laSalle ENG
Ramon Llull University

-

Escola Tècnica Superior d'Enginyeria Electrònica i Informàtica La Salle

Trabajo Final de Máster

Máster en Ciberseguridad

Análisis de Keyloggers mediante ingeniería inversa.

(Estudio, Análisis y Desarrollo de Keyloggers)

Alumno

Gabriel Martí Fuentes

Profesor Ponente

Marc Rivero López

ACTA DEL EXAMEN

DEL TRABAJO FINAL DE MÁSTER

Reunido el Tribunal calificador en el día de la fecha, el alumno

D. Gabriel Martí Fuentes

expuso su Trabajo Final de Máster, el cual trató sobre el tema siguiente:

Análisis de Keyloggers mediante ingeniería inversa.

Acabada la exposición y contestadas por parte del alumno las objeciones formuladas por los Sres. miembros del tribunal, éste valoró dicho Trabajo con la calificación de

Barcelona,

VOCAL DEL TRIBUNAL VOCAL DEL TRIBUNAL

PRESIDENTE DEL TRIBUNAL

Resumen

La seguridad de los sistemas va más allá del control de acceso a estos, del análisis de vulnerabilidades del sistema o de infecciones por virus. Muchas veces el objetivo no es vulnerar el sistema en sí mismo, sino obtener información del usuario que lo usa. El espionaje comercial o industrial, y la revelación de secretos, es en la mayoría de veces el objetivo de los ciberdelincuentes, y una manera rápida de obtener información es saber todo lo que escribe el usuario que es objeto del espionaje.

Es por este motivo que los *keyloggers*[1] han sido siempre una herramienta de uso bastante extendido, que ocupan poco espacio en memoria y pueden pasar inadvertidas durante mucho tiempo en un sistema.

En este documento se estudiarán los diferentes tipos de *keyloggers*, su origen, las técnicas utilizadas para introducirlos en los sistemas, los métodos de ocultación, y como registran y envían la información a los ciberdelincuentes.

Para finalizar, se llevará a cabo el desarrollo de un *keylogger* con funcionalidades similares a alguno de los analizados.

[1] Un *keylogger* es un programa (o dispositivo hardware) que se encarga de registrar todas las pulsaciones de teclas que realiza el usuario y las almacena en un fichero de datos. Este fichero se almacena oculto en el propio equipo (o en el interior del dispositivo), y habitualmente suele ser enviado posteriormente por internet a un servidor.

Índice

Resumen ... 1
Índice ... 2
1. Introducción ... 4
1.1. Contexto ... 4
1.2. Definición básica de KEYLOGGER ... 5
2. Objetivos ... 6
3. Historia y Estado del Arte ... 7
4. Aspectos Legales ... 14
5. Tipología ... 16
6. Técnicas de distribución ... 17
7. Técnicas de ocultación y evasión ... 18
8. Análisis de Keylogger Hardware ... 19
8.1. Keelog KeyGrabber Pico 16Mb ... 21
8.2. Maltronics WiFi KeyLogger Pro ... 23
9. Análisis de Keylogger Software ... 27
9.1. Ingenieria inversa del código ... 29
9.2. Caracteristica 1 ... 29
9.3. Caracteristica 2 ... 29
9.4. Caracteristica 3 ... 29
10. Otras variantes de keyloggers ... 30
10.1. Dispositivos móviles ... 30
10.2. Keyloggers Javascript ... 30
10.3. Keyloggers CSS ... 30
11. Anti-Keyloggers ... 31
12. Desarrollo de un Keylogger ... 32
12.1. Elección del lenguaje para programarlo, ventajas e inconvenientes ... 32
12.2. Caracteristicas del Keylogger ... 32
12.3. Problemas y soluciones ... 32
12.4. Implantación ... 32
12.5. Mejoras posibles ... 32
12.6. Notas finales ... 32
13. Resultados finales ... 33
14. Coste del proyecto ... 33
14.1. Coste temporal ... 33

14.2. Coste económico 34
15. Conclusiones 35
16. Líneas de futuro 35
17. Referencias 36
18. Bibliografía 38
Índice de Ilustraciones 40
Índice de tablas 41

1. Introducción

1.1. Contexto

El espionaje digital es una actividad que va en aumento, y se realiza tanto a nivel gubernamental, como político o privado. Las herramientas y técnicas utilizadas son múltiples, y muchas utilizan sistemas combinados, pero el registro de pulsaciones en los teclados de los ordenadores, y más recientemente también en dispositivos móviles, es una de las características comunes a todos ellos.

El registro de audio o vídeo es más complejo, requiere de más recursos (más uso de memoria, almacenamiento o uso de procesador) y en muchos casos su actividad alerta más fácilmente al usuario.

En cambio, un pequeño programa que, a priori, simplemente registre las pulsaciones del teclado puede pasar desapercibido durante mucho tiempo y puede ser mucho más útil a los ciberdelincuentes o espías digitales.

Existen también dispositivos hardware que realizan esta misma función, aunque tienen sus ventajas e inconvenientes que comentaremos más adelante.

Ilustración 1. Dos modelos de keylogger hardware. Para teclado ps/2 y USB.

En este trabajo se citarán y analizarán brevemente un par de modelos de estos dispositivos hardware, pero nos centraremos principalmente en el estudio de los *keyloggers* por software.

1.2. Definición básica de KEYLOGGER

Keylogger, proveniente de la unión de dos palabras inglesas: ***key*** (tecla) y ***logger*** (registrador), es un dispositivo o programa que registra pulsaciones de teclas. Esta es la definición más corta y básica del *keylogger*.

No obstante si profundizamos podremos ver que los *keyloggers* (sobre todo los implementados por software), llegan a niveles de sofisticación más altos, y muchos no se limitan solo al registro de pulsaciones de teclado, sino que además pueden registrar movimientos y pulsaciones del ratón, información sobre las ventanas de las aplicaciones sobre las que se registran las pulsaciones del teclado o acciones del ratón, añaden capturas de pantalla, y en algunos casos, llegan a abrir un canal de "comando y control" para que se puede acceder y controlar remotamente el equipo dotándolo así de más funcionalidades y características. No obstante, si nos atenemos a su definición original estos últimos aspectos se salen del concepto de keylogger.

2. Objetivos

Los objetivos principales sobre los que se justifica la elaboración de este proyecto son los que se detallan a continuación:

1. Mostrar el Estado del arte de los keyloggers.
2. Conocer los aspectos legales, y saber que dice la legislación Española y Europea sobre su uso.
3. Conocer las técnicas empleadas en la distribución e instalación de estos.
4. Estudiar las funcionalidades que incorporan.
5. Investigar las técnicas de ocultación o evasión que utilizan.
6. Desarrollo de un keylogger.

3. Historia y Estado del Arte

La historia exacta de los keyloggers no se conoce (y es difícil que alguien la conozca), pero sí que existen algunos hechos históricos que nos sitúan cronológicamente en sus orígenes y evolución. Parte de este supuesto origen se puede establecer en la época de la "*Guerra Fría*"[2] entre Estados Unidos y la Unión Soviética. En esa época no era habitual el uso de ordenadores, sino que se utilizaban máquinas de escribir en oficinas y dependencias gubernamentales. En dicho contexto, hacia finales de los años 70, los Rusos desarrollaron unos dispositivos electromagnéticos que implantaron en las máquinas de escribir, en concreto los modelos ***IBM Selectric II y III*** [3], para poder transmitir todo lo que se tecleaba en ellas.

Ilustración 2. IBM Selectric II (1971-1981)

En enero de 1983, mientras reparaban un Teletipo de la Embajada Francesa en Moscú, se descubrió un dispositivo que estaba diseñado para transmitir información hacia el exterior. Los franceses, aliados, alertaron a EEUU, y estos encontraron dispositivos similares en las máquinas de escribir de su Embajada en Moscú y el Consulado en Leningrado[4]. Tras este hallazgo, la NSA (Agencia de Seguridad Nacional, de EEUU) puso en marcha el "***Proyecto Gunman***"[5] que tenía como objetivo detectar, analizar, y responder ante el implante de estos dispositivos, llamados "bugs"[6]. Estos se pueden considerar los precursores de los keyloggers que surgieron posteriormente.

[2] La Guerra Fría fue un enfrentamiento político, económico, social, militar, informativo y científico iniciado tras finalizar la Segunda Guerra Mundial entre el bloque Occidental (occidental-capitalista) liderado por Estados Unidos, y el bloque del Este (oriental-comunista) liderado por la Unión Soviética.
[3] La máquina de escribir IBM Selectric (conocida también como la IBM de bola) fue un influyente diseño de máquina de escribir eléctrica de IBM, cuyo primer modelo salió al mercado en 1961.
[4] Leningrado, conocida hoy en día como San Petersburgo.
[5] Lincoln Faurer, Director de la NSA, creó el "Proyecto Gunman" porque no confiaba que, ni en el Departamento de estado, ni la CIA, manejaran correctamente el asunto. Fue aprobado por Ronald Reagan en febrero de 1984.
[6] Los pequeños dispositivos que son escondidos y utilizados para grabar o interceptar conversaciones o comunicaciones son conocidos como "bugs" (bichos o insectos, si traducimos literalmente).

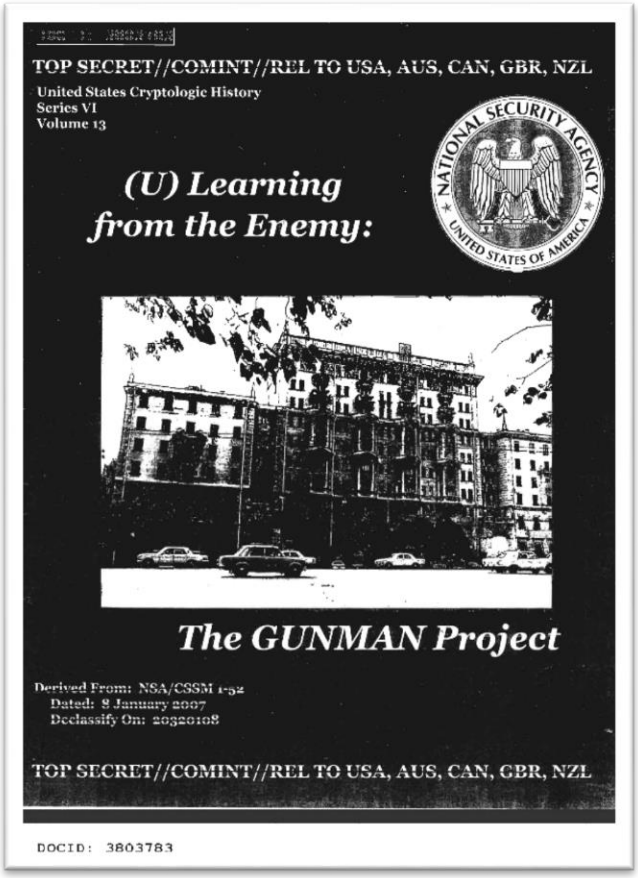


Ilustración 3. Portada del documento de la NSA, "The GUNMAN Project". Desclasificado en Diciembre de 2011

El análisis complejo y exhaustivo de las máquinas de escribir no reveló la modificación de éstas hasta que se hicieron radiografías de toda la máquina y descubrieron la manipulación y los circuitos ocultos. La modificación de las máquinas era compleja, y virtualmente invisible e indetectable.

La modificación contenía circuitos integrados de última generación con una memoria central de 1 solo bit, ocultos dentro un soporte hueco en la parte inferior del teclado. Los datos se almacenaban en un buffer y posteriormente se enviaban en ráfagas cortas y de alta velocidad en las bandas de radio de 30, 60 y 90 Mhz. Estas frecuencias eran cercanas a la de estaciones de TV y ayudó a su ocultación y evitó la detección del envío de datos.

Para saber que teclas se estaban pulsando, disponía de un complejo sistema que detectaba la elevación, inclinación y rotación de la bola para saber qué carácter se estaba tecleando. La cantidad de caracteres existentes en la bola hacia que fueran necesarios 6 bits de datos, pero debido las limitaciones de la época[7] los datos se comprimían en palabras de 4 bits. Se ignoraban teclas especiales como Mayúsculas, Espacio, Retroceso, Tabulador, Retorno de carro, Guiones y algunos caracteres podían

[7] No se sabe exactamente, pero algunas conjeturas apuntan a que los rusos solo tenían acceso a tecnología digital de 4 bits en ese momento, y por ese motivo comprimían los datos de 6 bits a 4 bits.

ser ambiguos ya que se hacía una agrupación binaria de combinaciones de caracteres para poder tenerlo todo en 4 bits. Posteriormente, con los datos recuperados podían adivinar los caracteres ambiguos basándose en un análisis de frecuencias y con teorías de probabilidad.

Ilustración 4. Bola "pelota de golf" de la IBM Selectric, con los caracteres.

El 17 de noviembre de 1983, podemos situarlo como la fecha en la que se conoce el código fuente del primer keylogger creado por software por Perry Kivolowitz, el cual lo publicó en los grupos de noticias de Usenet[8] y dio motivo a una discusión entre usuarios para reforzar la seguridad del sistema operativo Unix.

Situándonos ya en el año 1999, se sabe que el FBI utilizó un keylogger para vigilar al jefe de La Cosa Nostra, Nicodemo Salvatore Scarfo, Jr., conocido como "Little Nicky".

Este hecho es relevante por dos motivos. Fue el primer sospechoso criminal conocido en ser monitorizado con un keylogger. Y el keylogger, aparentemente, no era un desarrollo propio del FBI, sino que era un dispositivo comercial. Esto fue motivado porque Scarfo utilizaba un cifrado para proteger sus comunicaciones y el objetivo era conocer la clave de cifrado de estas. El FBI tuvo que entrar en la oficina de Scarfo 2 veces. Una para instalar el dispositivo, y otra para recuperar el contenido registrado.

En noviembre de 2001, el periodista Bob Sullivan de MSNBC reveló que el FBI estaba desarrollando un software llamado "Magic Lantern" cuya funcionalidad principal era la de keylogger y que además podían instalar y manejar en remoto. Un portavoz del FBI confirmó la existencia de este software en 2002, pero negó que se hubiera distribuido. En 2005 el FBI lo usó extensamente en muchos casos y en 2007 aparecieron los primeros documentos oficiales confirmando su uso y ese mismo año pasó a formar parte de un nuevo software del FBI llamado CIPAV[9]. Magic Lantern se instalaba silenciosamente y no actuaba hasta que detectaba el uso de la herramienta PGP para poder capturar las claves de cifrado. Algunas compañías de antivirus cooperaron junto

[8] Usenet es el acrónimo de Users Network (Red de usuarios), consistente en un sistema global de discusión en Internet, que evolucionó de las redes UUCP.

[9] CIPAV (Computer and Internet Protocol Address Verifier), es un software desarrollado por el FBI en el año 2007, con el objetivo de interceptar y detener hackers, extorsionadores, usuarios de pornografía infantil y delincuentes en general. En 2013 se consideró ilegal el uso de CIPAV.

al FBI para que su herramienta no fuera detectada y se incluyó en listas blancas para no ser detectada por los antivirus. McAffee y Symantec fueron dos de estas empresas.

Pero no solo para cazar a mafiosos se usan los keyloggers. En este caso, fue el ladrón el que lo utilizó. En febrero de 2003, un estudiante Universitario, Douglas Boudreau, fue arrestado por haber instalado un keylogger en más 100 ordenadores del Boston College. Recopiló información sobre unos 4800 profesores, empleados y estudiantes de dicha Universidad. Con los datos recopilados consiguió robar cerca de $2000.

En enero de 2004, un gusano, llamado MyDoom[10] provocó una gran epidemia convirtiéndose en el gusano de correo electrónico que más rápido se propagó. El hecho es que contenía un keylogger para capturar los números de tarjetas de crédito.

Con la llegada del nuevo milenio parece ser que los keyloggers se empezaron a popularizar entre los delincuentes, y a finales de 2004, un grupo de ciberdelincuentes formado por jóvenes rusos y ucranianos, enviaron múltiples correos electrónicos a clientes de bancos en Francia. Estos correos electrónicos contenían un archivo adjunto con un keylogger o enlaces a sitios web que contenían dicho keylogger. Los usuarios eran engañados mediante métodos de ingeniería social, y una vez instalado el malware[11], este quedaba oculto e inactivo y solo entraba en funcionamiento al detectar que el usuario accedia al sitio web de la entidad bancaria, para proceder en ese momento a registrar las contraseñas y los códigos bancarios.

En febrero de 2005, un empresario de Florida, Joe Lopez, presentó una demanda contra Bank of America por que le habían robado $90,000 de su cuenta y habían sido transferidos a una cuenta de Letonia. En realidad, el ordenador de Lopez había sido infectado por el virus “Backdoor Coreflood” que abría una puerta trasera al ordenador e incorporaba un keylogger. Los hackers consiguieron así los datos de acceso a las cuentas bancarias. Joe Lopez perdió el juicio porque consideraron que había sido negligente y no había tomado precauciones al manejar sus cuentas bancarias por internet.

En mayo de 2005 la policía israelí detuvo a un matrimonio en Londres que elaboraba programas maliciosos a medida para realizar espionaje industrial. Evidentemente, con la funcionalidad de keylogger. Estos programas eran vendidos a compañías israelíes que los utilizaban para espiar a sus competidores. El creador, Michael Haephrati[12], fue sentenciado a dos años de prisión, pero mantiene su compañía de seguridad, “Target Eye Limited”, donde anuncia sus productos de “vigilancia y monitorización para capturar la actividad de ordenadores remotos”.

[10] Mydoom, también conocido como W32.MyDoom@mm, Novarg, MiMail.R y "Shimgapi", fue un gusano informático que afecta a sistemas Windows. Su velocidad de propagación superó los registros anteriores establecidos por el gusano Sobig y ILoveYou.

[11] El concepto de malware procede de la expresión inglesa “malicious software”. Se trata de un software malicioso: es decir, de un programa informático cuya finalidad es provocar un daño en un sistema.

[12] Michael Haephrati. Se puede consultar su perfil en LinkedIn en el siguiente enlace: https://www.linkedin.com/in/haephrati/

Ilustración 5. Muestra de una sección del perfil de LinkedIn de Michael Haephrati. Detenido en 2005 por la creación y venta de un keylogger.

Keyloggers en dispositivos móviles, Android …..

https://www.newscientist.com/article/mg21128255-200-smartphone-jiggles-reveal-your-private-data/

El éxito de los keyloggers para llevar a cabo ciberdelitos estaba consolidado y con éxito asegurado. Tal es así que en el año 2013 se empezó a gestar el mayor ataque de robo financiero dirigido contra un banco. En este caso el keylogger era una pieza clave del malware pero que además estaba dotado de muchos más elementos y funcionalidades de malware, como captura de pantalla y comandos remotos. La operación, llamada “Carbanak”, culminó con un robo de 1000 millones de dólares.

---------- ¿???? ----------

https://www.kaspersky.es/blog/el-mayor-atraco-del-siglo-los-hackers-roban-mil-millones-de-dolares/5370/

https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf

https://www.lasexta.com/tecnologia-tecnoxplora/internet/asi-robaron-ciberdelincuentes-1000-millones-dolares-bancos_2015022257f790ce0cf2fd8cc6aaa1d2.html

Abril 2015

https://www.telegraph.co.uk/news/uknews/law-and-order/11560173/Exam-cheat-jailed-for-hacking-into-university-computer-system.html

https://nakedsecurity.sophos.com/es/2015/04/27/student-jailed-for-using-keylogger-to-up-his-exam-marks/

En octubre de 2017 se conoció la noticia de que un estudiante de la Universidad de Kansas había sido expulsado por haber usado un keylogger de hardware y haber usado los datos adquiridos para acceder al sistema de calificaciones y cambiarse las notas.

A finales del año 2017, el experto en seguridad Michael Myng detecto un problema en el software controlador del teclado del fabricante Synaptics instalado en algunos modelos de ordenadores portátiles de la marca HP. Dicho controlador tenía la capacidad de poder registrar los códigos de escaneo del teclado sobre un archivo de log mediante las herramientas WPP Tracing de Microsoft. Esto abría la posibilidad de que un malware pudiera activar un keylogger en dichas maquinas con solo cambiar unos valores en el registro de Windows. A pesar de que el keylogger no estaba activo, el riesgo existía y obligó al Synaptics y HP a actuar lo antes posible para corregir el driver y publicar una actualización de este para todos los modelos afectados.

En diciembre de 2017, la empresa de seguridad SUCURI, alertó en su blog de la presencia de miles de sitios WordPress[13] infectados con un keylogger desarrollado íntegramente en JavaScript[14]. En enero de 2018 apareció una evolución de este.

```
function process_event(event) {
    var result = JSON.stringify({
        key: event.target.value,
        element: event.target.id
    });
    socket.send(result);
}

var i_fields = document.getElementsByTagName('input');
for (var i = 0; i < i_fields.length; i++) {
    i_fields[i].addEventListener('blur', process_event);
}
```

Ilustración 6. Código del keylogger inyectado después de su decodificación.

Un descubrimiento reciente, en Julio de 2019, del experto en seguridad Marcus Mengs, ha puesto al descubierto un fallo de seguridad en los dispositivos inalámbricos (teclados y ratones) del fabricante Logitech que utilizan la tecnología Unifying para usar un solo

[13] WordPress es un sistema de gestión de contenidos, enfocado a la creación de cualquier tipo de página web. Originalmente alcanzó una gran popularidad en la creación de blogs, para convertirse con el tiempo en una de las principales herramientas para la creación de páginas web comerciales.

[14] JavaScript es un lenguaje de programación interpretado, dialecto del estándar ECMAScript. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico.

receptor para los mismos dispositivos. Este fallo de seguridad demuestra como un usuario que se encuentre en las inmediaciones, puede capturar todo lo que se teclea en el ordenador que usa los teclados de Logitech e incluso enviar comandos personalizados al equipo.

Hay muchos más casos, y los mostrados aquí son una pequeña selección, quizás los más relevantes, para podernos hacer una idea de los usos y evolución de los keyloggers.

De estos casos se puede vislumbrar una cierta evolución que empieza en el espionaje entre estados o poderes políticos, pasando al uso para la vigilancia policial, llegando ya al uso para el robo de credenciales y datos bancarios y el espionaje industrial.

En cualquier caso, existe multitud de empresas que venden su producto de moitorización (keylogger y muchas más funcionalidades) como algo perfectamente legal y que se puede usar desde monitorizar el uso de equipos en entorno laboral hasta el control parental, para que los padres puedan tener un control de lo que hacen sus hijos.

4. Aspectos Legales

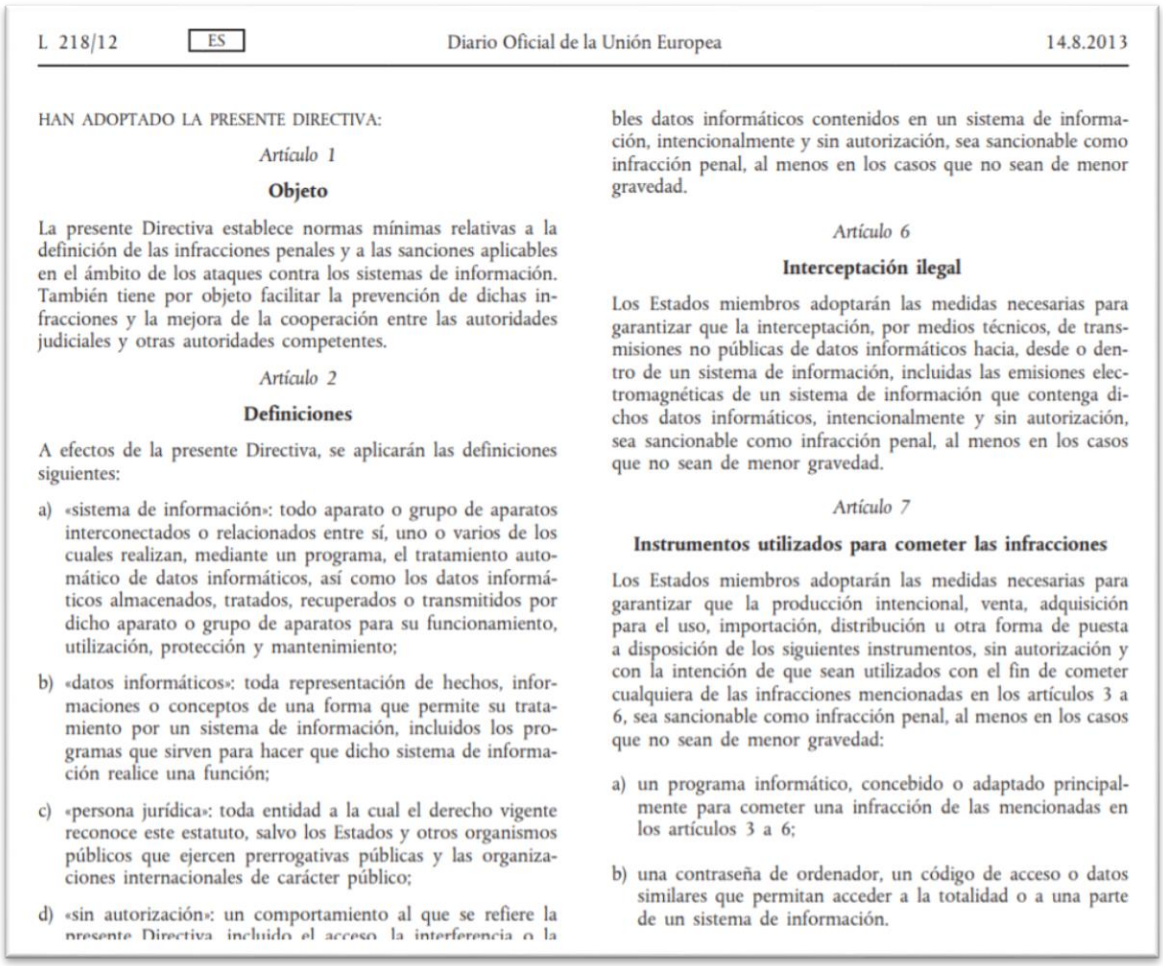
Como se ha comentado en el punto anterior, existen keyloggers (o software que lo incorporan) que se veden comercialmente y, por lo tanto, supuestamente es legal.

Veremos en este apartado que dice la legislación Española y, la Europea, para ver en qué situación se encuentra este tipo de dispositivos y/o programas.

Notas:

https://eynde.es/es/derecho-penal-europeo-delitos-informaticos/

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013L0040&qid=1442911632730&from=EN



L 218/12 ES Diario Oficial de la Unión Europea 14.8.2013

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Objeto

La presente Directiva establece normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información. También tiene por objeto facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes.

Artículo 2

Definiciones

A efectos de la presente Directiva, se aplicarán las definiciones siguientes:

a) «sistema de información»: todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento;

b) «datos informáticos»: toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función;

c) «persona jurídica»: toda entidad a la cual el derecho vigente reconoce este estatuto, salvo los Estados y otros organismos públicos que ejercen prerrogativas públicas y las organizaciones internacionales de carácter público;

d) «sin autorización»: un comportamiento al que se refiere la presente Directiva, incluido el acceso, la interferencia o la

bles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Artículo 6

Interceptación ilegal

Los Estados miembros adoptarán las medidas necesarias para garantizar que la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Artículo 7

Instrumentos utilizados para cometer las infracciones

Los Estados miembros adoptarán las medidas necesarias para garantizar que la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de los siguientes instrumentos, sin autorización y con la intención de que sean utilizados con el fin de cometer cualquiera de las infracciones mencionadas en los artículos 3 a 6, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad:

a) un programa informático, concebido o adaptado principalmente para cometer una infracción de las mencionadas en los artículos 3 a 6;

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Ilustración 7. Diario Oficial de la Unión Europea.
DIRECTIVA 2013/40/UE. 12 agosto 2013.
Extracto del contenido relativo a los ataques contra los sistemas de información.

Asf asfdasdf asfa sdf as asdf lasjkdf

Asdfasdfasfasa
Asdfasfadsfasf
asfdsafas

5. Tipología

Como se ha comentado anteriormente, podemos dividir los keyloggers en 2 grandes grupos: Hardware y Software.

La funcionalidad principal, el registro de teclas, la cumplen a la perfección los dos tipos, pero cada uno tiene unas ventajas en inconvenientes que resumimos en la siguiente tabla:

Tipo	Ventajas	Inconvenientes
Hardware	• No se necesita acceso al sistema operativo, y por lo tanto no se requieren credenciales de usuario. • Los datos se almacenan dentro del propio dispositivo no dejando rastro en el equipo. • No se requiere drivers, ni software adicional que se tenga que instalar en el sistema. • Registra las pulsaciones de teclas para todos los usuarios que usen el equipo. • Indetectable para los antivirus o escáneres de seguridad. • Rapidez de instalación: Plug&Play. • Compatibilidad para diferentes sistemas: MS-DOS, Windows, Linux, Mac.	• Visible externamente por el usuario, por lo tanto, detectable si inspecciona las conexiones. • No tiene posibilidad de saber que usuario ha escrito el texto almacenado. • No tiene posibilidad de saber en qué ventana de aplicación se estaba escribiendo el texto almacenado. • Se requiere tener un dispositivo físico por cada máquina a controlar.
Software	• Permite identificar que usuario ha escrito el texto almacenado. • Se puede saber en qué ventana de aplicación se estaba escribiendo el texto almacenado. • Versátil y actualizable. Puede tener más funcionalidades que complementen su utilidad. • Difícilmente detectable por el usuario medio.	• Se requiere acceso a la cuenta de usuario para instalarlo. • Requiere versión específica para el sistema operativo que se vaya a usar. • Para acceder al contenido registrado se debe de enviar a un servidor externo o el usuario debe acceder a la máquina para ver el contenido.

6. Técnicas de distribución

Las técnicas de distribución en el caso de los keyloggers hardware son claras; el acceso físico al equipo del que se quieren registrar las teclas.

En el caso de los keyloggers por software la distribución varía en función de los intereses o motivos de quien lo distribuya o instale.

En el caso de Padres cuyo objetivo es tener un control sobre el uso que hacen los hijos del ordenador y saber a qué lugares acceden, la técnica de distribución es la instalación directa en el equipo a monitorizar, pues son también propietarios de ellos.

En el caso de empresas, la distribución es la misma, y los motivos pueden ser similares, o incluso conocer si el empleado si está llevando algún tipo de competencia desleal en la empresa, pero la instalación del keylogger suele ser directa en el equipo, o incluso usar un keylogger hardware. Conviene remarcar que aun siendo un equipo propiedad de la empresa, el hecho de instalar un keylogger se considera una actuación delictiva.

Cuando se trata de ciberdelincuentes no es habitual el uso de un keylogger hardware por el hecho que implica acceder físicamente al equipo de la víctima y por lo evidente que sería al ver el dispositivo. Así que el uso es mayoritariamente un keylogger software y su distribución puede ser por diferentes medios, aunque la técnica común es usar la ingeniería social con el objeto de hacer creer al usuario de que esta descargando o recibiendo un documento o una aplicación legítima.

- Memoria USB con software que induce al usuario, mediante ingeniería social, a ejecutarlo: demostración de un juego, software comercial falso, software pirata, etc, el cual tras intalar-se instala silenciosamente el keylogger en el sistema.
- Web que ofrece al usuario la descarga de un programa que “promete hacer algo” y en realidad, aunque podría hacer lo que dice sigilosamente instala también el keylogger. Muchas veces estas webs tienen detrás una red de anuncios publicitarios para la distribución (Malvertising). En muchos casos dicho anuncio falso se muestra en sitios legítimos los cuales incitan al usuario a hacer ‘click’ en el anuncio y en ese momento se descarga el keylogger en el equipo.
- Envio de email phishing o spread phishing. Dependiendo de si es un intento al azar o con una víctima concreta (spread phishing), se hace un envío de un email falso, con la intención de que el usuario acceda a una web, o se descargue una aplicación la cual instalará el keylogger en su equipo.
-

7. Técnicas de ocultación y evasión

Cuando hablamos de técnicas de ocultación y evasión nos referiremos a los keyloggers software, ya que en el caso de un keylogger hardware es evidente que su ocultación es prácticamente imposible. No obstante, haré un inciso, pues bien es cierto que existen algunos fabricantes que tienen circuitos con función de keylogger preparados para ser instalados en el interior de teclados normales. Hecho que implica tener que desmontar el teclado, hacer el montaje, probablemente con necesidad de hacer soldaduras y volver a cerrar el teclado.

Ilustración 8. Muestra de keylogger instalado en el interior de un teclado.

Pendiente --- pendiente --- pendiente --- pendiente ---

8. Análisis de Keylogger Hardware

En este apartado se han estudiado dos keyloggers de diferentes características de dos fabricantes diferentes. Se ha evaluado su facilidad o dificultad en la instalación y puesta en marcha, así como la eficacia, seguridad y utilidad de los resultados obtenidos. La diferencia más notable es que uno de los modelos tiene conexión Wifi, y esto también se evidencia en su coste, aunque curiosamente tienen exactamente las mismas dimensiones y factor de forma por lo que puestos uno al lado del otro no se puede distinguir uno del otro.

Ilustración 9. Foto de los keyloggers hardware analizados

Ilustración 10. Vista en detalle de los dos keyloggers

A continuación, se muestra una tabla comparativa, a modo de resumen de las características de cada uno de los keyloggers.

	Keelog KeyGrabber Pico	Maltronics WiFi KeyLogger Pro
Tipo	USB	USB
Precio	29 €	44 £
Dimensiones	20mm x 18mm x 12mm	20mm x 18mm x 12mm
Memoria	16Mb	16Mb
Protección por Contraseña	✓	✗
Plug & Play	✓	✓
Configurable	✓	✓
Modo Flash Drive	✓	✓
Indetectable por Antivirus	✓	✓
Ajuste layout/idioma teclado	✓	✓
Borrado remoto Log	✗	✓
Guarda pulsaciones en un fichero Log	✓	✓
Registro de fecha y hora	✗	✓
Envio Log por email	✗	✓
Conexión Wifi	✗	✓
Modo Access Point	✗	✓
Data Streaming	✗	✓
Monitorización remota a través de servicio web	✗	✓

8.1. Keelog KeyGrabber Pico 16Mb

Este keylogger solo requiere la única acción de conectarse al puerto USB entre el ordenador y el teclado. Si se conecta a un equipo portátil, pero no se conecta un teclado externo no tiene ningún efecto pues es imprescindible que los datos pasen a través del keylogger para capturar las pulsaciones de las teclas.

Ilustración 11. KeyGrabber en su empaquetado original.

Ilustración 12. KeyGrabber conectado al teclado.

Una vez conectado no se requiere de ninguna acción más y a partir de ese momento cualquier tecla pulsada en el teclado en el que está conectado será capturada y guardada en la memoria interna del dispositivo para poder ser revisada posteriormente.

Para ver el contenido capturado se debe de tener acceso físico al equipo, y desde el mismo equipo o extrayendo el keylogger y conectándolo a otro ordenador de la misma manera que en el equipo monitorizado, se podrá acceder al contenido de la memoria para ver el contenido de las teclas capturadas.

Para ello, el keylogger espera una combinación de teclas a modo de contraseña que deben de ser pulsadas al mismo tiempo. Por defecto la combinación de teclas es K-B-S, la cual activará el modo Pendrive que habilitará una letra de unidad en el sistema y nos permitirá acceder al fichero de log llamado LOG.TXT

También se podrá observar un manual en PDF y un archivo CONFIG.TXT que permite ajustar algunos parámetros en caso de ser necesarios (pero no imprescindibles) como la configuración de idioma del teclado conectado, cambiar el password por defecto, o si se guardan las teclas especiales.

El contenido del fichero se puede examinar con la misma aplicación de “Bloc de Notas” de Windows o cualquier otra aplicación, en incluso sistema, que pueda abrir un fichero de texto. Las teclas especiales se indican como palabras clave encerradas entre corchetes “[ ]” de manera que la tecla de borrado hacia atrás, conocida como “Backspace” queda registrada como “[Bck]”.

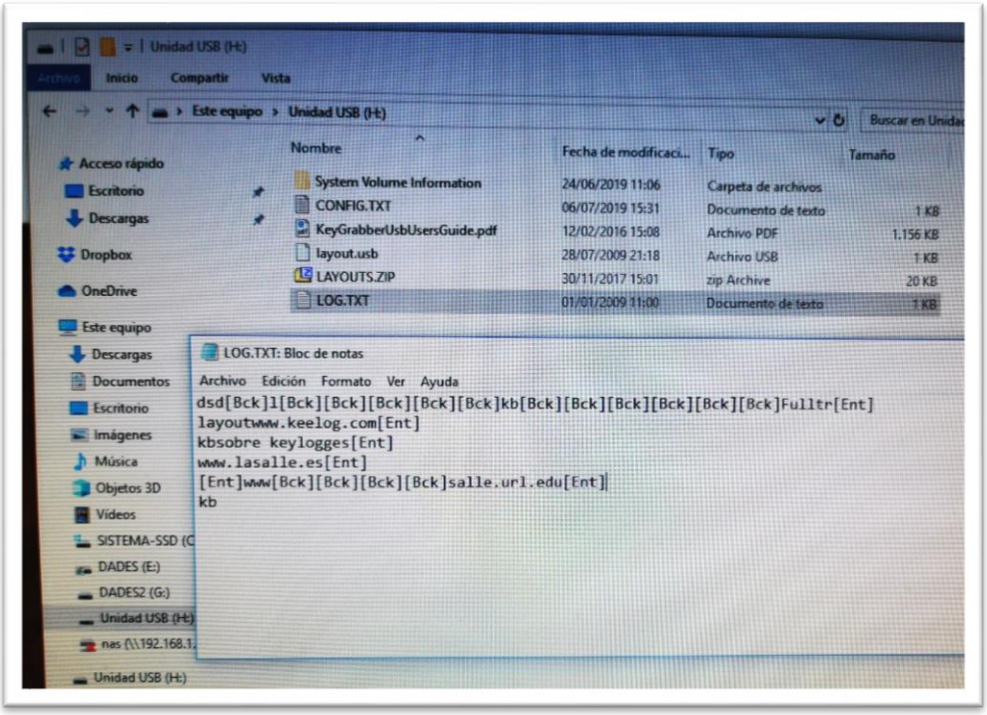


Ilustración 13. Ejemplo de fichero de LOG con el contenido capturado por el keylogger.

Se puede obtener más información de este keylogger en el siguiente sitio web:

http://www.keelog.com/keygrabber-pico-usb-16mb-tiny-usb-hardware-keylogger-with-16mb-flash-drive/

8.2. Maltronics WiFi KeyLogger Pro

Este keylogger, al igual que el analizado en el punto anterior, también se puede usar directamente conectándolo al equipo del que se desean registrar las pulsaciones del teclado. No obstante, tiene una serie de características adicionales que se pueden configurar, y que hacen aconsejable hacer unos ajustes previos desde otro equipo para aprovechar al máximo todas sus posibilidades.

Al conectarlo al puerto USB de un equipo activa un punto de acceso WiFi con el nombre "AIR_xxxxxx" donde "xxxxxx" es una combinación de números hexadecimales que varía con cada dispositivo. Esta conexión es inicialmente "abierta", lo que significa que cualquier equipo que pueda detectar dicha conexión en su ordenador podrá conectarse al keylogger, de ahí la importancia de configurar el keylogger inicialmente.

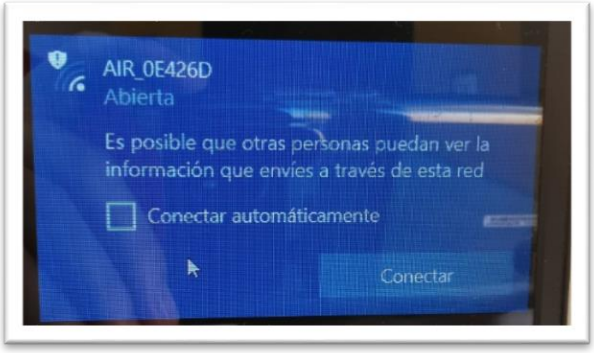


Ilustración 14. Vista del SSID activo del keylogger analizado.

Nos podremos conectar con un navegador a la administración del keylogger en la dirección IP (por defecto) 192.168.4.1, y el primer paso a efectuar será configurar el punto de acceso activando un cifrado de la comunicación y estableciendo una contraseña. Opcionalmente podemos cambiar el nombre del punto de acceso (SSID) y también establecer que sea oculto.

El siguiente punto a configurar es el nivel de detalle de las teclas especiales a registrar, el lenguaje del teclado utilizado o el nivel de filtrado del teclado que vendría a ser la sensibilidad que se puede ajustar en caso de no registrarse todas las teclas, aunque con el valor por defecto que trae parece ser suficiente.

Tras configurar estos valores, ya se puede conectar el keylogger en el equipo a monitorizar, y desde otro equipo (dentro de un radio de alcance WiFi) nos podríamos conectar al keylogger y ver el contenido de las pulsaciones de teclas que va registrando.

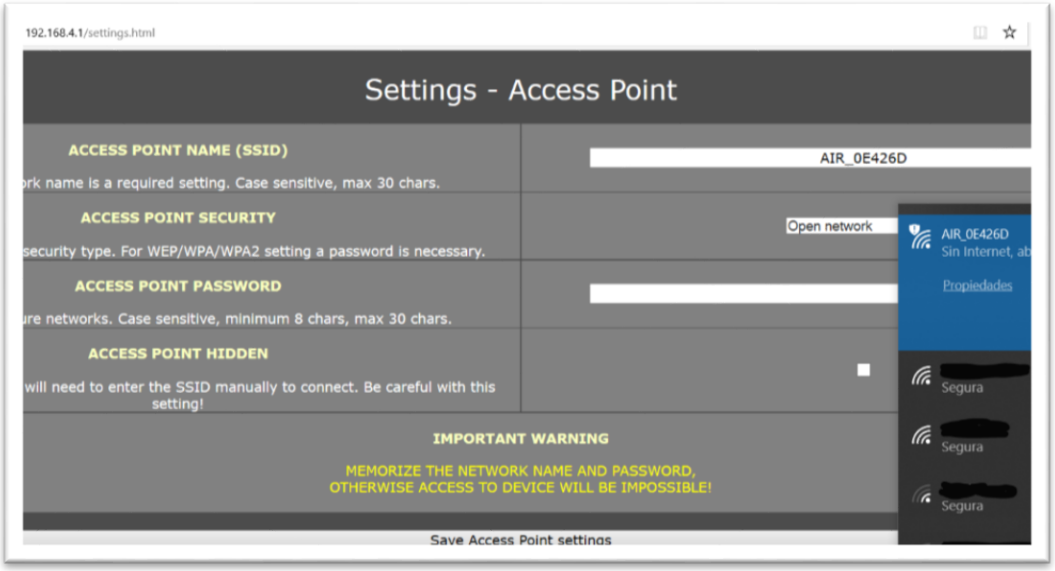


Ilustración 15. Pantalla de configuración del punto de acceso Wifi del keylogger.

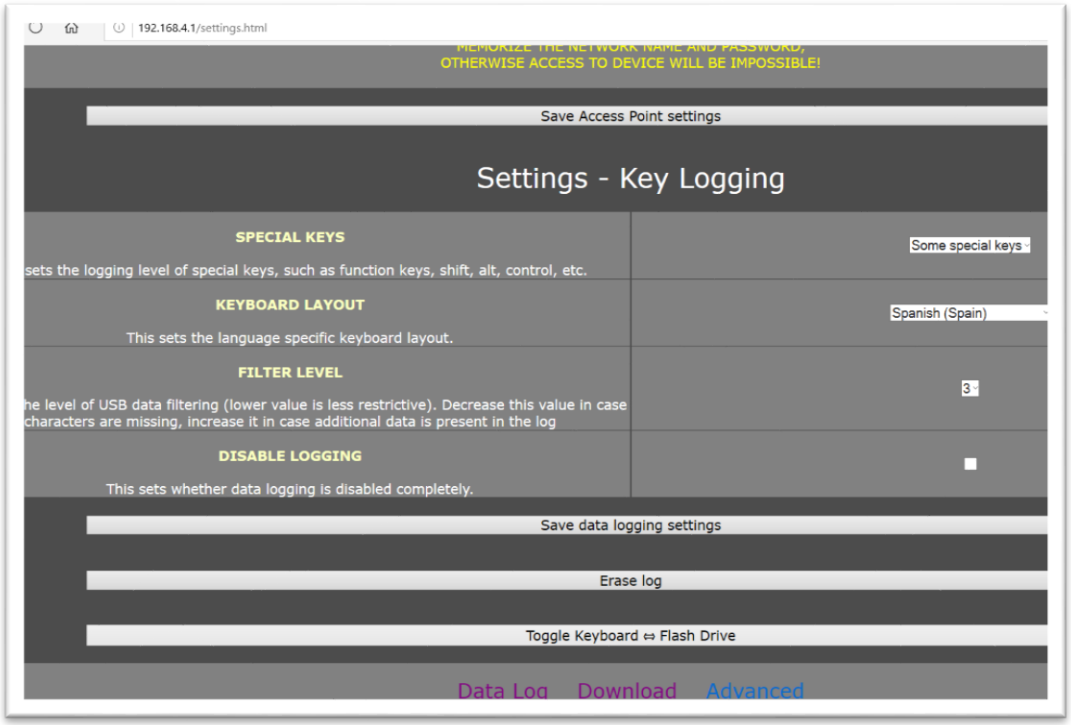


Ilustración 16. Pantalla de configuración del registro de teclas.

Al conectarnos al punto de acceso del keylogger podremos observar el contenido que va registrando. En esta pantalla el contenido no se muestra en tiempo real, sino que hay que acceder a un apartado donde se muestra el contenido y hay que recargar la página en caso de querer ver el contenido más reciente.

Dicho contenido también se puede descargar como un archivo de texto en nuestro equipo para poder ser examinado posteriormente con cualquier editor de texto, como el bloc de notas.

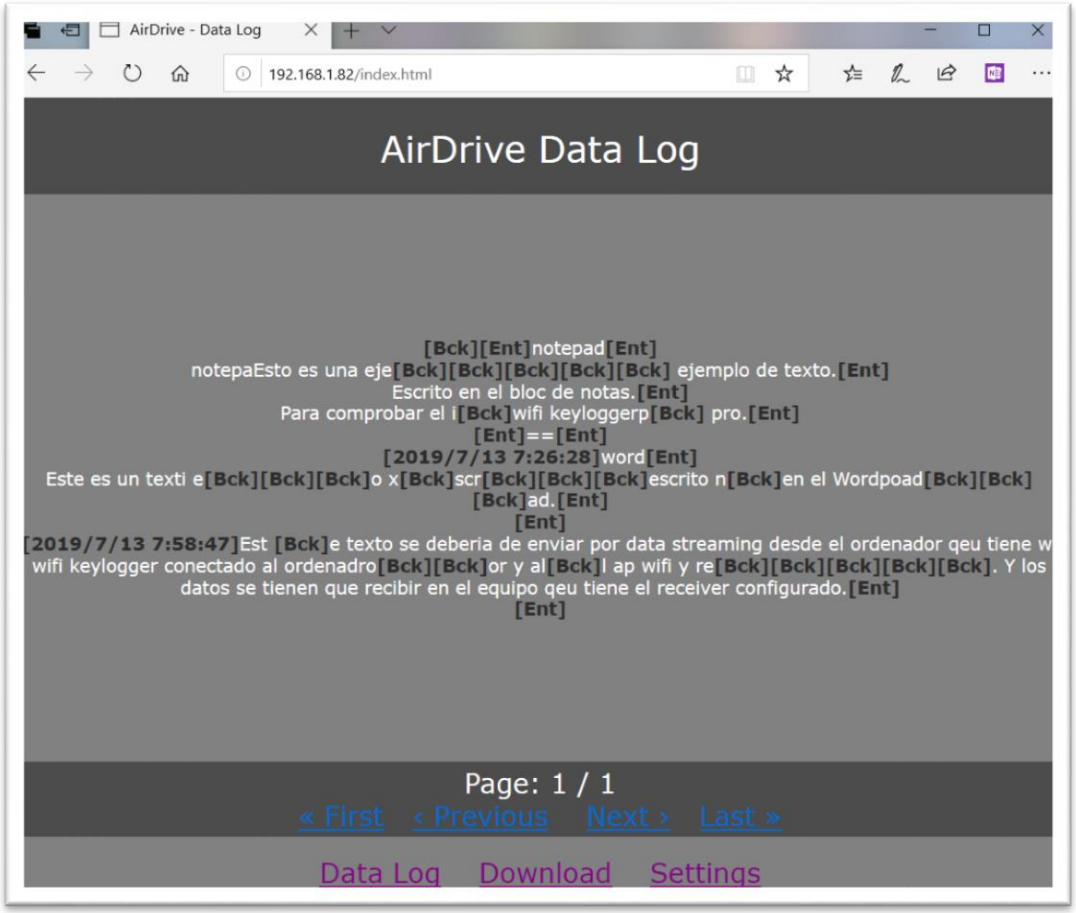


Ilustración 17. Muestra del contenido registrado por el keylogger accedido a través de la conexión WiFi.

Existe la posibilidad de configurar el keylogger para que envíe en tiempo real el contenido a otro equipo. Para ello el equipo receptor debe de tener una aplicación que esté a la escucha en un puerto concreto para recibir las teclas. Se adjunta el enlace para descargar un fichero ejecutable de ejemplo para comprobar el funcionamiento.

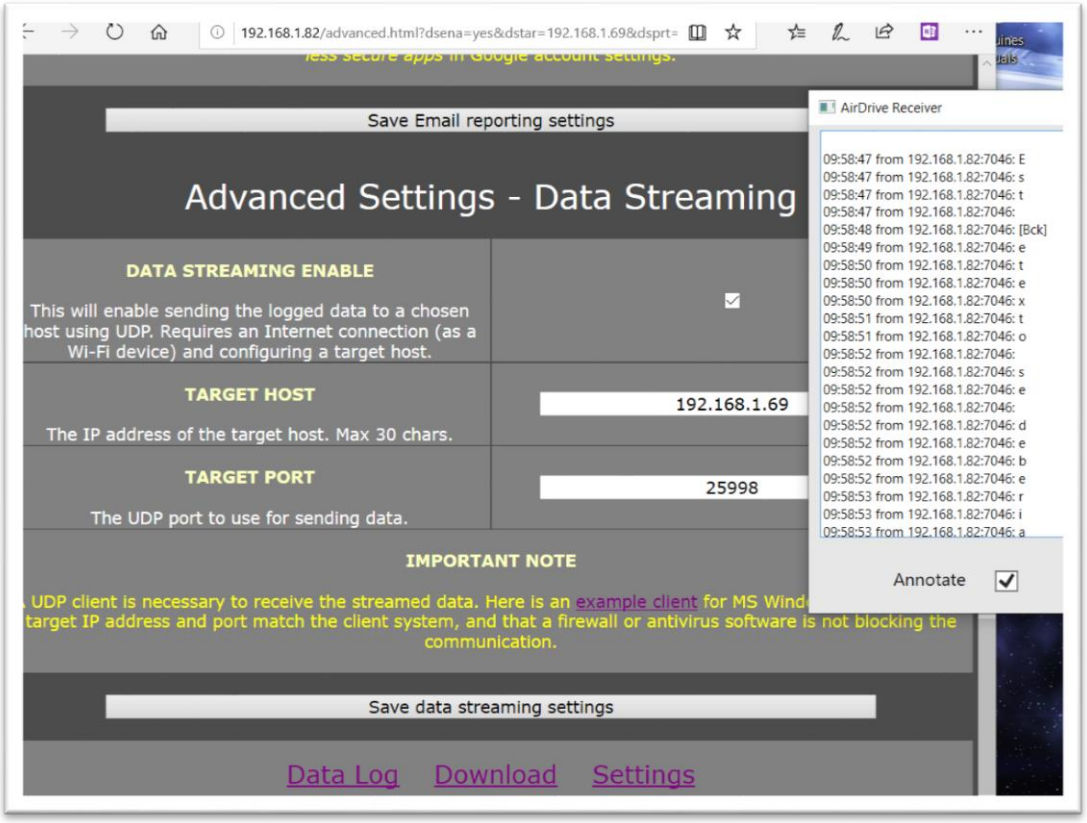


Ilustración 18. Ejemplo de recepción de las teclas del keylogger en tiempo real mediante data streaming.

……

solo requiere la única acción de conectarse al puerto USB entre el ordenador y el teclado. Si se conecta a un equipo portátil, pero no se conecta un teclado externo no tiene ningún efecto pues es imprescindible que los datos pasen a través del keylogger para capturar las pulsaciones de las teclas.

El keylogger pertime configurar otras opciones avanzadas como por ejemplo que el mismo keylogger se conecte como cliente a la propia red WiFi del usuario (previa configuración) y posteriormente el acceso a este se puede hacer a través de la red local, pero se echa en falta una cuestión básica en importante de seguridad en este aspecto, pues cualquier usuario conectado a la red tendrá la posibilidad de acceder al panel de control de keylogger sin necesidad de autenticarse, ya que no tiene la opción de activar un control de acceso mediante contraseña.

9. Análisis de Keylogger Software

En el caso de los keyloggers por software se ha hecho una selección previa de xxx keyloggers, algunos "free" y otros comerciales con versión "demo" o "free". De esta lista hemos confeccionado una tabla de características para ver que ofrece cada uno.

Cuadro comparativo (provisional)

	Windows Spy Keylogger 3.0	Revea-ler Key-logger Free	Spyrix Key-logger Gratis	Heaven-ward KeyLog-ger	Best Free Keylog-ger Lite	Windows Keylog-ger Free	Kid-Logger Stan-dart	IwantSoft FreeKey-logger
Tipo	Free	Free	Free	Free	Free	Free	Free	Free
Protección Contraseña	✗	✓	?	✓		✓	✗	
Inicio automático	✓						✓	
No requiere Administra-dor	✓							
Indetectable por Antivi-rus	?	?	✓					
Modo Invisible	✓	✗	✗	✓	✓	✓	✓	✓
Path fichero Log configu-rable	✓							
Guarda pul-saciones en un solo fichero Log	✓							
Nombre fi-chero Log Configurable	✓							
Autobo-rrado Log					✓			
Cifrado de Log	✗	✗	✗	✗	✓			
Envio Log por email	✗	✗	✗	✓	✗			
Log compri-mido con contra-seña	✗	✗	✗	✓	✗			
Captura de Pantalla	✗	✗	✓		✓	✓	✓	✗

Registra Eventos Sistema							✓	
Monitoriza Sitios Web Visitados							✓	
Monitorización Remota a través de una web	✗	✗	✓					
Monitoriza aplicaciones	✗	✗	✓			✓	✓	✓
Registro Fecha y Hora	✗	✗	✓			✓		
Control Portapapeles	✗	✗	✓			✓	✓	
Control Unidades USB	✗	✗	✓					
Comtrol Impresoras	✗	✗	✓					
Registra Audio							✓	
Foto Webcam Selfie							✓	
Notas	Se debe de configurar por separado en cada sesión de usuario. Crea carpeta oculta en el sistema donde se instala la aplicación.							Bloqueo de aplicaciones

Posteriormente analizamos un par de estos keyloggers.

9.1. Ingenieria inversa del código

Pendiente --- pendiente --- pendiente --- pendiente ---

9.2. Caracteristica 1

Pendiente --- pendiente --- pendiente --- pendiente ---

9.3. Caracteristica 2

Pendiente --- pendiente --- pendiente --- pendiente ---

9.4. Caracteristica 3

Pendiente --- pendiente --- pendiente --- pendiente ---

10. Otras variantes de keyloggers

Existen otros tipos / variantes de keyloggers los cuales solo mencionamos en este estudio, aunque no se ha profundizado en su análisis.

10.1. Dispositivos móviles

Pendiente --- pendiente --- pendiente --- pendiente ---

10.2. Keyloggers Javascript

Pendiente --- pendiente --- pendiente --- pendiente ---

10.3. Keyloggers CSS

Pendiente --- pendiente --- pendiente --- pendiente ---

11. Anti-Keyloggers

De la misma manera que hay software keylogger, también existe software anti-keylogger.

12. Desarrollo de un Keylogger

Pendiente --- pendiente --- pendiente --- pendiente ---

12.1. Elección del lenguaje para programarlo, ventajas e inconvenientes

El lenguaje elegido finalmente para el desarrollo ha sido Python versión 3.7.

Los lenguajes que se han tenido en cuenta para el desarrollo han sido:

- Delphi (Object Pascal)
- C
- Go
- Python

12.2. Caracteristicas del Keylogger

Pendiente --- pendiente --- pendiente --- pendiente ---

12.3. Problemas y soluciones

Pendiente --- pendiente --- pendiente --- pendiente ---

12.4. Implantación

Pendiente --- pendiente --- pendiente --- pendiente ---

12.5. Mejoras posibles

Pendiente --- pendiente --- pendiente --- pendiente ---

12.6. Notas finales

Pendiente --- pendiente --- pendiente --- pendiente ---

13. Resultados finales

Pendiente --- pendiente --- pendiente --- pendiente ---

…

14. Coste del proyecto

Pendiente --- pendiente --- pendiente --- pendiente ---

14.1. Coste temporal

El volumen de trabajo que ha comportado la realización del proyecto se puede clasificar en los siguientes apartados:

- …
- …
- …

A continuación, explicamos detalladamente en qué ha consistido y cuánto tiempo ha requerido cada uno de los apartados mencionados anteriormente:

…

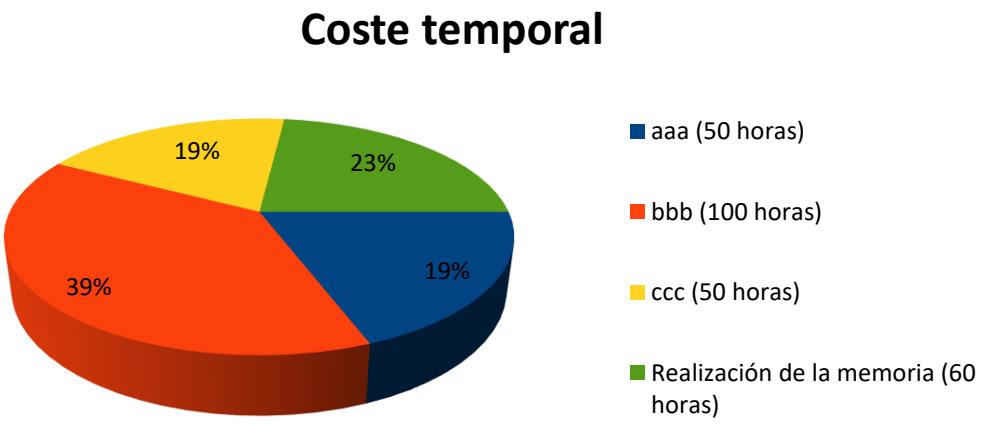


Figura 3. Coste temporal

14.2. Coste económico

El coste económico necesario para el desarrollo del proyecto …

15. Conclusiones

Pendiente --- pendiente --- pendiente --- pendiente ---

16. Líneas de futuro

Lorem ipsum ad his scripta blandit partiendo, eum fastidii accumsan euripidis in, eum liber hendrerit an. Qui ut wisi vocibus suscipiantur, quo dicit ridens inciderint id. Quo mundi lobortis reformidans eu, legimus senserit definiebas an eos. Eu sit tincidunt incorrupte definitionem, vis mutat affert percipit cu, eirmod consectetuer signiferumque eu per. In usu latine equidem dolores. Quo no falli viris intellegam, ut fugit veritus placerat per:

…

…

…

17. Referencias

[1] TODAY WE'RE WORRIED ABOUT SMART TVS, BUT IN THE 1980S RUSSIAN SPIES WERE HACKING TYPEWRITERS.
https://qz.com/932448/forget-smart-tvs-in-the-1980s-spies-were-hacking-typewriters/

[2] IBM SELECTRIC BUG. OPERATION GUNMAN - HOW THE SOVIETS BUGGED IBM TYPEWRITERS.
https://www.cryptomuseum.com/covert/bugs/selectric/

[3] LEARNING FROM THE ENEMY: THE GUNMAN PROJECT. Sharon A. Maneki. Center for Cryptologic History. National Security Agency. 2012.
http://www.foo.be/docs/intelligence/Learning_From_the_Enemy_The_GUNMAN_Project.pdf
https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-histories/Learning_from_the_Enemy.pdf

[4] LA HISTÓRIA (QUE SE CONOCE) DE LOS ATAQUES INFORMÁTICOS REALIZADOS POR EL FBI.
https://r3d.mx/2016/05/18/la-historia-que-se-conoce-de-los-ataques-informaticos-realizados-por-el-fbi/

[5] SPYING ON THE MOB: UNITED STATES V. SCARFO – A CONSTITUTIONAL ANALYSIS. Nathan E. Carrell.
http://illinoisjltp.com/journal/wp-content/uploads/2013/10/Carrell.pdf

[6] THE ULTIMATE KEYLOGGER: FBI'S MAGIC LANTERN.
https://www.mobistealth.com/blog/ultimate-keylogger-magic-lantern/

[7] FBI SOFTWARE CRACKS ENCRYPTION WALL.
http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall/

[8] THE CASE FOR MAGIC LANTERN: SEPTEMBER 11 HIGHLIGHTS THE NEED FOR INCREASED SURVEILLANCE. Christopher Woo & Miranda So. Harvard Journal of Law & Technology.
http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf

[9] NEW FBI DOCUMENTS PROVIDE DETAILS ON GOVERNMENT'S SURVEILLANCE SPYWARE.
https://www.eff.org/es/deeplinks/2011/04/new-fbi-documents-show-depth-government

[10] Creador y Código fuente del primer keylogger por software. Perry Kivolowitz.
http://pages.cs.wisc.edu/~perryk/
http://securitydigest.org/unix/archive/006

[11] Student Expelled for Using Hardware Keylogger to Hack School, Change Grades.
https://www.bleepingcomputer.com/news/security/student-expelled-for-using-hardware-keylogger-to-hack-school-change-grades/

[12] Boston College Student Steals Around $2,000 with Keylogger.
https://www.neowin.net/news/boston-college-student-steals-around-2000-with-keylogger

[13] NOTICIAS Y ENLACES RELACIONADOS CON EL KEYLOGGER EN LOS PORTATILES HP.
https://www.techrepublic.com/article/built-in-keylogger-found-in-hp-laptops-again/
https://mashable.com/2017/12/11/keylogger-found-on-hundreds-of-hp-computer-models/
https://zwclose.github.io/HP-keylogger/
https://support.hp.com/us-en/document/c05827409

[14] Keyloggers: How they work and how to detect them (Part 1).
https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/

[15] 'Sleeper bugs' used to steal 1m in France
https://www.theguardian.com/technology/2006/feb/07/news.france

[16] El mayor atraco del siglo: los ciberdelincuentes roban mil millones de dólares.
https://www.kaspersky.es/blog/el-mayor-atraco-del-siglo-los-hackers-roban-mil-millones-de-dolares/5370/

[17] Análisis del código fuente de Carbanak.
https://unaaldia.hispasec.com/2019/04/analisis-del-codigo-fuente-de-carbanak.html

[18] SUCURI. Cloudflare[.]Solutions Keylogger on Thousands of Infected WordPress Sites.
https://blog.sucuri.net/2017/12/cloudflare-solutions-keylogger-on-thousands-of-infected-wordpress-sites.html

[19] SUCURI. Cloudflare[.]solutions Keylogger Returns on New Domains.
https://blog.sucuri.net/2018/01/cloudflare-solutions-keylogger-returns-on-new-domains.html

[20]

[21] DIRECTIVA 2013/40/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013L0040&qid=1442911632730&from=EN

[22]

18. Bibliografía

[1] TODAY WE'RE WORRIED ABOUT SMART TVS, BUT IN THE 1980S RUSSIAN SPIES WERE HACKING TYPEWRITERS.
https://qz.com/932448/forget-smart-tvs-in-the-1980s-spies-were-hacking-typewriters/

[2] IBM SELECTRIC BUG. OPERATION GUNMAN - HOW THE SOVIETS BUGGED IBM TYPEWRITERS.

[3]

Índice de Ilustraciones

Ilustración 1. Dos modelos de keylogger hardware. Para teclado ps/2 y USB. 4
Ilustración 2. IBM Selectric II (1971-1981) 7
Ilustración 3. Portada del documento de la NSA, “The GUNMAN Project”. Desclasificado en Diciembre de 2011 8
Ilustración 4. Bola “pelota de golf” de la IBM Selectric, con los caracteres. 9
Ilustración 5. Diario Oficial de la Unión Europea. DIRECTIVA 2013/40/UE. 12 agosto 2013. Extracto del contenido relativo a los ataques contra los sistemas de información. 14
Ilustración 6. Foto de los keyloggers hardware analizados 19
Ilustración 7. Vista en detalle de los dos keyloggers 19
Ilustración 8. KeyGrabber en su empaquetado original. 21
Ilustración 9. KeyGrabber conectado al teclado. 21
Ilustración 10. Ejemplo de fichero de LOG con el contenido capturado por el keylogger. 22
Ilustración 11. Vista del SSID activo del keylogger analizado. 23
Ilustración 12. Pantalla de configuración del punto de acceso Wifi del keylogger. 24
Ilustración 13. Pantalla de configuración del registro de teclas. 24
Ilustración 14. Muestra del contenido registrado por el keylogger accedido a través de la conexión WiFi. 25
Ilustración 15. Ejemplo de recepción de las teclas del keylogger en tiempo real mediante data streaming. 26

Índice de tablas