ESCALANDO

Paola Andrea Pedraza
Código: 21109014
e-mail:pao8905@hotmail.com
Paola Marcela Parra
Código: 21109014
e-mail: paoparra231818@hotmail.com

RESUMEN: *en este taller se aplicó la encriptación cifrado, codificación). La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptado sólo puede leerse aplicándole una clave.*

Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números. de tarjetas de crédito, conversaciones privadas, etc.

Índice de Términos: Encriptación, claves, contraseña, archivo, imagen, seguridad, información, correo ,Excel, Word, jpg, carácter, ImageHide, Keylogger, merge.

INTRODUCCIÓN

Un keylogger (derivado del inglés: key (tecla) y logger (registrador); registrador de teclas) es un tipo de software o un dispositivo hardwareespecífico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

Suele usarse como malware del tipo daemon, permitiendo que otros usuarios tengan acceso a contraseñas importantes, como losnúmeros de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener.

El registro de lo que se teclea puede hacerse tanto con medios de hardware como de software. Los sistemas comerciales disponibles incluyen dispositivos que pueden conectarse al cable del teclado (lo que los hace inmediatamente disponibles pero visibles si un usuario revisa el teclado) y al teclado mismo (que no se ven pero que se necesita algún conocimiento de cómo soldarlos para instalarlos en el teclado). Escribir aplicaciones para realizar keylogging es trivial y, como cualquier programa computacional, puede ser distribuido a través de un troyano o como parte de un virus informático o gusano informático. Se dice que se puede utilizar un teclado virtual para evitar esto, ya que sólo requiere clics del ratón. Sin embargo, las aplicaciones más nuevas también registran screenshots (capturas de pantalla) al realizarse un clic, que anulan la seguridad de esta medida.

A. UNA IMAGEN EN FORMATO PNG CON UN TEXTO ENCRIPTADO QUE TENGA EL CORREO PERSONAL DEL ESTUDIANTE, PARA REALIZARLO ES NECESARIO UTILIZAR LA HERRAMIENTA IMAGE HIDE.

- Se descarga la herramienta image hide de la página http://www.dancemammal.com/imagehide.htm , donde encontramos las siguientes características sobre del software:

- Ocultar un montón de texto en imágenes
- Sencillo cifrar y descifrar los datos (edad 1,0 Ver)
- Ver cuántos datos se pueden agregar en bytes
- Ningún aumento en el tamaño de la imagen
- Imagen se ve igual a los paquetes normales de pintura
- Obtenga más allá de todos los rastreadores de correo
- Nueva versión 2.0
- Mejor cifrado

- Ahora utiliza el cifrado más RC_4 hashing SHA
- Las contraseñas con algoritmo hash (ahora en la imagen)
- cargas y vistas archivos Ver. 1.0
- Ahora sabe Versión y cuando estén cifrados o no
- Ahora puede imprimir las imágenes
- Guardar archivos de imagen como BMP o PNG
- Puede utilizar muchos diferentes formatos de imagen

➢ Se instala el software en el equipo (ver anexo 1)

Figura N° 1

➢ Donde nos muestra el menú de la aplicación.
➢ Se llama la imagen guardada en el equipo donde se ejecuta el programa.

Figura N° 2

➢ Se selecciona la opción de Write Data:

➢ Lo que permite escribir la cuenta de correo que se va a encriptar :

➢ Se selecciona la opción “Encrypt” la cual es la que permite dar una contraseña de seguridad al correo:

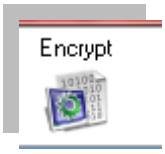
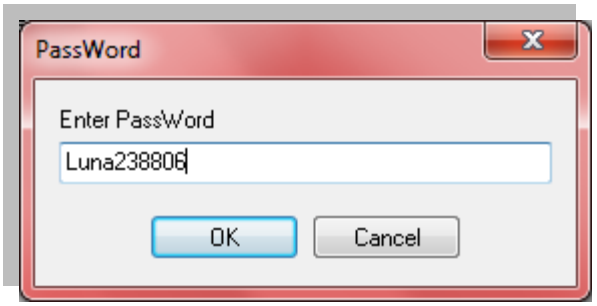


Figura N° 3

➢ Luego el software nos pide asignar una contraseña:



➢ La cual se proporciona y se da en la opción OK.
➢ Después de esto el software le asigna caracteres al correo logrando asi el cifrado del mismo.

Figura N° 4 - Figura N° 5

B. HACER UN MERGE CON 1 ARCHIVO DE WORD Y OTRO DE EXCEL.

➢ Lo primero es tener la base de datos que vamos a usar en el Merge ya lista en excel. Es importante que cada columna tenga su encabezado.

Figura N° 6

Antes de cerrar, es recomendable seleccionar el rango de celdas y darle un nombre (yo uso -tabla- en este ejemplo) (el nombre se pone en la parte donde normalmente sale la celda actual)

- Ahora vamos a Word a hacer el Mail-Merge , La opcion para hacer el merge está en Tools -> Letter and Mailings

  Figura N° 7

- esto va a abrir un asistente en la parte derecha del word.
  A partir de ahora vamos a seguir este asistente paso por paso En el tercer paso, hay que buscar el archivo de excel porque es en el cual se va a basar Word para los datos.

Figura N° 8

- cuando selecciones el archivo, te va a aparecer todas las listas de datos que tiene excel, aqui es donde vemos la importancia de haber nombrado toda la tabla con un nombre diferente

Figura N° 9

C. PROBAR OTROS KEYLOGGER Y DETALLAR SUS CARACTERÍSTICAS MAS IMPORTANTES

- Un keylogger (derivado del inglés: key (tecla) y logger (registrador); registrador de teclas) es un tipo de software o un dispositivo hardwareespecífico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

- Suele usarse como malware del tipo daemon, permitiendo que otros usuarios tengan acceso a contraseñas importantes, como losnúmeros de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener.

- El registro de lo que se teclea puede hacerse tanto con medios de hardware como de software. Los sistemas comerciales disponibles incluyen dispositivos que pueden conectarse al cable del teclado (lo que los hace inmediatamente disponibles pero visibles si un usuario revisa el teclado) y al teclado mismo (que no se ven pero que se necesita algún conocimiento de como soldarlos para instalarlos en el teclado). Escribir aplicaciones para realizar keylogging es trivial y, como cualquier programa computacional, puede ser distribuido a través de un troyano o como parte de un virus informático o gusano informático. Se dice que se puede utilizar un teclado virtual para evitar esto, ya que sólo requiere clics del ratón. Sin embargo, las aplicaciones más nuevas también registran screenshots (capturas de pantalla) al realizarse un click, que anulan la seguridad de esta medida.

- Funcionammiento:

- El registro de las pulsaciones del teclado se puede alcanzar por medio de hardware y de software:

- Keylogger con hardware

- Un keylogger tipo hardware.

- Son dispositivos disponibles en el mercado que vienen en tres tipos:

- Adaptadores en línea que se intercalan en la conexión del teclado, tienen la ventaja de poder ser instalados inmediatamente. Sin embargo, mientras que pueden ser eventualmente inadvertidos se detectan fácilmente con una revisión visual detallada.

- Dispositivos que se pueden instalar dentro de los teclados estándares, requiere de habilidad para soldar y de tener acceso al teclado que se modificará. No son detectables a menos que se abra el cuerpo del teclado.

- Teclados reales del reemplazo que contienen el Keylogger ya integrado. Son virtualmente imperceptibles, a menos que se les busque específicamente.

- Keylogger con software
- Contrariamente a las creencias populares, el código de un keylogger por software es simple de escribir, con un conocimiento básico de la API proporcionada por el sistema operativo objetivo. Los keyloggers de software se dividen en:
- Basado en núcleo: Este método es el más difícil de escribir, y también de combatir. Tales keyloggers residen en el nivel del núcleo y son así prácticamente invisibles. Derriban el núcleo del sistema operativo y tienen casi siempre el acceso autorizado al hardware que los hace de gran alcance. Un keylogger que usa este método puede actuar como driver del teclado por ejemplo, y accede así a cualquier información registrada en el teclado mientras que va al sistema operativo.
- Enganchados: Estos keyloggers registran las pulsaciónes de las teclas del teclado con las funciones proporcionadas por el sistema operativo. El sistema operativo activa elkeylogger en cualquier momento en que se presione una tecla, y realiza el registro.
- Métodos creativos: Aquí el programador utiliza funciones como GetAsyncKeyState, GetForegroundWindow, etc. Éstos son los más fáciles de escribir, pero como requieren la revisión el estado de cada tecla varias veces por segundo, pueden causar un aumento sensible en uso de la CPU y pueden ocasionalmente dejar escapar algunas pulsaciones del teclado.
- Protección
- *En algunas computadoras podemos darnos cuenta si están infectadas por un keylogger (dependiendo de la velocidad y uso de CPU de nuestro procesador) por el hecho de que el programa registrara cada una de nuestras teclas de la siguiente manera: FicheroLog = FicheroLog + UltimaTecla, este evento será ejecutado por el keylogger cada vez que el usuario presione una tecla. Si bien este evento no será una carga relevante para nuestro procesador si se ejecuta a una velocidad normal, pero si mantienes unas 10 teclas presionadas por unos 30 segundos con la palma de tu mano y tu sistema se congela o su funcionamiento es demasiado lento podríamos sospechar que un keylogger se ejecuta sobre nuestro computador. Otro signo de que un keylogger se está ejecutando en nuestro computador es el problema de la tilde doble (´´) al presionar la tecla para acentuar vocales, salen dos tildes seguidas y la vocal sin acentuar. Esto ocurre en keyloggers configurados para otros idiomas.*

- 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.
- Firewall
- Habilitar un cortafuegos 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.
- 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 envie la información obtenida a terceros
- Software anti-keylogging
- El software para la detección de keyloggers está también disponible. Este tipo de software graba una lista de todos los keyloggers conocidos. Los usuarios legítimos del PC 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.