Un atacante desconocido apuntó a decenas de miles de servidores de Redis no autenticados expuestos en Internet en un intento de instalar un minero de criptomonedas.

No se sabe hasta ahora si todos los hosts se vieron comprometidos exitosamente. No obstante, fue posible gracias a una *«técnica menos conocida»* diseñada para engañar a los servidores para que escriban datos en archivos arbitrarios, un caso de acceso no autorizado que se documentó por primera vez en septiembre de 2018.

> *«La idea general detrás de esta técnica de explotación es configurar Redis para escribir su base de datos basada en archivos en un directorio que contenga algún método para autorizar a un usuario (como agregar una clave a '.ssh/auhorized_keys'), o iniciar un proceso (como agregar un script para '/etc/cron.d')»*, dijo Censys.

La plataforma de administración de superficie de ataque dijo que descubrió evidencia (es decir, comandos de Redis) que indican los esfuerzos por parte del atacante para almacenar entradas crontab maliciosas en el archivo *«/var/spool/cron/root»,* lo que resultó en la ejecución de un script de shell alojado en un servidor remoto.

El script de shell, al que aún se puede acceder, está diseñado para realizar las siguientes acciones:

- Terminar los procesos de monitoreo del sistema y relacionados con la seguridad
- Purgar archivos de registro e historiales de comandos
- Agregar una nueva clave SSH («backup1») al archivo authorized_keys del usuario raíz para habilitar el acceso remoto
- Deshabilitar el firewall de iptables
- Instalar herramientas de escaneo como Masscan
- Instalar y ejecutar la aplicación de minería de criptomonedas XMRig

Se cree que la clave SSH se configuró en 15,526 de los 31,239 servidores Redis no

autenticados, lo que sugiere que el ataque se intentó en *«más del 49% de los servidores Redis no autenticados conocidos en Internet».*

Sin embargo, una razón principal por la que este ataque podría fallar es que el servicio Redis debe ejecutarse con permisos elevados (root) para permitir que el adversario escriba en el directorio cron mencionado anteriormente.

> *«Aunque, este puede ser el caso cuando se ejecuta Redis dentro de un contenedor (como una ventana acoplable), donde el proceso podría verse ejecutándose como root y permitir que el atacante escriba estos archivos. Pero en este caso, solo el contenedor se ve afectado, no el host físico»*, dijeron los investigadores de Censys.

El informe de Censys también reveló que hay alrededor de 350,675 servicios de base de datos Redis accesibles por Internet que abarcan 260,534 hosts únicos.

«Aunque la mayoría de estos servicios requieren autenticación, el 11% (39,405) no la requiere», dijo la compañía, agregando que *«del total de 39.405 servidores Redis no autenticados que observamos, la exposición potencial de datos es de más de 300 GB».*

Los principales países con servicios Redis expuestos y no autenticados incluyeron China (20,011), Estados Unidos (5108), Alemania (1724), Singapur (1236), India (876), Francia (870), Japón (711), Hong Kong (512), Países Bajos (433) e Irlanda (390).

China también lidera en lo que respecta a la cantidad de datos expuestos por país, con 146 gigabytes de datos, con Estados Unidos en un distante segundo lugar con aproximadamente 40 gigabytes.

Censys dijo que también encontró numerosos casos de servicios de Redis que se han configurado mal, y dijo que *«Israel es una de las únicas regiones donde la cantidad de servidores Redis mal configurados supera a los configurados de forma correcta».*

Para mitigar las amenazas, se recomienda a los usuarios que habiliten la autenticación del cliente, configuren Redis para que se ejecute solo en las interfaces de red orientadas hacia el interior, eviten el abuso del comando CONFIG renombrándolo a algo que no se pueda adivinar y configuren los firewalls para que acepten conexiones de Redis solo de hosts confiables.