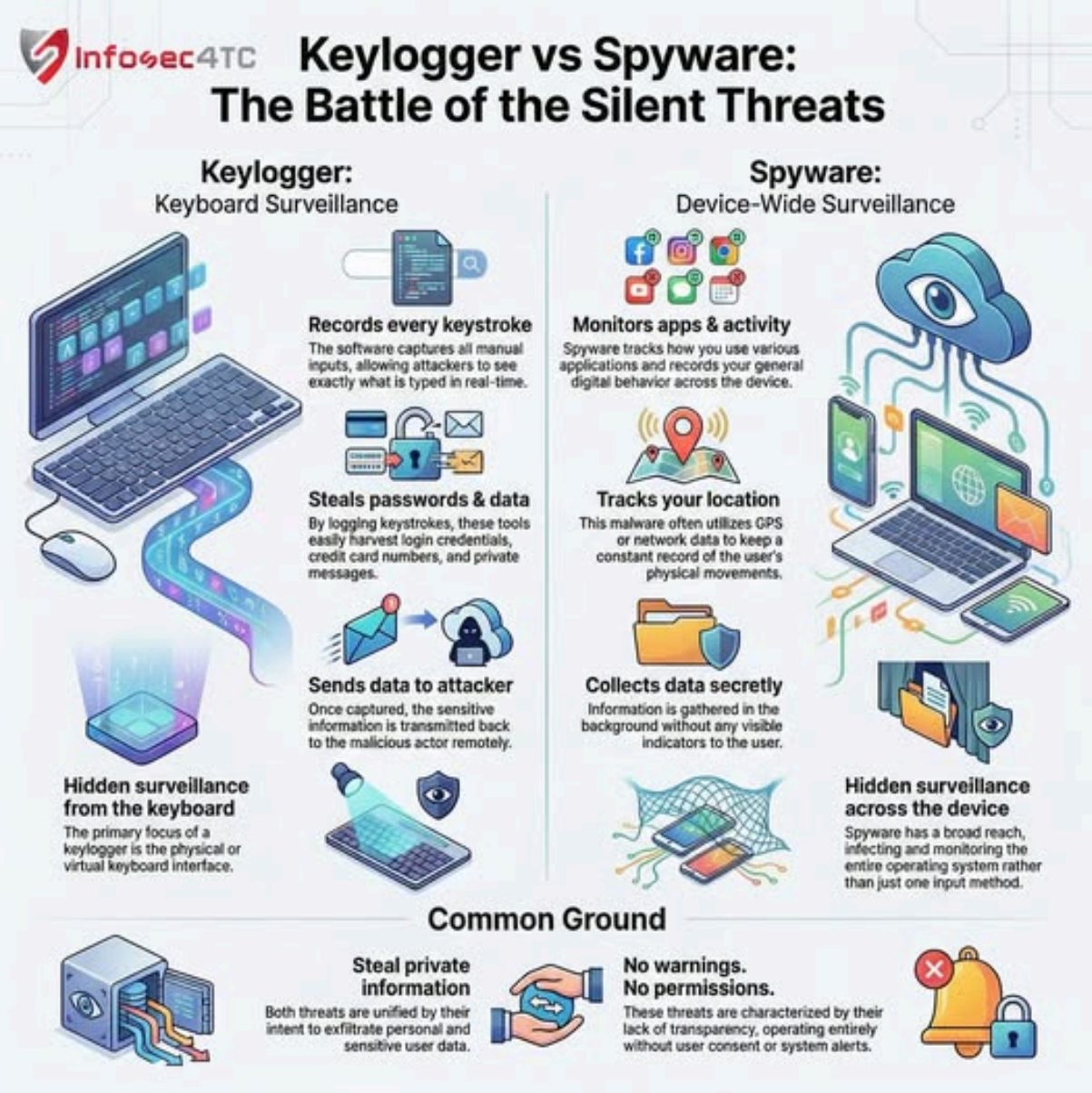
Universidad de Buenos Aires
Facultad de Ciencias Económicas

Key Loggers versus Spyware

Material de Estudio



Traducción y Comentarios

Keylogger vs Spyware: La batalla de las amenazas silenciosas

1. ¿Qué es un Keylogger? (Vigilancia del teclado)

Un **Keylogger** es un tipo de software malicioso (malware) diseñado para registrar cada tecla que el usuario presiona en su dispositivo.

Características principales:

- **Registra cada pulsación de teclado**

  Captura todas las teclas presionadas, permitiendo al atacante ver exactamente lo que el usuario escribe en tiempo real.

- **Roba contraseñas y datos**

  Al registrar las pulsaciones, puede obtener credenciales de acceso, números de tarjetas, información bancaria y mensajes privados.

- **Envía la información al atacante**

  Los datos capturados se transmiten de forma remota al ciberdelincuente.

- **Vigilancia oculta desde el teclado**

  Su foco principal es la interfaz física o virtual del teclado.

Enfoque desde Tecnologías de la Información

Desde la administración de sistemas:

- Es una amenaza directa a la confidencialidad.
- Compromete controles de acceso.
- Afecta auditorías digitales.
- Puede invalidar esquemas de autenticación basados solo en contraseñas.

---

2. ¿Qué es un Spyware? (Vigilancia integral del dispositivo)

El **Spyware** es un software malicioso que realiza vigilancia amplia sobre el dispositivo del usuario.

Características principales:

- **Monitorea aplicaciones y actividad**

Rastrea cómo se utilizan las aplicaciones y recopila comportamiento digital general.

- **Rastrea la ubicación**

  Puede usar GPS o datos de red para registrar movimientos físicos.

- **Recopila datos en segundo plano**

  Extrae información sin indicadores visibles para el usuario.

- **Vigilancia oculta en todo el dispositivo**

  Tiene un alcance más amplio que el keylogger.

Enfoque desde Tecnologías de la Información

Desde la gestión empresarial:

- Compromete datos corporativos.
- Puede exfiltrar información estratégica.
- Afecta cumplimiento normativo en protección de datos.
- Genera riesgo reputacional.

---

3. Diferencias clave

Aspecto	Keylogger	Spyware
Alcance	Solo teclado	Todo el dispositivo
Objetivo principal	Capturar credenciales	Recopilar información general
Tipo de vigilancia	Específica	Integral
Riesgo corporativo	Accesos no autorizados	Fuga masiva de información

---

4. Elementos en común

Ambos presentan características compartidas:

- **Roban información privada**

  Buscan extraer datos personales y sensibles.

- **Sin advertencias visibles**

Operan sin transparencia ni alertas del sistema.

Desde la perspectiva de TI, ambos constituyen amenazas silenciosas que afectan:

- Seguridad de la información.
- Gobernanza digital.
- Continuidad del negocio.
- Confianza institucional.

---

5. Implicancias para estudiantes de Administración

Desde la gestión de Tecnologías de la Información, es fundamental comprender que:

- La seguridad no depende únicamente del área técnica.
- Los mecanismos de autenticación deben complementarse con controles adicionales.
- Es necesaria la implementación de:
    - Antivirus y sistemas EDR (Endpoint Detection and Response – Detección y Respuesta en Puntos Terminales).
    - MFA (Multi-Factor Authentication – Autenticación Multifactor).
    - Políticas de seguridad.
    - Capacitación en ciberseguridad.

Un keylogger puede vulnerar controles débiles de contraseña.

Un spyware puede comprometer bases de datos completas.

La administración moderna exige entender que la protección de la información es una responsabilidad estratégica y no solo técnica.

---

6. Consideraciones de Gobernanza Digital

Para mitigar estos riesgos, las organizaciones deben considerar:

- Gestión de accesos.

- Segmentación de redes.
- Monitoreo de actividad sospechosa.
- Auditoría periódica.
- Cumplimiento de normativas de protección de datos.

En sistemas financieros, logísticos o de recursos humanos, estas amenazas pueden derivar en:

- Fraude.
- Robo de identidad.
- Pérdidas económicas.
- Sanciones regulatorias.

La comprensión de estas amenazas es parte esencial de la formación en administración con enfoque tecnológico.

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.