Monedas digitales y ciberdelito, ¿una explosiva combinación?

Elaborado por: Samuel Ardila, Socio de Asesoría en Riesgos en Deloitte Spanish Latin America

Desde su entrada al mundo digital en la anterior década, las criptomonedas han generado interés y han captado la atención de entidades financieras, gobiernos, medios y del público en general, siendo *bitcoin* la más popular y reconocida de estas.

Las criptomonedas son consideradas bienes digitales que, 1) operan de forma **independiente** del sistema financiero tradicional, 2) utilizan redes **descentralizadas** basadas en la tecnología de cadena de bloques (más conocida como "*blockchain"*) y 3) centran su seguridad en técnicas de **criptografía** (de ahí el prefijo "cripto") y las características propias de la tecnología de cadena de bloques.

Su promesa de valor se fundamenta en la posibilidad de realizar transacciones sin intermediarios, lo cual conlleva a un menor costo y una mayor agilidad en su ejecución. Estas características impulsan la realización de miles de transacciones por montos multimillonarios a través de este medio de intercambio. Además, dado que se trata de dinero virtual, cuyo precio varía constantemente, las criptomonedas presentan grandes oportunidades de negocios e inversión, ya que funcionan como una divisa digital.

Muchas compañías aceptan actualmente las criptomonedas como medio de pago, entre ellas se encuentran algunas de gran reconocimiento. Asimismo, grandes fondos han invertido en estas divisas digitales.

Sin embargo, tal como ocurre con algunas invenciones humanas creadas con buenos propósitos, las criptomonedas también se utilizan para propósitos maliciosos o criminales. Las billeteras digitales utilizadas por los usuarios de las criptomonedas no permiten la identificación de su dueño, ya que esta información está protegida con una llave de cifrado. Dicha condición, y la operación en un ambiente no regulado, han convertido a las criptomonedas en el medio preferido por los maleantes para ocultar sus ganancias de origen ilícito, lo que facilita el lavado de activos. Igualmente, este medio es utilizado internamente entre las organizaciones criminales para pagar servicios prestados y suministros, tales como armamento o drogas.

Aunque se han llegado a conocer casos de extorsión y secuestro tradicional para los que se han usado criptodivisas como medio de pago, la práctica criminal en la que es más común el uso de criptomonedas es la ciberdelincuencia, siendo el caso más notable el secuestro digital de datos, comúnmente conocido como *ransomware*.

El *ransomware* es una de las variedades de *malware* (*software* malicioso) desarrollado por los maleantes para hacer inaccesibles los recursos informáticos "secuestrados" a sus propietarios hasta que paguen un rescate (en inglés "*ransom*"). Estos ataques no son nuevos en el ambiente tecnológico y de negocios, convivimos con ellos especialmente desde que *Cryptolocker* y *Wannacry* se extendieron en la anterior década. Ahora, el secuestro de datos ha captado la atención y la preocupación del mundo empresarial dado que se ha convertido en una plaga mundial. Estos son algunos datos que así lo confirman:

- De 2019 a 2020, el *ransomware* dirigido (utilizado para extorsionar a objetivos de alto perfil, tales como corporaciones, agencias gubernamentales y organizaciones municipales) aumentó en un 767%.[1]
- El pago promedio de rescate de un *ransomware* aumentó un 82% desde 2020 llegando a un valor récord de $570,000 en la primera mitad de 2021.[2]
- El costo total promedio de recuperación de un ataque de *ransomware* se ha más que duplicado en un año, aumentando de $761,106 en 2020 a $1.85 millones en 2021.[3]

¿Qué ha contribuido a este disparado crecimiento del *ransomware*?

Desde que se creó el *ransomware* la forma de pagar el secuestro de datos evolucionó. En el pasado, los ciberatacantes intentaron usar sistemas de pago en línea para cobrar el rescate, pero debido a que estos sistemas estaban vinculados a una cuenta bancaria, los investigadores podían identificar a los delincuentes. Con el nacimiento de la criptomoneda, este problema fue resuelto.

A través del uso de criptomonedas, los ciberdelincuentes pueden ocultar sus verdaderas identidades cuando piden un rescate en monedas digitales. Adicionalmente, los *hackers* pueden fácilmente lavar el dinero obtenido en criptomonedas en la red oscura, la porción de internet a la que solo se puede acceder mediante un *software* especializado, la cual, al igual que las monedas virtuales, también está basada en el anonimato de los usuarios.

Por otro lado, un par de características adicionales que promueven el uso de criptomonedas por parte de los ciberatacantes, son que las transacciones en criptomonedas ocurren al instante y que estas no dependen de la aplicación de tasas de cambio entre divisas que en ocasiones traen problemas en la ejecución de transacciones financieras.

En conclusión, cada vez más empresas e instituciones financieras relevantes han comenzado a reconocer las monedas digitales. Su extensión de uso alrededor del mundo seguirá facilitando la consolidación del ciberdelito como una amenaza real para los negocios. El robo y tráfico de datos y, sobre todo, el *ransomware* continuarán siendo muy atractivos para los cibercriminales. Por lo anterior, es muy importante que toda compañía identifique su perfil de riesgo cibernético y evalué sus capacidades para gestionar las ciberamenazas y, en especial, el *ransomware*.

---

[1] Fuente: https://www.kaspersky.com/about/press-releases/2021_the-era-of-targeted-ransomware-attacks-on-high-profile-victims-grows-nearly-eightfold-from-2019-to-2020

[2] Fuente: https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/

[3] Fuente: https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.aspx