Nro. Alerta:	EC-2022-93	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	12-octubre-2022	**Backdoor Maggie**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Backdoor
Nivel de riesgo: Alto

II. INTRODUCCIÓN

Maggie es el nuevo backdoor diseñado para afectar servidores Microsoft SQL a nivel global.

Maggie puede forzar los inicios de sesión en otros servidores MS SQL y añadir un nuevo usuario backdoor codificado después de forzar los inicios de sesión del administrador

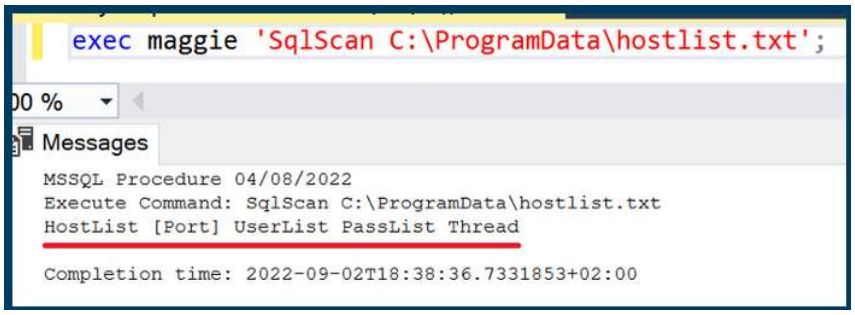

Figura 1. Parámetros válidos para el comando SqlScan
Fuente: DCSO CyTec Blog

Length	Type	String
0000001C	C	Socks5 Stopped Successfully
00000017	C	Socks5 Stopped Failure
00000015	C	Socks5 Isn't Running
00000016	C	Socks5 Thread Failure
0000001C	C	Socks5 Running Successfully
00000019	C	Socks5 Thread Successful
00000017	C	Socks5 Already Running

Figura 2. Mensajes de depuración para la funcionalidad SOCKS5
Fuente: DCSO CyTec Blog

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-93	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	12-octubre-2022	**Backdoor Maggie**	V 1.1

III. ALERTA

Este malware fue descubierto recientemente por los analistas alemanes Johann Aydinbas y Axel Wauer de DCSO CyTec. 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.

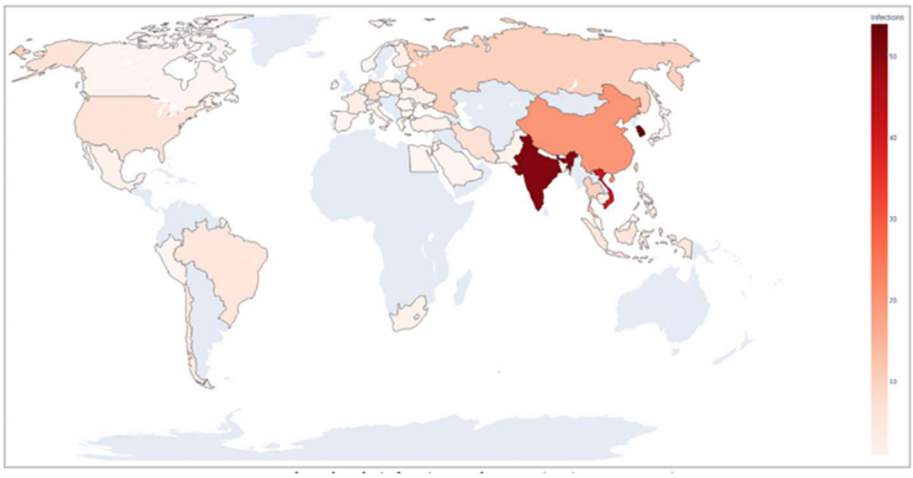

Figura 3. Infecciones de Backdoor Maggie en el mundo.
Fuente: DCSO CyTec Blog

Según los investigadores Maggie puede forzar los inicios de sesión en otros servidores MS SQL y añadir un nuevo usuario backdoor codificado después de forzar los inicios de sesión del administrador.

Maggie se presenta en forma de DLL "procedimiento almacenado extendido", que es un tipo especial de extensión utilizada por los servidores Microsoft SQL. Una vez cargado en un servidor por un atacante, se controla únicamente mediante consultas SQL y ofrece una variedad de funcionalidades para ejecutar comandos, interactuar con archivos y funcionar como un puente de red en el entorno del servidor infectado".

Tras su instalación, el backdoor incluye múltiples comandos para consultar información del sistema; interactuar con archivos y carpetas; ejecutar programas; y diversas funcionalidades relacionadas con la red como: habilitar TermService, ejecutar un servidor proxy Socks5 o configurar el reenvío de puertos.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-93	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	12-octubre-2022	**Backdoor Maggie**	V 1.1

El backdoor es capaz, según se informa, de realizar una simple redirección TCP, lo que le permite funcionar como un puente de red desde Internet a cualquier dirección IP alcanzable por el servidor infectado. El backdoor redirige entonces las conexiones entrantes a una IP y un puerto designado si la IP de origen coincide con una máscara IP especificada por el usuario. Esto permite la reutilización de puertos, haciendo que la redirección sea transparente para los usuarios autorizados, mientras que cualquier otra IP de conexión es capaz de utilizar el servidor sin ninguna interferencia o conocimiento del backdoor Maggie.

Cabe destacar que de un total de 600.000 servidores analizados por investigadores, se detectaron 285 servidores comprometidos en 42 países diferentes, sin embargo aún no es posible perfilar qué actor de amenazas se encuentra detrás de estos ataques ni cuales son sus motivaciones u objetivos.

IV. VECTOR DE ATAQUE

- Fuerza bruta
- Conexión Proxy

V. IMPACTO:

- Los atacantes pueden utilizar técnicas de fuerza bruta para acceder a las cuentas cuando se desconocen las contraseñas o cuando se obtienen los hashes de las mismas. Sin conocer la contraseña de una cuenta o conjunto de cuentas, un adversario puede adivinar sistemáticamente la contraseña mediante un mecanismo repetitivo o iterativo. La fuerza bruta de las contraseñas puede tener lugar a través de la interacción con un servicio que compruebe la validez de esas credenciales o fuera de línea contra los datos de credenciales previamente adquiridos, como los hashes de las contraseñas. (T1110: Brute Force)

- Los atacantes pueden utilizar un proxy de conexión para dirigir el tráfico de red entre sistemas o actuar como intermediario de las comunicaciones de red hacia un servidor de mando y control para evitar las conexiones directas a su infraestructura. Existen muchas herramientas que permiten redirigir el tráfico a través de proxy o redireccionamiento de puertos, incluyendo HTRAN, ZXProxy y ZXPortMap. Los adversarios utilizan estos tipos de proxy para gestionar las comunicaciones de mando y control, reducir el número de conexiones de red salientes simultáneas, proporcionar resistencia ante la pérdida de la conexión o

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

utilizar las rutas de comunicación de confianza existentes entre las víctimas para evitar sospechas. Los adversarios pueden encadenar varios proxy para disfrazar aún más el origen del tráfico malicioso.

Los atacantes también pueden aprovechar los esquemas de enrutamiento de las redes de entrega de contenidos (CDN) para delegar el tráfico de mando y control. (T1090: Connection Proxy)

VI. INDICADORES DE COMPROMISO:

En la siguiente Tabla se indican IoC de este Backdoor.

Ítem	Parámetro	Descripción
1	**Firmado digitalmente por:**	DEEPSoft Co. Ltd
2	**País de Origen de Maggie**	South Korea
3	**Archivo:**	Extended Stored Procedure DLL (sqlmaggieAntiVirus_64.dll)
4	**Ubicación de los archivos:**	C:\ProgramData\success.dat <MAGGIE_LOCATION>\success.dat Failure.dat AccessControl.Dat
5	**Maggie ESP DLLs - Hash**	f29a311d62c54bbb01f675db9864f4ab0b3483e6cfdd15a745d4943029dcdf14 a375ae44c8ecb158895356d1519fe374dc99c4c6b13f826529c71fb1d47095c3 eb7b33b436d034b2992c4f40082ba48c744d546daa3b49be8564f2c509bd80e9 854bb57bbd22b64679b3574724fafd7f9de23f5f71365b1dd8757286cec87430
6	**RAR SFX with Maggie - Hash**	4311c24670172957b4b0fb7ca9898451878faeb5dcec75f7920f1f7ad339d958 d0bc30c940b525e7307eca0df85f1d97060ccd4df5761c952811673bc21bc794
7	**ITW URLs**	http://58.180.56.28/sql64.dll http://106.251.252.83/sql64.dll http://183.111.148.147/sql64.dll http://xw.xxuz.com/VV61599.exe http://58.180.56.28/vv61599.exe
8	**Hardcoded User-Agent**	Mozilla/4.0 (compatible)

Tabla 1. IoC de Backdoor Maggie

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-93	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	12-octubre-2022	**Backdoor Maggie**	V 1.1

VII. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Instalar actualizaciones disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de la organización.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- Actualizar el sistema operativo de los equipos a las últimas versiones.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Diseñar una política de revisión de logs, que permita detectar comportamientos fuera de lo normal en procesos legítimos del sistema.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-93	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	12-octubre-2022	**Backdoor Maggie**	V 1.1

- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social. Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 “Concienciación con educación y capacitación en seguridad de la información” o NIST PR.AT-1: “Todos los usuarios se encuentran entrenados e informados”, a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. BIBLIOGRAFÍA.

- **Toulas, B. (2022).** *Hundreds of Microsoft SQL servers backdoored with new malware.* BleepingComputer , recuperado el 11 de octubre de 2022 de: https://www.bleepingcomputer.com/news/security/hundreds-of-microsoft-sql-servers-backdoored-with-new-malware/

- **Krasnogolovy, V. (2022).** *Hundreds of Microsoft SQL servers backdoored with new Backdoor.* GridinSoft.blog , recuperado el 11 de octubre de 2022 de: https://gridinsoft.com/blogs/maggie-backdoor-in-microsoft-sql/

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-93	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	12-octubre-2022	**Backdoor Maggie**	V 1.1

- **Haynes, I. (2022).** *Maggie malware has gained backdoor access to hundreds of Microsoft SQL servers.* Techzinw , recuperado el 11 de octubre de 2022 de: https://www.techzine.eu/news/security/90934/maggie-malware-has-gained-backdoor-access-to-hundreds-of-microsoft-sql-servers/

- **Goldman, J. (2022).** *New MSSQL Backdoor 'Maggie' Infects Hundreds of Servers Worldwide.* eSecurity Planet , recuperado el 11 de octubre de 2022 de: https://www.esecurityplanet.com/threats/mssql-backdoor-maggie/

- **CyberSecure (2022).** *Backdoor Maggie dirigido a Servidores MS SQL a nivel global.* Entel CyberSecure, recuperado el 11 de octubre de 2022 de: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1380/

- **Medium (2022).** *MSSQL, meet Maggie*. DCSO CyTec Blog, recuperado el 11 de octubre de 2022 de: https://medium.com/@DCSO_CyTec/mssql-meet-maggie-898773df3b01

- **MITRE ATT&CK (2022).** *Brute Force*. Techniques, recuperado el 11 de octubre de 2022 de: https://attack.mitre.org/techniques/T1110/

- **MITRE ATT&CK (2022).** *Proxy*. Techniques, recuperado el 11 de octubre de 2022 de: https://attack.mitre.org/techniques/T1090/

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec