Un ataque contra la billeteras Bitcoin de Electrum se ha vuelto cada vez más fuerte y los hackers están apuntando a toda la infraestructura del exchanger con una red de bots de más de 152,000 usuarios infectados, aumentando la cantidad de fondos robados a 4.6 millones de dólares.

Electrum ha enfrentado ataques cibernéticos desde diciembre del año pasado, cuando un equipo de delincuentes informáticos explotó una debilidad en la infraestructura de Electrum para engañar a los usuarios de la billetera para que descarguen las versiones maliciosas del software.

En resumen, los hackers agregaron algunos servidores maliciosos a la red de parte de Electrum que fueron diseñados para mostrar deliberadamente un error para legitimar las aplicaciones de billetera de Electrum, instándolos a descargar una actualización de software de billetera maliciosa desde un repositorio no oficial de GitHub.

El ataque de phishing finalmente permitió a los atacantes robar fondos de la billetera (alrededor de 250 Bitcoins, equivalentes a 937,000 dólares en ese momento) y tomar el control total de los sistemas infectados.

Para contrarrestar lo sucedido, los desarrolladores de Electrum explotaron la misma técnica que los atacantes para alentar a los usuarios a descargar la última versión parcheada de la aplicación de billetera.

> *«Los clientes de Electrum anteriores a 3.3 ya no pueden conectarse a servidores públicos de Electrum. Comenzamos a explotar una vulnerabilidad de DoS en esos clientes, para forzar a sus usuarios a actualizar y evitar la exposición a mensajes de phishing. Los usuarios de Linux Tail deben descargar nuestro Appimage»,*
> escribieron los desarrolladores en marzo.

Mensaje falso de Electrum

En respuesta, los atacantes iniciaron DDoSing a los servidores de Electrum en un intento de engañar a los clientes más antiguos para que se conecten a nodos maliciosos.

Según una publicación del equipo de investigación de Malwarebytes Labs, la cantidad de máquinas infectadas que descargaron el software cliente malicioso y están participando involuntariamente en los ataques DDoS ha alcanzado los 152,000, siendo más de cien mil que la semana pasada.

Los atacantes detrás de estas campañas básicamente distribuyen un malware de red de bots, denominado *«ElectrumDoSMiner»,* al aprovechar principalmente el kit de explotación RIG, el cargador de humo y un nuevo cargador BeamWinHTTP previamente no documentado.

> *«Hay cientos de binarios maliciosos que recuperan el ElectrumDoSMiner. Suponemos que probablemente haya muchos más vectores de infección más allá de los tres que hemos descubierto hasta ahora»*, dicen los investigadores.

De acuerdo con los investigadores, la mayor concentración de los bots Electrum DDoS se encuentra en la región de Asia Pacífico, Brasil y Perú, con la red de bots en continuo crecimiento.

> *«El número de víctims que forman parte de esta botnet está cambiando constantemente. Creemos que a medida que algunas máquinas se limpian, se infectan otras nuevas y se unen a las otras para realizar ataques DoS. Malwarebytes detecta y elimina las infecciones de ElectrumDoSMiner en más de 2,000 puntos finales diariamente»*, agregaron los investigadores.

Dado que las versiones actualizadas de Electrum no son vulnerables a los ataques de

phishing, se recomienda a los usuarios actualizar sus aplicaciones de billetera a la última versión, la 3.3.4, en el sitio oficial electrum.org.