Los servidores de bases de datos Redis mal configurados están siendo objetivo de una nueva campaña de cryptojacking que aprovecha un servicio de transferencia de archivos de línea de comandos legítimo y de código abierto para implementar su ataque cibernético.

> *«Apuntalar esta campaña fue el uso de transfer[.]sh. Es posible que sea un intento de evadir las direcciones basadas en otros dominios de alojamiento de código comunes (como pastebin[.]com)»,* dijo Cado Security

La compañía de seguridad cibernética en la nube dijo que la interactividad de la línea de comandos asociada con transfer[.]sh la ha convertido en una herramienta ideal para alojar y entregar cargas maliciosas.

La cadena de ataque comienza apuntando a implementaciones inseguras de Redis, seguido por el registro de un trabajo cron que conduce a la ejecución de código arbitrario cuando el programador lo analiza. El trabajo está diseñado para recuperar una carga útil alojada en transfer[.]sh.

Cabe mencionar que otros atacantes como TeamTNT y WatchDog han empleado mecanismos de ataque similares en sus operaciones de cryptojacking.

La carga útil es una secuencia de comandos que allana el camino para un minero de criptomonedas XMRig, pero no sin antes tomar medidas preparatorias para liberar memoria, terminar con los mineros de la competencia e instalar una utilidad de escáner de red llamada pnscan para encontrar servidores Redis vulnerables y propagar la infección.

> *«Aunque está claro que el objetivo de esta campaña es secuestrar los recursos del sistema para extraer criptomonedas, la infección por este malware podría tener efectos no deseados. La configuración imprudente de los sistemas de administración de memoria de Linux podría fácilmente resultar en la corrupción de datos o la pérdida de disponibilidad del sistema»*, dijo la compañía.

El desarrollo lo convierte en la última amenaza que afecta a los servidores de Redis luego de Redigo y HeadCrab en los últimos meses.

Los hallazgos también se producen cuando Avertium reveló un nuevo conjunto de ataques en lo que los servidores SSH usan la fuerza bruta para implementar el malware de botnet XorDos en servidores comprometidos con el objetivo de lanzar ataques distribuidos de denegación de servicio (DDoS) contra objetivos ubicados en China y Estados Unidos.

La compañía de seguridad cibernética dijo que observó 1.2 millones de intentos de conexión SSH no autorizados en 18 honeypots entre el 6 de ocutbre de 2022 y el 7 de diciembre de 2022. Atribuyó la actividad a un actor de amenazas con sede en China.

El 42% de esos intentos se originaron en 49 direcciones IP asignadas a ChinaNet Jiangu Province Network, y el resto se originó en 8000 direcciones IP repartidas por todo el mundo.

> *«Se descubrió que una vez que el escaneo identificaba un puerto abierto, estaría sujeto a un ataque de fuerza bruta contra la cuenta 'raíz' usando una lista de aproximadamente 17,000 contraseñas. Una vez que el ataque de fuerza bruta tuvo éxito, se instaló un bot XorDDoS»,* dijo Avertium.