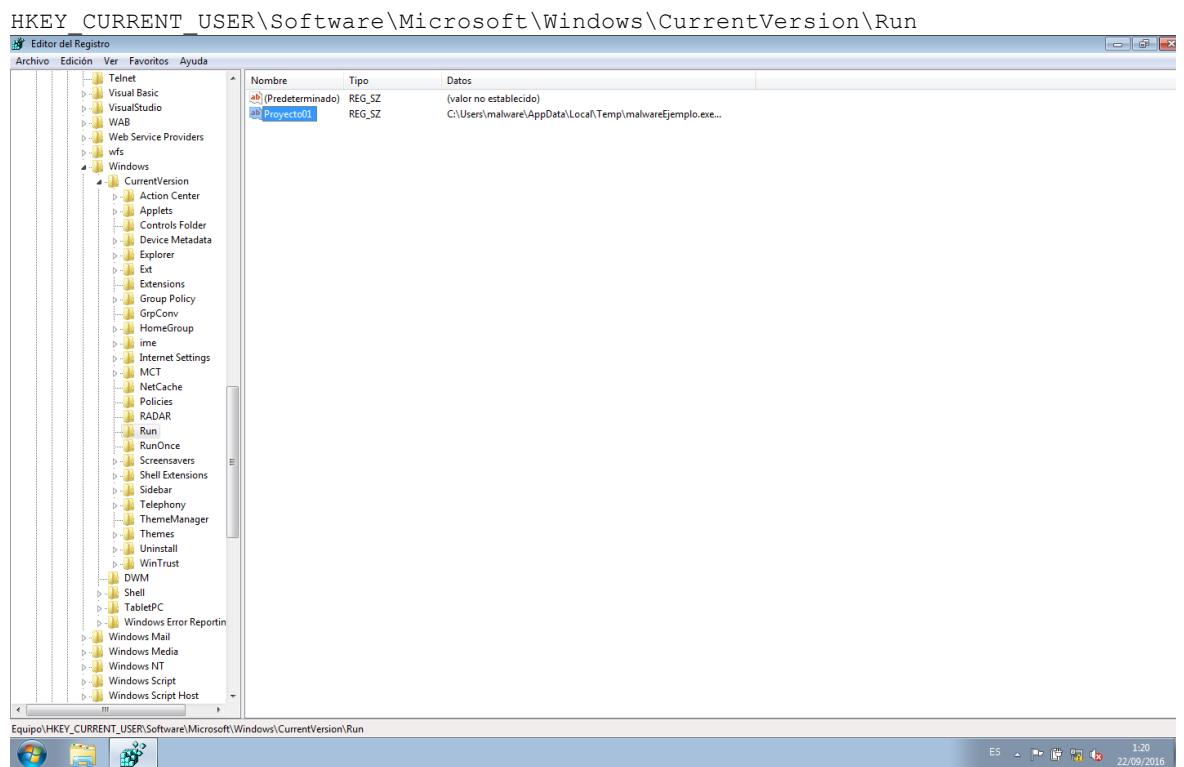
- c. Podemos observar que el archivo malwareEjemplo.exe ahora se encuentra en la dirección de la variable de entorno %tmp%



- d. El malware generó dos llaves de registro en las siguientes rutas:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

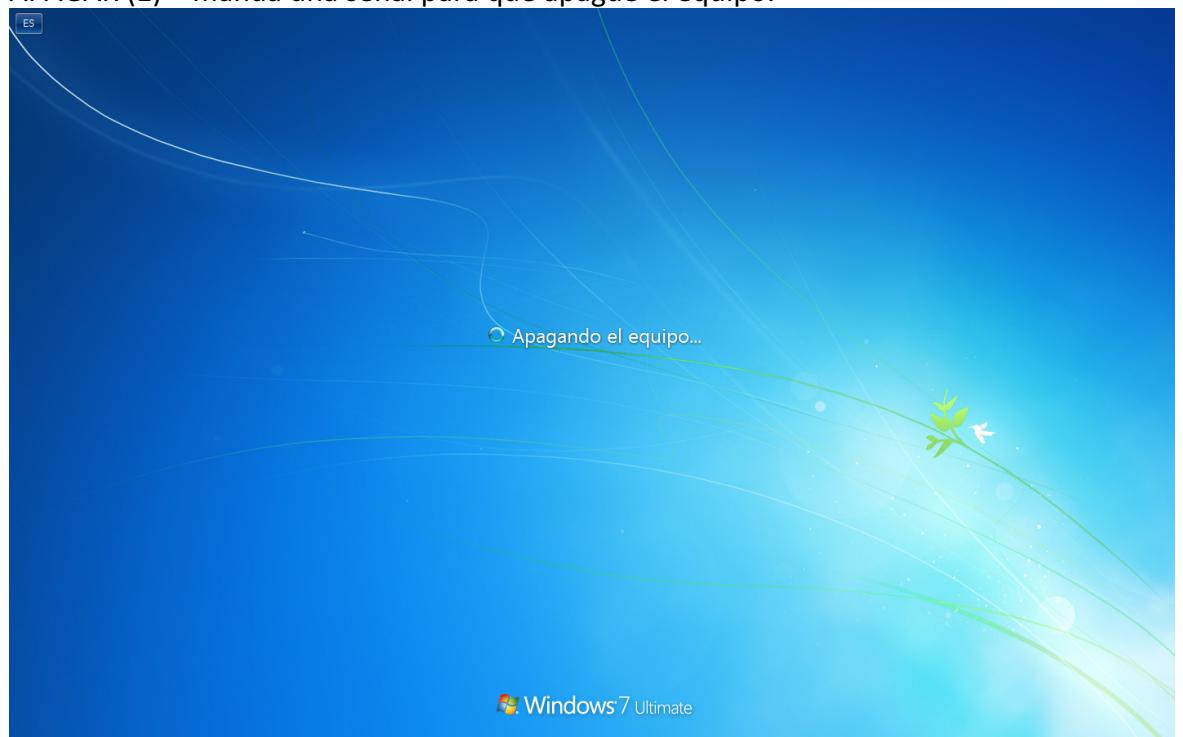




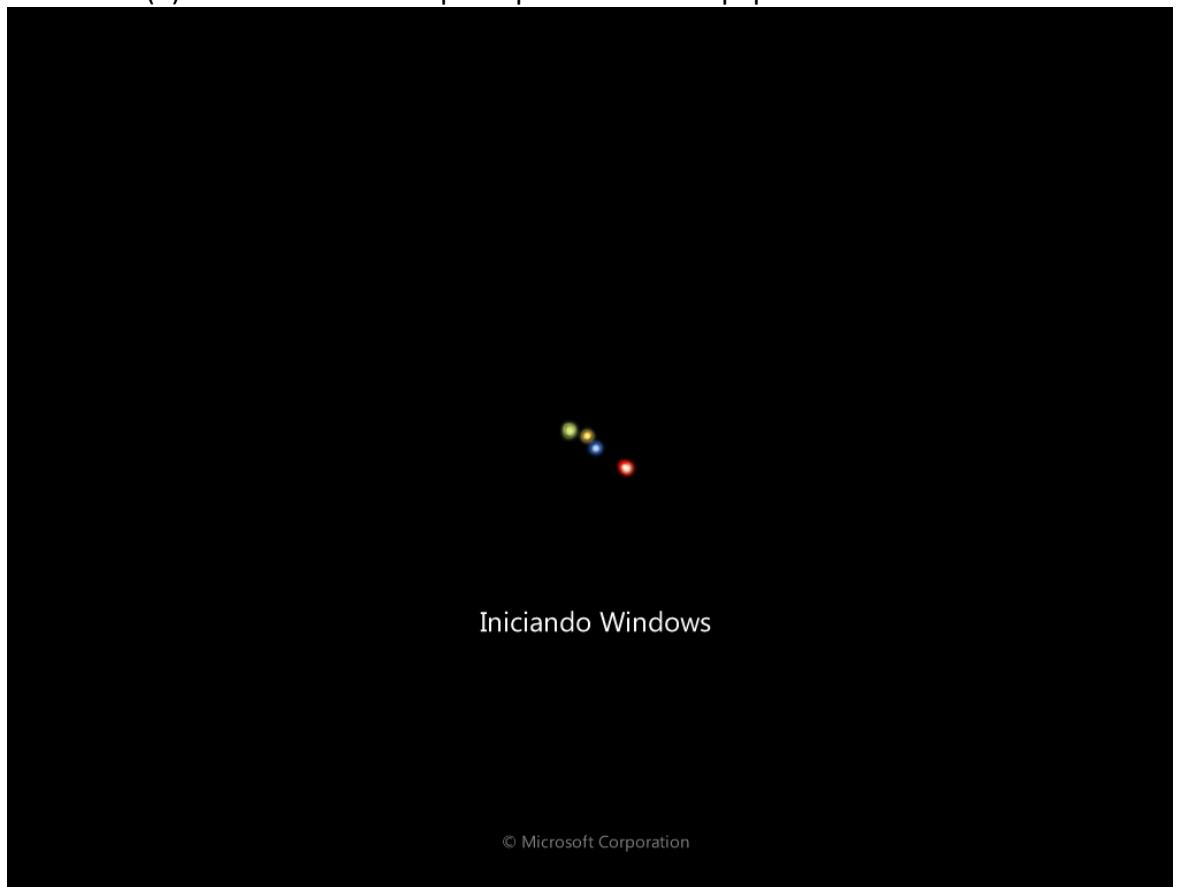
- e. El malware inmediatamente inicia las posibles acciones maliciosas que se describen en el punto 11 de este documento.

11. Acciones maliciosas:

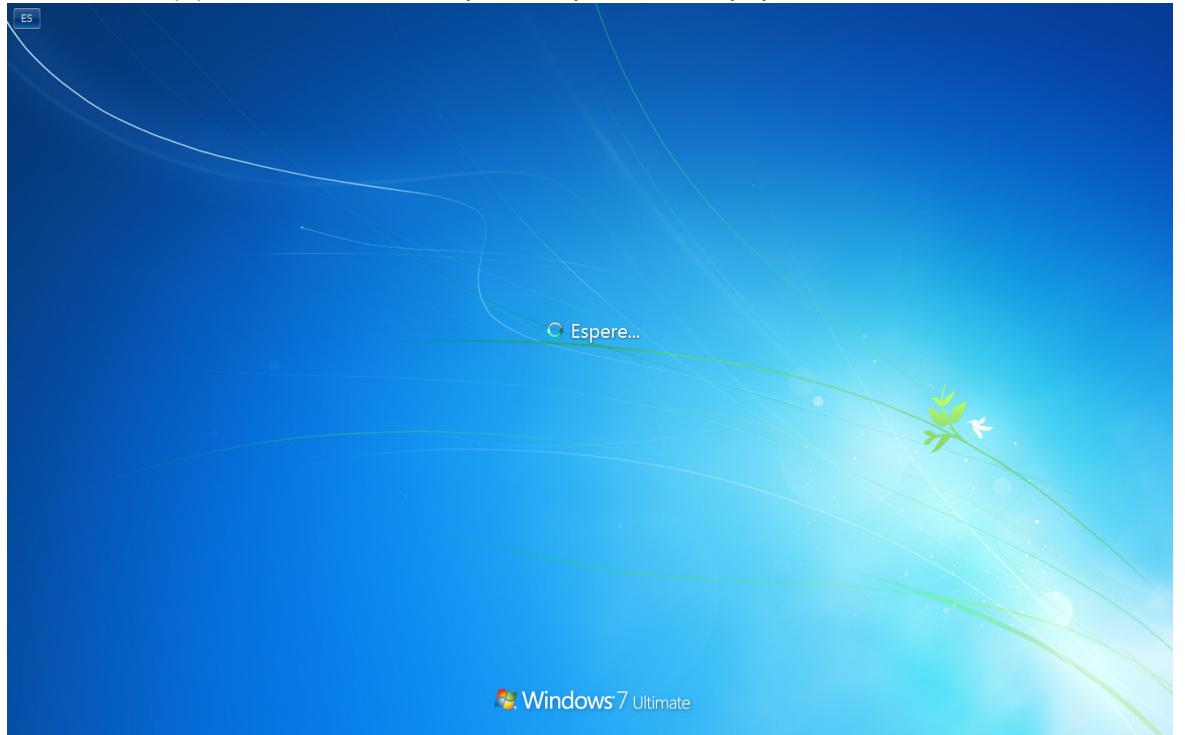
- a. APAGAR (1) – manda una señal para que apague el equipo.



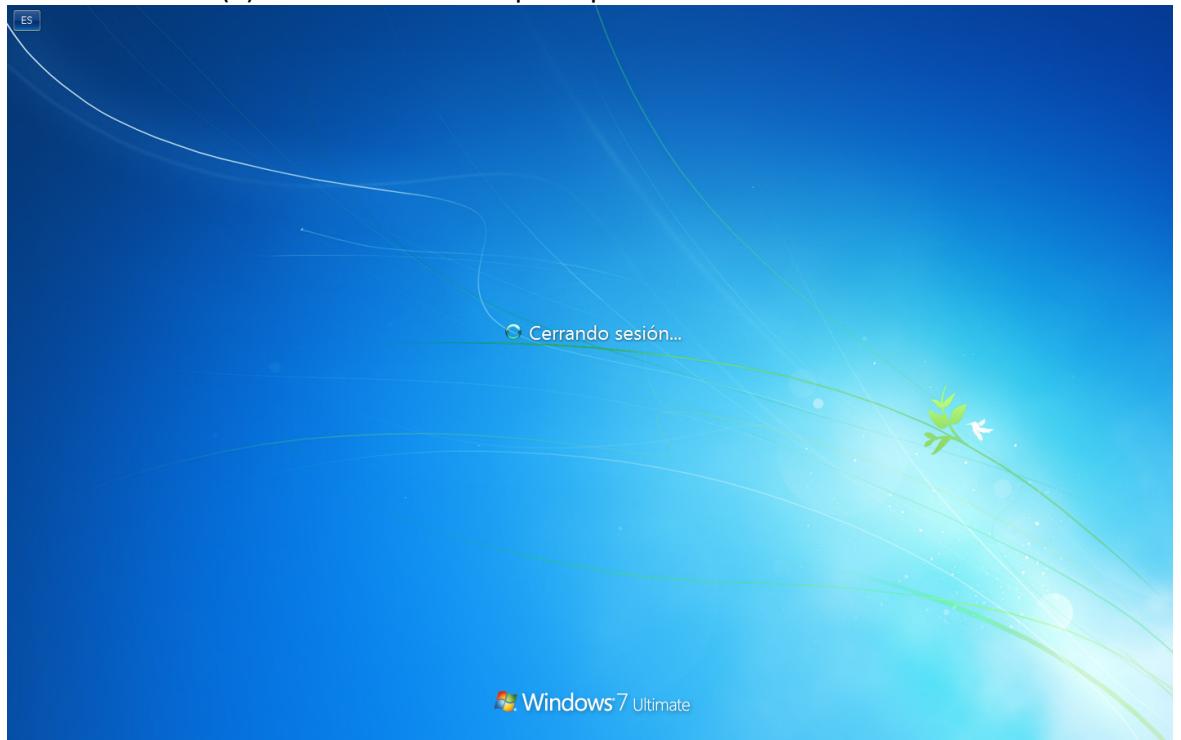
- b. REINICIAR (2) – manda una señal para que reinicie el equipo.



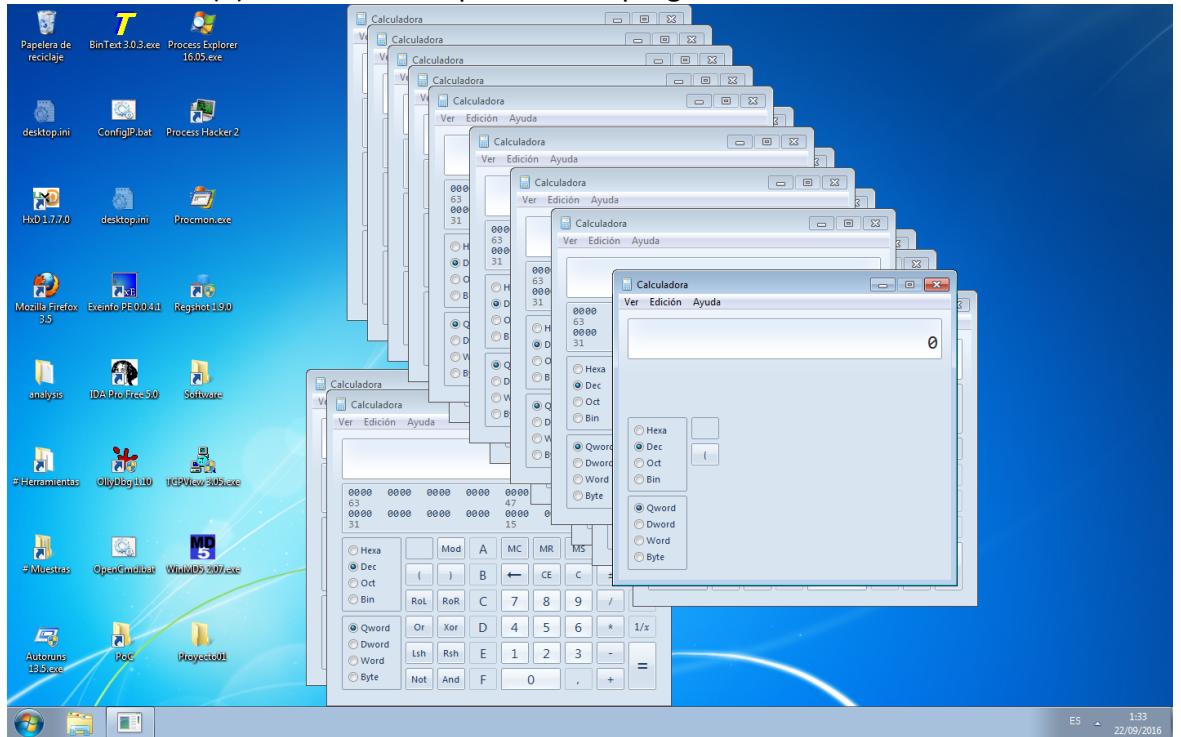
- c. SUSPENDER (3) – manda una señal para suspender el equipo.

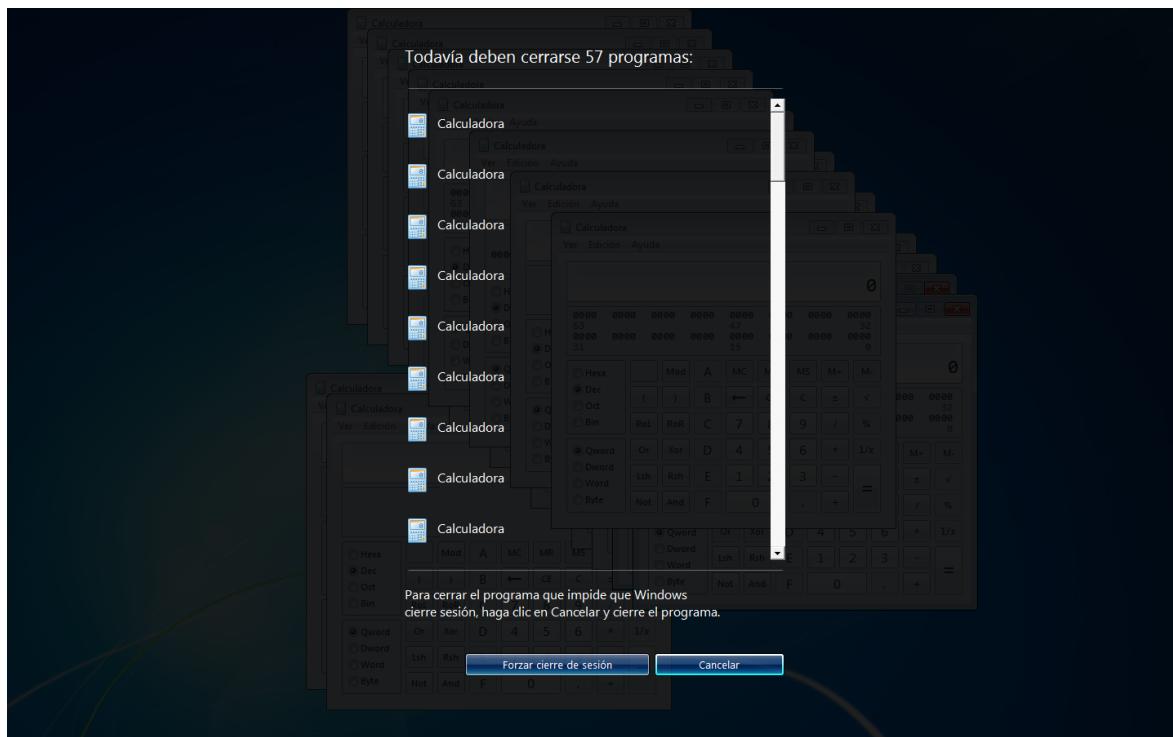


d. CERRAR SESIÓN (4) – manda una señal para que cierre la sesión actual.

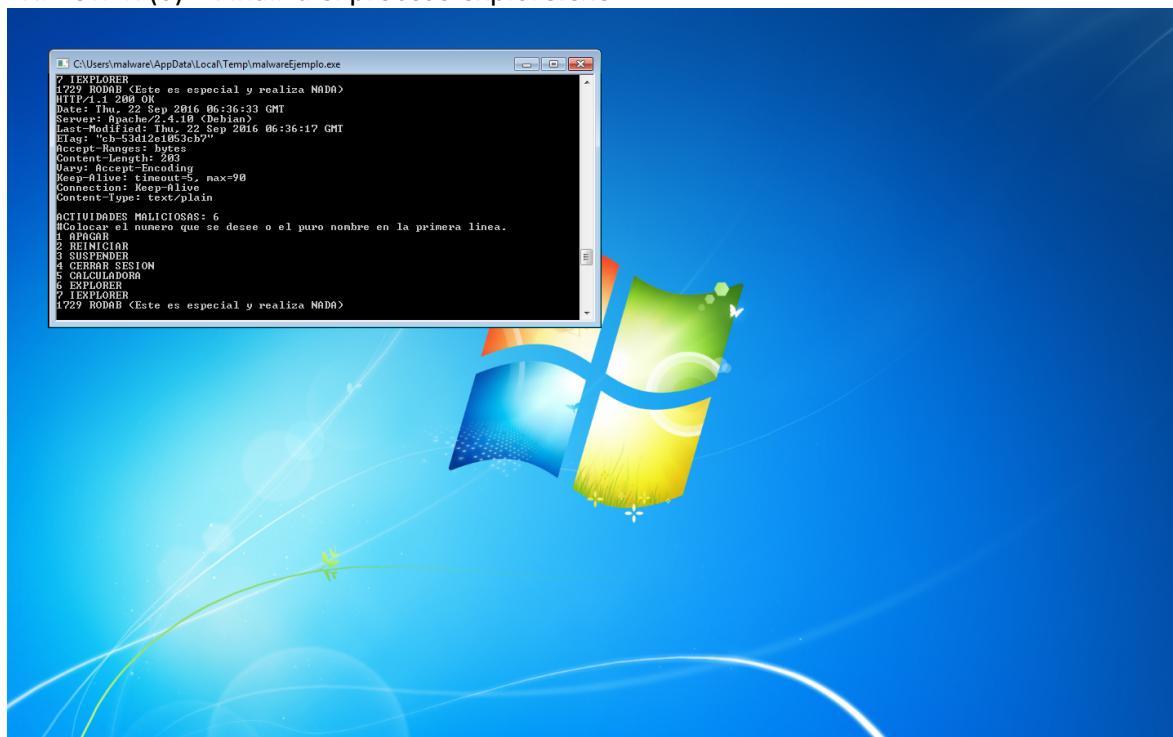


e. CALCULADORA (5) – Abre infinitos procesos de programa calc.exe

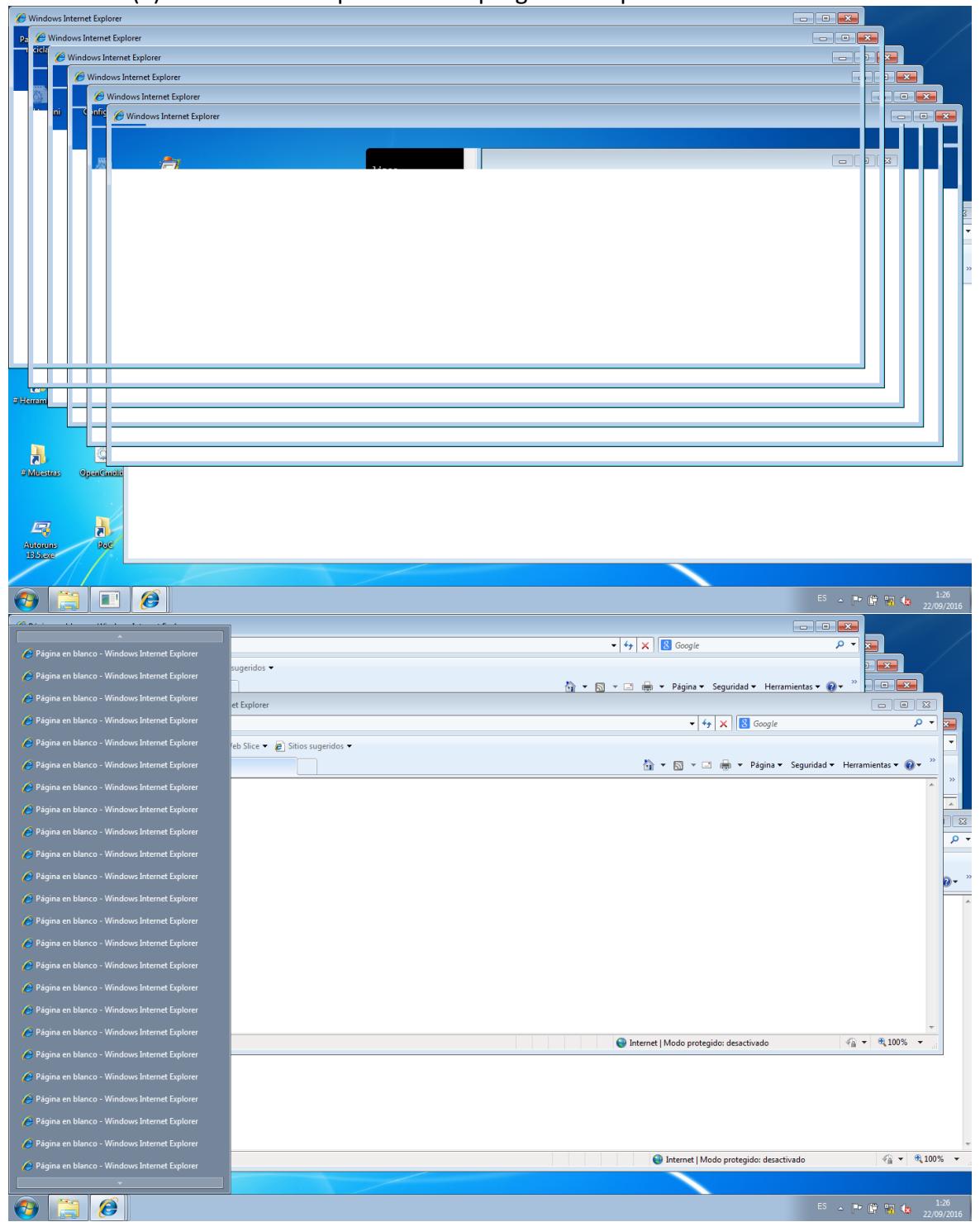




f. EXPLORER (6) – Finaliza el proceso explore.exe



g. IEXPLORER (7) – Abre infinitos procesos del programa iexplore.exe



h. RODAB (1729) – Mata al proceso malwareEjemplo.exe

