EdicionProgramadores

Todos, en algún momento de nuestras vidas, hemos estado expuestos a ser infectados por algún tipo de virus informático. Y, si bien en muchas situaciones conseguimos frenar la amenaza, es importante conocer sobre el tema para estar protegidos.
Por eso hoy queremos contarte los diferentes virus informáticos a los que podés enfrentarte y sus características.

¿Qué es un virus informático?

-Un virus informático es un software malicioso (malware en inglés), que suele presentarse como un tipo de programa o código que está diseñado para instalarse y modificar el funcionamiento de un equipo. Tienen la función de autoreplicarse y seguir propagándose de un equipo a otro.

-Un virus informático, en cierta forma, se asemeja a un virus humano. Una vez que los contraemos, quedan latentes, esperando activarse en el momento menos pensado.
-Si se logran identificar sus síntomas a tiempo y se toman las precauciones necesarias, se consigue frenar su avance. Pero si no se realizan acciones para evitarlos, pueden propagarse rápidamente y causar daños.

¿Cómo actúa un virus informático?

-Una vez que el virus se encuentra alojado en un archivo, programa o documento, está latente a la espera de que se realice alguna acción. De este modo, pasan desapercibidos.

-Cuando se ejecuta su código, el virus informático puede propagarse a otros dispositivos dentro de la misma red, borrando o robando información, datos, cuentas o contraseñas.

Clasificación de los virus informáticos

Los virus informáticos se pueden clasificar en 3 tipos:[su_list icon=»icon: arrow-circle-o-right» icon_color=»#0057ff»]

Virus Residentes y No Residentes

Los virus residentes permanecen activos en la memoria, infectando archivos constantemente mientras el sistema esté encendido. Los no residentes actúan solo cuando se ejecuta el archivo infectado.

Virus Directos e Indirectos

Los virus directos atacan archivos de inmediato, mientras que los indirectos esperan ciertas condiciones para activarse.

Virus de Sobreescritura vs. No Sobreescritura

Los virus de sobreescritura borran el contenido del archivo infectado, mientras que los no sobreescriben permanecen sin alterar el archivo original.

Virus de Acción Directa

Son aquellos que actúan rápidamente en el sistema y se eliminan al apagar el equipo.[/su_list]

¿Cuáles son los distintos tipos de virus informáticos y sus características?

-Existen distintos tipos de virus informáticos. Es importante conocer algunas de sus características para poder identificarlos y evitar su propagación:

-Virus de Archivo

Este tipo de virus infecta archivos ejecutables (.exe, .com) y se activa al abrir el archivo contaminado, propagándose al sistema y a otros archivos. Generalmente, busca dañar o modificar archivos esenciales para el funcionamiento del sistema operativo.

-Gusano

A diferencia de otros virus, los gusanos no necesitan infectar un archivo; se propagan por sí solos a través de redes, especialmente cuando el sistema está conectado a internet. Estos pueden causar sobrecarga en redes, ralentizando el rendimiento o incluso dejándolas inoperantes.

-Troyano

El troyano se disfraza de software legítimo para engañar al usuario y obtener acceso al sistema. Una vez dentro, permite que el atacante controle el equipo o robe datos sensibles, siendo uno de los tipos de malware más difíciles de detectar y combatir.

-Virus de Macro

Estos virus afectan archivos de programas como Microsoft Word o Excel. Usan las macros para ejecutarse al abrir el archivo, lo que permite su propagación rápida en entornos donde se comparten documentos frecuentemente.

Virus de Sector de Arranque

Infecta el sector de arranque del disco duro, área donde se almacena la información inicial para iniciar el sistema operativo. Este tipo de virus es particularmente difícil de eliminar y puede requerir un formateo completo del disco.

-Ransomware

Este virus es conocido por secuestrar archivos o el acceso al dispositivo, solicitando un “rescate” para devolver el acceso. Es uno de los ataques más peligrosos y con mayor impacto, tanto en usuarios individuales como en empresas.

-Spyware y Adware

El spyware recopila información sin el conocimiento del usuario, mientras que el adware genera anuncios no deseados. Aunque no siempre son destructivos, estos virus invaden la privacidad del usuario y afectan la experiencia de navegación.

-Virus Polimórfico

Este tipo de virus cambia su código cada vez que infecta un archivo para evitar ser detectado por los antivirus. Su capacidad de modificación continua lo convierte en una de las amenazas más difíciles de combatir.
-Virus Multipartito
Infecta múltiples partes del sistema simultáneamente, incluyendo archivos y el sector de arranque. Esta habilidad lo hace especialmente peligroso, ya que su eliminación es compleja y puede reaparecer si no se erradica completamente.

¿Cuáles son los virus informáticos mas comunes?

-Existieron numerosos virus informáticos que se hicieron mundialmente conocidos por sus daños.[su_list icon=»icon: arrow-circle-o-right» icon_color=»#0057ff»]

-ILoveYou: creado en el año 2000, circulaba un correo electrónico con el asunto “ILoveYou” con un documento adjunto que contenía un virus que se hacía pasar por un archivo .txt. Cuando se abría el correo, se enviaba a todos los contactos del usuario y se sobreescribían archivos.

-Zeus: el troyano Zeus fue detectado en el 2007, comprometió cuentas de corporaciones multinacionales y bancos como Amazon y Bank of América. Al ser un virus personalizado, era capaz de recopilar cualquier tipo de información, desde detección de teclas, hasta datos bancarios y credenciales.
-Sasser: en 2004, el gusano Sasser causó estragos en Windows XP y 2000 afectando a millones de computadoras, bloqueándolas y dificultando su arranque. [/su_list

¿Que pasa hoy en el 2025?

-El avance desde esos años hasta la fecha a sido enorme, detectando nuevas amenazas diariamente. En nuestros tiempos el robo de información de uno de los principales problemas a nivel usuario.
-Los nuevos virus son indetectables por el usuario de la pc y es una responsabilidad compleja para los programadores y el ingenio de cada uno de ellos es hacer que no se multiplique o no salga información valiosa a menos que el usuario lo haga.

Cómo Protegerse de los Virus Informáticos

-Actualización del Software: Mantén el sistema operativo y los programas actualizados para evitar vulnerabilidades.
-Evitar Descargas Sospechosas: No abras archivos ni descargues aplicaciones de fuentes no verificadas.
-No descomprimas archivos directamente en la carpeta descarga.
-No descomprima archivos en la memoria usb.

Confía en nuestra protección

-Teo Antivirus es una solución liviana y efectiva para mantener tu PC libre de amenazas.
-Ideal para usuarios que quieren seguridad sin complicaciones
-Dotado de dos motores de Inteligencia Artificial

Características destacadas:

-Análisis automático y silencioso
-Icono activo en bandeja
-Interfaz sencilla e intuitiva
-Teo ofrece una experiencia clara y rápida, para que cualquier usuario pueda proteger su equipo sin conocimientos técnicos

Protección en tiempo real

-Monitorea automáticamente las carpeta en tu pc, detectando y neutralizando amenazas en cuanto aparecen.

Lista blanca integrada

-Incluye una lista predefinida de archivos confiables para mejorar la velocidad de escaneo.
-Puedes agregar muy fácil archivos a la lista blanca, aunque no será necesario, el software no dañará archivos que no contengan virus reales, aquí no detectamos falsos positivos como otros antivirus.

Historial de escaneos

-Guarda en Documentos un registro detallado con fecha y hora de cada análisis, para que siempre tengas control de tu sistema.

Notificaciones discretas

-Te avisa de forma visual y sin interrupciones que tu equipo está protegido en todo momento.

Rapidez, velocidad y precisión

-La rapidez de escaneo en toda la pc, es realmente eficiente, y sin consumos significativos de recursos, no esperarás dos horas a que termine el proceso.

-Instalación rápida y personalizada, logrando un contacto directo con el usuario.

Análisis por comportamiento simple

-Monitorea los accesos al registro y carpetas clave.

-Detecta si el .exe crea nuevos archivos o intenta copiarse.

-Usa un pequeño watchdog por proceso que solo actúa si se cumple alguna regla de "comportamiento malicioso".

Propuesta de comportamiento:

-Cuando detecta un un archivo nuevo (por ejemplo en el Escritorio, Descargas, USB.etc)

-Lo vigila un minuto, monitoreando cada 5 segundos si hay comportamientos sospechosos.

-Si no hace nada, se considera inofensivo.

Podríamos enumerar cientos de las funciones de nuestro antivirus que el usuario normal no quiere saber, solo necesita protección en su pc, trabajar con tranquilidad sin que se le dañen programas por culpa de los antivirus convencionales.

Nuestro antivirus línea de código por línea de código se armó dentro de servidores trabajando en tiempo real, con cientos de usuarios trabajando y ejecutando diferentes programas . Logramos así avanzar en el uso de la inteligencia artificial incorporada dentro de Teo Antivirus.

En definitiva, Teo es lo que es, amigable con el usuario y letal con las amenazas.