KeyLogger

Univ. José Luis Mollo Mamani
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de Información
Jose.luis.mm25@hotmail.com

RESUMEN

- El siguiente artículo hace mención al *keylogger* que es un registrador de pulsaciones del teclado, estos se presentan en dispositivos de *hardware* y en programas de *software*. Ahora bien los *Hackers* o personas maliciosas que tienen acceso al sistema de la computadora de otro usuario a través de medios no autorizados y que emplean como una herramienta para robar información al *Keyloggers*, al o los usuarios que visitan sus correos electrónicos, realizar transacciones bancarias y otras actividades, son blanco fácil de estos piratas, porque uno no sabe o no podría identificar a la primera si el computador en el que se está trabajando puede estar o no con el *keylogger*. Es por eso que debemos de tener muy en cuenta que herramientas o métodos sencillos debemos de usar para prevenir el ser espiados.

PALABRAS CLAVE

Anti-logger, *anti-keylogger*, pulsaciones, *anti-spyware*, espionaje virtual, heurística.

1. INTRODUCCION

Un *keylogger* es derivado del inglés *key* (tecla) y *logger* (registrador) registrador de teclas o pulsaciones. Son dispositivos o programas con el que se puede grabar todo lo que el usuario digite mediante el teclado y mandar toda esa información a terceros. Esta herramienta, que inicialmente se usaba para el desarrollo de *software*, es muy utilizada para espiar a la víctima, para el robo de contraseñas, cuentas bancarias o de foros, documentos privados, y beneficiar de alguna manera al que haya hecho la instalación, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

A continuación veremos cómo identificar y prevenir que personas maliciosas roben información confidencial de nuestro ordenador y además que cuando acudamos a un internet, seamos capaces de saber si el ordenar está o no con un *keylogger*.

2. REGISTRADORES DE PULSACIONES DE SOFTWARE Y HARDWARE

Los registradores de pulsaciones de *software*; son los más utilizados por los *hackers*, ya que se lo pueden instalar a través de la red, o en un computador que está desprotegido, también se presentan como virus y/o troyano, etc. Los registradores de *software* a menudo tienen la capacidad de obtener muchos más información, ya que no están limitados por la memoria física, como lo hacen los registradores de pulsaciones de *hardware*.

Los registradores de pulsaciones de *hardware*; como lo dice su nombre son dispositivos *hardware* que se conectan físicamente al teclado.Estos dispositivos generalmente se ven como un adaptador de teclado estándar (Véase **Figura 1** y **Figura 2**), por lo general no tienen la capacidad para transmitir o enviar esa información a través de una red como lo hacen los registradores de pulsaciones de *software*, además están limitados en la recolección de información de acuerdo a su capacidad.Una de las ventajas de *hardwarekeyloggers* es que no van a ser descubiertos por cualquiera de los *anti-spyware*, programas de seguridad anti-virus o de escritorio.

Figura 1
Dispositivo de registro de teclado tipo *flash memory*.

Figura 2
Dispositivo de registro de teclado tipo adaptador *minidi*.

3. ¿COMO PROTEGERCE DE LOS KEYLOGGER?

Para proteger a nuestra PC de cualquier *keylogger* y sentir privacidad al estar frente al computador lo primero que se debe saber es cómo funciona estos programas espías. Cuando se realizan las pulsaciones en el teclado, ocurre lo siguiente, el sistema manda al microprocesador (*Bios*) un pulso del teclado, este lo compara con su cuadro de caracteres ASCII, luego el sistema hace un pequeño receso del *hardware* para así poder crear un registro de lo que está escribiendo la persona. Todo este proceso se hace en un instante pero si el computador cuenta con un *keylogger*, ese proceso tardará un poco más llegando a ser más perceptible y peor aun cuando se escribe rápidamente, ocasionando que el *keylogger* no pueda registrar algunas teclas o simplemente tardar el proceso normal del sistema percibiendo una interrupción anormal. Una manera sencilla de comprobar si algún registro carga memoria o se está ejecutando es abriendo el administrador de tareas presionando las teclas

Ctrl+Alt+Supr, se puede sospechar que uno de ellos sea un *keylogger*. Otra forma de evitar ser espiados es procurar ir a cafés internet donde no cuenta con una seguridad apropiada. Para protegerse de una manera eficaz, es conveniente tener instalado un buen antivirus (ya que muchos *keyloggers* son detectados como troyanos) o específicamente un *anti-keylogger* que es muy ligero y se puede descargar gratuitamente.

4. PROTECCIÓN DE SU PC CONTRA LOS KEYLOGGERS

4.1. Anti-spyware

Los programas *Anti-spyware* pueden detectar diversos *keyloggers* y limpiarlos. Vendedores responsables de supervisar la detección del *software* apoyan la detección de *keyloggers*, así previniendo el abuso del *software*.

4.2. Firewall

Habilitar un cortafuego o *firewall* puede salvar el sistema del usuario no solo del ataque de *keyloggers*, sino que también puede prevenir la descarga de archivos sospechosos, troyanos, virus, y otros tipos de *malware*.

4.3. Monitores de red

Los monitores de red (llamados también cortafuegos inversos) se pueden utilizar para alertar al usuario cuando el *keylogger* use una conexión de red. Esto da al usuario la posibilidad de evitar que el *keylogger* envié la información obtenida a terceros.

4.4. Software anti-keylogging

Este tipo de *software* graba una lista de todos los *keyloggers* conocidos. Los usuarios legítimos del ordenador pueden entonces hacer, periódicamente, una exploración de esta lista, y el *software* busca los artículos de la lista en el disco duro. Una desventaja de este procedimiento es que protege solamente contra los *keyloggers* listados, siendo vulnerable a los *keyloggers* desconocidos o relativamente nuevos.

Otro *software* que detecta *keyloggers* no utiliza una lista de estos, sino que, por el contrario, analiza los métodos de funcionamiento de muchos módulos en el ordenador, permitiéndole bloquear el trabajo del supuesto *keylogger*. Una desventaja de este procedimiento es que puede también bloquear *software* legítimo, que no son *keyloggers*. Algunos *software* contra *keyloggers* basados en heurística tienen la opción para desbloquear un *software* conocido, aunque esto puede causar dificultades para los usuarios inexpertos.

4.5. Anti-keyloggers

Este grupo de programas se especializa en detectar programas de monitoreo en un computador o servidor. Pueden venir incorporados en *software* antivirus o ser obtenido de diferentes compañías a través de Internet. Las versiones gratuitas por lo general se limitan únicamente a reportar la existencia de estos programas maliciosos, lo cual no es muy útil si su eliminación manual es dificultosa. Las versiones pagadas rastrean la existencia de programas que escriban archivos de los que sean generados durante la ejecución del programa *anti-logger*. Sin embargo, muchas de las soluciones de detección de estos intrusos resultan siendo programas espía, ya que envían archivos a los desarrolladores del supuesto *anti-keylogger*.

4.6. Otros métodos

La mayoría de los *keyloggers* pueden ser engañados sin usar un *software* especializado en su combate. Se puede copiar y pegar caracteres disponibles en la pantalla hasta formar la contraseña. La persona puede copiar esos caracteres de una página *web* escrita por ella misma, de forma de facilitar el acceso a la contraseña desde cualquier computador.

5. CONCLUSION

Como alguien te diría “es importante mantener en secreto tus datos de cuenta, nadie, excepto tú mismo debería saber tu número de cuenta, tu *password*, ni algún dato que pueda comprometer tu información”, pero esto no importa para los *hackers* ya que con los *keyloggers* te pueden quitar todo, porque no sabes si en el computador en el que estas puede estar o no con este programa.
Hay que tener en cuenta que realizar espionaje virtual resulta una actividad muy sencilla, y los *keyloggers* son solo una de las tantas maneras para ejecutarlas; aun cuando sus acciones, procesos y lineamientos están dentro del marco de la legalidad y un código ético, estas deben ser utilizados para fines totalmente lícitos y gestionar la seguridad desde la perspectiva de un atacante informático al interior de las organizaciones. Por ello, además de utilizar soluciones especializadas en el combate de estos programas maliciosos, el sentido común y la precaución deben ser elementos esenciales para la seguridad y la protección de los recursos informáticos, es por eso espero se tome muy en cuenta estas herramientas y métodos que se describieron en este artículo.

6. REFERENCIAS

[1] **Titulo**: Como detectar Keyloggers
Autor: Cabinas Net
Disponible en:
http://www.cabinas.net/informatica/keyloggers.asp
Fecha de acceso: 26/05/13 Hrs. 17:40

- [2]**Titulo**: Keyloggers prevención (nos están controlando)

Autor: Fedexx96
Disponible en:
http://www.taringa.net/posts/info/13952239/Keyloggers-prevencion-nos-estan-controlando.html
Fecha de acceso: 26/05/13 Hrs. 17:50

[3] **Titulo**:keyloggers: ¿espionaje en tu pc, nada más?
Autor: Juan Eladio Sánchez Rosas
Disponible en:
http://juansanchez.webcindario.com/trabajos/keylogger.php