**Spanish**

**¿Qué es el *cryptojacking*? ¿Cómo evitarlo?**

El *cryptojacking* o el hackeo para criptominería se ha convertido en una de las principales amenazas cibernéticas en el mundo. Para comenzar, las criptomonedas, también conocidas como criptodivisas, son una forma de dinero digital, que no tiene ningún respaldo físico. Se llaman ‘cripto’ porque utilizan principios de cifrado matemático complejo (es dinero ‘encriptado’). No hay bancos físicos que manejen el dinero, y los usuarios gestionan sus propias cuentas de manera anónima (la información de los usuarios también está encriptada).

El Blockchain es una tecnología que funciona como una base de datos distribuida y segura. El cifrado protege todos los datos que se guardan en blockchain (también llamada cadena de bloques). Un bloque es un conjunto de transacciones que se guardan sin la intervención de personas. Los mineros reciben las solicitudes para validar si las transacciones guardadas en un bloque son correctas. Este proceso se hace sin intervención humana, pues el sistema envía una serie de cálculos matemáticos complejos a varios equipos de cómputo.

Una vez completen esta tarea y validan las transacciones del bloque, como recompensa reciben criptomonedas. A esta tarea se le llama minería de criptomonedas. Para obtener más criptomonedas, se requieren más computadoras conectadas la mayor cantidad de tiempo posible solucionando cálculos.

***Criptojacking:* así funciona**

El *criptojacking* podría traducirse como una forma de minería de criptomonedas ilegal, que secuestra el poder de procesamiento de las computadoras, para ponerlas a resolver cálculos matemáticos y recibir criptomonedas.

El software malicioso puede ingresar bien sea a través de una descarga o al visitar una página web. Una vez instalado, el software usa nombres de procesos legítimos de Windows para pasar desapercibido y ocupar el rendimiento de la CPU en labores de minería de criptodivisas.

La popularidad del bitcoin en México, ha llegado a 1 millón de cuentas que operaban este tipo de activos en el país. Esta tendencia se ve reflejada en la [encuesta global de consumo,](https://es.statista.com/grafico/18425/adopcion-de-las-criptomonedas-en-el-mundo/) elaborada por Statista, posicionando a México con un 9% de la población adoptando la moneda. Gracias a ello se han vuelto un blanco fácil para los ciberataques, formando parte del 24% de incremento en comparación con 2021 para América Latina, según datos de Kaspersky.

El malware de criptomonedas funciona como un parásito que pone la potencia de las computadoras al servicio de la minería de criptodivisas. Esto puede generar interrupciones en los servicios, afectar el rendimiento de los dispositivos y reducir drásticamente su vida útil.

Puede incluso, dejar puertas abiertas para ataques de ransomware, pues una vez se ha vulnerado el sistema, será más fácil para otras amenazas tomar el control del dispositivo y de la información que guarda.

**Pero ¿Cómo saber si soy víctima de *cryptojacking*? ManageEngine te aconseja cómo evitarlo.**

Constantes fallos en el sistema, aumento en el consumo de energía, interrupciones o degradaciones de los servicios y bajo rendimiento de red, son algunos de los ‘síntomas’ de un ataque de esta clase.

Para evitar ser víctima del *cryptojacking* es esencial implementar las buenas prácticas mínimas de ciberseguridad: mantener el software actualizado, usar contraseñas complejas, no descargar archivos de correos o sitios web sospechosos y controlar las políticas de privilegios del sistema.

Además, también se recomienda desinstalar el software que no se usa (puede estar corriendo malware en segundo plano), aplicar listas blancas y negras de aplicaciones (para controlar lo que se instala en los equipos) y monitorear la actividad del CPU (para detectar anomalías).

---------

**Acerca de ManageEngine**

ManageEngine es la división de gestión de TI empresarial de Zoho Corporation. Las empresas establecidas y emergentes, incluidas 9 de cada 10 organizaciones Fortune 100, confían en nuestras herramientas de administración de TI en tiempo real para garantizar un rendimiento óptimo de su infraestructura de TI, incluidas redes, servidores, aplicaciones, desktops y más. Tenemos oficinas en todo el mundo, incluidos los Estados Unidos, los Países Bajos, India, Singapur, Japón, China y Australia, así como una red de más de 200 Partners globales para ayudar a las organizaciones a alinear estrechamente sus negocios y TI.

Para obtener más información, visite [www.manageengine.com](http://www.manageengine.com/); siga el blog de la compañía en [blogs.manageengine.com](http://blogs.manageengine.com/) y en LinkedIn en [www.linkedin.com/company/manag...](http://www.linkedin.com/company/manageengine), Facebook en [www.facebook.com/ManageEngine](http://www.facebook.com/ManageEngine) y Twitter [@ManageEngine](https://twitter.com/ManageEngineLA?lang=en).

**Contacto de prensa:**

Lenin Zamudio | PR Expert Manager, another

lenin.zamudio@another.co

55 2857 7150

Ernesto Nicolas | JR Executive PR, another

ernesto.nicolas@another.co

5578967193