Un análisis en curso de una red de bots de minería de criptomonedas conocida como KmsdBot, llevó a que esta se elimine de forma accidental.

KmsdBot, como la nombró el Equipo de Respuesta de Inteligencia de Seguridad (SIRT) de Akamai, salió a la luz a mediados de noviembre de 2022 por su capacidad para utilizar sistemas de fuerza bruta con credenciales SSH débiles.

La red de bots ataca a dispositivos Windows y Linux que abarcan una amplia gama de microarquitecturas con el objetivo principal de implementar software de minería y acorralar a los hosts comprometidos en un bot DDoS.

Algunos de los objetivos principales incluyeron empresas de juegos, empresas de tecnología y fabricantes de automóviles de lujo.

El investigador de Akamai, Larry W. Cashdollar, en una nueva actualización, explicó cómo los comandos enviados al bot para comprender su funcionalidad en un entorno controlado neutralizaron inadvertidamente el malware.

> *«Curiosamente, después de un solo comando con formato incorrecto, el bot dejó de enviar comandos. No todos los días te encuentras con una botnet en la que los propios actores de amenazas bloquean su propia obra»,* dijo Cashdollar.

Esto, a su vez, fue posible gracias a la falta de un mecanismo de verificación de errores integrado en el código fuente para validar los comandos recibidos.

Específicamente, una instrucción emitida sin un espacio entre el sitio web de destino y el puerto hizo que todo el binario de Go que se ejecutaba en la máquina infectada fallara y dejara de interactuar con su servidor de comando y control, matando efectivamente a la red de bots.

El hecho de que KmsdBot no tenga un mecanismo de persistencia también significa que el

operador de malware tendrá que volver a infectar las máquinas y reconstruir la infraestructura desde cero.

> *«Esta botnet ha estado persiguiendo a algunas marcas de lujo y compañías de juegos muy grandes y, sin embargo, con un comando fallido no puede seguir. Este es un fuerte ejemplo de la naturaleza voluble de la tecnología y cómo incluso el explotador puede ser explotado por ella»*, dijo Cashdollar.