KEYLOGGERS

Los Keyloggers son programas para el espionaje que plantean muchos problemas éticos y legales. Son utilizados muy a menudo en las oficinas de trabajo para que el director pueda espiar a sus empleados sin el conocimiento de estos. También los padres espían los hábitos en Internet de sus hijos con estos programas. Conozca realmente qué es un Keylogger.

Los Keyloggers suelen ser partes muy importantes de los troyanos. En realidad nada tenían en común en un principio. Los primeros troyanos no llevaban keyloggers y éstos eran programas aparte que se vendían en la Internet en páginas de espionaje junto a los artículos de espías de toda la vida. La función del keylogger es registrar todas las pulsaciones del teclado en un archivo del sistema para luego proceder a su lectura. Así pues, si escribimos cualquier texto en Word, tecleamos cualquier contraseña en nuestro ordenador o chateamos en el IRC, todo lo que hayamos escrito habrá quedado registrado en un archivo (generalmente un archivo *.log).

Para qué sirve esto, podemos preguntarnos. Bien, en un principio el keylogger se justificaba en casa para controlar la actividad de los menores en Internet, o en la oficina para seguir de cerca las actividades de los empleados. Cuando los Keyloggers se destinaban a ese uso, las compañías antivirus no los identificaban como una amenaza para la seguridad. En realidad los hackers tampoco se fijaban en esos programas porque no permitían el control remoto de otra computadora.

Pero todo evoluciona y cuando el Keylogger se une al troyano o backdoor es cuando la amenaza se percibe como tal. De esta forma el keylogger registra las pulsaciones y el troyano envía los datos al hacker.

Hay que señalar también que hay keyloggers legales de pago que hacen cosas muy parecidas a los troyanos que tienen keyloggers. Estos nuevos keyloggers llevan un novedoso sistema que comunica el archivo logueado a una cuenta de correo electrónico mediante Internet. Esto generalmente se consigue de dos formas:

1- Envío por e-mail del archivo logueado cada cierto tiempo prefijado (por ejemplo, cada 24 horas).

2- Envío por e-mail del archivo logueado cada cierta cantidad de bytes (por ejemplo, cada 500 kb de información).

3- Envio por a una cuenta FTP de el usuario cada cierto tiempo.

4- Envio de los logs a una pagina php que los guarda y mas tarde pueden ser visualizados.

¿Y qué tienen que decir las compañías antivirus aquí?. Una vez más la manera de comportarse del keylogger es fundamental. Si el programa se instala de manera silenciosa en el ordenador de la víctima, entonces es identificado como código peligroso.

Pero aquí nos encontramos con una dificultad añadida: un keylogger se vende para el espionaje, por tanto ha de correr silencioso en un ordenador. De no ser así, no sería un buen keylogger.

También las compañías antivirus tienen en cuenta otro factor: si tiene comunicación por e-mail es peligroso, si no la tiene, puede ser inofensivo.

La verdad es que uno a veces tiene la sensación de que si el keylogger lo hace una persona que nadie conoce, será identificado como amenaza vírica y todo el trabajo de esa humilde persona se irá al garete; en cambio, si el keylogger lo ha registrado una gran empresa de software, entonces no habrá ni una compañía antivirus que se atreva a identificarlo por miedo a las represalias judiciales. Hasta hace poco estaba usando un keylogger legal que había crackeado en un ordenador con su antivirus actualizado.

Curiosamente ese programa lleva incluso su notificación por e-mail, pero los antivirus no lo detectan. Tal vez la diferencia esté en que si bien corre silente en cada inicio de Windows, la primera instalación en cambio requirió una configuración manual. Si el keylogger llega desde la internet y la víctima lo ejecuta sin saberlo, no funcionará si no activa los parámetros. Pero esto es suponer que el hacker nunca va a poder acceder físicamente al ordenador de la víctima; y eso es mucho suponer.

Una vez más la política de los antivirus queda en entredicho y uno tiene la sensación de que si Microsoft inventara un virus, nadie sería capaz de identificarlo por miedo al gigante de Redmon. De cualquier forma,

un keylogger no es un virus ni tampoco un troyano: tiene una función muy específica que consiste en grabar todo tipo de pulsaciones del teclado e incluso algunos recogen también los clics de ratón, las páginas visitadas en la Internet y las conversaciones tanto entrantes como salientes en el chat. No hace ningún daño a ningún ordenador. Aquí juega una vez más la intención de la persona que lo utiliza: exactamente igual que con los troyanos.

Aquí tienen Ustedes unos keyloggers para descargar. Algunos antivirus los detectan. Tengan cuidado.

Iklogger 0.1

Indetectables Keylogger, desarrolado en esta página por Sr Sombrero y Thor.

Envío de logs por FTP, 6 métodos de inicio, encriptación de logs.

La forma de uso es sencilla, abrir editor.exe, dad a Crear Server, en envío elegid si queréis que se envien los logs a un FTP o que se guarden en el equipo que se logea. Si elegis envío por FTP tendréis que introducir vuestros datos y dar a Test FTP para probar que todo ha ido bien. Se puede configurar la carpeta del FTP donde se guardaran los logs y cada cuánto tiempo se envian (por defecto cada 3 horas de logeo).
Setear las opciones que creáis convenientes, encriptación, melt...
En métodos de inicio selecionar uno, varios o ninguno (buena opción si lo que queréis es probarlo en vuestro PC, basta reiniciar para quedar desinfectado).
Activar capturas de clicks si se ve necesario y crear server.

Descarga: http://thor.webcindario.com/IKlogger0.1.rar

LttLogger v2.0

Muy buen keylogger, envío FTP, notificación PHP, 7 métodos de inicio. Vamos a ver cómo usarlo.
Abrir CreateServer.exe, en main poner un nombre al azar.
En FTP setting como el iklogger, poner los datos y comprobar que funciona.
En Logfile el nombre del log y con qué tamaño máximo se envía por defecto 15000 bytes.
Pasamos a la pestaña Startup, selecionar los métodos que se crea necesarios.
En notificación se puede activar la notificación PHP, para que funcione tenéis que subir el fichero log.php de la carpeta **PHPNOTIFY** a un alojamiento que soporte php , poner la URL completa en el editor y dad a probar, os dirá que valláis a la página http://tuhosting/view.php allí poned el password “pass”, es el password por defecto, se puede y se debe cambiar así como el nombre de el archivo de log en el fichero log.php. Sino cualquiera que sepa que en nuestro hosting usamos la notificacion podría intentar ver el fichero http://tuhosting/log.txt y tendría los logs que la notificación php guarda allí.

lll Logger

Posiblemente el keylogger más pequeño del mundo programado en ASM por un genio excéntrico llamado **lllWill.** Sólo 2 kb dan para guardar todas las pulsaciones del teclado y reiniciar el keylogger cada vez que Windows se carga. ¡Increíble!.

KeySpy

Otro keylogger para Win 9x y Windows ME. Son 64 kb (480 kb con el programa de instalación). Los antivirus lo detectan.

Tiny Keylogger

Otro minúsculo keylogger que algunos antivirus detectan. Sólo son 7.5 kb cuando se instala. Corre totalmente silente, así que es indicado para el espionaje.

Perfect Keylogger

Keylogger legal, muy poco detectado por las compañias de antivirus. Envio de logs por email, FTP y todas las opciones imaginables. De aquí se puede descargar una version de prueba para 3 días:
http://www.blazingtools.com/downloads/i_bpk2003.exe

Hay muchos mas keyloggers, sabiendo usar un par de ellos el resto no tendrá ningun misterio para nosotros.
En esta página encontraréis unos cuantos mas:

http://www.trojanfrance.com/index.php?dir=KeyLoggers/

Autor: **Coolvibes**

Página: Indetectables.com.ar