CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Software malicioso

Fecha: 10/03/2023

Problemática: Nuevo malware “Maggie” para servidores Microsoft SQL Server

Correlativo: AC-0025

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Recientemente un nuevo malware de puerta trasera denominado “Maggie” fue diseñado para afectar servidores Microsoft SQL. Esta pieza de malware fue descubierta recientemente por analistas en ciberseguridad alemanes. Según los investigadores, los datos de telemetría han demostrado que la afectación de este malware ha sido más recurrente en países como Corea del Sur, India, Vietnam, China, Rusia, Tailandia, Alemania y los Estados Unidos. Sin embargo, puede extenderse a otros países del mundo en los próximos días.

SITUACIÓN

Este nuevo malware se gestiona a través de consultas SQL para ejecutar comandos e interactuar con archivos. Puede aplicar la fuerza bruta a los inicios de sesión de administrador en otros servidores de Microsoft SQL y actuar como cabeza de puente dentro del servidor.
Además, Maggie ofrece una funcionalidad de redirección TCP simple. Permite a los atacantes remotos conectarse a cualquier dirección IP que el servidor MS-SQL comprometido pueda alcanzar.
La puerta trasera se esconde como una DLL de procedimiento almacenado extendido (sqlmaggieAntiVirus_64[.]dll.
Maggie abusa del comportamiento de los archivos de procedimientos almacenados extendidos para permitir el acceso remoto de puerta trasera con 51 comandos. La lista de comandos incluye cuatro comandos Exploit para confiar en fallas conocidas para algunas acciones.
Una variedad de comandos permite consultar los detalles del sistema, ejecutar programas (como el proxy SOCKS5), interactuar con archivos y carpetas, permitir servicios de escritorio remoto y reenvío de puertos.
Las contraseñas de administrador se fuerzan brutamente a través de los comandos WinSockScan y SqlScan después de definir un recuento de subprocesos y un archivo de lista de contraseñas. Posteriormente, se agrega al servidor un usuario de puerta trasera codificado de forma rígida.
Además, los atacantes pueden agregar argumentos a estos comandos. En algunos casos, Maggie tiene instrucciones de uso para los argumentos admitidos.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

RECOMENDACIONES

Recomendaciones generales aplicando Mittre:

- Filtrar tráfico de red: El tráfico a las redes de anonimato conocidas y la infraestructura C2 se puede bloquear mediante el uso de listas de bloqueo y permisos de red. Cabe señalar que este tipo de bloqueo puede evitarse mediante otras técnicas como Domain Fronting.
- Prevención de intrusiones en la red: Los sistemas de detección y prevención de intrusiones en la red que usan firmas de red para identificar el tráfico de malware adversario específico se pueden usar para mitigar la actividad a nivel de red.
- Inspección SSL/TLS: Si es posible inspeccionar el tráfico HTTPS, las capturas se pueden analizar en busca de conexiones que parezcan estar al frente del dominio.

Adicionalmente a las recomendaciones dadas en el párrafo anterior, se recomienda a los usuarios de sistemas SQL Server estar atentos al parche de actualización que emitirá el fabricante para mitigar la falla encontrada.

DICCIONARIO DE DATOS

Ataque de fuerza bruta: Procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.
Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit).
Código arbitrario (RCE): Hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos.
Parche de seguridad: Conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos.

REFERENCIAS

1. https://medium.com/@DCSO_CyTec/mssql-meet-maggie-898773df3b01
2. https://conciber.gob.gt/?page_id=1208
3. https://attack.mitre.org/techniques/T1090/
4. https://github.com/DCSO/Blog_CyTec/commit/d4f88b33c74488a9b5fdd2443364ff5da857d035