Investigadores en ciberseguridad han descrito dos métodos innovadores que pueden utilizarse para interrumpir las botnets dedicadas a la minería de criptomonedas.

Según un nuevo informe publicado hoy por Akamai, estos métodos aprovechan el diseño de diversas arquitecturas comunes de minería para detener el proceso de minado.

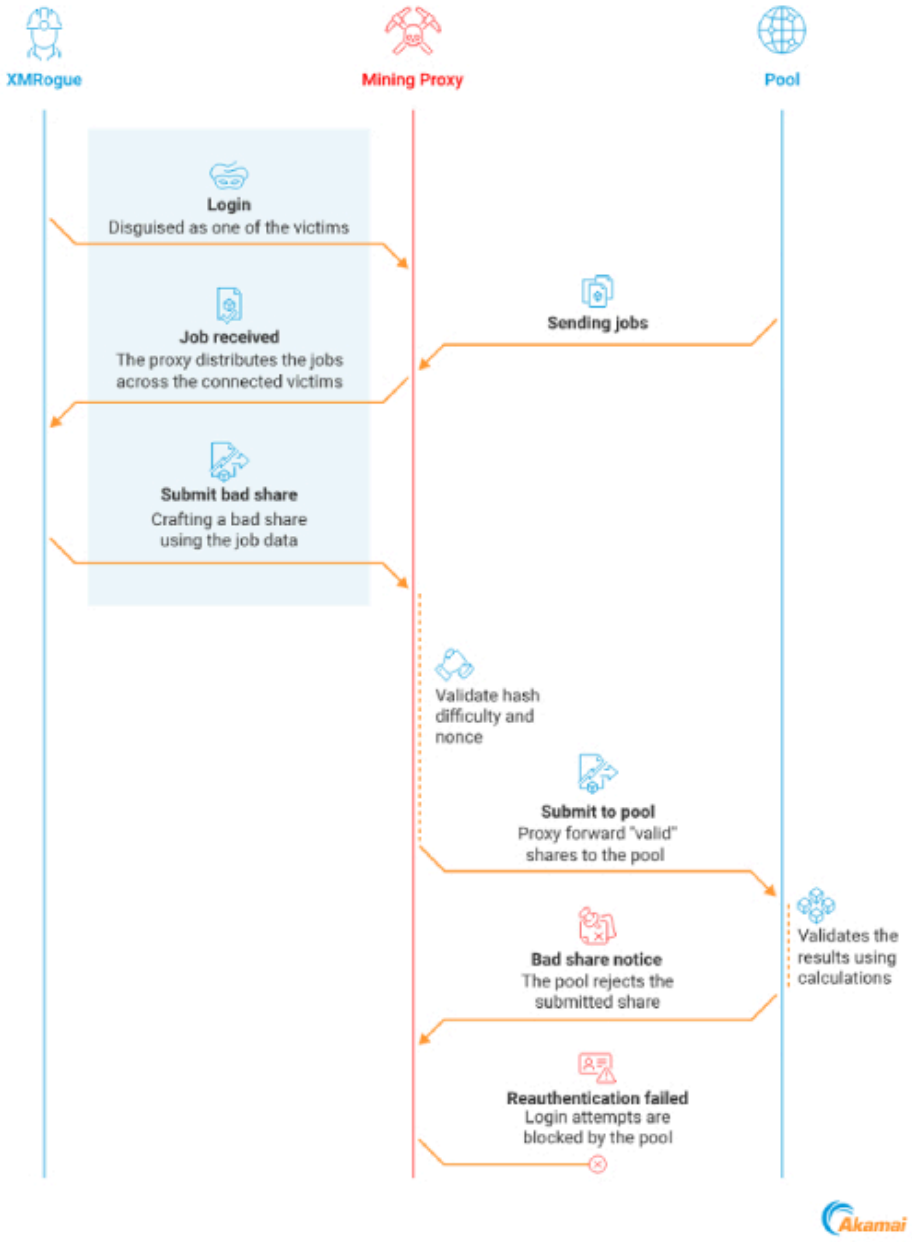
«Desarrollamos dos técnicas aprovechando las topologías de minería y las políticas de los pools, lo que nos permite reducir la efectividad de una botnet de criptominería hasta el punto de apagarla por completo. Esto obliga al atacante a realizar cambios drásticos en su infraestructura o incluso a abandonar la campaña por completo,» explicó el investigador de seguridad Maor Dahan.

La compañía de infraestructura web indicó que estas técnicas se basan en explotar el protocolo de minería Stratum, provocando que el proxy de minería o la cartera del atacante sea bloqueada, interrumpiendo así toda la operación.

La primera de las dos estrategias, llamada “acciones inválidas”, consiste en lograr que el proxy de minería sea expulsado de la red, lo que provoca que toda la operación se detenga y que el uso del CPU de la víctima caiga de un 100% a 0%.

Aunque un proxy de minería actúa como intermediario y oculta el pool de minería del atacante —y, por ende, sus direcciones de cartera—, también se convierte en un punto único de fallo cuando se altera su funcionamiento normal.

«La idea es sencilla: al conectarnos como mineros a un proxy malicioso, podemos enviar resultados inválidos de trabajos de minería —acciones erróneas— que pasarán el filtro del proxy y llegarán al pool,» explicó Dahan. *«El envío repetido de acciones inválidas acabará por hacer que el proxy sea bloqueado, deteniendo efectivamente las operaciones de minería de toda la botnet.»*



Para lograrlo, se utiliza una herramienta interna desarrollada por Akamai llamada XMRogue, que simula ser un minero, se conecta al proxy de minería, envía acciones inválidas de forma continua y finalmente provoca el bloqueo del proxy en el pool.

El segundo enfoque diseñado por Akamai se aplica en casos donde el minero víctima está conectado directamente a un pool público sin pasar por un proxy. Se aprovecha el hecho de que un pool puede suspender temporalmente una cartera si detecta más de 1,000 trabajadores asociados a ella.

En otras palabras, si se generan más de 1,000 intentos de conexión simultánea usando la cartera del atacante, el pool suspenderá esa cartera por una hora. Sin embargo, esta no es una solución definitiva, ya que el atacante podría recuperar el acceso una vez que cesen las conexiones múltiples.

Akamai subrayó que, si bien estas técnicas han sido aplicadas principalmente contra mineros de Monero, pueden adaptarse a otras criptomonedas también.

«Las técnicas presentadas arriba demuestran cómo los defensores pueden desactivar campañas maliciosas de criptominería sin afectar las operaciones legítimas del pool, simplemente aprovechando sus propias políticas,» señaló Dahan.

«Un minero legítimo podrá recuperarse rápidamente de este tipo de ataques, ya que puede cambiar fácilmente su IP o cartera localmente. Pero para un criptominero malicioso, esto implicaría modificar toda su botnet. Para los mineros menos sofisticados, esta defensa podría inutilizar por completo la botnet.»