Los actores de amenazas están aprovechando servidores Microsoft SQL (MS SQL) poco seguros para desplegar Cobalt Strike y una cepa de ransomware llamada FreeWorld.

Securonix, una firma de ciberseguridad, ha nombrado a esta campaña como DB#JAMMER, y se destaca por la forma en que se emplean las herramientas y la infraestructura.

«Algunas de estas herramientas incluyen software de enumeración, cargas RAT, software de explotación y robo de credenciales, y, por último, cargas de ransomware», señalan los investigadores de seguridad Den Iuzvyk, Tim Peck y Oleg Kolesnikov en un desglose técnico de la actividad.

> *«La elección de carga de ransomware parece ser una variante más reciente del ransomware Mimic llamada FreeWorld».*

La entrada inicial al host víctima se logra mediante ataques de fuerza bruta al servidor MS SQL, utilizando este para listar las bases de datos y aprovechando la opción de configuración xp_cmdshell para ejecutar comandos de consola y realizar reconocimiento.

La siguiente etapa involucra tomar medidas para debilitar el cortafuegos del sistema y establecer persistencia conectándose a un recurso compartido SMB remoto para transferir archivos hacia y desde el sistema víctima, así como instalar herramientas maliciosas como Cobalt Strike.

Esto, a su vez, allana el camino para la distribución del software AnyDesk con el fin de finalmente lanzar el ransomware FreeWorld, pero no sin antes realizar un movimiento lateral. Se informa que los atacantes desconocidos también intentaron sin éxito establecer la persistencia de RDP a través de Ngrok.

> *«El ataque tuvo éxito inicialmente debido a un ataque de fuerza bruta contra un servidor MS SQL. Es importante destacar la importancia de contraseñas sólidas,*

> *especialmente en servicios expuestos públicamente»,* subrayan los investigadores.

Esta revelación coincide con la afirmación por parte de los operadores del ransomware Rhysida de haber afectado a 41 víctimas, con más de la mitad de ellas ubicadas en Europa.

Rhysida es una de las cepas de ransomware emergentes que surgieron en mayo de 2023, adoptando la táctica cada vez más popular de cifrar y sustraer datos confidenciales de organizaciones y amenazar con filtrar la información si las víctimas se niegan a pagar.

También sigue al lanzamiento de un descifrador gratuito para un ransomware llamado Key Group debido a múltiples errores criptográficos en el programa. Sin embargo, el script de Python solo es eficaz en muestras compiladas después del 3 de agosto de 2023.

> *«El ransomware Key Group utiliza una clave estática codificada en base64 N0dQM0I1JCM= para cifrar los datos de las víctimas»,* informó la empresa de ciberseguridad holandesa EclecticIQ en un informe publicado el jueves.

> *«El actor de amenazas intentó aumentar la aleatoriedad de los datos cifrados mediante el uso de una técnica criptográfica denominada salting. Sin embargo, la sal era estática y se utilizaba en cada proceso de cifrado, lo que constituye una falla significativa en el proceso de cifrado».*

El año 2023 ha sido testigo de un drástico aumento récord en los ataques de ransomware, tras un período de relativa calma en 2022, incluso a pesar de que el porcentaje de incidentes que resultaron en que las víctimas pagaran ha descendido a un mínimo histórico del 34%, según estadísticas compartidas por Coveware en julio de 2023.

En cambio, la cantidad promedio de rescate pagada ha alcanzado los $740,144, lo que

representa un incremento del 126% con respecto al primer trimestre de 2023.

Las variaciones en las tasas de monetización han venido acompañadas de la continua evolución de las tácticas de extorsión por parte de los actores de amenazas de ransomware, que incluyen compartir detalles de sus técnicas de ataque para demostrar por qué las víctimas no cumplen los requisitos para recibir un pago de su seguro cibernético.

> *«Bajo la premisa de que Snatch divulgará información sobre cómo lograron tener éxito en los ataques contra las víctimas que no pagaron, con la esperanza de que las aseguradoras decidan que los incidentes no deben estar cubiertos por el seguro contra ransomware»,* comentó el investigador de seguridad de Emsisoft, Brett Callow, en una publicación compartida en la plataforma X (anteriormente conocida como Twitter) el mes pasado.