Los servidores Microsoft SQL (MS SQL) mal administrados son el objetivo de una nueva campaña diseñada para propagar una categoría de malware llamada CLR SqlShell que, en última instancia, facilita la implementación de mineros de criptomonedas y ransomware.

> *«Similar a web shell, que se puede instalar en servidores web, SqlShell es una variedad de malware que admite varias funciones después de instalarse en un servidor MS SQL, como ejecutar comandos de actores de amenazas y llevar a cabo todo tipo de comportamiento malicioso»,* dijo AhnLab Centro de Respuesta a Emergencias de Seguridad (ASEC) en un informe.

Un procedimiento almacenado es una subrutina que contiene un conjunto de declaraciones de lenguaje de consulta estructurado (SQL) para usar en múltiples programas en un sistema de administración de bases de datos relacionales (RDBMS).

Los procedimientos almacenados CLR disponibles en SQL Server 2005 y versiones posteriores, se refieren a procedimientos almacenados escritos en un lenguaje .NET como C# o Visual Basic.

El método de ataque descubierto por la firma de seguridad cibernética de Corea del Sur implica el uso del procedimiento CLR almacenado para instalar el malware en servidores MS SQL usando el comando xp_cmdshell, que genera un shell de comandos de Windows y pasa por una instrucción como entrada para la ejecución.

Algunas de las técnicas empleados por los hackers, incluidas las asociadas con LemonDuck, MyKings (también conocido como DarkCloud o Smominru) y Vollgar, se refieren a la explotación de servidores MS SQL expuestos a Internet mediante ataques de fuerza bruta y de diccionario para ejecutar comandos xp_cmdshell y OLE almacenado.

El uso de procedimientos almacenados CLR es la última incorporación a esta lista, con atacantes que aprovechan las rutinas de SqlShell para descargar cargas útiles de próxima etapa como Metasploit y mineros de criptomonedas como MrbMiner, MyKings y LoveMiner.

Además, distintos adversarios han usado SqlShells llamados SqlHelper, CLRSQL y CLR_module para escalar privilegios en servidores comprometidos y lanzar ransomware, proxyware e incorporar capacidades para llevar a cabo esfuerzos de reconocimiento en redes obetivo.

> *«SqlShell puede instalar malware adicional, como backdoors, mineros de criptomonedas y proxyware, o puede ejecutar comandos maliciosos recibidos de hackers de una forma similar a WebShell»*, dijo ASEC.