Microsoft ha presentado detalles de una nueva campaña en la que los atacantes intentaron, sin éxito, moverse de manera lateral hacia un entorno en la nube a través de una instancia de SQL Server.

> *«Los atacantes inicialmente aprovecharon una vulnerabilidad de inyección SQL en una aplicación dentro del entorno del objetivo»,* informaron los expertos en seguridad Sunders Bruskin, Hagai Ran Kestenberg y Fady Nasereldeen en un informe publicado el martes.

> *«Esto permitió al atacante obtener acceso y permisos elevados en una instancia de Microsoft SQL Server desplegada en una Máquina Virtual (VM) de Azure».*

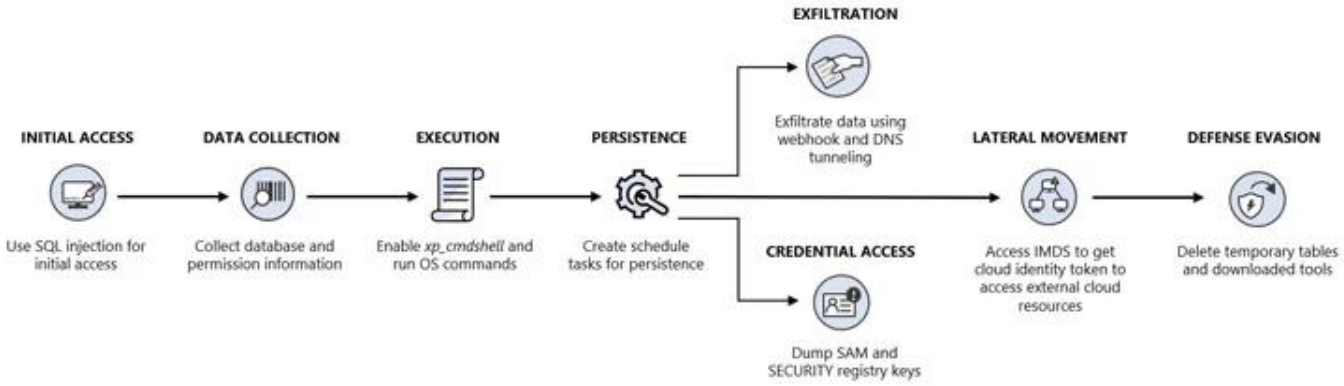
En la siguiente etapa, los actores de amenazas utilizaron los nuevos permisos para intentar moverse de manera lateral hacia recursos adicionales en la nube mediante el abuso de la identidad en la nube del servidor, la cual podría tener permisos elevados para llevar a cabo diversas acciones maliciosas en la nube a las que tiene acceso.

Microsoft afirmó que no encontró pruebas que sugieran que los atacantes lograron moverse de manera exitosa de manera lateral hacia los recursos en la nube utilizando esta técnica.

> *«Los servicios en la nube, como Azure, utilizan identidades gestionadas para asignar identidades a los distintos recursos en la nube. Estas identidades se utilizan para la autenticación con otros recursos y servicios en la nube»*, explicaron los investigadores.

El punto de inicio de la cadena de ataque es una inyección SQL contra el servidor de base de datos que permite al adversario ejecutar consultas para recopilar información sobre el host, las bases de datos y la configuración de la red.

En las intrusiones observadas, se sospecha que la aplicación objetivo con la vulnerabilidad de inyección SQL tenía permisos elevados, lo que permitió a los atacantes habilitar la opción xp_cmdshell para ejecutar comandos del sistema operativo y avanzar a la siguiente fase.



Esto incluyó la realización de reconocimiento, la descarga de ejecutables y scripts de PowerShell, y la configuración de la persistencia mediante una tarea programada para iniciar un script de puerta trasera.

La exfiltración de datos se logra aprovechando una herramienta de acceso público llamada webhook[.]site en un esfuerzo por pasar desapercibidos, ya que el tráfico saliente hacia el servicio se considera legítimo y poco probable que sea detectado.

> *«Los atacantes intentaron utilizar la identidad en la nube de la instancia de SQL Server accediendo al servicio de metadatos de la instancia y obteniendo la clave de acceso de la identidad en la nube.»La solicitud al punto final de la identidad de IMDS devuelve las credenciales de seguridad (token de identidad) para la identidad en la nube»*, señalaron los investigadores.

El objetivo final de la operación parece haber sido abusar del token para llevar a cabo

diversas operaciones en los recursos en la nube, incluyendo el movimiento lateral en el entorno de la nube, aunque terminó en fracaso debido a un error no especificado.

Este desarrollo resalta la creciente sofisticación de las técnicas de ataque basadas en la nube, con actores maliciosos constantemente en busca de procesos con permisos excesivos, cuentas, identidades gestionadas y conexiones de bases de datos para llevar a cabo actividades maliciosas adicionales.

> *«Esta es una técnica con la que estamos familiarizados en otros servicios en la nube como VM y clústeres de Kubernetes, pero que no habíamos visto antes en instancias de SQL Server»,* concluyeron los investigadores.

> *«No asegurar adecuadamente las identidades en la nube puede exponer tanto a las instancias de SQL Server como a los recursos en la nube a riesgos similares. Este método brinda a los atacantes la oportunidad de lograr un mayor impacto no solo en las instancias de SQL Server, sino también en los recursos en la nube asociados».*