Ciberexpertos en seguridad han descubierto cargas no registradas previamente asociadas a un actor de amenazas rumano conocido como Diicot, revelando su potencial para llevar a cabo ataques de denegación de servicio distribuido (DDoS).

> *«El nombre Diicot es importante, ya que también es el nombre de la unidad de lucha contra el crimen organizado y el antiterrorismo de Rumania. Además, los artefactos de las campañas del grupo contienen mensajes e imágenes relacionados con esta organización»,* dijo Cado Security

Diicot (antes conocido como Mexals) fue identificado por primera vez por Bitdefender en julio de 2021, descubriendo que el actor utilizaba una herramienta de ataque de fuerza bruta de SSH basada en Go llamada Diicot Brute para infiltrarse en hosts de Linux como parte de una campaña de cryptojacking.

Posteriormente, en abril de este año, Akamai reveló lo que describió como un *«resurgimiento»* de la actividad del 2021, que se cree que comenzó alrededor de octubre de 2022, generando al actor alrededor de $10,000 en ganancias ilícitas.

> *«Los atacantes utilizan una serie extensa de cargas antes de finalmente introducir un minero de Monero. Las nuevas capacidades incluyen el uso de un módulo de gusano del Protocolo Secure Shell (SSH), mayor generación de informes, mejor ocultamiento de las cargas y un nuevo módulo de propagación LAN»,* dijo en ese momento el investigador de Akamai, Stiv Kupchik.

El último análisis de Cado Security muestra que el grupo también está utilizando un botnet comercial llamado Cayosin, una familia de malware que comparte características con Qbot y Mirai.

Este desarrollo indica que el actor de amenazas ahora posee la capacidad de llevar a cabo

ataques DDoS. Otras actividades realizadas por el grupo incluyen la exposición de información personal de grupos de piratas informáticos rivales y su dependencia de Discord para el control y el robo de datos.

> *«El despliegue de este agente se dirigió a enrutadores que ejecutan el sistema operativo de dispositivos incorporados basado en Linux, OpenWrt. El uso de Cayosin demuestra la disposición de Diicot para llevar a cabo una variedad de ataques (no solo cryptojacking) según los objetivos con los que se encuentren»,* afirmó la empresa de seguridad cibernética.

Las cadenas de compromiso de Diicot han permanecido en gran medida consistentes, aprovechando la herramienta personalizada de ataque de fuerza bruta de SSH para obtener acceso y distribuir malware adicional, como la variante de Mirai y el minero de criptomonedas.

Algunas de las otras herramientas utilizadas por el actor son las siguientes:

- Chrome: un escáner de Internet basado en Zmap que puede guardar los resultados de la operación en un archivo de texto («bios.txt»).
- Update: un ejecutable que obtiene y ejecuta el ataque de fuerza bruta de SSH y Chrome si no están presentes en el sistema.
- History: un script de shell diseñado para ejecutar la Actualización.

La herramienta de ataque de fuerza bruta de SSH (también conocida como alias), por su parte, analiza el archivo de texto generado por Chrome para acceder a cada una de las direcciones IP identificadas y, si tiene éxito, establece una conexión remota con esa dirección IP.

Posteriormente, se ejecutan una serie de comandos para analizar el host infectado y utilizarlo para desplegar un minero de criptomonedas o utilizarlo como propagador si la CPU de la máquina tiene menos de cuatro núcleos.

Para mitigar tales ataques, se recomienda a las organizaciones implementar medidas de endurecimiento de SSH y reglas de firewall para limitar el acceso SSH a direcciones IP específicas.

> *«Esta campaña se dirige específicamente a servidores SSH expuestos a Internet con autenticación de contraseña habilitada. La lista de nombres de usuario y contraseñas que utilizan es relativamente limitada e incluye pares de credenciales predeterminadas y fácilmente identificables»,* afirmó Cado Security.