Las actividades del ransomware Mallox en 2023 han experimentado un aumento del 174% en comparación con el año anterior, según revelan nuevos descubrimientos de Palo Alto Networks Unit 42.

> *«El ransomware Mallox, al igual que muchos otros actores de amenazas de ransomware, sigue la tendencia de doble extorsión: roba datos antes de cifrar los archivos de una organización y luego amenaza con publicar la información robada en un sitio de filtraciones como forma de persuadir a las víctimas de pagar el rescate»,* informaron los investigadores de seguridad Lior Rochberger y Shimi Cohen en un reciente informe.

Mallox está vinculado a un grupo de amenazas que también está relacionado con otras variantes de ransomware, como TargetCompany, Tohnichi, Fargo y, más recientemente, Xollam. Hizo su primera aparición en junio de 2021.

Algunos de los sectores destacados que son atacados por Mallox son la industria manufacturera, los servicios profesionales y legales, y el comercio mayorista y minorista.

Un aspecto destacado del grupo es su patrón de explotación de servidores MS-SQL poco seguros mediante ataques de diccionario como vector de penetración para comprometer las redes de las víctimas. Xollam se desvía de lo habitual, ya que se ha observado que utiliza archivos adjuntos maliciosos de OneNote para obtener acceso inicial, tal como detalló Trend Micro el mes pasado.

Una vez que ha logrado un punto de apoyo exitoso en el host infectado, se ejecuta un comando de PowerShell para obtener el código malicioso del ransomware desde un servidor remoto.

El binario, por su parte, intenta detener y eliminar los servicios relacionados con SQL, borrar copias de sombra del volumen, limpiar los registros de eventos del sistema, terminar los procesos de seguridad y evadir Raccine, una herramienta de código abierto diseñada para

contrarrestar ataques de ransomware, antes de iniciar su proceso de cifrado, después del cual deja una nota de rescate en cada directorio.

TargetCompany sigue siendo un grupo reducido y cerrado, pero también se ha observado que está reclutando afiliados para el programa de ransomware Mallox-as-a-service (RaaS) en el foro de cibercrimen RAMP.

Este desarrollo se produce en un momento en que el ransomware sigue siendo un esquema financiero altamente lucrativo, generando ganancias de al menos $449.1 millones solo en la primera mitad de 2023, según el informe de Chainalysis.

El repentino aumento en las infecciones de Mallox también es sintomático de una tendencia más amplia en la que los ataques de ransomware han experimentado un salto del 221% interanual hasta junio de 2023, con 434 ataques reportados solo en junio de ese año, en gran medida debido a la explotación de la vulnerabilidad del software de transferencia de archivos MOVEit por parte del grupo Cl0p.

> *«El grupo de ransomware Mallox ha estado más activo en los últimos meses, y sus esfuerzos recientes para reclutar podrían permitirles atacar a más organizaciones si el proceso de reclutamiento tiene éxito»,* indicaron los investigadores.