Los servidores SSH de Linux con deficiencias en su seguridad están siendo objeto de ataques por parte de individuos malintencionados que buscan instalar herramientas de exploración de puertos y aplicaciones de ataque basadas en diccionario. Su objetivo es comprometer otros servidores vulnerables y sumarlos a una red, todo con el fin de realizar actividades de minería de criptomonedas y lanzar ataques de denegación de servicio distribuido (DDoS).

El Centro de Respuesta de Emergencia de Seguridad de AhnLab (ASEC) mencionó en un informe reciente que *«los delincuentes también podrían simplemente optar por instalar herramientas de exploración y luego comercializar las direcciones IP y credenciales de acceso en el mercado negro de la web profunda».*

En el curso de estos ataques, los adversarios intentan penetrar en un servidor SSH probando una serie de combinaciones conocidas de nombres de usuario y contraseñas, un proceso denominado ataque de diccionario.

Si esta técnica tiene éxito, el atacante procede a instalar otro tipo de software malicioso, incluidos escáneres, con el objetivo de identificar y comprometer otros sistemas en la web.

Concretamente, este software de exploración busca sistemas donde el puerto 22, que corresponde al servicio SSH, esté activo. Posteriormente, repite el ataque basado en diccionario para difundir la amenaza.

Un detalle interesante de este tipo de ataque es que los delincuentes ejecutan comandos específicos, como *«grep -c ^processor /proc/cpuinfo«,* para determinar la cantidad de núcleos del procesador.

ASEC destacó que *«estas herramientas parecen haber sido desarrolladas originalmente por el equipo conocido como PRG antiguo, aunque cada atacante suele hacer pequeñas modificaciones antes de usarlas».* Además, indicaron que hay registros de actividad maliciosa de este tipo desde 2021.

Para reducir la exposición a estos riesgos, se aconseja a los usuarios emplear contraseñas

robustas, cambiarlas regularmente y mantener al día sus sistemas operativos.

Estos descubrimientos coinciden con el anuncio de Kaspersky sobre una nueva amenaza, denominada NKAbuse, que utiliza un protocolo de comunicación descentralizado llamado NKN (Nuevo Tipo de Red) para coordinar sus ataques DDoS.