Keyloggers: Qué son y cómo detectarlos (primera parte)

29.03.2007 | **Comentar**

Nikolay Grebennikov

En febrero de 2005, Joe López, un empresario de Florida, enjuició al Bank of America después de que unos hackers desconocidos robaran 90.000 dólares de su cuenta en este banco. El dinero robado había sido transferido a Latvia.

Una investigación reveló que el ordenador de López había sido infectado con el virus conocido como Backdoor Coreflood, el cual registra cada pulsación del teclado y envía esta información a ciberdelincuentes vía Internet. Fue de esta manera que los hackers obtuvieron el nombre de usuario y la contraseña de Joe López, ya que él a menudo realizaba sus transacciones bancarias a través de Internet.

Sin embargo, el veredicto de la corte no favoreció al interpelante pues se adujo que Joe López había sido negligente por no tomar precauciones al manejar su cuenta bancaria a través de Internet. La signatura del código malicioso encontrado en su sistema había sido añadida a las bases de datos de casi todos los antivirus ya en 2003.

Las pérdidas de Joe López fueron causadas por una combinación de un descuido general y un programa keylogger ordinario.

Sobre Keyloggers

Por sí mismo, el término 'keylogger' es neutral y describe una función que registra las pulsaciones de las teclas del ordenador.

La mayoría de las fuentes consultadas definen keylogger como un programa diseñado para, en secreto, monitorear y registrar cada pulsación del teclado. Esta definición no es correcta del todo, pues un keylogger no necesariamente tiene que ser un programa, sino que también puede ser un dispositivo físico. Los dispositivos keylogger son menos conocidos que el software keylogger, pero es importante tener en cuenta la existencia de ambos cuando se habla de seguridad informática.

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 (por ejemplo el teclado Ninja). Se encuentra disponible un gran número de programas diseñados 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.

La mayoría de los modernos keyloggers se consideran software o hardware legítimo y se venden abiertamente en el mercado. Los desarrolladores y vendedores ofrecen una larga lista de casos en los cuales resulta legal el uso de los keyloggers, como por ejemplo:

- Control para padres: los padres pueden rastrear las actividades de sus hijos en Internet y pueden solicitar que se les envíe notificaciones en caso de acceso a sitios Internet con contenido para adultos;

Las esposas o esposos celosos pueden recurrir a un keylogger para rastrear las actividades de su pareja en Internet si llegan a sospechar que están envueltos en una “relación virtual”;

Seguridad corporativa: rastreado del uso de ordenadores con propósitos extralaborales, o el uso de las estaciones fuera de las horas de trabajo;

Seguridad corporativa: uso de keyloggers para rastrear la introducción de palabras y frases clave asociadas con información comercial que podría perjudicar a la empresa (ya sea en el orden material u otro) si llegara a revelarse;

Otro tipo de seguridad: uso de registros de keyloggers para analizar y rastrear incidentes relacionados con el uso de ordenadores personales;

Otras razones.

Aunque las justificaciones arriba mencionadas son más subjetivas que objetivas, todas las situaciones pueden resolverse mediante otros métodos. 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 en línea, y los elaboradores de virus no cesan en su afán de elaborar nuevos troyanos keyloggers con tal propósito.

Asimismo, muchos keyloggers se esconden en el sistema, por ejemplo, pueden camuflarse como rootkits, lo cual los convierte en programas troyanos completamente furtivos.

Considerando que los keyloggers pueden usarse para cometer actos delictivos, la detección de tales programas se ha convertido en una prioridad para las compañías antivirus. El sistema clasificatorio de Kaspersky Lab tiene una categoría especial llamada Trojan-Spy, que resulta ser una perfecta definición para los keyloggers. Los troyanos-espía, tal como sugiere su nombre, rastrean la actividad del usuario, almacenan la información en el disco duro del ordenador del usuario y luego se la envían al autor o ‘dueño’ del troyano. La información robada incluye las teclas pulsadas por el usuario y fotografías de pantallas, las cuales se utilizan en el robo de información bancaria para llevar a cabo los fraudes en línea.

Por qué constituyen una amenaza

A diferencia de otros tipos de programas maliciosos, los keyloggers no representan una amenaza para el sistema mismo. Sin embargo, pueden significar una seria amenaza para los usuarios ya que pueden usarse para interceptar contraseñas y otro tipo de información confidencial ingresada a través del teclado. Como resultado, los ciberdelincuentes pueden obtener códigos PIN y números de cuentas de sistemas de pagos en línea, contraseñas para cuentas de usuarios de juegos en línea, direcciones de correo electrónico, nombres de usuario, contraseñas de correo electrónico, etcétera.

Una vez que el ciberdelincuente tiene en su poder la información confidencial del usuario, puede con toda facilidad proceder a transferir los fondos desde la cuenta del usuario o puede obtener acceso a la cuenta del usuario de juegos en línea. Por desgracia, este acceso a información personal a veces conlleva consecuencias de mayor gravedad que la pérdida de unos cuantos dólares por parte del usuario. Los keyloggers pueden ser usados como herramientas en el espionaje industrial y político, ya que se logra obtener datos que pudieran incluir información de propiedad comercial y material gubernamental clasificado que podrían llegar a comprometer la seguridad de organismos estatales, por ejemplo, mediante el robo de llaves privadas de cifrado.

Los keyloggers junto al phishing y a los métodos de ingeniería social (ver el artículo "El robo de propiedad virtual en las redes informáticas") son los principales métodos utilizados en el fraude electrónico moderno. Sin embargo, no es difícil para un usuario cauto protegerse. Basta ignorar aquellos correos electrónicos claramente identificados como phishing y no brindar ningún tipo de información personal a sitios Internet sospechosos. En cambio, no hay mucho que un usuario pueda hacer para prevenir el fraude cometido mediante los keyloggers, excepto recurrir a medios especializados de protección, puesto que resulta casi imposible comprobar un fraude cometido mediante un keylogger.

Según Cristine Hoepers, gerente del Equipo de Respuesta a Emergencias Informáticas del Brasil que trabaja en el marco de la Comisión sobre Internet de aquel país, los keyloggers han desplazado al phishing del primer lugar en la lista de los métodos más utilizados en el robo de información confidencial. Más aún, los keyloggers se están volviendo cada vez más sofisticados pues pueden rastrear sitios Internet visitados por el usuario y sólo registrar el uso del teclado en aquellos sitios de particular interés para el ciberdelincuente.

Durante los últimos años hemos presenciado un notable crecimiento en el número de los diferentes tipos de programas maliciosos con funciones de keyloggers. Ningún usuario de Internet se libra del riesgo de caer en manos de los ciberdelincuentes, sin importar en qué parte del mundo se encuentre ni la organización para la que trabaje.

Cómo utilizan los ciberdelincuentes los keyloggers

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. Era de esta manera que 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.

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 keylogger troyano 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 delincuente con similares características conformada por jóvenes rusos y ucranianos de entre 20 y 30 años . A fines de 2004, este grupo comenzó enviando 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. 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

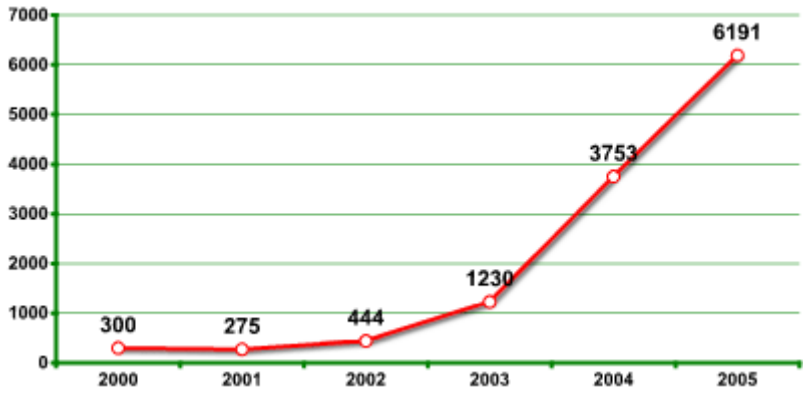
para luego remitirla a los ciberdelincuentes. En el transcurso de once meses, robaron más de un millón de dólares.

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 comprehensiva y confiable para rastrear información electrónica.

Aumento del uso de keyloggers por parte de los ciberdelincuentes

El hecho de que los ciberdelincuentes opten por los keyloggers de manera tan recurrente es confirmado por las compañías de seguridad informática.

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 para los keyloggers.



Fuente: iDefense, una compañía de VeriSign

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 en línea, 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.

Principios de construcción de keyloggers

La principal idea que guía a los keyloggers es colocarse entre dos puntos cualquiera en la cadena de eventos, entre el momento de pulsar una tecla y cuando la información aparece en el monitor. Esto se logra mediante el uso de dispositivos de video vigilancia, un dispositivo de hardware en el teclado, el

cableado del ordenador, la intercepción de entradas y salidas, el cambio del driver del teclado, el cambio del driver de filtrado en la pila del teclado, la intercepción de funciones esenciales mediante cualquier método, (sustituyendo direcciones en las tablas del sistema, cortando códigos de funciones, etc.), la intercepción de funciones DLL en el modo del usuario, y por último, solicitando información desde el teclado mediante métodos estándar documentados.

La experiencia muestra que cuanto más complejo sea el enfoque, tanto más improbable será su uso en programas troyanos comunes y tanto más probable será su uso en programas troyanos especialmente diseñados para robar datos financieros de una determinada compañía.

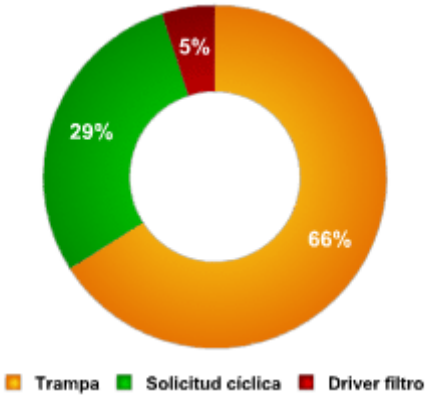
Los keyloggers se pueden dividir en dos categorías: dispositivos físicos y programas. Los dispositivos keylogger por lo general son pequeños y pueden ser acoplados al teclado o colocados dentro de un cable o dentro del mismo ordenador. Los programas keylogger están diseñados para rastrear y registrar las digitaciones en el teclado.

Los métodos más comunes usados para construir programas keylogger son los siguientes:

- un sistema que intercepta notificaciones de que una tecla ha sido pulsada (se instala usando WinAPI SetWindowsHook para mensajes enviados por el procedimiento de ventana. Por lo general se escribe en C);
- una solicitud desde el teclado sobre información cíclica del teclado (usando WinAPI Get(Async)KeyState o GetKeyboardState, por lo general escrito en VisualBasic, y a veces en Borland Delphi);
- Usando el driver de filtrado (requiere conocimientos especializados y está escrito en C).

En la segunda parte de este artículo se brindará una explicación detallada sobre las diferentes formas de construir keyloggers. Pero primero, es necesario considerar algunas estadísticas.

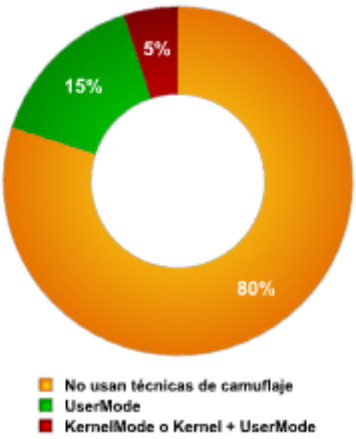
El siguiente gráfico muestra los diferentes tipos de keyloggers:



Los keyloggers que disfrazan sus archivos para evitar ser detectados manualmente o por un programa antivirus se están volviendo muy comunes en estos últimos tiempos. Tales métodos se llaman tecnologías rootkit. Los keyloggers utilizan dos principales tecnologías de camuflaje:

- enmascaradas en el Modo del Usuario;
- enmascaradas en Modo Kernel.

El siguiente gráfico muestra las técnicas usadas por keyloggers para enmascarar sus actividades:



Cómo se propagan los keyloggers

Los keyloggers se propagan de manera muy parecida a como lo hacen otros programas maliciosos. Exceptuando aquellos casos en los que los keyloggers son adquiridos e instalados por una pareja celosa, o son usados por servicios de seguridad, por lo general se propagan mediante los siguientes métodos:

Un keylogger se puede instalar cuando un usuario abre un archivo adjunto a un mensaje de correo electrónico;

Un keylogger se puede instalar cuando un archivo se ejecuta desde un directorio de acceso abierto en una red P2P;

Un keylogger puede instalarse a través de una rutina de una página de Internet que aprovecha una vulnerabilidad de un navegador y automáticamente ejecuta el programa cuando el usuario visita un sitio Internet infectado;

Un keylogger puede instalarse mediante un programa malicioso previamente instalado, capaz de descargar e instalar otros programas maliciosos en el sistema.

Cómo protegerse contra los keyloggers

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.

Demos una mirada más detallada a los métodos que se pueden utilizar como protección contra keyloggers desconocidos o contra un keylogger diseñado para atacar un sistema en particular.

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 autentificación 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:

1. una tecla USB (tal como Aladdin eToken NG OTP):

2. 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 autentificación.

Si alguno de los mecanismos arriba descritos se usa para generar contraseñas, el procedimiento a seguir se describe a continuación:

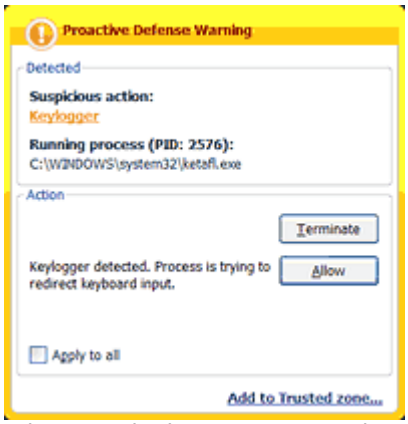
1. el usuario se conecta a Internet y abre una ventana de diálogo en la cual se puede ingresar los datos personales;
2. luego, pulsa un botón en el mecanismo para generar una contraseña de uso único, la cual aparecerá en la pantalla LCD del dispositivo durante 15 segundos;
3. ingresa su nombre de usuario, 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.

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.



Protección proactiva contra keyloggers en Kaspersky Internet Security

El principal problema de este método 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 legítimas de keyloggers 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.

Un ejemplo del 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 ser especialmente diseñado para poder asegurar que la información ingresada o transmitida por este medio no sea interceptada.

Conclusiones

Este artículo ha brindado información general sobre cómo funcionan los keyloggers, tanto programas como dispositivos, y cómo se los usa.

Aunque los desarrolladores de keyloggers comercializan sus productos como software legítimo, la mayoría de los keyloggers pueden ser utilizados para robar información personal de los usuarios y para fines de espionaje político e industrial.

Actualmente, los keyloggers son, junto al phishing y a los métodos de ingeniería social ,uno de los métodos más utilizados para cometer fraudes cibernéticos.

Las compañías de seguridad informática han registrado un permanente aumento del número de programas maliciosos con funciones de keykoggers.

Los informes muestran que hay una marcada tendencia en el uso de tecnologías rootkit en los programas keyloggers con el fin de permitir que éstos evadan la detección manual y la de soluciones antivirus.

Sólo una protección especial puede detectar que un keylogger esta siendo utilizado con propósitos de espionaje.

Se pueden tomar las siguientes medidas para protegerse contra los keyloggers:

- Usar un antivirus estándar que pueda ser adaptado para la detección de programas potencialmente maliciosos (opción preconfigurada en muchos productos), la protección proactiva protegerá el sistema contra nuevas modificaciones de keyloggers existentes;
- Uso de un teclado virtual o de un sistema para generar contraseñas de uso único para protegerse contra programas y dispositivos keylogger.

Fuente:

- Kaspersky Lab