Consejos para prevenir el Ransomware, cómo prevenirlo

Consejos para prevenir el Ransomware, cómo prevenirlo. El Ransomware es un software malintencionado utilizado por los ciberdelincuentes para cifrar datos importantes de su computadora o servidor web y extorsionarlo a cambio de recuperar el acceso a sus datos. El ransomware es un malware notorio que no solo ataca las computadoras domésticas sino también los sistemas de empresas de alto perfil, incluidas las de las industrias de educación, TI, salud y servicios financieros.

En los últimos años, el ransomware se ha convertido en un esquema lucrativo para los delincuentes cibernéticos y continúa intensificándose como un problema crónico tanto para individuos como para empresas. Con los delincuentes cibernéticos abandonando sus esquemas anteriores en favor de este software malintencionado, aprender a prevenir ataques de ransomware debería estar en la preeminencia

Nadie está a salvo del ransomware. No importa quién o dónde se encuentre y sin importar a qué industria pertenece su empresa, siempre que tenga datos guardados en su sistema que no pueda permitirse perder, no está a salvo de las atroces habilidades y las mentes de estos ciberdelincuentes.

De hecho, en 2017, los ataques de ransomware alcanzaron su punto máximo con informes de que 7 de cada 10 cargas de malware eran variantes de ransomware. Solo el 12 de mayo de ese año, más de 200,000 máquinas fueron infectadas por el malware en un curso de pocas horas. Este ataque de ransomware había infectado incluso a grandes organizaciones europeas.

Cl

Hay dos tipos de ransomware actualmente en circulación. El primero se llama el cifrado ransomware que es el más común. El cifrado de ransomware está diseñado para bloquear archivos del sistema y solicitar a la víctima el pago a cambio de la clave de acceso necesaria para desbloquear los datos cifrados. El segundo es conocido como el casillero ransomware. A pesar de que los cyberthieves (Personas que roban a otros usando una computadora) también le pedirán dinero, el ransomware de los casilleros no encripta ningún dato, sino que bloquea su sistema operativo y le prohíbe acceder a su escritorio o cualquier archivo.

Los usuarios domésticos son un objetivo principal de los creadores de ransomware debido a su falta de educación sobre la concienciación sobre seguridad cibernética. Esto hace que sean más fáciles de manipular para hacer clic en cualquier enlace malicioso que pueda infectar sus computadoras. Por otro lado, las empresas tampoco están libres de ataques de ransomware. Son mucho más rentables que los usuarios domésticos y, por lo tanto, se convierten en una víctima más ideal a los ojos de los creadores de ransomware. De hecho, todos deben ser conscientes de cómo prevenir los ataques de

ransomware de manera efectiva.
Sin embargo, al igual que otros programas maliciosos, el ransomware encuentra el camino al sistema de una víctima explotando el agujero de seguridad de un software vulnerable o engañando a una posible víctima para que lo descargue o instale. Apuesto que incluso en este momento, alguien está haciendo clic en un enlace malicioso que, después de unos momentos, descargará el ransomware en la computadora de ese usuario y cifrará todos sus datos.

Con estos datos alarmantes sobre lo peligrosos que pueden ser los ataques de ransomware, debe equiparse con un adepto para comprender cómo prevenir los ataques de ransomware. No espere hasta que llegue una amenaza y conviértase en la próxima víctima de ransomware. Infórmese acerca de este malware y aprenda los métodos a seguir para prevenir el ransomware.

Parchear y actualizar el software

Para evitar ataques de ransomware, asegúrese de que todos los sistemas y software estén actualizados. Las computadoras que se ejecutan con un software obsoleto son más propensas a un ataque. Un software actualizado puede reducir

significativamente la posibilidad de que el ransomware dañe sus datos. La mayoría de los proveedores publican regularmente actualizaciones de seguridad y parches. Sería mejor si puede habilitar las actualizaciones automáticas de su software para asegurarse de que su software siempre estará actualizado.

No haga clic en enlaces y correos electrónicos desconocidos.

Otra forma de prevenir ataques de ransomware es estar atentos a hacer clic en enlaces y correos electrónicos desconocidos. Las campañas de correo electrónico no deseado son uno de los métodos de infección más comunes que usan los atacantes. Estos correos electrónicos contienen enlaces maliciosos o archivos adjuntos que pueden descargar el ransomware a su computadora. Tenga en cuenta: siempre piense dos veces antes de hacer clic para que pueda mantener los enlaces infectados y otras fuentes maliciosas lejos de su computadora y datos importantes.

Copia de seguridad de sus archivos

Por último, pero definitivamente no menos importante, asegúrese de realizar copias de seguridad de sus archivos (especialmente los más importantes). Hacer copias de seguridad de sus archivos regularmente es su mejor remedio cuando el ransomware ha infectado su computadora. Almacene una copia de sus datos en la nube (Google Drive, Dropbox) o en un disco duro portátil. Es posible que este método no mantenga alejados los ataques de ransomware de su computadora, pero

definitivamente hará que el daño sea mucho menor, ya que no necesita lidiar más con el atacante para recuperar el acceso a su contenido cifrado.

Siendo uno de los programas maliciosos más peligrosos y más difundidos en el planeta, el ransomware sin lugar a dudas llevó la extorsión a una escala global. Con esta amenaza de malware, debe tomar precauciones extensas sobre cómo prevenir los ataques de ransomware para evitar la pérdida de datos y cualquier infección relacionada con el malware. Incluso puede intentar buscar un software de escaneo confiable que pueda identificar archivos desconocidos y malintencionados en su red, lo que puede ayudarlo a avanzar en la prevención de ataques de ransomware. Nunca permita que un archivo malicioso continúe residiendo en su computadora para evitar que los ataques de ransomware lo golpeen y obstruya el trato con los ciberthieves que pueden hacer que pierda mucho dinero.

Enconclusión

El software malintencionado que utiliza el cifrado para retener los datos para obtener un rescate se ha convertido en un gran éxito en los últimos años. El propósito de este

software es extorsionar el dinero de las víctimas con la promesa de restaurar los datos cifrados. Al igual que otros virus informáticos, por lo general encuentra su camino en un dispositivo explotando un agujero de seguridad en software vulnerable o engañando a alguien para que lo instale.
El ransomware, como se le conoce, califica a víctimas de alto perfil como hospitales, escuelas públicas y departamentos de policía. Ahora ha encontrado su camino en las computadoras del hogar y servidores web, entre otros destinos.
El infame modelo de negocio de ransomware se ha convertido en una industria lucrativa para los delincuentes. A lo largo de los años, su mala reputación ha hecho que la policía se asocie con agencias internacionales para identificar y derribar a los operadores de estafa.

La mayoría de los ataques de ransomware que han tenido lugar en el pasado se han relacionado con malas prácticas de protección por parte de los empleados.

Hay algunas cosas que se deben y no se deben hacer cuando se trata de ransomware.

- No pague el rescate. Sólo alienta y financia a estos atacantes. Incluso si se paga el rescate, no hay garantía de que pueda recuperar el acceso a sus archivos.
- Restaurar los archivos afectados de una buena copia de seguridad conocida. La restauración de sus archivos desde una copia de seguridad es la forma más rápida de recuperar el acceso a sus datos.
- No proporcione información personal al responder un correo electrónico, una llamada telefónica no solicitada, un mensaje de texto o un mensaje instantáneo. Los phishers intentarán engañar a los empleados para que instalen malware o adquirir inteligencia para los ataques afirmando que son de TI. Asegúrese de comunicarse con su departamento de TI si usted o sus compañeros de trabajo reciben llamadas

sospechosas.

- Utilice un software antivirus de buena reputación y un firewall. Es fundamental mantener un firewall sólido y mantener actualizado su software de seguridad. Es importante usar el software antivirus de una empresa de renombre debido a todo el software falso que existe.
- Emplee análisis de contenido y filtrado en sus servidores de correo. Los correos electrónicos entrantes deben analizarse en busca de amenazas conocidas y deben bloquear cualquier tipo de archivo adjunto que pueda representar una amenaza.
- Asegúrese de que todos los sistemas y software estén actualizados con los parches relevantes.
- Los kits de explotación alojados en sitios web comprometidos se utilizan comúnmente para propagar malware. Es necesario parchear regularmente el software vulnerable para ayudar a prevenir la infección.
- Si viaja, avise de antemano a su departamento de TI, especialmente si va a utilizar Internet inalámbrico público. Asegúrese de usar una Red privada virtual (VPN) confiable cuando acceda a una red Wi-Fi pública.

Los delincuentes de ransomware a menudo atacan a las pequeñas y medianas empresas. Entre otros ataques cibernéticos, el ransomware es una actividad delictiva que puede solucionarse fácilmente con las soluciones mencionadas anteriormente.

Leer también: ¿Ransomware puede afectar a servidores web Linux?; Ransomware, mejores prácticas para prevenir daños irrecuperables; Ransomware en Windows server, características y patrones de ataque, qué hacer