CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS DE SEGURIDAD **para prevenir la amenza del keylogger**

Espías digitales en tu dispositivo

¿Qué es un keylogger?

Se conoce como keyloggers a programas o aparatos que registran todo lo que un usuario teclea en su computador o celular. Programas más avanzados pueden registrar lo que copiamos en el portapapeles, llamadas realizadas, datos del GPS o lo grabado por la cámara y el micrófono. Estos programas luego envían la información a los ciberdelincuentes.

Usos maliciosos

- Un keylogger puede ser usado por ciberdelincuentes para robar información confidencial, como contraseñas y números de tarjeta de crédito, y acceder a las cuentas bancarias, o secuestrar sus cuentas de redes sociales y plataformas de juego.
- También pueden conseguir información privada y fotos personales para humillar o chantajear a su víctima.

Usos maliciosos

- Más aún, con los datos reunidos se puede reconstruir todo lo que la víctima hizo durante su día en materia de interacción digital. Así, pueden ser usados para espiar a otros, como una pareja, o con fines políticos o de espionaje industrial.
- No descargues programas desde anuncios en internet, pop-ups o emails. Uno de los usos del phishing es, simulando ser un correo confiable, hacer que el usuario descargue malware, incluyendo keyloggers.

Formatos de keyloggers

- **Físicos (hardware):**
  - **En el teclado:** Pueden ser pequeños dispositivos conectados entre el tablero y el computador, o incluso haber sido instalados dentro del mismo teclado.
  - **Cámaras ocultas:** Para espiar lo que se teclea en computadores de uso público, como en cibercafés y bibliotecas.
  - **USB infectados:** Pendrive infectados con software keylogger que los delincuentes dejan en lugares concurridos o entregan a sus víctimas.

Formatos de keyloggers

- **Digitales (software):**
  - **Basados en API:** Interceptan los datos entre el teclado y los programas en los que estamos tipeando.
  - **Ladrones de formularios:** Roban todos los datos que se ingresan en formularios web.
  - **Basados en el kernel:** Ingresan al núcleo del sistema obteniendo permisos de Administrador, teniendo a su disposición toda la información que se ha ingresado al sistema.

Precauciones contra los keyloggers

1.- Usar programas de seguridad que escaneen tu equipo en busca de este tipo de software.

2.- Mantener tus equipos actualizados, para que detecten los keyloggers más modernos.

3.- Emplear administradores de contraseñas, que rellenan las claves en lugar de tener que tipearlas cada vez.

Precauciones contra los keyloggers

4.- Hacer una revisión física del aparato, para chequear que no haya conexiones extrañas entre el teclado y el resto del equipo.

5.- Activar la autenticación de dos pasos en las cuentas y apps que lo permitan.

6.- Evitar el uso de pendrives desconocidos o discos de almacenamiento externos en los que no se tenga confianza.

Es muy difícil detectar un keylogger, se recomienda tener actitudes de seguridad en internet para evitar estos programas maliciosos.