



## Ransomware: El Peligro Oculto en Navegadores Web

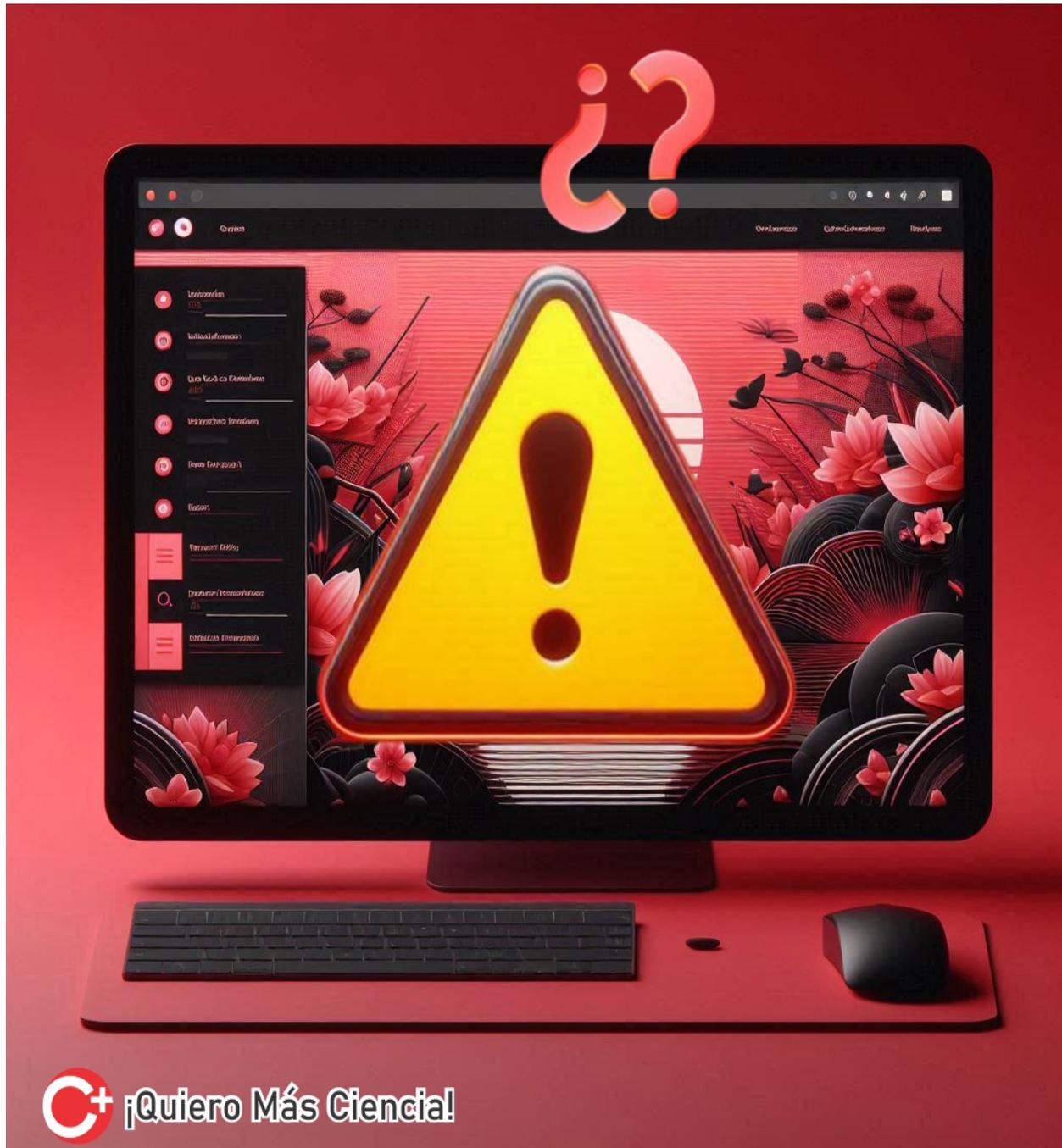
### Description

El ransomware puede bloquear el acceso a los archivos a través de los navegadores web. Los usuarios deben ser conscientes de esta amenaza emergente.

### CONTENIDOS

## Ransomware en los Navegadores Web: La Amenaza Silenciosa

Hace un tiempo, me tocó lidiar con un extorsionador que me mandó un mail diciendo que pagara a cambio de desbloquear los archivos que se encriptaron en mi computadora. Este ataque se produjo luego de que descargué un archivo desde una “plataforma segura” de drivers para mi PC. En un momento tuve la mayoría de los archivos inaccesibles para poder utilizar. A esto decidí no pagar la extorsión y tratar de rehacer muchos archivos nuevamente a medida que los fui necesitando. Allí conocí el Ransomware, y hoy se presenta como una nueva amenaza.



**Los navegadores web son ahora el nuevo campo de batalla para el ransomware. Los ciberdelincuentes están explotando sus capacidades para lanzar ataques.**

En la era digital, la seguridad cibernética se ha convertido en un campo de batalla constante. [Los navegadores web modernos](#), con su capacidad para manipular datos dentro del sistema de archivos local, han abierto una puerta trasera para los ciberdelincuentes. La interfaz de programación de aplicaciones (API) del sistema de archivos permite a las aplicaciones web interactuar con los archivos locales del usuario, creando una nueva oportunidad para el ransomware. [El ransomware es un tipo de malware que bloquea los datos](#) o el dispositivo de una víctima y amenaza para mantenerlo bloqueado. Según el IBM Security X-Force Threat Intelligence Index 2023, los ataques de ransomware representaron el 17 por ciento de todos los ciberataques en 2022.

---

## El Poder Oculto de los Navegadores Web con Ransomware

Los navegadores de hoy no son solo herramientas para acceder a internet; son casi sistemas operativos en sí mismos. Con la habilidad de ejecutar programas y cifrar archivos, los navegadores pueden ser armados por hackers para lanzar ataques de ransomware directamente desde la web, sin necesidad de descargar archivos maliciosos. Si utiliza navegadores y aplicaciones obsoletos, es especialmente vulnerable a esta técnica. Es posible que los ataques de ransomware no se desencadenen inmediatamente.

Te Puede Interesar:

### El Experimento RAB

Un equipo de investigadores ha demostrado la facilidad con la que se puede diseñar y ejecutar un ransomware basado en navegador. El ransomware RAB, creado por ellos, muestra cómo los ciberatacantes pueden cifrar archivos directamente a través del navegador, evadiendo los sistemas tradicionales de detección de antivirus. Usando la API del sistema de archivos y la tecnología WebAssembly, demostramos este nuevo ransomware basado en navegador llamado RAB como una aplicación web maliciosa que cifra los archivos del usuario desde el navegador.

### Un Nuevo Tipo de Ransomware en Navegadores Web

El ransomware basado en navegador es una cepa emergente de malware. A diferencia del ransomware tradicional, que requiere que el usuario descargue un archivo malicioso, [este nuevo tipo opera dentro del navegador](#) y puede cifrar archivos sin ser detectado por programas antivirus convencionales. Este tipo de ransomware [es especialmente peligroso](#) porque puede extenderse rápidamente a través de una red y moverse entre diferentes organizaciones. Los ciberdelincuentes utilizan la encriptación para hacer que los archivos sean inaccesibles, y solo proporcionan la clave de descryptación si la víctima paga el rescate.



Uno de los enfoques de defensa implica informar a los usuarios sobre los riesgos asociados con permitir que las aplicaciones web accedan al sistema de archivos de su computadora. Un diálogo de permisos mejorado podría ser clave para prevenir ataques de ransomware basados en navegador.

## Protegiendo Nuestros Archivos

La investigación propone tres enfoques de defensa para mitigar este nuevo tipo de ransomware. Estos enfoques operan a diferentes niveles: navegador, sistema de archivos y usuario, y se complementan entre sí para ofrecer una protección más robusta. Las estrategias de prevención incluyen el escaneo de todos los archivos y del tráfico de red en busca de malware, filtrado de consultas de DNS, uso de aislamiento de navegador para prevenir los ataques,

---

y formar a los usuarios sobre las mejores prácticas de seguridad relacionadas con la información.

## La Importancia de la Conciencia del Usuario

Uno de los enfoques de defensa implica informar a los usuarios sobre los riesgos asociados con permitir que las aplicaciones web accedan al sistema de archivos de su computadora. Un diálogo de permisos mejorado podría ser clave para prevenir ataques de ransomware basados en navegador. La concienciación en ciberseguridad es una actividad que tiene como objetivo [educar a los usuarios técnicos y no técnicos sobre las amenazas](#) y riesgos que existen y a los que se exponen diariamente al compartir información a través de un dispositivo. La concienciación en ciberseguridad es esencial para mantener la seguridad de la información y prevenir ataques de ransomware.

## El Costo del Ransomware

El ransomware es un problema creciente, con ataques que afectan tanto a individuos como a organizaciones. [En 2023, se pagaron más de 1.1 mil millones de dólares en pagos de rescate a atacantes](#), y se produjeron 19 ataques de ransomware cada segundo. Un estudio realizado por Datto indica que en promedio un ataque de ransomware cuesta a las organizaciones más de \$84 mil dólares. Además, los [costos de recuperación](#) son de 2.03 millones de dólares, una cifra que supera la media global, la cual se ubica en 1.85 millones de dólares. Según las estimaciones de los expertos, el pago del rescate solo representa una pequeña parte, a menudo tan solo el 15%, de los costos totales asociados con el ataque de ransomware.



El ransomware es actualmente la carrera armamentista número uno entre hackers y especialistas en seguridad, En 2023, se pagaron más de 1.1 mil millones de dólares en pagos de rescate a atacantes

**Para seguir pensando**

El ransomware es actualmente la carrera armamentista número uno entre hackers y especialistas en seguridad. A medida que la IA se vuelve más avanzada, tanto los actores maliciosos como los equipos de defensa en ciberseguridad utilizarán técnicas de IA más sofisticadas en sus operaciones. Esto podrá llevar a una carrera armamentista digital en la que la IA juegue un papel crucial en ambos lados del conflicto cibernético. La carrera armamentista en el ciberespacio cobra cada vez más importancia. Ataques como el de Solarwinds o el último que ha afectado al SEPE, pone de manifiesto la importancia que tiene la ciberseguridad.