UABDIVULGA
BARCELONA RECERCA I INNOVACIÓ

29/09/2022

Ataques de denegación de servicio en canales de pago sobre Bitcoin

La Lightning Network (LN) es una red de pago que puede operar sobre Bitcoin y que podría potencialmente procesar infinidad de pagos de forma simultánea. Pero es vulnerable. Investigadores de la UAB han detectado que es posible llevar a cabo un ataque que bloquea los canales de pago.

istock/your_photo

La Lightning Network (LN) es una red de pago que puede operar sobre Bitcoin, y se concibió para poder superar la limitación de escalabilidad de Bitcoin. Mientras Bitcoin solo puede procesar unas 7 transacciones (pagos) por segundo, LN podría potencialmente procesar infinidad de pagos de forma simultánea.

La red LN está compuesta por nodos que suelen operar también como nodos Bitcoin. Dos nodos puede establecer un canal de pago entre ellos con un balance inicial sobre el que los nodos puede intercambiarse pagos. La parte relevante es que la mayoría de transacciones que comportan el funcionamiento del canal pueden efectuarse entre los dos nodos sin que la red Bitcoin tenga que procesarlas. Esto permite efectuar estas transacciones de manera muy rápida.

Una de las grandes ventajas de LN es que permite ejecutar pagos *multihop*. Si existe un canal de pago entre A y B, y otro entre B y C, A puede hacer un pago a C sin necesidad de que exista un canal directo entre los dos. A realiza un pago a B y B repercute dicho pago a C. Es decir, se hace un pago en cadena donde los nodos intermedios reciben una pequeña comisión para incentivar su colaboración.

Para permitir pagos *multihop*, el nodo inicial tiene que poder determinar un camino (o cadena) de canales de pagos hasta el destinatario. Esto comporta que la existencia de un canal de pago entre dos nodos deba ser pública. Por otra parte, y para mantener los pagos anónimos, el balance de los canales es privado. Cualquiera puede conocer que existe un canal entre A y B, pero no podemos saber su balance ni cómo éste evoluciona en el tiempo. Es decir, no podemos saber qué pagos se efectúan entre A y B.

En este artículo presentamos un ataque que permite bloquear canales de pago entre nodos en LN. Dicho ataque, al que denominamos *lockdown*, realiza una denegación de servicio a canales de pago e inhabilita la posibilidad de un nodo de actuar como intermediario en pagos *multihop*. Para ello se explota el hecho de que al hacer un intento de pago *multihop*, el balance de los nodos participantes queda bloqueado de manera temporal. El ataque permite aislar a una víctima de la red LN de manera que ningún nodo pueda utilizar sus canales de pago durante un periodo de tiempo razonable y con un bajo coste económico.

Aunque se proponen también algunas posibles contramedidas, éstas son difíciles de aplicar sin que ello afecte al funcionamiento de LN de forma importante. La principal contramedida es hacer que dicho ataque no resulte rentable en términos económicos. Esto se podría conseguir introduciendo limitaciones en el tipo de caminos de canales de pago que se pueden utilizar en la LN. Antes de publicar el artículo se notificó el ataque a los desarrolladores de la LN, y aunque actualmente no podemos asegurar que el problema esté totalmente solucionado, sí que se está trabajando en posibles soluciones o maneras de mitigarlo.

Guillermo Navarro-Arribas i Jordi Herrera-Joancomartí
CYBERCAT
Departamento de Ingeniería de la Información y de las Comunicaciones
Universitat Autònoma de Barcelona

Cristina Pérez-Solà
CYBERCAT
Universitat Oberta de Catalunya

Alejandro Ranchal-Pedrosa
University of Sydney

Joaquin Garcia-Alfaro
Institut Polytechnique de Paris, Telecom SudParis

Referencias

Pérez-Solà, C., Ranchal-Pedrosa, A., Herrera-Joancomartí, J., Navarro-Arribas, G., Garcia-Alfaro, J. (2020). **LockDown: Balance Availability Attack Against Lightning Network Channels**. In: Bonneau, J., Heninger, N. (eds) *Financial Cryptography and Data Security. FC 2020. Lecture Notes in Computer Science*, vol 12059. Springer, Cham. https://doi.org/10.1007/978-3-030-51280-4_14

View low-bandwidth version