Cryptojacking: ¿qué tan vulnerables son las criptomonedas?

CIUDAD DE MÉXICO. 27 de marzo de 2023.- Las criptomonedas son activos digitales que desde hace algunos años dejaron de ser vistos como las divisas del futuro. Por el contrario, en la actualidad su popularidad crece día con día al grado que **12 millones de mexicanos son poseedores de este tipo de monedas**, siendo *Bitcoin* la más popular con 21%, según Finder.

Este tipo de divisas digitales conforman un ecosistema sumamente variado de opciones más allá del *Bitcoin*, en donde el *Ethereum*, el *Dogecoin*, y el *Cardano* figuran entre las más utilizadas. Además de que se trata de divisas que definen su valor en la demanda y con base en algoritmos criptográficos, todas ellas coinciden en algo: también son vulnerables al cibercrimen.

Los robos de alto perfil en diversas plataformas de criptomonedas como las billeteras digitales en las que se alojan, han hecho que se desconfíe a la hora de pensar en la posibilidad de colocar su dinero en este mercado.

Cuando emergió blockchain se pensaba que era algo 100% seguro e impenetrable, pero con el tiempo se fue evidenciando que el tipo de tecnología que se aplica en esta cadena es solo una parte de la ecuación, siendo también de igual relevancia el cómo se la implementa. Por ello, la misma no ha sido esquiva a hackeos. Solamente en 2022 se perdieron más de USD $1.6 mil millones en robos de criptomonedas a nivel global.

Es por eso que este tipo de divisas que forman parte de las finanzas Descentralizadas (DeFi) atraviesan por un momento sombrío gracias a que el *cryptojacking*, o la práctica de 'secuestrar' o intervenir un dispositivo para el minado de divisas digitales, ha socavado la confianza del sector y llevado a bancarrota a diversos entes.

- ¿Cómo se ejecuta el cryptojacking?

Principalmente los cibercriminales que se enfocan en este sector utilizan tácticas como el hackeo de billeteras digitales, utilizando como puntos débiles las claves privadas de acceso a dichos métodos de almacenamiento.

Los *hackers* maliciosos también buscan vulnerar los intercambios de divisas. Debido a que en dichos procesos se comparten claves de acceso y 'llaves' de seguridad de la cadena de bloques en la que se aloja la moneda, los criminales están atentos a dichos intercambios para obtener esas claves y hacerse de su posesión.

Otro de los métodos que no es exclusivo de este tipo de ataques, sino que es común en todo tipo de amenazas cibernéticas, es la suplantación de identidad. Mediante el uso de sitios web apócrifos los criminales engañan a las personas para hacerles creer que tratan con negociantes genuinos, en un intercambio de criptodivisas convencional.

Mediante el uso de correos apócrifos y estrategias de *phishing* pueden solicitar la confirmación de la operación, redirigiendo a los usuarios a plataformas falsas en donde se les piden sus datos de autenticación, para luego ser robados.

Finalmente, debemos destacar a las infecciones de *malware* como una técnica estándar de la piratería de criptodivisas. Los atacantes inyectan secuencias de comandos cruzadas en las páginas web para que cuando los usuarios legítimos ingresen, sean redirigidos a sitios maliciosos que que se hacen pasar por benignos. Ahí, el usuario descarga sin saberlo archivos con *malware* que una vez instalados en el dispositivo, permiten el acceso a datos del usuario.

Por ello es importante, primero, concientizar a todos aquellos interesados en transaccionar con *Bitcoin*, o cualquier criptodivisa, sobre la alta volatilidad y el riesgo que implican estos activos. Además, es importante saber que los piratas informáticos están altamente interesados en este tipo de monedas debido a la ausencia de supervisión centralizada, es decir, que no interviene ningún ente gubernamental.

Las empresas que decidan admitir estas monedas digitales deben hacer uso de métodos de seguridad periódicos como el *pentesting*, entre otras técnicas de *hacking* ético, que permitan que un experto en ciberamenazas con conocimientos en diversos ámbitos, como el *crypto*, se inmiscuya en su sistema y encuentre potenciales vulnerabilidades que los ciberdelincuentes podrían aprovechar, en caso de llegar primero que el equipo de ciberseguridad.

Sobre Strike

Strike es la plataforma de ciberseguridad en Latinoamérica. Su principal misión es ayudar a que las compañías estén protegidas a través de la detección y resolución de vulnerabilidades en sus sistemas. Esto se realiza a través de tests de penetración - o pentests - llevados a cabo por su red global de hackers éticos, conocidos como “Strikers”, una comunidad global que reúne a los mejores expertos de ciberseguridad con reconocimientos y certificaciones internacionales. Su objetivo es impulsar una cultura de ciberseguridad de calidad y accesible, en la que la misma sea parte del ciclo de vida de las empresas y no algo estanco o independiente. Más información en: https://strike.sh/

Síguenos en nuestras redes sociales:
Instagram - @strikesecurity
Twitter - @strike_secure
LinkedIn - Strike

Contacto para prensa México
another
Ahtziri Rangel | PR Expert
+ 52 1 55 1395 6970
ahtziri.rangel@another.co