Investigadores en ciberseguridad han advertido sobre una nueva campaña de *cryptojacking* dirigida a servidores Redis expuestos públicamente que operan en sistemas Linux.

Esta actividad maliciosa ha sido nombrada RedisRaider por el equipo de Datadog Security Labs.

> "RedisRaider escanea agresivamente porciones aleatorias del espacio IPv4 y utiliza comandos legítimos de configuración de Redis para ejecutar tareas *cron* maliciosas en sistemas vulnerables", explicaron los investigadores Matt Muir y Frederic Baguelin.

El propósito de la campaña es instalar una carga útil principal escrita en Go, que se encarga de desplegar un minero XMRig en los sistemas comprometidos.

El proceso incluye el uso de un escáner personalizado para detectar instancias de Redis accesibles en internet. Luego se utiliza el comando `INFO` para verificar si los servidores funcionan sobre Linux. Si es así, se aprovecha el comando SET de Redis para introducir una tarea programada mediante *cron*.

El código malicioso emplea el comando `CONFIG` para modificar el directorio de trabajo de Redis a `/etc/cron.d` y escribir allí un archivo de base de datos llamado «apache», lo que permite que el programador *cron* lo ejecute de forma periódica. Este archivo contiene un *script* codificado en Base64 que descarga el ejecutable RedisRaider desde un servidor remoto.

Esta carga útil actúa como instalador de una versión personalizada de XMRig, además de que facilita la propagación del malware a otras instancias Redis, ampliando así el alcance de la campaña.

> "Además del *cryptojacking* del lado del servidor, la infraestructura de RedisRaider

> también alojaba un minero web basado en Monero, lo que permite una estrategia de generación de ingresos con múltiples enfoques", comentaron los investigadores.
>
> "La campaña incorpora medidas sutiles de antiforense, como la configuración de tiempos de vida (TTL) cortos para claves y cambios en la configuración de la base de datos, con el fin de reducir la detección y dificultar el análisis posterior al incidente."

Este hallazgo coincide con otra campaña identificada por Guardz, que detalla el uso de protocolos heredados en Microsoft Entra ID para ejecutar ataques de fuerza bruta contra cuentas. Esta actividad, que ocurrió entre el 18 de marzo y el 7 de abril de 2025, explotó la funcionalidad BAV2ROPC (*Basic Authentication Version 2 – Resource Owner Password Credential*) para eludir defensas como la autenticación multifactor (MFA) y el Acceso Condicional.

> "El seguimiento y análisis revelaron intentos sistemáticos de explotación que aprovechaban limitaciones inherentes al diseño de BAV2ROPC, que preceden a las arquitecturas de seguridad modernas", indicó Elli Shlomo, jefe de investigación de seguridad en Guardz. "Los actores detrás de esta campaña demostraron un conocimiento profundo de los sistemas de identidad."

Se ha informado que los ataques se originaron principalmente desde Europa del Este y la región de Asia-Pacífico, con un enfoque particular en cuentas administrativas que aún utilizan puntos finales de autenticación obsoletos.

> "Mientras que los usuarios normales recibieron la mayoría de los intentos de autenticación (50,214), las cuentas de administrador y los buzones compartidos fueron blanco de un patrón específico, con 9,847 intentos dirigidos a cuentas de

> administrador desde 432 direcciones IP en un periodo de 8 horas, lo que representa un promedio de 22.79 intentos por IP y una velocidad de 1,230.87 intentos por hora", detalló la compañía.
>
> "Esto evidencia una campaña de ataque altamente automatizada y enfocada en comprometer cuentas con privilegios, sin dejar de mantener un frente de ataque más amplio contra usuarios comunes."

Este tipo de abusos a protocolos obsoletos no es nuevo. En 2021, Microsoft reveló una campaña masiva de *Business Email Compromise (BEC)* que utilizó BAV2ROPC e IMAP/POP3 para eludir MFA y robar datos de correo electrónico.

Como medida de protección, se recomienda bloquear la autenticación heredada mediante políticas de Acceso Condicional, desactivar el uso de BAV2ROPC y deshabilitar SMTP AUTH en Exchange Online si no se requiere.