Un ataque de minería de criptomonedas dirigido al sistema operativo Linux también involucró el uso de un troyano de acceso remoto (RAT) de código abierto denominado CHAOS.

La amenaza, que fue detectada por Trend Micro en noviembre de 2022, permanece prácticamente sin cambios en todos los demás aspectos, incluso cuando se trata de eliminar el malware de la competencia, el software de seguridad y la implementación del minero de criptomonedas Monero (XMR).

> *«El malware logra su persistencia alterando el archivo /etc/crontab, un programador de tareas de UNIX que, en este caso, se descarga cada 10 minutos desde Pastebin»,* dijeron los investigadores David Fiser y Alfredo Oliveira.

Este paso se logra mediante la descarga de las cargas útiles de siguiente etapa que consisten en el minero XMRig y el CHAOS RAT basado en Go.

La compañía de seguridad cibernética dijo que el script de descarga principal y otras cargas útiles están alojadas en múltiples ubicaciones para garantizar que la campaña permanezca activa y que sigan ocurriendo nuevas infecciones.

CHAOS RAT, una vez descargado e iniciado, transmite metadatos detallados del sistema a un servidor remoto, y también cuenta con capacidades para realizar operaciones con archivos, tomar capturas de pantalla, apagar y reiniciar la computadora y abrir direcciones URL arbitrarias.

> *«En la superficie, la incorporación de un RAT en la rutina de infección de un malware de minería de criptomonedas puede parecer relativamente menor»,* dijeron los investigadores.

> *«Sin embargo, dada la variedad de funciones de la herramienta y el hecho de que esta evolución muestra que los atacantes basados en la nube siguen desarrollando sus campañas, es importante que tanto las organizaciones como las personas se mantengan más alertas en lo que respecta a la seguridad»*, agregaron.