Investigadores de seguridad cibernética descubrieron una campaña maliciosa sostenida que figura desde mayo de 2018, y que apunta a máquinas Windows que ejecutan servidores MS-SQL para implementar puertas traseras y otros tipos de malware, incluidas herramientas de acceso remoto multifuncionales (RAT) y criptomineros.

Nombrado como *«Vollgar»,* por la criptomoneda Vollar que extrae y su modo de operar *«vulgar»* ofensivo, los investigadores de Guardicore Labs afirmaron que el ataque emplea una fuerza bruta de contraseña para violar servidores Microsoft SQL con credenciales débiles expuestas a Internet.

Los investigadores aseguran que los atacantes lograron infectar con éxito entre 2 mil y 3 mil servidores de bases de datos diariamente durante las últimas semanas, con víctimas potenciales pertenecientes a los sectores de salud, aviación, TI y telecomunicaciones y educación superior en China, India, Estados Unidos, Corea del Sur y Turquía.

Afortunadamente para los interesados, los investigadores también lanzaron un script para permitir que los administradores de sistemas detecten si alguno de sus servidores MS-SQL de Windows se ha visto comprometido con esta amenaza en particular.

El ataque Vollgar comienza con intentos de inicio de sesión de fuerza bruta en servidores MS-SQL, que, de tener éxito, permiten al intruso ejecutar una serie de cambios de configuración para ejecutar comandos MS-SQL maliciosos y descargar binarios de malware.

> *«Los atacantes validan que ciertas clases COM están disponibles: WbemScripting.SWbemLocator, Microsoft.Jet.OLEDB.4.0 y Windows Script Host Object Model (wshom). Estas clases admiten tanto la secuencia de comandos WMI como la ejecución de comandos por medio de MS-SQL, que luego se usará para descargar el binario inicial de malware»,* dijeron los investigadores.

Además de garantizar que los ejecutables cmd.exe y ftp.exe tengan los permisos de ejecución necesarios, el operador detrás de Vollgar también crea nuevos usuarios de puerta trasera para la base de datos MS-SQL, así como en el sistema operativo con privilegios elevados.

Una vez completada la configuración inicial, el ataque procede a crear scripts de descarga (dos VBScripts y un script FTP), que se ejecutan *«un par de veces»*, cada vez con una ubicación de destino diferente en el sistema de archivos local para evitar posibles fallas.

Una de las descargas iniciales, denominada SQLAGENTIDC.exe o SQLAGENTVDC.exe, primero elimina una larga lista de procesos con el objetivo de asegurar la máxima cantidad de recursos del sistema, así como eliminar la actividad de otros actores de la amenaza y eliminar su presencia de la máquina infectada.

Además, actúa como un gotero para diferentes RAT y un cripto minero basado en XMRig que extrae Monero y una criptomoneda alternativa llamada VDS o Vollar.

Guardicore informó que los atacantes tenían toda su infraestructura en máquinas comprometidas, incluido su servidor primario de comando y control ubicado en China, que fue encontrado comprometido por más de un grupo de ataque.

> *«Entre los archivos estaba la herramienta de ataque MS-SQL, responsable de escanear rangos de IP, forzar la base de datos de destino y ejecutar comandos de forma remota»,* según la empresa de seguridad cibernética.
>
> *«Además, encontramos dos programas CNC con GUI en chino, una herramienta para modificar los valores hash de los archivos, un servidor de archivos HTTP portátil (HFS), un servidor Serv-U FTP y una copia del mstsc.exe ejecutable (Microsoft Terminal Services Client) que solía conectarse con las víctimas a través*

> *de RDP».*

Una vez que un cliente de Windows infectado hace ping al servidor C2, este último también recibe una variedad de detalles sobre la máquina, como su IP pública, ubicación, versión del sistema operativo, nombre de la computadora y modelo de CPU.

Al asegurar que los dos programas C2 instalados en el servidor con sede en China fueron desarrollados por dos proveedores diferentes, Guardicore dijo que existen similitudes en sus capacidades de control remoto, es decir, descargar archivos, instalar nuevos servicios de Windows, registro de teclas, captura de pantalla, activación de la cámara y el micrófono, e incluso iniciar un ataque de denegación de servicio distribuido (DDoS).

Alrededor de medio millón de máquinas que ejecutan el servicio de base de datos Microsoft SQL, la campaña es otra indicación de que los atacantes persiguen servidores de bases de datos mal protegidos en un intento por desviar información confidencial. Es esencial que los servidores MS-SQL que están expuestos a Internet estén protegidos con credenciales sólidas.

> *«Lo que hace que estos servidores de bases de datos sean atractivos para los atacantes además de su valiosa potencia de CPU es la gran cantidad de datos que tienen. Estas máquinas posiblemente almacenan información personal como nombres de usuario, contraseñas, números de tarjetas de crédito, etc., que pueden caer en manos del atacante con solo una simple fuerza bruta»*, dijeron los investigadores de Guardicore.