Investigadores de seguridad cibernética descubrieron una puerta trasera previamente indocumentada diseñada para servidores Microsoft SQL, que podría permitir a un hacker remoto controlar de forma sigilosa un sistema ya comprometido.

Apodado como Skip-2.0, el malware de backdoor es una herramienta posterior a la explotación que se ejecuta en la memoria y permite a los atacantes remotos conectarse a cualquier cuenta del servidor que ejecute MSSQL versión 11 y versión 12 mediante el uso de una *«contraseña mágica».*

El malware logra permanecer en el servidor MS SQL de la víctima sin ser detectado, luego de habilitar las funciones de registro de la máquina comprometida, la publicación de eventos y mecanismos de auditoría cada vez que se utiliza la «contraseña mágica».

Con estas capacidades, un atacante puede copiar, modificar o eliminar sigilosamente el contenido almacenado en una base de datos, cuyo impacto varía de una aplicación a otra integrada con los servidores de destino.

> *«Esto podría usarse, por ejemplo, para manipular monedas en el juego para obtener ganancias financieras. Ya se han informado manipulaciones de la base de datos de monedas en juegos por parte de los operadores Winnti»*, dijeron los investigadores.

En el último reporte publicado por la compañía de seguridad cibernética, ESET, los investigadores atribuyeron la puerta trasera Skip-2.0 a un grupo de actores de amenazas patrocinado por el grupo chino llamado Winnti Group, debido a que el malware contiene múltiples similitudes con otras herramientas conocidas de Winnti Group, en particular, PortReuse backdoor y ShadowPad.

Documentado por primera vez por ESET a inicios de este mes, PortReuse backdoor es un implante de red pasivo para Windows que se inyecta en un proceso de ejecución que ya está corriendo en un puerto TCP, «reutiliza» un puerto ya abierto y espera un paquete mágico entrante para activar el código del malware.

Visto por primera vez durante el ataque de la cadena de suministro contra el fabricante de software NetSarang en julio de 2017, ShadowPad es una backdoor de Windows que los atacantes implementan en las redes de las víctimas para obtener capacidades flexibles de control remoto.

Al igual que otras cargas útiles del grupo Winnti, Skip-2.0 también utiliza un iniciador cifrado VMProtected, un empaquetador personalizado, un inyector de cargador interno y un marco de enganche para instalar la puerta trasera, y persiste en el sistema objetivo cuando explota una vulnerabilidad de secuestro de DLL en un proceso de Windows que pertenece a un servicio de inicio del sistema.

Debido a que el malware Skip-2.0 es una herramienta posterior a la explotación, un atacante primero debe comprometer los servidores MSSQL específicos para tener los privilegios administrativos necesarios para lograr persistencia y sigilo.

> *«Tenga en cuenta que a pesar de que MSSQL Server 11 y 12 no son las versiones más recientes, son las más utilizadas según los datos de Censys»*, dijeron los investigadores.