Ransomware: El Peligro Oculto en Navegadores Web

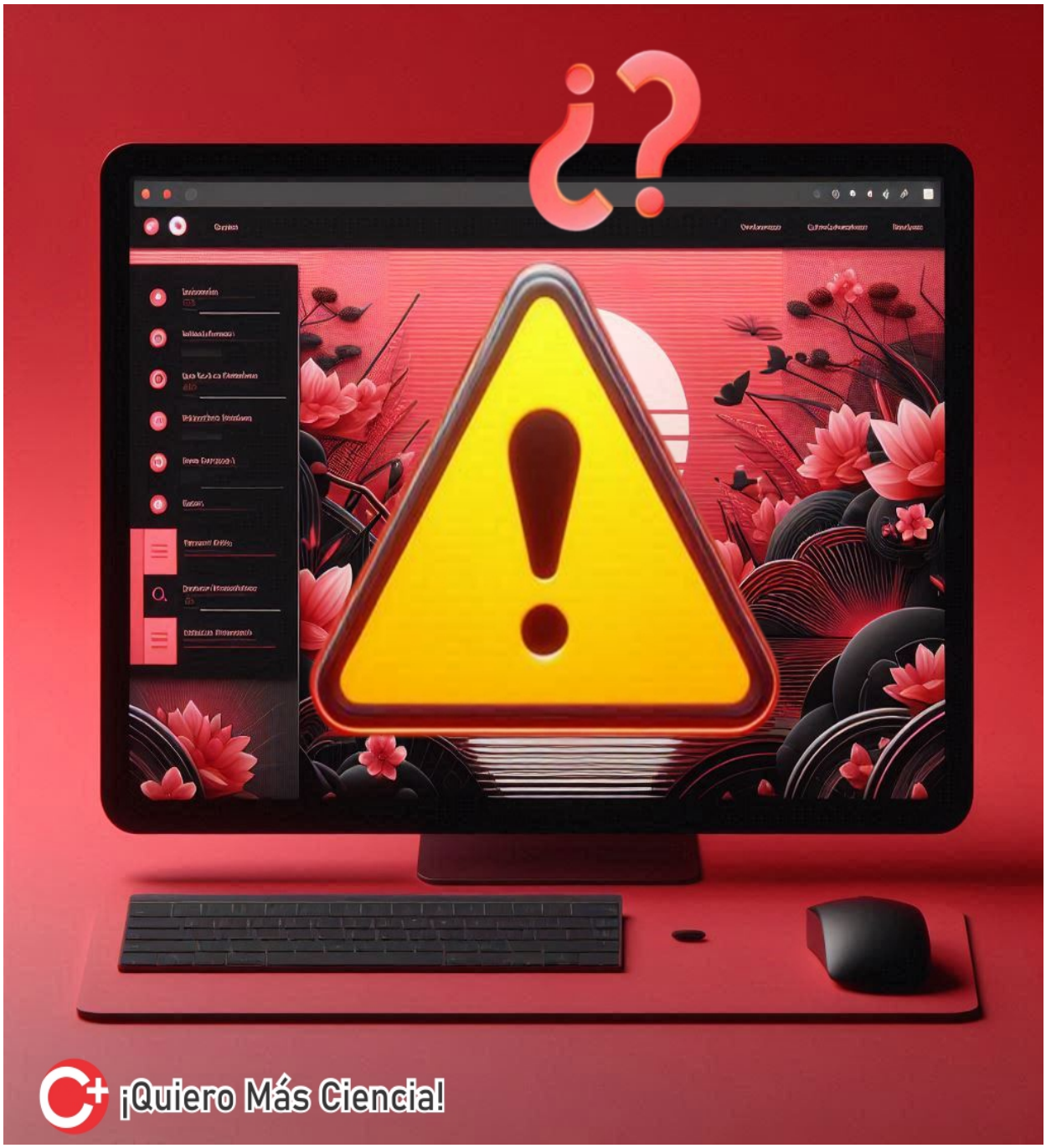
Description

El ransomware puede bloquear el acceso a los archivos a travÃ©s 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 tocÃ³ lidiar con un extorsionador que me mandÃ³ un mail diciendo que pagara a cambio de desbloquear los archivos que se encriptaron en mi computadora. Este ataque se produjo luego de que descarguÃ© un archivo desde una “plataforma segura” de drivers para mi PC. En un momento tuve la mayorÃa de los archivos inaccesibles para poder utilizar. A esto decidÃ no pagar la extorsiÃ³n y tratar de rehacer muchos archivos nuevamente a medida que los fui necesitando. AllÃ conocÃ 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 estÃ¡n explotando sus capacidades para lanzar ataques.

En la era digital, la seguridad cibernÃ©tica 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 programaciÃ³n 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 vÃctima y amenaza para mantenerlo bloqueado. SegÃºn 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 sÃ 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 tÃ©cnica. Es posible que los ataques de ransomware no se desencadenen inmediatamente.

Te Puede Interesar:

El Experimento RÃ¸B

Un equipo de investigadores ha demostrado la facilidad con la que se puede diseÃ±ar y ejecutar un ransomware basado en navegador. El ransomware RÃ¸B, creado por ellos, muestra cÃ³mo los ciberatacantes pueden cifrar archivos directamente a travÃ©s del navegador, evadiendo los sistemas tradicionales de detecciÃ³n de antivirus. Usando la API del sistema de archivos y la tecnologÃa WebAssembly, demostramos este nuevo ransomware basado en navegador llamado RÃ?B como una aplicaciÃ³n 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 rÃ¡pidamente a travÃ©s de una red y moverse entre diferentes organizaciones. Los ciberdelincuentes utilizan la encriptaciÃ³n para hacer que los archivos sean inaccesibles, y solo proporcionan la clave de desencriptaciÃ³n si la vÃctima 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 diÃ¡logo de permisos mejorado podrÃa ser clave para prevenir ataques de ransomware basados en navegador.

Protegiendo Nuestros Archivos

La investigaciÃ³n 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 sÃ para ofrecer una protecciÃ³n mÃ¡s robusta. Las estrategias de prevenciÃ³n incluyen el escaneo de todos los archivos y del trÃ¡fico de red en busca de malware, filtrado de consultas de DNS, uso de aislamiento de navegador para prevenir los ataques,

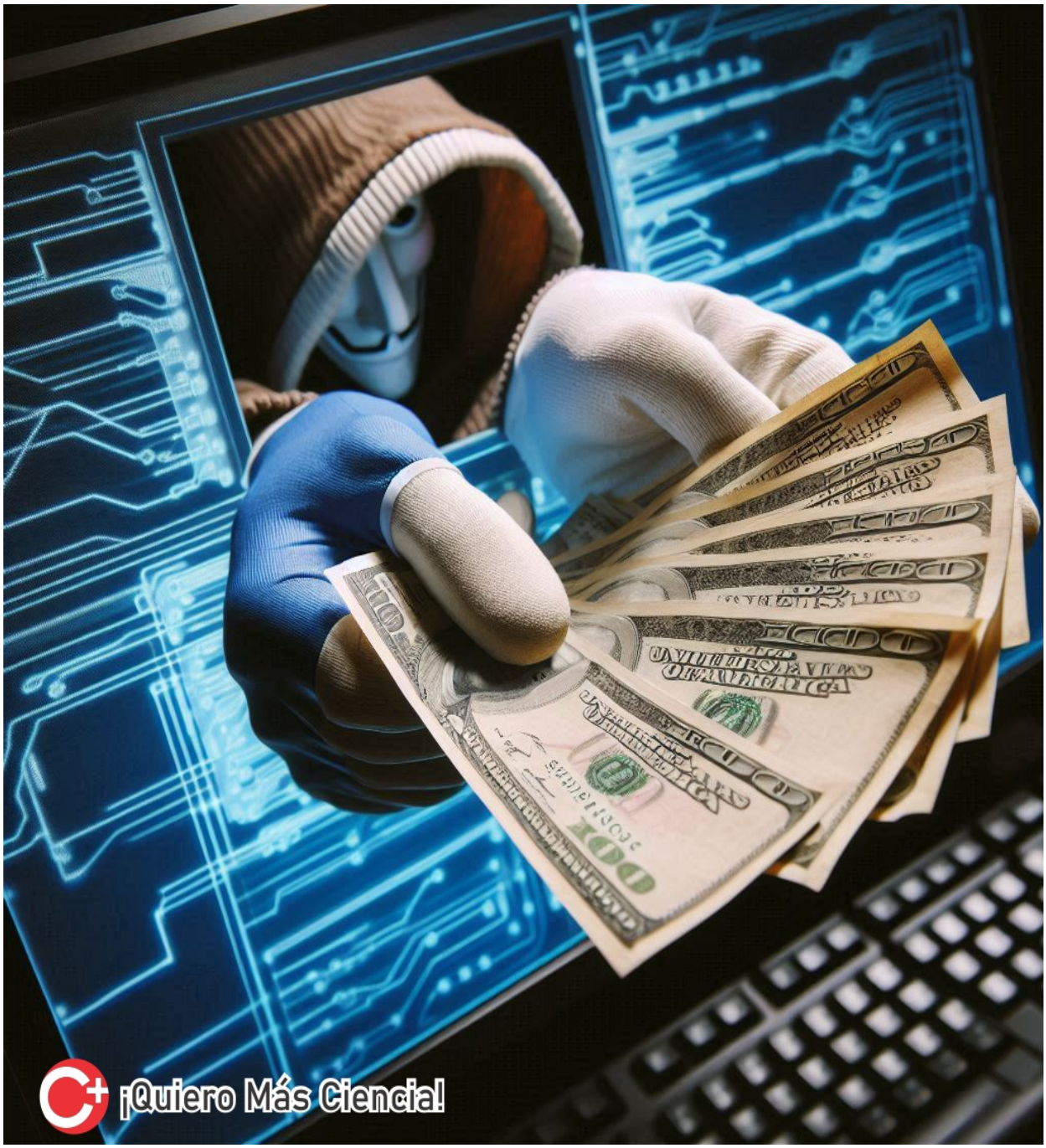
y formar a los usuarios sobre las mejores prÃ¡cticas de seguridad relacionadas con la informaciÃ³n.

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 diÃ¡logo de permisos mejorado podrÃa ser clave para prevenir ataques de ransomware basados en navegador. La concienciaciÃ³n en ciberseguridad es una actividad que tiene como objetivo educar a los usuarios tÃ©cnicos y no tÃ©cnicos sobre las amenazas y riesgos que existen y a los que se exponen diariamente al compartir informaciÃ³n a travÃ©s de un dispositivo. La concienciaciÃ³n en ciberseguridad es esencial para mantener la seguridad de la informaciÃ³n 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 mÃ¡s de 1.1 mil millones de dÃ³lares 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 mÃ¡s de $84 mil dÃ³lares. AdemÃ¡s, los costos de recuperaciÃ³n son de 2.03 millones de dÃ³lares, una cifra que supera la media global, la cual se ubica en 1.85 millones de dÃ³lares. SegÃºn las estimaciones de los expertos, el pago del rescate solo representa una pequeÃ±a parte, a menudo tan solo el 15%, de los costos totales asociados con el ataque de ransomware.



El ransomware es actualmente la carrera armamentista nÃºmero uno entre hackers y especialistas en seguridad, En 2023, se pagaron mÃ¡s de 1.1 mil millones de dÃ³lares en pagos de rescate a atacantes

Para seguir pensando

El ransomware es actualmente la carrera armamentista nÃºmero uno entre hackers y especialistas en seguridad. A medida que la IA se vuelva mÃ¡s avanzada, tanto los actores maliciosos como los equipos de defensa en ciberseguridad utilizarÃ¡n tÃ©cnicas de IA mÃ¡s sofisticadas en sus operaciones. Esto podrÃa llevar a una carrera armamentista digital en la que la IA juegue un papel crucial en ambos lados del conflicto cibernÃ©tico. La carrera armamentista en el ciberespacio cobra cada vez mÃ¡s importancia. Ataques como el de Solarwinds o el Ãºltimo que ha afectado al SEPE, pone de manifiesto la importancia que tiene la ciberseguridad.