Aplicación del Software de registro de actividades en el computador: “Keylogger”

Mamani Laura Ronald Efraín
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
ronnygheo7@hotmail.com

RESUMEN.

El objetivo del presente artículo nos ayudará a tener un conocimiento más claro acerca de lo que son los keyloggers, no solo como herramienta de inseguridad informática, sino como herramienta administrativa, y de recolección de información legal. Además de mostrar como un usuario común puede detectar si su terminal de trabajo está siendo monitoreada o no por un software de éstas características.

Palabras clave.

Registro, actividades, software, keylogger, computadora, anti-keyloggers, monitoreo

1. INTRODUCCIÓN

El “Software de registro de actividades del Computador" o "keylogger", es un programa que registra secretamente todas las actividades que tuvieron lugar en un equipo y/o en redes de computadores, de manera individual o corporativa, respectivamente.

Los keyloggers son dispositivos de software o hardware, que se encargan de capturar las teclas que son digitadas en la computadora, siempre y cuando hayan sido instaladas correctamente. Pero a pesar de ser herramientas de uso común para efectos de intrusión con fines criminales, también pueden ser usados con otros propósitos.

Un keylogger registra los datos y las actividades son representadas con cierto grado de certeza su confiabilidad, pero también determina la invasión a la privacidad de la persona o empresa monitoreada.

Su gran fortaleza radica en la capacidad de ser invisible a los ojos del usuario de la computadora que es monitoreada, y la facilidad de instalación y extracción de datos.

Son herramientas poderosas para la obtención de datos, y ser monitoreado por este tipo de dispositivos implica dar a quien lo administra toda la información clasificada como confidencial (transacciones electrónicas, como los nombres de usuario y las contraseñas, las claves de tarjetas de crédito, números de cuenta, etc).

Así, el monitoreo de información es una prueba contundente en casos legales, y puede ser útil para certificar el buen o mal uso de recursos.

Aplicado a la informática forense este tipo de software nos ayudará a que esta prueba o evidencia contenida en las computadoras, pueda ser suficiente y óptima, para utilizarlo como evidencia en un proceso judicial, desde el envio de un e-mail, a fotografías o documentos confidenciales, testeo de alguna maquina sospechosa e inclusive si el dueño o usuario de esta máquina borró la información, desfragmentó el disco o si lo formateó.

Es aquí donde aparece un área nueva de la Ciencia Forense, siendo la definición básica del área: "La práctica especializada y las actividades realizadas y operadas en el computador con el propósito de descubrir y analizar información disponible, borrada u oculta que pueda ser usada como evidencia en un proceso legal".

La Informática Forense se enfoca en descubrir evidencia potencial en una variedad de casos, como son:

- Lavado de Dinero transacciones ilegales.
- Acceso no autorizado a propiedad intelectual
- Fraude (en apuestas, compras, etc. Vía e-mail)
- Robo de Propiedad Intelectual y Espionaje industrial.

También combina muy bien las técnicas especializadas con el uso de software sofisticado para ver y analizar información a la que no puede acceder un empleado o usuario común. Esta información pudo haber sido “borrada” por el usuario meses o años antes de la investigación o inclusive pudo no haber sido guardada, pero puede aún estar presente en la computadora.

2. ¿QUÉ ES UN KEYLOGGER?

Los logs son una herramienta muy efectiva para obtener información acerca de sucesos que ocurren en una computadora. Muchas veces, los logs, son archivos que registran acontecimientos tanto normales como anormales.

Existen muchos tipos de logs, pero consideramos para este caso a los key loggings.

Un key logging es, como su nombre lo indica, un log que registra las teclas que son oprimidas en un teclado por algún usuario, sea este o no de la empresa.

Este log llega a generar un programa especial al cual se denomina como keylogger, el cual está descrito como programa

espía.

Un programa espía es cualquier programa que se oculta, el cual sirve o es utilizado para obtener cualquier tipo de información no autorizada, sobre algún usuario de la organización.

Entonces, los keyloggers son capaces de obtener información muy importante. Pero en general poseen la capacidad de obtener cualquier información que sea introducida a un computador vía teclado. Existen dos clases de keyloggers, por software y por hardware.

Entonces, cuando mencionamos a "todas las actividades o a la obtención de información", nos referimos a cada golpe de teclado digitado por un usuario, donde además determinamos las palabras “claves” que se introdujeron en la computadora, además permitirán realizar un análisis de lo que ocurre en el computador de un usuario común y corriente o de un usuario en redes computacionales.

3. ¿EN QUÉ SISTEMAS OPERATIVOS FUNCIONAN?

Podríamos mencionar muchas versiones de keyloggers para diferentes sistemas operativos, pero sólo como ejemplo mencionaremos algunos conocidos.

3.1. Keyloggers a nivel de hardware

Estos funcionan como tarjetas de hardware que se insertan a la computadora, son muy pequeñas, además, no usan recursos de software y sirven como herramientas de soporte en tiempo real. Otros, del tamaño de pilas Doble AA, se conectan al teclado, y cumplen ésta función.

Figura 1. Un keylogger por hardware

Estos dispositivos son conectados al teclado, y sin utilización de un software especial, se capturan las teclas que se digitan, las cuales se almacenan en una memoria extraíble, que puede ser bloqueada, de modo que solo el administrador pueda tener accesos a esta información. Además posee la ventaja, sobre el software keyloggers, de ser mucho más difícil de descubrir y el anular con anti-keyloggers.

3.2. Keyloggers a nivel de software

En Windows se observa muchas maneras de capturar información del teclado, a continuación analizamos una de esas maneras.

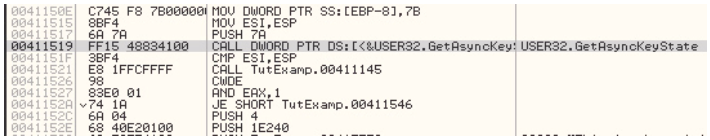

Figura 2. Un keylogger por software

```
Numbers = 65

Do Until Numbers = 91 ' checa as letras
    rs = GetAsyncKeyState(Numbers)
    If rs = -32767 Then
        rs = GetKeyState(sk)
        Press = IIf(rs < 0, Chr(Numbers), LCase(Chr(Numbers)))
        GoTo KeyFound
    End If
    Numbers = Numbers + 1
Loop
Numbers = 48


Do Until Numbers = 57 ' checa os numeros
    rs = GetAsyncKeyState(Numbers)
    If rs = -32767 Then
        rs = GetKeyState(sk)
        If rs < 0 Then
            If Numbers = 48 Then Press = ")"
            If Numbers = 49 Then Press = "!"
            If Numbers = 50 Then Press = "@"
            If Numbers = 51 Then Press = "#"
            If Numbers = 52 Then Press = "$"
            If Numbers = 53 Then Press = "%"
            If Numbers = 54 Then Press = "^"
            If Numbers = 55 Then Press = "&"
            If Numbers = 56 Then Press = "*"
            If Numbers = 58 Then Press = "("
        Else
            Press = Chr(Numbers)
        End If
        GoTo KeyFound
    End If
    Numbers = Numbers + 1
Loop
```

Figura 3. Un programa de usuario utilizando GetAsyncKeyState

Esta manera consiste en usar una función del sistema llamada GetAsyncKeyState, esta función registra si una tecla se oprimió o no, además si esta tecla es la misma que se detecto desde la última vez que fue llamada esta función.

La función existe en todos los sistemas operativos Windows, pero se comporta de diferente manera en cada versión. Por ejemplo en Windows NT/2000/XP existen unas constantes que determinan si la tecla fue oprimida por primera vez o si es por segunda.

Para lograr esto, el sistema operativo tiene un vector de

interrupciones, que es una estructura donde está almacenada la información de cómo manejar cada interrupción, una interrupción es cuando el hardware le dice al procesador que tiene que procesar información.

4. ¿QUIÉNES USAN LOS KEYLOGGERS?

Los programas de keyloggers pueden ser usados por padres y madres que deseen controlar discretamente la actividad de sus hijos menores en el computador. Además estos pueden ser usados por organizaciones gubernamentales (como el FBI de Estados Unidos), para recolectar información o evidencia para combatir el crimen. También pueden servir como herramienta de soporte, para recuperar contraseñas olvidadas, correos electrónicos o cualquier otro tipo de información o actividades realizadas.

5. ¿QUÉ ES UN ANTI-KEYLOGGER?

Los Anti-Keyloggers son software que detecta programas de monitoreo en un computador o servidor. Este tipo de programas puede estar incluido en algunos antivirus, o puede ser comprado o descargado de diferentes compañías en Internet.

Para prevenir el monitoreo no autorizado de un computador se pueden tener en cuenta varios consejos, como evitar ejecutar software desconocido, o que provenga de fuentes desconocidas, usar un firewall o corta fuegos, mantener actualizado el antivirus, y tener instalado un programa anti-monitoreo.

6. ¿LOS KEYLOGGERS SON ILEGALES?

Muchos autores nos indican que NO, entonces cuando se habla de software espía o keyloggers, no hay nada ilegal sobre la aplicación en sí.

Porque, los desarrolladores de las aplicaciones keyloggers, desde sus comienzos y en la actualidad siguen trabajando para crear sus programas exclusivamente con fines legales.

Pero en muchos países, hay algunas personas y empresas que utilizan de foma negativa el mismo software, siendo las más frecuentes:

- Robo de contraseñas.
- Plagio de úmeros de tarjetas de crédito o secretos empresariales.
- Violación de la privacidad personal.

Ante esta situación se llega a la pregunta: ¿Se pueden violar las leyes, la privacidad de personas o empresas que usen software keylogger?

Todo dependerá de la forma de utilizarlos. Porque en muchos casos es permisiva la instalación de cualquier aplicación o programa legal y original en el equipo que nos pertenezca. También tenemos el derecho a instalar programas en computadoras de otras personas desde luego si cuentan con su consentimiento. La instalación del software de monitoreo en computadores de otras personas o de sus empleados sin el permiso correspondiente puede ser ilegal llegando a casos de acciones legales y judiciales.

Sin embargo, podemos mencionaremos algunos ejemplos de usos perfectamente legales en el monitoreo de actividades en un computador.

Controlar a sus hijos en el uso del Internet para asegurarse de que no visiten sitios web pornográficos.

Mantener un registro de actividades de los usuarios inexpertos para localizar y solucionar rápidamente problemas operativos.

Controlar a los empleados en las actividades sobre un computador para asegurarse de que están realmente trabajando.

7. CONCLUSIONES

Existen programas de keylogger para prácticamente todas las plataformas y sistemas operativos, por lo que es mas adecuado clasificarlos de acuerdo a las características que ofrecen, si es invisible o no, si guarda los registros en memoria o los envía por Internet.

Las herramientas de detección de monitoreo no son cien por ciento útiles, de hecho pueden fallar en muchos casos; las medidas preventivas seguirán siendo necesarias, y medianamente confiables, si son atadas a la utilización de anti-keyloggers, y si son realizadas con conocimiento de las políticas a las que pueda estar sometida la máquina en cuestión.

8. REFERENCIAS

[1] 18 U.S.C. 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited. (2000, Abril). Disponible en: **http://www.cybercrime.gov/usc2511.htm**

[2] What about hardware KeyLoggers?. Disponible en: **http://spycop.com/keyloggerremoval.htm**

[3] A Stealthy Windows Keylogger, Phrack Magazine Volume 8, Issue 53. (1998, July 8). Documento disponible en la dirección: **http://www.phrack.org/show.php?p=53&a=7**