La red Ethereum fue objetivo de un ataque coordinado, según confirmaron distintos analistas. Después de los informes de que algunos nodos de Parity Ethereum perdieron la sincronización con la red, el 31 de diciembre, la compañía de infraestructura central de blockchain, Parity Technology, dijo que posiblemente se trata de un ataque en curso, por lo que lanzó actualizaciones de red para protegerse.

Según Sergio Demian Lerner, consultor de seguridad de criptomonedas, el ataque se implementó de una forma simple, en la que *«se envía a un nodo Parity un bloque con transacciones no válidas, pero un encabezado válido (tomado de otro bloque). El nodo marcará el encabezado del bloque como no válido y prohibirá este encabezado del bloque para siempre, pero el encabezado sigue siendo válido».*

El desarrollador de software Liam Aharon, analizó el ataque y concluyó que estaba cerca de destruir toda la red y que Ethereum podría volverse mucho más vulnerable a ataques similares el siguiente año.

Según Aharon, el ataque no logró derribar toda la red porque tiene un cliente llamado Geth, que es inmune al ataque. Sin embargo, teniendo en cuenta la intención de Parity de hacer una transacción de Parity Ethereum a un modelo de propiedad y mantenimiento de DAO, Geth podría convertirse en el único cliente bien mantenido en 2020.

> *«Si este escenario se hiciera realidad, ataques similares a los de hoy devastarían la red, en lugar de ser simplemente inconvenientes»,* dijo Aharon.

Durante el año pasado, *Parity lanzó múltiples actualizaciones destinadas a corregir la vulnerabilidad de los nodos.* En marzo, el CEO de Parity, Jutta Steiner, dijo que la nueva y controvertida función Create2 Ethereum, habría evitado la congelación multigrado de Parity, luego de un incidente cuando un usuario «*mató accidentalmente*» la biblioteca multigrado de Parity cuando activó una vulnerabilidad para convertirse en el propietario de la biblioteca.

En mayo, el colectivo global de investigación de piratería SRLabs, afirmó que solo dos tercios

del software del cliente Ethereum que se ejecutaba en los nodos Ethereum fueron reparados contra una falla de seguridad crítica descubierta a inicios de 2019.

Según los informes, los datos indicaron que los nodos de paridad sin parches comprendían el 15% de todos los nodos escaneados, lo que implica que el 15% de todos los nodos de Ethereum eran vulnerables a un posible ataque del 51%.

Por otro lado, el 29 de diciembre, los titulares de IOTA no pudieron confirmar las transacciones durante 24 horas debido a un incidente en la red principal causado por un conjunto inusual de transacciones que pueden haberse construido como un ataque.

La fundación IOTA enfatizó que el incidente no fue causado por cambios en el software ni por ningún otro componente de la red, sino que se produjo debido a la *«ausencia de lógica de procesamiento de transacciones para un conjunto inusual de transacciones».*

A comienzos de diciembre, el principal proveedor de servicios de pago con criptomonedas BitPay, confirmó que su servicio tenía una interrupción temporal de los pagos de Bitcoin.