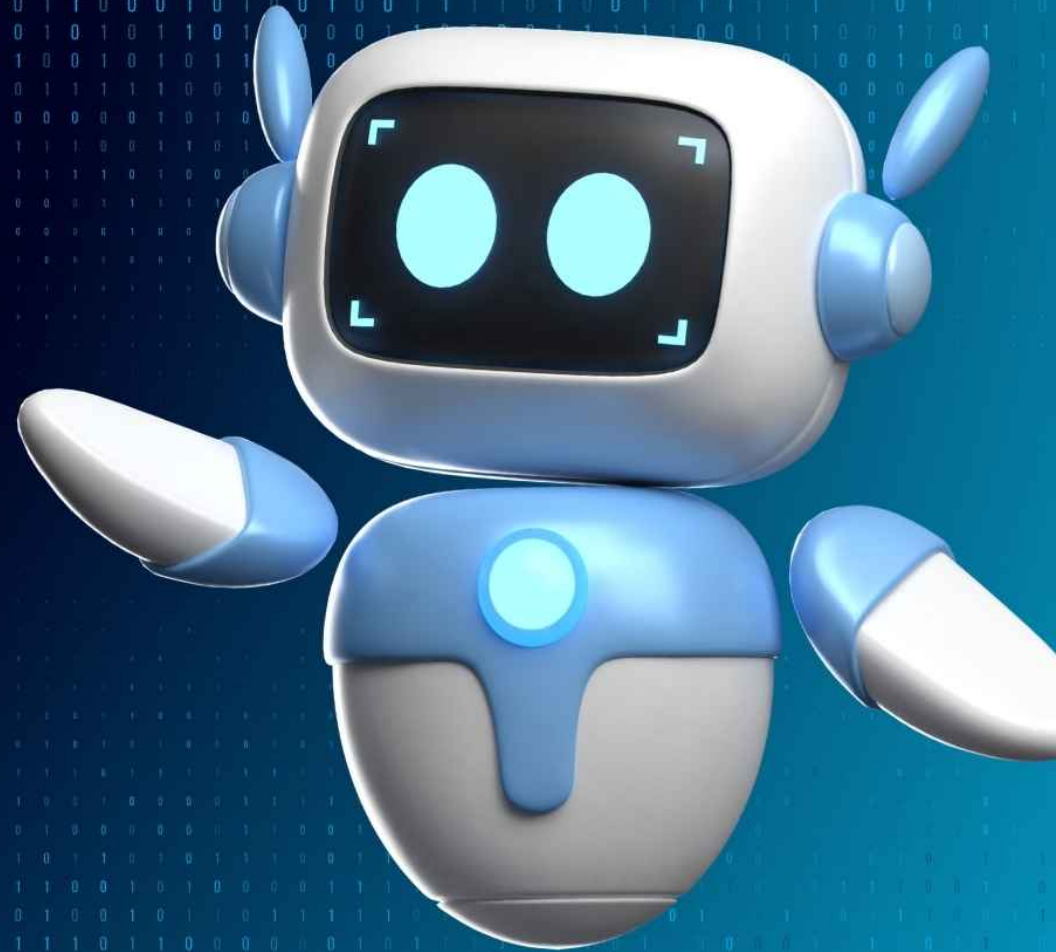


ANTIKEY LOGGER

Andrade Santiago
De la Cruz Samia
Rosales Carlos



1

¿QUÉ ES UN KEYLOGGER?

Definición:

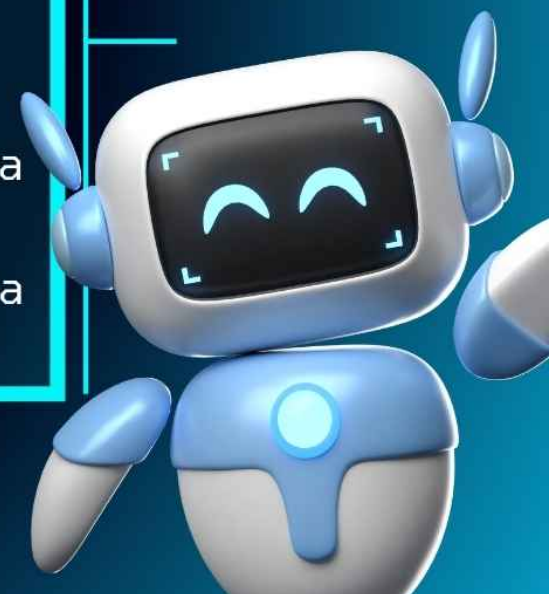
- Un keylogger es un software o hardware que registra cada pulsación de teclas en un teclado.

Objetivo:

- Capturar información confidencial como contraseñas, datos bancarios y conversaciones privadas.

Tipos:

- Software: Programas maliciosos que se instalan en el sistema operativo.
- Hardware: Dispositivos físicos conectados entre el teclado y la computadora.



2

INTRODUCCIÓN AL ANTIKEYLOGGER

Definición:

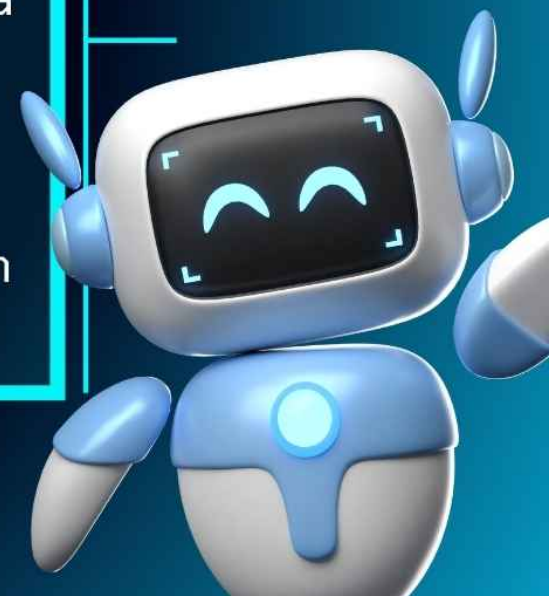
- Un antikeylogger es un software diseñado para detectar y bloquear keyloggers.

Función Principal:

- Proteger la privacidad y seguridad de los datos al evitar la captura de pulsaciones de teclas.

Importancia:

- Previene el robo de información sensible.
- Protege contra ataques de ciberdelincuentes que buscan explotar datos personales y financieros.





FUNCIONAMIENTO DE LOS ANTIKEYLOGGERS

Detección Basada en Firmas:

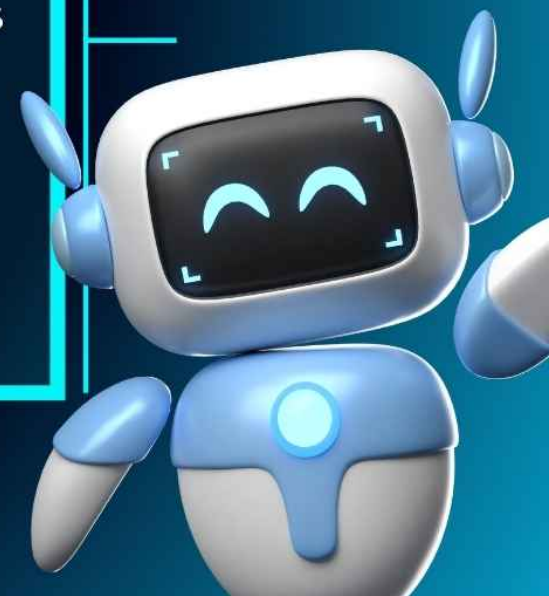
- Identifica keyloggers conocidos mediante una base de datos de firmas de malware.
- Limitación: Solo detecta keyloggers previamente identificados.

Detección Basada en Comportamiento:

- Monitoriza el sistema para detectar comportamientos sospechosos asociados con la actividad de keyloggers.
- Ventaja: Puede identificar amenazas nuevas y desconocidas.

Encriptación de Pulsaciones:

- Encripta las pulsaciones del teclado en tiempo real.
- Beneficio: Incluso si un keylogger captura los datos, estos serán ilegibles.





TIPOS DE ANTIKEYLOGGERS

Antikeyloggers Basados en Firmas:

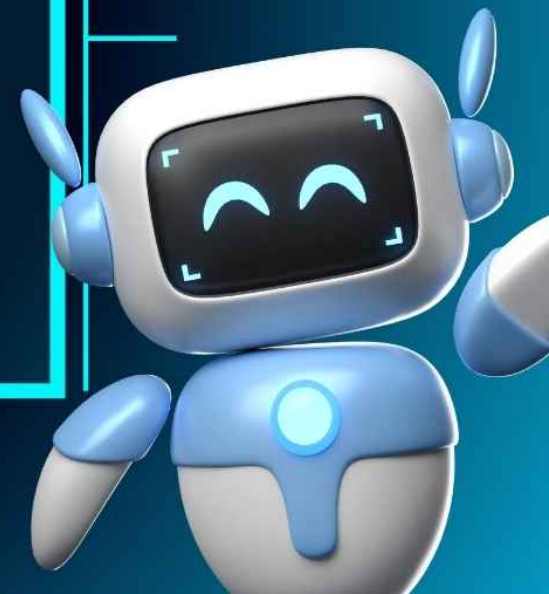
- Ejemplo: Zemana AntiLogger.
- Característica: Comparación constante con una base de datos actualizada de malware conocido.

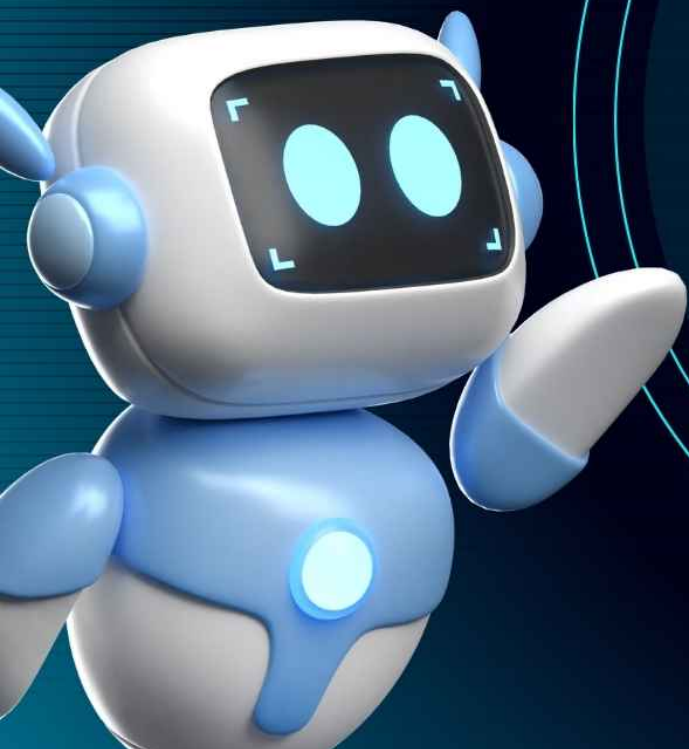
Antikeyloggers Basados en Comportamiento:

- Ejemplo: SpyShelter.
- Característica: Monitoreo continuo del sistema en busca de actividades anómalas.

Antikeyloggers de Encriptación:

- Ejemplo: Ghostpress.
- Característica: Encripta las pulsaciones del teclado para proteger la información.





PROGRAMAS

Zemana AntiLogger
SpyShelter Anti-Keylogger
Complemento para Firefox:
Keylogger Beater
Ghostpress

5

IMPORTANCIA DE UTILIZAR ANTIKEYLOGGERS

Protección de Información Personal:

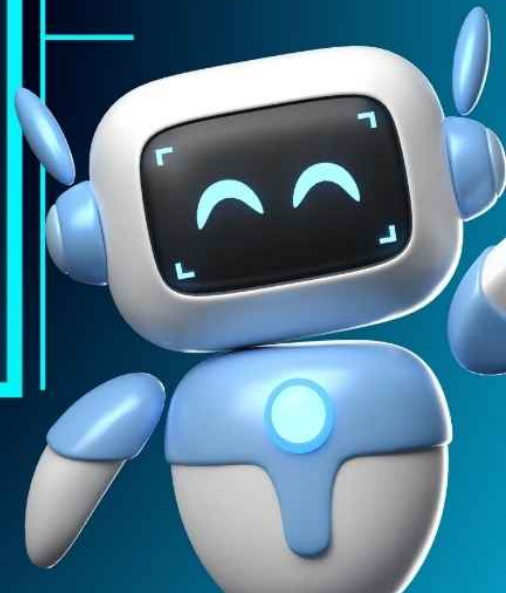
- Seguridad en cuentas bancarias, correos electrónicos y redes sociales.
- Prevención de robo de identidad.

Relevancia para Empresas:

- Protección de datos sensibles de clientes y empleados.
- Evita daños reputacionales y pérdidas financieras significativas.

Cumplimiento Normativo:

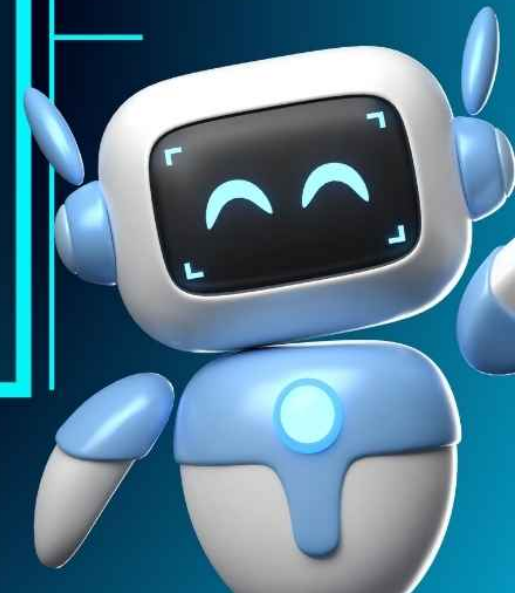
- Ayuda a cumplir con regulaciones de protección de datos como GDPR y CCPA.

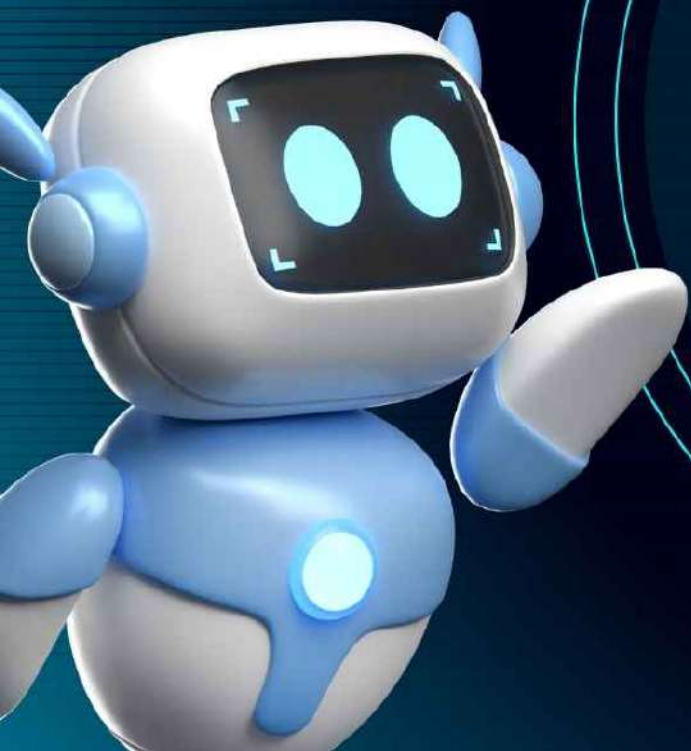


6

EJEMPLOS POPULARES DE ANTIKEYLOGGERS

- Zemana AntiLogger:
 - Detección en tiempo real.
 - Protección contra capturas de pantalla y webcam.
- SpyShelter:
 - Protección contra múltiples tipos de malware.
 - Función de encriptación de pulsaciones.
- Ghostpress:
 - Encriptación de teclas.
 - Gratuito y ligero.
- Malwarebytes Anti-Malware:
 - Ofrece protección integral contra malware, incluyendo keyloggers.
- HitmanPro.Alert:
 - Proporciona seguridad adicional contra exploits y keyloggers.





PRACTICA