Microsoft advirtió el martes que recientemente detectó una campaña maliciosa dirigida a servidores SQL, que aprovecha un binario integrado de PowerShell para lograr la persistencia en los sistemas comprometidos.

Las intrusiones, que aprovechan los ataques de fuerza bruta como vector de compromiso inicial, se destacan por el uso de la utilidad «sqlps.exe», dijo la compañía.

Se desconocen los objetivos finales de la campaña, al igual que la identidad del atacante que la organiza. Microsoft está rastreando el malware bajo el nombre de «SuspSQLUsage«.

La utilidad sqlps.exe, que viene de forma predeterminada con todas las versiones de SQL Server, permite que SQL Agent, un servicio de Windows para ejecutar tareas programadas, ejecute trabajos utilizando el susbsistema PowerShell.

> *«Los atacantes logran una persistencia sin archivos al generar la utilidad sqlps.exe, un contenedor de PowerShell para ejecutar cmdlets construidos en SQL, para ejecutar comandos de reconocimiento y cambiar el modo de inicio del servicio SQL a LocalSystem»,* dijo Microsoft.

Además, también se observó que los atacantes utilizan el mismo módulo para crear una nueva cuenta con la función de administrador del sistema, lo que les permite tomar el control de SQL Server.

Esta no es la primera vez que los atacantes arman binarios legítimos que ya están presentes en un entorno, una técnica llamada living-off-the-land (LotL), para lograr sus objetivos.

Una ventaja que ofrecen dichos ataques es que tienden a no tener archivos porque no dejan ningún artefacto y es menos probable que las actividades sean marcadas por el software antivirus debido a que utilizan un software confiable.

La idea es permitir que el atacante se mezcle con la actividad regular de la red y las tareas

administrativas normales, mientras permanece oculto durante largos períodos de tiempo.

> *«El uso de este binario poco común que vive fuera de la tierra (LOLBin) destaca la importancia de obtener una visibilidad completa del comportamiento en tiempo de ejecución de los scripts para exponer el código malicioso»,* dijo Microsoft.