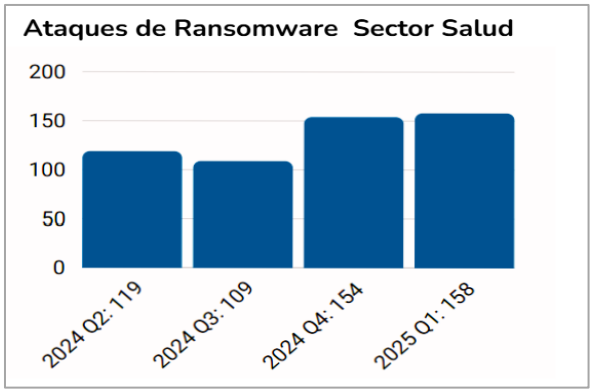
El Centro de análisis e intercambio de información sanitaria Health-ISAC ha venido observando una tendencia continua de incidentes de ciberseguridad y violaciones de datos que han afectado a organizaciones del sector salud durante el último año. Aunque los eventos de ransomware disminuyeron levemente en el tercer trimestre de 2024, estos continuaron aumentando en el cuarto trimestre de 2024 y primer trimestre de 2025. Las vulnerabilidades en **proveedores de VPN** y las **credenciales comprometidas** siguen siendo un riesgo constante para las organizaciones.

Health-ISAC identificó 220 alertas dirigidas a organizaciones con infraestructura potencialmente vulnerable. El presente Boletín ofrece información estadística sobre ataques de ransomware, tendencias del crimen cibernético y publicaciones en foros maliciosos que podrían impactar al sector Salud.

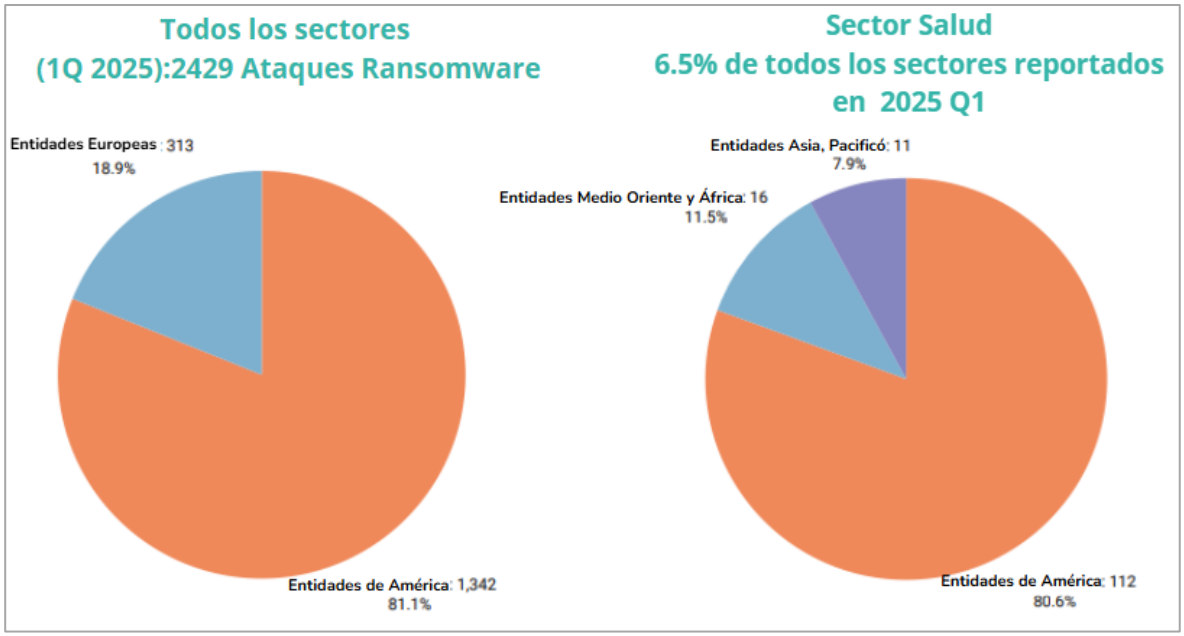
Estadísticas del sector Salud:

Durante el primer trimestre de 2025, se reportaron 158 ataques de Ransomware en el sector Salud, representando el 6.5% de todos los sectores (2,429 ataques en total). Desde 2021, se han rastreado 1,370 violaciones en el sector Salud, lo que representa el 5.8% del total de 23,606 violaciones registradas globalmente.



Análisis de eventos globales:

A continuación, se puede observar el comportamiento de los ataques en el sector Salud a nivel global.



Tendencias de alertas dirigidas al sector Salud

- **Software BeyondTrust Potencialmente Vulnerable**

El 28 de marzo de 2025, se notificaron productos potencialmente vulnerables de BeyondTrust "Privileged Remote Access" o "Remote Support" en entornos de organizaciones del sector Salud. Se enviaron 62 alertas para que los equipos de respuesta de las entidades investigaran y aplicaran los parches necesarios.

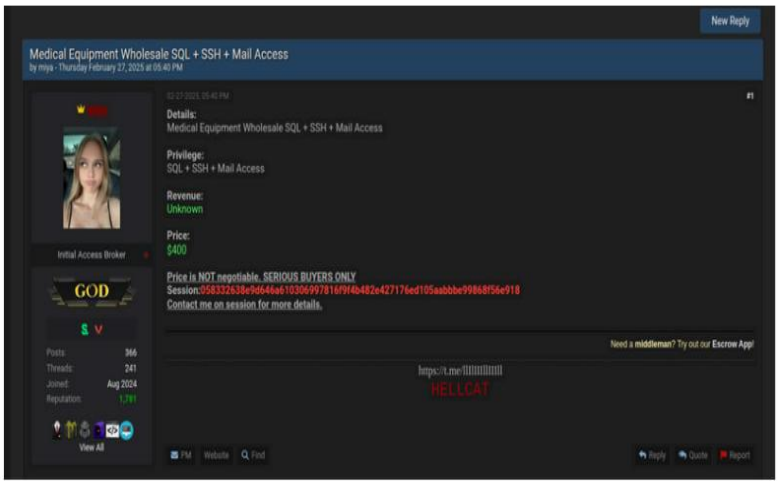
CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- **Vulnerabilidad Crítica en Next.js Middleware**

El 26 de marzo de 2025, se anunció una vulnerabilidad de evasión de autorización crítica que afecta a versiones de Next.js (11.1.4 a 13.5.6, 14.x < 14.2.25, 15.x < 15.2.3). Se emitieron 33 alertas específicas a organizaciones del sector Salud debido a su dependencia en aplicaciones web críticas.

- **Actividad en Foros Subterráneos**

Actores maliciosos publicaron datos robados y/o accesos comprometidos a organizaciones del sector Salud en foros como BreachForums. Se destaca el actor MIYAK000, quien ofreció accesos a una clínica quirúrgica y a una empresa de gestión de ciclo de ingresos médicos en EE.UU.



- **Perfil del Actor de Amenaza: INC Ransomware**

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

INC Ransomware, también conocida como GOLD IONIC, es una operación de ransomware como servicio activo desde julio de 2023. Esta se encuentra enfocada en sectores de alto valor como Salud y utiliza técnicas avanzadas para maximizar el impacto operacional, así como extorsionar con grandes sumas de dinero.

Guía de mitigación de Ransomware

- **Gestión de parches**

  Actualizar y aplicar parches periódicamente a todos los sistemas, especialmente a las aplicaciones públicas como Citrix NetScaler, para mitigar vulnerabilidades conocidas (por ejemplo, CVE-2023-3519).

- **Seguridad del correo electrónico**
  - Implementar soluciones avanzadas de filtrado de correo electrónico para detectar y bloquear intentos de phishing.
  - Capacitar al personal para que reconozcan los correos electrónicos de phishing y reporten actividades sospechosas.

- **Protección Endpoint**
  - Implementar soluciones de detección y respuesta de endpoints (EDR) para identificar y bloquear actividades maliciosas.
  - Activar listas blancas de aplicaciones para evitar la ejecución de software no autorizado.

- **Control de acceso**
  - Aplicar el principio de Mínimo Privilegio para limitar el acceso de los usuarios únicamente a lo estrictamente necesario.

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

- Implementar la autenticación multifactor (MFA) para todas las cuentas, especialmente para el acceso remoto.

- **Segmentación de red**
  - Aislar los sistemas críticos dentro de redes segmentadas para evitar el movimiento lateral.
  - Restringir el acceso RDP únicamente a direcciones IP de confianza y monitorear la actividad inusual.

- **Copia de seguridad y recuperación**
  - Realizar copias de seguridad periódicas y sin conexión de los datos críticos y probar los procedimientos de recuperación.
  - Asegurarse de que las copias de seguridad estén cifradas y almacenadas en una ubicación segura.

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) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

Fuentes:

- https://attack.mitre.org/groups/G1032/
- https://cyble.com/threat-actor-profiles/inc-ransom/
- https://gbhackers.com/inc-ransom-group-exfiltratration/
- https://www.secureworks.com/research/threat-profiles/gold-ionic

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