

En el centro de las miradas: Registradores de pulsaciones

Un sistema registrador de pulsaciones o *keylogger*, es una herramienta utilizada para monitorizar y guardar eventos del teclado, como cuando un usuario escribe una contraseña y otros datos valiosos.

Esa información, después se envía encubiertamente al perpetrador, propietario o instalador del registrador de pulsaciones. La monitorización del teclado también tiene usos legítimos, pero en la mayoría de los casos estas aplicaciones son instaladas clandestinamente para realizar un seguimiento de las actividades de empleados, padres, o esposos.

Los criminales en línea, usan registradores de pulsaciones para recolectar contraseñas y credenciales de acceso de los ordenadores de sus víctimas. Después, agregan estos datos en repositorios especiales como el correo electrónico o el sitio personal de un atacante, generalmente de forma cifrada. Por último, utilizan las identidades robadas con propósitos maliciosos, tales como saquear los fondos de la cuenta bancaria en línea de sus víctimas.

Tipos de registradores de pulsaciones

Existen dos tipos de registradores de pulsaciones:

- **Registradores de pulsaciones físicos**

Estos registradores, son dispositivos físicos que se conectan al teclado por un extremo, y a un puerto PS/2 o USB de un ordenador por el otro.

Están diseñados para interceptar, grabar y almacenar datos en memoria, para su posterior recuperación.

Los registradores de pulsaciones físicos, pueden incluirse directamente en los teclados, y ser vendidos como una sola unidad en sitios en línea de dudosa reputación.

Por ello, hay que ser cuidadoso cuando alguien en el hogar o espacio de trabajo reemplaza sorpresivamente un teclado, sin causa aparente. En estos casos, se deben investigar los verdaderos motivos de este cambio.

Este tipo de dispositivo es difícil de identificar visualmente, y habría que inspeccionar manualmente las conexiones del teclado, o desarmarlo para encontrar un chip especial que monitoriza las pulsaciones.

Esta tarea es un tanto complicada para un usuario común.

Desde el punto de vista del atacante, el beneficio de los registradores físicos es que permiten capturar las pulsaciones desde el mismo instante en que se enciende el ordenador. Toda la información introducida, desde las entradas del sistema básico de entrada y salida (BIOS, *Basic Input-Output System*), hasta las subsiguientes contraseñas de acceso al sistema, podría terminar en las manos equivocadas.

Estos registradores de pulsaciones son prácticamente imposibles de detectar, incluso para los programas de seguridad modernos, y esto implica una gran amenaza.

La desventaja de estas herramientas, es que necesitan acceso físico al ordenador de la víctima, con el fin de instalar, mantener y recuperar la información obtenida.

El resto de este documento está dedicado a la otra clase de registradores de pulsaciones: los programas que monitorizan y guardan las teclas presionadas.

- **Programas registradores de pulsaciones**

Los registradores de pulsaciones de este tipo, son aplicaciones que probablemente nunca aparezcan en la lista de **Agregar o quitar programas** del Panel de control. La mayoría de ellos se instala sin el conocimiento ni la autorización del usuario, y su misión es transmitir la información registrada a las direcciones predeterminadas de los delincuentes informáticos, actuando en modo oculto, y espiando al usuario en la mira.

Estos registradores también pueden dividirse en dos grupos distintos:

- **Registradores de pulsaciones del núcleo del sistema operativo (*kernel keyloggers*)**

Son aplicaciones maliciosas más elaboradas, que se integran directamente al núcleo de Windows, el corazón del sistema operativo.

Debido a los privilegios del acceso a bajo nivel, los registradores de pulsaciones de este tipo pueden interactuar con el sistema operativo del ordenador anfitrión, y monitorizar directamente la actividad del teclado.

Eventualmente, también podrían instalar controladores de teclado propietarios, facilitando el proceso de control de las teclas presionadas.

Este tipo de registradores son los más evasivos y mejor encubiertos en un sistema, y es necesario realizar un gran esfuerzo para detectarlos y erradicarlos. Un ejemplo de ellos es “**Klog**”.

- **Registradores de pulsaciones basados en desvíos de procesos (hook-based keyloggers)**

Estos registradores trabajan con funciones legítimas de Windows, que interceptan transacciones de procesos, comandos o cuadros de mensaje. Al instalar uno de estos interceptores en un programa, un registrador de pulsaciones puede capturar su contenido, incluyendo los eventos del teclado.

Un ejemplo de un programa legítimo que utiliza esta técnica es **Punto Switcher**, que automáticamente alterna la distribución del teclado en base al lenguaje en que escribe el usuario.

Métodos de propagación

Además de la instalación intencional de un registrador de pulsaciones a través de una persona que tiene acceso físico al ordenador, las rutas habituales de propagación incluyen:

- Descargas dirigidas que aprovechan vulnerabilidades presentes en los programas navegadores, predominantemente componentes ActiveX y guiones Java corruptos.
- Ejecución de archivos adjuntos maliciosos, contenidos en correos masivos o mensajes falsificados, abiertos con la aplicación de correo electrónico o de mensajería instantánea.
- Descarga y ejecución de archivos maliciosos a través de Internet.
- Programas maliciosos encapsulados en las versiones de evaluación de ciertas aplicaciones (*shareware*), y en contenido transmitido a través de redes punto a punto.
- Descarga de registradores de pulsaciones debido a la infestación general del sistema.

Indicadores de una infección

Si un registrador de pulsaciones está correctamente diseñado, como los que se integran al núcleo del sistema operativo, las posibilidades de notar su presencia son nulas.

Los registradores avanzados tienden a copiar funcionalidades de los *rootkits*, hecho que les permite permanecer ocultos ante las herramientas genéricas de monitorización de procesos.

Solo los programas especializados, como los detectores de *rootkits*, podrían señalar los posibles indicios de la presencia de un registrador de pulsaciones.

En un escenario más habitual, donde estas aplicaciones usan solamente técnicas de interceptación para capturar la actividad del teclado, el nombre de su proceso debería ser visible en el **Administrador de tareas** de Windows. Habría que investigar manualmente cada uno de los procesos sospechosos que aparecen en la lista, con la ayuda de un buscador en línea. Un análisis de este tipo ayudará a aclarar las dudas acerca de la legitimidad de los procesos desconocidos.

Los cortafuegos, también muestran la actividad de procesos específicos en la red, y con la meticulosidad suficiente es posible encontrar un transgresor.

Outpost Firewall, por ejemplo, con su **Visor de registros** permite revisar las últimas actividades de la red, filtradas para un proceso específico.

De este modo, es fácil verificar qué es lo que ha funcionado mal en el sistema.

Desinfección y prevención

Prevenir la instalación de los programas registradores de pulsaciones, es un enfoque mucho mejor que tratar de eliminarlos una vez que ya han infestado el sistema.

Los programadores de código malicioso pueden modificar fácilmente estas aplicaciones para evitar que sean detectados por programas antivirus que usan técnicas convencionales para verificar el código.

Es mejor combatir las intrusiones en tiempo real, y no tratar de reparar el daño que causan.

Algunas herramientas, como **HIPS** (*Host Intrusion Protection System*, Sistema de protección contra intrusos), que monitorizan y previenen la actividad no autorizada o inapropiada de aplicaciones, puede evitar la activación y el daño en tiempo real causado por los registradores de pulsaciones, mientras estos capturan las teclas presionadas.

Outpost Firewall Pro, con su módulo **Anti-Leak**, **Outpost Security Suite Pro**, de próxima aparición, y otras soluciones de seguridad avanzadas, monitorizan el comportamiento entre programas para asegurar que una aplicación maliciosa no intercepte acciones, contenidos ni otros datos compartidos que pertenecen a aplicaciones legítimas.

Los cortafuegos por sí solos no pueden proteger directamente contra los intentos de obtención de información de los registradores de pulsaciones, pero pueden prevenir que la información interceptada sea transmitida a los atacantes remotos.

Consejos prácticos de prevención

A continuación presentamos algunos consejos prácticos para evitar que los registradores de pulsaciones roben su información.

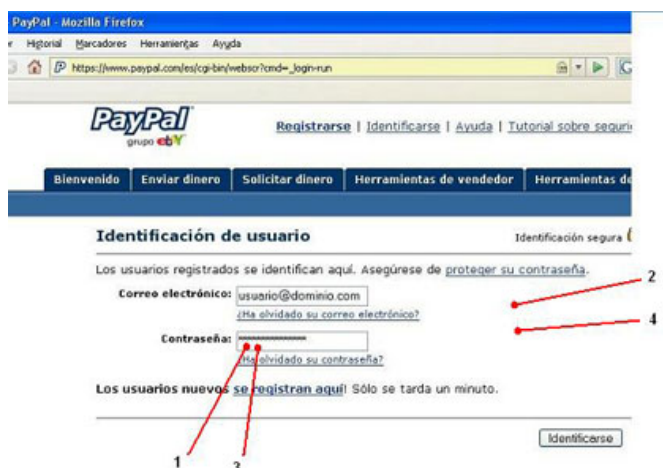
Si accede a la Red desde un lugar público, como un cibercafé o un puesto de Internet en un aeropuerto, no acceda a páginas privadas que necesitan sus credenciales personales.

Fundamentalmente, no es seguro porque aun si se registra tomando las debidas precauciones, alguien podría inspeccionar y extraer información valiosa de la memoria intermedia del navegador.

Si es absolutamente necesario a acceder a esas páginas, siga los pasos a continuación para minimizar el riesgo de que un registrador de pulsaciones robe sus datos:

Al introducir su información de acceso

1. Teclee solamente los primeros caracteres de su clave.
2. Posicione el cursor del ratón sobre un espacio en blanco de la página, y escriba algo allí. Obviamente, no aparecerá ningún texto, pero el registrador de pulsaciones creerá que estas letras forman parte de su frase secreta, porque el programa no puede diferenciar los campos exactos de una aplicación, solo registra entradas. Así, se grabará una sucesión de teclas pulsadas, sin que el programa registrador pueda discriminar su procedencia.
3. Después de teclear una cadena de caracteres al azar en el espacio en blanco, regrese al campo donde tiene que ingresar su contraseña, y continúe cargando allí los símbolos válidos.
4. Repita el procedimiento unas pocas veces más, de modo que la contraseña sea imposible de reconocer. La pantalla que sigue ilustra la secuencia.



Como resultado, su frase secreta (contraseña válida) será, por ejemplo "vjrfkrifajfkrjlrhfrhfhfjrefhndrfjkf_fjjkrjfpjkrjfkafifjfsrfkjlwjfklodkfdkdf", y el registrador de pulsaciones no servirá de nada.

Utilice un teclado en pantalla, en vez de pulsar los caracteres en su teclado físico

Siempre que pueda, utilice un teclado virtual para introducir los caracteres en una ventana, en lugar de usar el teclado físico; algunos sitios de Internet lo han implementado así como algunos sistemas operativos lo incluyen accediendo a partir del menú **Inicio**, **Accesorios**, **Accesibilidad**, **Teclado en pantalla**.

Conclusión

Los registradores de pulsaciones son códigos maliciosos peligrosos y molestos.

Sin embargo, si los usuarios están informados, usan los ordenadores con inteligencia, y mantienen buenas aplicaciones antivirus y de monitorización de comportamiento, se puede disminuir significativamente, e incluso eliminar su impacto.