Al menos 1200 servidores de bases de daos de Redis en todo el mudo fueron secuestrados en una red de bots usando una *«amenaza elusiva y grave»* denominada HeadCrab desde principios de septiembre de 2021.

> *«Este actor de amenazas avanzado utiliza un malware personalizado de última generación que es indetectable por las soluciones antivirus tradicionales y sin agente para comprometer una gran cantidad de servidores Redis»,* dijo el investigador de seguridad de Aqua, *Asaf Eitani.*

Hasta ahora, se ha registrado una concentración significativa de infecciones en China, Malasia, India, Alemania, Reino Unido y Estados Unidos. Actualmente se desconocen los orígenes del actor de amenazas.

Los hallazgos se producen dos meses después de que la compañía de seguridad en la nube informara sobre un malware basado en Go, con nombre en código Redigo, que fue descubierto comprometiendo los servidores de Redis.

El ataque está diseñado para apuntar a los servidores Redis que están expuestos a Internet, seguido de la emisión de un comando SLAVEOF desde otro servidor Redis que ya está bajo el control del atacante.

Al hacerlo, el servidor «maestro» malicioso inicia una sincronización del servidor recién hackeado para descargar la carga útil maliciosa, que contiene el sofisticado malware HeadCrab en este último.

> *«El atacante parece apuntar principalmente a los servidores de Redis y tiene un profundo conocimiento y experiencia en los módulos y API de Redis, como lo demuestra el malware»,* dijo Eitani.

Aunque el objetivo final de usar el malware residente en la memoria es secuestrar los recursos del sistema para la minería de criptomonedas, también cuenta con muchas otras opciones que permiten al atacante ejecutar comandos de shell, cargar módulos de kernel sin archivos y filtrar datos a un servidor de control remoto.

Además, un análisis de seguimiento del malware Redigo reveló que utiliza como arma la misma técnica maestro-esclavo para la proliferación, y no la falla de escape de sandbox de Lua (CVE-2022-0543) como se reveló anteriormente.

Se recomienda a los usuarios que se abstengan de exponer los servidores de Redis directamente a Internet, deshabiliten la función «SLAVEOF» en sus entornos si no están en uso y configuren los servidores para que solo acepten conexiones de hosts confiables.

Eitani dijo que *«HeadCrab persistirá en el uso de técnicas vanguardistas para penetrar en los servidores, ya sea mediante la explotación de configuraciones incorrectas o vulnerabilidades».*