Los servidores vulnerables de Microsoft SQL (MS SQL) orientados a Internet, están siendo atacados por hackers como parte de una nueva campaña para implementar la herramienta de simulación de adversarios Cobalt Strike en hosts compartidos.

> *«Los ataques dirigidos a servidores MS SQL incluyen ataques al entorno donde su vulnerabilidad no ha sido reparada, fuerza bruta y ataque de diccionario contra servidores mal administrados»,* dijo la compañía de ciberseguridad de Corea del Sur, AhnLab Security Emergency Response Center (ASEC) en un informe.

Cobalt Strike es un marco comercial de prueba de penetración con todas las funciones que permite a un atacante implementar un agente llamado *«Beacon»* en la máquina de la víctima, otorgando al operador acceso remoto al sistema.

Aunque se anuncia como una plataforma de simulación de amenazas del equipo rojo, una amplia gama de atacantes ha utilizado activamente versiones descifradas del software.

Las intrusiones observadas por ASEC involucran al actor no identificado que escanea el puerto 1433 para verificar si hay servidores MS SQL expuestos para realizar ataques de fuerza bruta o de diccionario contra la cuenta del administrador del sistema, es decir, la cuenta «sa«, para intentar iniciar sesión.

Eso no significa que los servidores a los que no se puede acceder a través de Internet no sean vulnerables, ya que el actor de amenazas detrás del malware LemonDuck escanea el mismo puerto para moverse de forma lateral por medio de la red.

> *«Administrar las credenciales de la cuenta de administrador para que sean vulnerables a la fuerza bruta y los ataques de diccionario como se indicó anteriormente o no cambiar las credenciales periódicamente puede hacer que el servidor MS-SQL sea el objetivo principal de los atacantes»*, dijeron los investigadores.

Al obtener un punto de apoyo exitosamente, la siguiente fase del ataque funciona al generar un shell de comandos de Windows a través del proceso MS SQL «sqlservr.exe» para descargar la carga útil de la siguiente etapa que alberga el binario Cobalt Strike codificado en el sistema.

Los ataques culminan en última instancia con el malware que decodifica el ejecutable Cobalt Strike, seguido de su inyección en el proceso legítimo de Microsoft Build Engine (MSBuild), que ha sido previamente abusado por hackers para entregar troyanos de acceso remoto sin archivos y malware que roba contraseñas en sistemas objetivo Windows.

Además, el Cobalt Strike que se ejecuta en MSBuild.exe viene con configuraciones adicionales para evadir la detección del software de seguridad. Lo logra cargando «wwanmm.dll», una biblioteca de Windows para WWan Media Manager, luego escribiendo y ejecutando Beacon en el área de memoria de la DLL.

> *«Como la baliza que recibe el comando del atacante y realiza el comportamiento malicioso no existe en un área de memoria sospechosa, y en cambio, opera en el módulo normal wwanmm.dll, puede eludir la detección basada en la memoria»*, dijeron los investigadores.