Se han identificado dos paquetes maliciosos en el registro de paquetes npm que emplean GitHub para almacenar claves SSH cifradas en Base64, las cuales fueron sustraídas de los sistemas de desarrolladores donde fueron instalados.

Los módulos conocidos como warbeast2000 y kodiak2k fueron publicados al comienzo del mes, atrayendo 412 y 1,281 descargas respectivamente antes de ser retirados por los mantenedores de npm. Las descargas más recientes se registraron el 21 de enero de 2024.

ReversingLabs, una firma de seguridad especializada en la cadena de suministro de software, fue la encargada de descubrir estos paquetes maliciosos y señaló que existen ocho versiones diferentes de warbeast2000 y más de 30 versiones de kodiak2k.

Ambos módulos están diseñados para ejecutar un script postinstalación que busca recuperar y ejecutar dos archivos JavaScript distintos.

Mientras que warbeast2000 intenta acceder a la clave SSH privada, kodiak2k está configurado para buscar una clave denominada «meow», sugiriendo que el actor de amenazas probablemente utilizó un nombre provisional en las etapas iniciales del desarrollo.

> *«Este script malicioso en la segunda fase lee la clave SSH privada almacenada en el archivo id_rsa ubicado en el directorio /.ssh. Luego, carga la clave codificada en Base64 en un repositorio GitHub controlado por el atacante»,* explicó la investigadora de seguridad Lucija Valentić.

Versiones posteriores de kodiak2k fueron descubiertas ejecutando un script encontrado en un proyecto GitHub archivado que alberga el framework de post-explotación Empire. Este script tiene la capacidad de lanzar la herramienta de hacking Mimikatz para extraer credenciales de la memoria del proceso.

> *«Esta campaña es simplemente el último ejemplo de cómo los ciberdelincuentes y*

> *actores maliciosos aprovechan los administradores de paquetes de código abierto y la infraestructura relacionada para respaldar campañas maliciosas en la cadena de suministro de software, dirigidas tanto a organizaciones de desarrollo como a organizaciones de usuarios finales»,* señaló Valentić.