TIC

Informe de apreciación

Sector Salud

COLCERT

Contenido

Informe de apreciación
Sector Salud

COLCERT IN-20260703-034

TLP: CLEAR

INTRODUCCIÓN

En un entorno donde la digitalización de los servicios médicos es fundamental para la atención al paciente, la seguridad de la información se convierte en un pilar de la ética y la continuidad operativa. El presente informe analiza el comportamiento de actores de amenazas con actividad documentada hasta mayo de 2026, los cuales han demostrado un interés persistente en infraestructuras de la región. Mediante la evaluación de más de 3,700 indicadores técnicos recopilados, este documento busca establecer un marco de referencia que permita a las instituciones de salud anticiparse a vectores de ataque que comprometan la privacidad de los datos sensibles y la estabilidad de los sistemas críticos de diagnóstico y tratamiento.

Lineamientos

- Identificación y monitoreo de adversarios activos.
- Análisis de indicadores de infraestructura de red (FQDN e IP).
- Detección de artefactos maliciosos mediante firmas de archivos.
- Evaluación de la vigencia de las amenazas en el tiempo.
- Protección de la confidencialidad de datos médicos y personales.
- Fortalecimiento de la resiliencia operativa frente a incidentes cibernéticos.

Informe de apreciación
Sector Salud

COLCERT IN-20260703-034

TLP: CLEAR

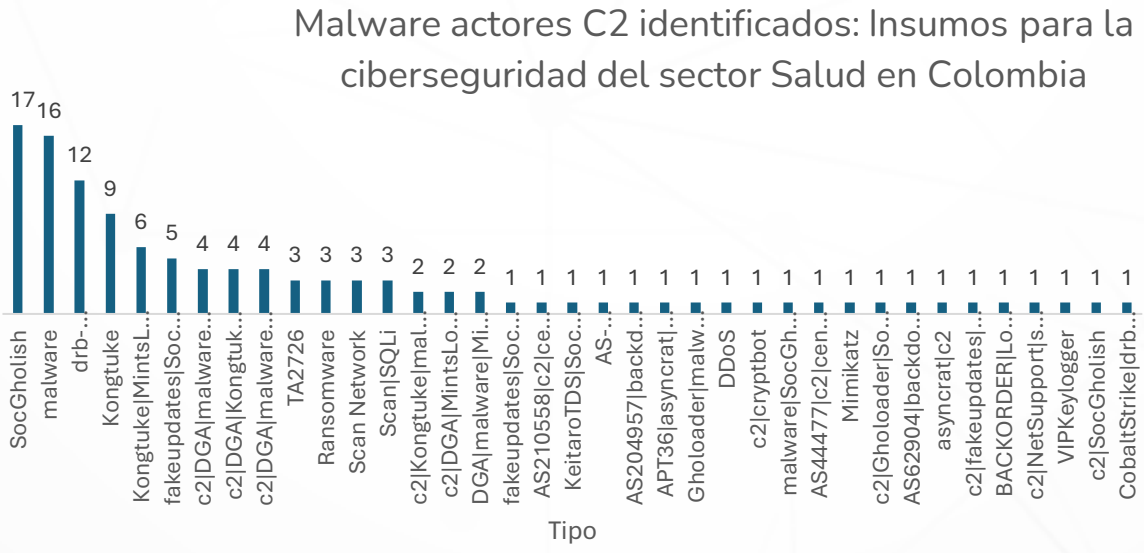
RESUMEN EJECUTIVO

El panorama actual de ciberseguridad para el sector salud se caracteriza por una exposición crítica ante diversos grupos de adversarios con actividad reciente y persistente en la región. El análisis de los datos recolectados hasta mayo de 2026 revela un volumen masivo de amenazas, con más de 3,700 indicadores de compromiso que apuntan a intentos de intrusión mediante el uso de infraestructuras de red y archivos maliciosos. Esta convergencia de actores especializados en espionaje y operaciones financieras representa un riesgo directo para la confidencialidad de la información médica y la disponibilidad de los servicios asistenciales. Por lo tanto, es imperativo transicional hacia un modelo de defensa proactiva que priorice la protección de datos sensibles y la resiliencia de la infraestructura tecnológica frente a este ecosistema de amenazas en constante evolución.

Aspectos clave

- Fortalecer la ciberinteligencia en el sector salud en Colombia
- Seguimiento al comportamiento de actores que afectan el sector
- Revisión de fuentes OSINT, comerciales e institucionales
- Detección y respuesta ante incidentes
- Protección de activos del sector salud en Colombia

Hallazgos Clave



- Se ha identificado una persistente actividad de diversos grupos de amenazas con presencia documentada en la región, los cuales demuestran un interés activo en infraestructura local.
- El análisis de datos revela una concentración masiva de indicadores de compromiso vinculados a infraestructuras de red (dominios y direcciones IP), sumando más de 3,200 elementos que representan vectores potenciales de intrusión.
- La presencia de múltiples actores con historial de espionaje y operaciones financieras sugiere un riesgo elevado de exfiltración de historias clínicas y datos sensibles de pacientes.
- Se observa una actualización constante de las tácticas de los adversarios, con registros de actividad tan recientes como abril y mayo de 2026.

Recomendaciones Prioritarias

- Fortalecer de inmediato el monitoreo sobre los activos de red externos, priorizando la validación de dominios y conexiones a direcciones IP sospechosas identificadas en el análisis.
- Implementar protocolos de segmentación de red estrictos para aislar sistemas de diagnóstico y bases de datos médicos de los segmentos con acceso a internet.
- Establecer un programa de actualización de seguridad urgente para mitigar las vulnerabilidades que los actores identificados suelen explotar para ganar acceso inicial.

Conclusión Estratégica

El sector salud enfrenta un panorama de amenazas sofisticado donde el valor de la información médica y la continuidad del servicio son los objetivos principales. La alta disponibilidad de indicadores técnicos sugiere que la prevención no debe ser reactiva;

se requiere una postura proactiva que integre la inteligencia de amenazas en la toma de decisiones para garantizar la integridad operativa y la privacidad del paciente.

OBJETIVO Y ALCANCE

Objetivo

Proporcionar una visión técnica y estratégica sobre las amenazas que impactan al sector salud, analizando el comportamiento de actores maliciosos y la vigencia de sus indicadores de compromiso para fortalecer las capacidades de detección, respuesta y prevención de incidentes que puedan comprometer la atención médica.

Alcance

El presente análisis se fundamenta en la correlación de inteligencia estratégica y datos operativos para identificar vectores de ataque dirigidos específicamente a la infraestructura crítica de servicios médicos. Dado que el sector salud es el eje de la integridad humana y la protección de la información sensible en Colombia, este alcance define el marco de monitoreo sobre los actores de amenazas más persistentes identificados en el ecosistema regional. Esto permite transformar los indicadores técnicos, como firmas de archivos y rastros de red, en una defensa proactiva contra el robo de datos clínicos, el secuestro de información y cualquier actividad que comprometa la continuidad de la atención asistencial.

Este informe abarca el análisis de:

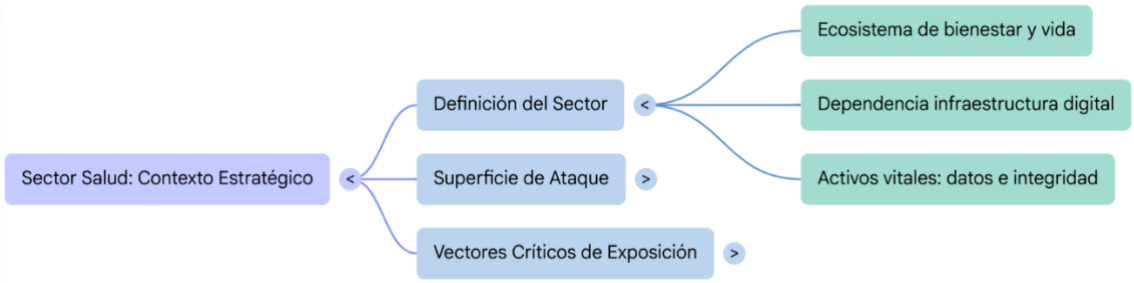
- Grupos de adversarios con actividad reciente y relevancia geográfica documentada.
- Consolidación y categorización de más de 3,700 indicadores técnicos, incluyendo nombres de dominio (FQDN), direcciones de red y firmas de archivos (hashes).
- Evaluación de tendencias de amenazas observadas hasta mayo de 2026.
- Definición de lineamientos estratégicos para la protección de activos críticos específicos del ecosistema de salud.

CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR

Definición y Entendimiento del Sector

El sector salud se define como un ecosistema crítico encargado de la preservación de la vida y el bienestar ciudadano, cuya operatividad depende de una red compleja de servicios de asistencia, investigación y suministro. En la actualidad, este sector ha evolucionado hacia una dependencia absoluta de la infraestructura digital para la gestión de historias clínicas electrónicas, sistemas de telemetría médica y plataformas de interoperabilidad entre entidades.

Esta transformación convierte a la disponibilidad e integridad de los datos en activos tan vitales como los insumos médicos físicos, ya que cualquier interrupción en los sistemas de información puede traducirse directamente en riesgos para la seguridad

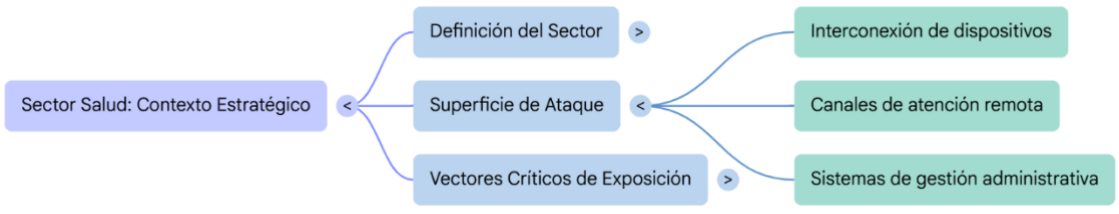


del paciente y la capacidad de respuesta ante emergencias sanitarias.

Superficie de Ataque

La superficie de ataque en el sector salud se ha expandido significativamente debido a la interconexión de dispositivos médicos y la apertura de canales digitales para la atención remota. Esta exposición no solo abarca los sistemas tradicionales de gestión administrativa, sino que se extiende a infraestructuras especializadas que, a menudo, carecen de capas de seguridad robustas, facilitando la entrada de los actores identificados en este análisis.

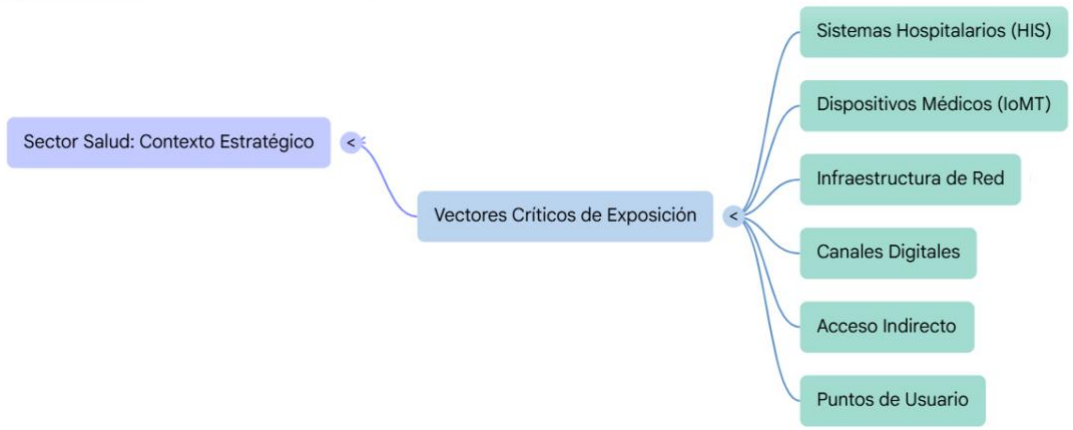
A continuación, se destacan los puntos más vulnerables de este ecosistema:



Vectores Críticos de Exposición:

- Sistemas de Información Hospitalaria (HIS): Bases de datos centrales que almacenan registros sensibles y son el objetivo principal de intentos de exfiltración.

- Dispositivos Médicos Interconectados (IoMT): Equipos de diagnóstico y monitoreo que operan en red, a menudo con protocolos de seguridad heredados.
- Infraestructura de Red y Dominios: Puntos de conexión externa que, según los datos analizados, concentran la mayor cantidad de indicadores de riesgo (FQDN y direcciones IP).
- Portales de Pacientes y Telemedicina: Aplicaciones web que actúan como puntos de entrada para posibles intrusiones mediante la suplantación de identidad.
- Cadena de Suministro Digital: Conexiones con proveedores externos de servicios en la nube y software de gestión que pueden servir como vectores de acceso indirecto.
- Puestos de Trabajo y Dispositivos de Usuario: Estaciones de consulta donde el factor humano y los archivos maliciosos representan un riesgo constante de infección inicial.



PANORAMA ACTUAL DE AMENAZAS

El sector salud en Colombia atraviesa un periodo de vulnerabilidad extrema, consolidándose como uno de los objetivos prioritarios para el cibercrimen organizado en el primer semestre de 2026. Recientes incidentes contra entidades reguladoras nacionales han confirmado la ejecución de ataques de alta criticidad, los cuales han resultado en la descarga masiva de información

confidencial y datos personales sensibles. La magnitud de la amenaza es sistemática: se han registrado más de 23 millones de intentos de ataque y sondeos en un solo mes, impulsados por el uso de inteligencia artificial para acelerar la explotación de vulnerabilidades y la proliferación de infraestructuras maliciosas en canales de la Dark Web. Este ecosistema de amenazas no solo busca el lucro económico mediante el secuestro de datos, sino que impacta directamente la soberanía de la información clínica de los ciudadanos.

TITULO	FECHA	FUENTE / ENLACE
Incidente de seguridad de alta criticidad en sistema SUPERARGO	31/03/2026	Supersalud
Reporte de 23 millones de intentos de ciberataques sistemáticos	29/03/2026	Caracol Radio
Detección de descarga masiva de documentos y datos sensibles (1.6% bodega)	7/04/2026	La Nota Económica
Informe Trimestral: Evolución de amenazas a dispositivos médicos e IA	29/04/2026	Health-ISAC
Aumento del 389% en víctimas de ransomware y ataques impulsados por IA	1/05/2026	Portal Innova
Alerta por robo masivo de credenciales en sector hospitalario (RedLine/Lumma)	1/05/2026	FortiRecon / Portal Innova

Tipología de Eventos Identificados

El análisis de los datos recolectados revela una infraestructura de ataque diversificada que prioriza el reconocimiento de red y el despliegue de artefactos maliciosos. La predominancia de identificadores de dominio y direcciones IP sugiere una fase avanzada de preparación para el movimiento lateral y la comunicación con centros de control externos, tácticas comunes en incidentes que buscan el secuestro de sistemas críticos hospitalarios. Asimismo, la presencia de múltiples firmas digitales de archivos confirma un riesgo latente de ejecución de software no autorizado en estaciones de trabajo médicas, orientado a la persistencia dentro de la red institucional para la posterior extracción de activos de información sensible.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector
FQDN (Dominios)	2113	Inteligencia de Amenazas / MISP	Identificación de portales falsos y centros de comando de adversarios.
Direcciones IP	1179	Inteligencia de Amenazas / MISP	Detección de conexiones no autorizadas desde infraestructura médica.
Hashes (MD5, SHA-1, SHA-256)	479	Repositorios de Malware / Malpedia	Bloqueo de archivos maliciosos en equipos de diagnóstico y servidores.
URL	21	Inteligencia de Amenazas / MISP	Prevención de enlaces de descarga para campañas de suplantación.

Fuente: https://www.datos.gov.co/stories/s/rgem-8mys

Análisis de la Distribución de Amenazas

A partir de la tipología presentada, se extraen las siguientes conclusiones clave sobre el comportamiento de los eventos en el sector:

- Predominio de Vectores de Red: La infraestructura maliciosa se concentra masivamente en nombres de dominio (FQDN), representando el 55.7% del total de los hallazgos con 2,113 registros. Esto indica una estrategia de los adversarios basada en el uso de sitios web fraudulentos y centros de comando externos para la exfiltración de datos.

- Alta Exposición de Direcciones de Internet: Se identificaron 1,179 direcciones IP únicas (aprox. 31.1% de la muestra), lo que sugiere una red activa de servidores distribuidos para facilitar ataques de fuerza bruta o escaneos de vulnerabilidades en los sistemas hospitalarios.

- Diversidad de Artefactos Maliciosos: Los registros de firmas digitales (hashes MD5, SHA-1 y SHA-256) suman un total de 479 indicadores únicos. Esta distribución evidencia el uso de múltiples variantes de software dañino diseñado para evadir detecciones básicas en estaciones de trabajo y servidores clínicos.

- Vigencia Operativa de los Adversarios: La distribución temporal muestra una actividad crítica y reciente, con grupos de amenazas actualizando sus

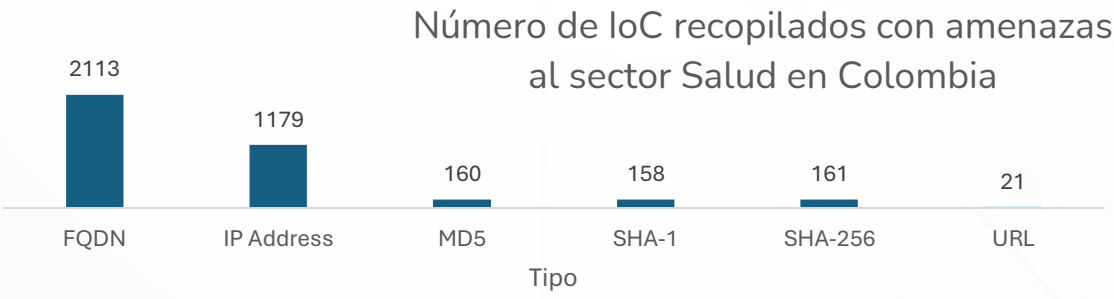
- infraestructuras en fechas tan próximas como abril y mayo de 2026. Esto confirma que los adversarios están en una fase de operación activa y no solo de reconocimiento histórico.

- Concentración de Actores Específicos: El análisis identifica a 12 adversarios principales con presencia documentada en la región. La distribución de estos actores sugiere una mezcla de motivaciones que van desde el espionaje (extracción de registros médicos) hasta el beneficio económico (secuestro de información institucional).

- Baja Incidencia de URLs Específicas: Con solo 21 registros identificados, el volumen de URLs es significativamente menor comparado con los dominios raíz, lo que implica que los atacantes prefieren rotar rápidamente las rutas específicas de sus archivos maliciosos mientras mantienen estables sus dominios de base.

INDICADORES DE COMPROMISO (IoCs)

El análisis de los Indicadores de Compromiso permite identificar las huellas técnicas dejadas por los adversarios durante las fases de reconocimiento y explotación. Estos elementos son fundamentales para la configuración de controles preventivos, ya que representan activos de red y archivos que han sido verificados como parte de infraestructuras maliciosas activas hasta mayo de 2026. Para el sector salud, estos indicadores son la base para prevenir el acceso no autorizado a sistemas de gestión hospitalaria y la protección de estaciones de trabajo asistenciales.



Análisis Cuantitativo de Inteligencia

- Concentración en Infraestructura Externa: El mayor volumen de inteligencia se centra en nombres de dominio (FQDN), con un total de 2,113 registros, lo que sugiere una alta dependencia de los atacantes en sitios web fraudulentos para sus operaciones.
- Capacidad de Conectividad Directa: Se han identificado 1,179 direcciones IP que funcionan como puntos de contacto para el tráfico de comando y control (C2), facilitando la comunicación con sistemas internos comprometidos.
- Diversidad de Artefactos de Ejecución: La presencia de 479 registros de firmas de archivos (MD5, SHA-1, SHA-256) evidencia un ecosistema de malware variado, diseñado para evadir defensas estáticas mediante diferentes variantes de código.
- Actualización de Amenazas en Tiempo Real: La inteligencia recolectada muestra una vigencia operativa crítica, con registros de actividad de grupos de amenazas actualizados durante los meses de abril y mayo de 2026.

Resumen de IoCs Relevantes

La siguiente tabla sintetiza los componentes de inteligencia extraídos de la plataforma, categorizando su naturaleza técnica y el nivel de riesgo que representan para la continuidad de los servicios de salud y la integridad de los datos clínicos.

Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
FQDN (Dominios)	Nombres de dominio utilizados para alojar contenido malicioso o recibir datos exfiltrados.	Crítico
Direcciones IP	Puntos de red específicos desde donde se originan ataques o se gestionan servidores C2.	Alto
Hashes de Archivo	Identificadores únicos de binarios maliciosos (ejecutables, scripts o documentos cargados).	Alto
URLs	Direcciones web específicas para la descarga directa de malware o captura de credenciales.	Medio

A continuación, se detallan dentro del monitoreo de afectación al sector Salud

Infraestructura de Red (Conectividad)

- **Dominios Identificados:** 2,113 registros de FQDN destinados a actividades de reconocimiento y engaño.
- **Puntos de Enlace:** 1,179 direcciones IP que actúan como infraestructura de soporte para los adversarios.

Artefactos de Software (Ejecución)

- **Firmas MD5:** 160 identificadores de archivos maliciosos únicos.
- **Firmas SHA-1:** 158 registros para la detección de integridad de código sospechoso.
- **Firmas SHA-256:** 161 indicadores de alta precisión para el bloqueo de amenazas persistentes.

Vectores de Acceso (Web)

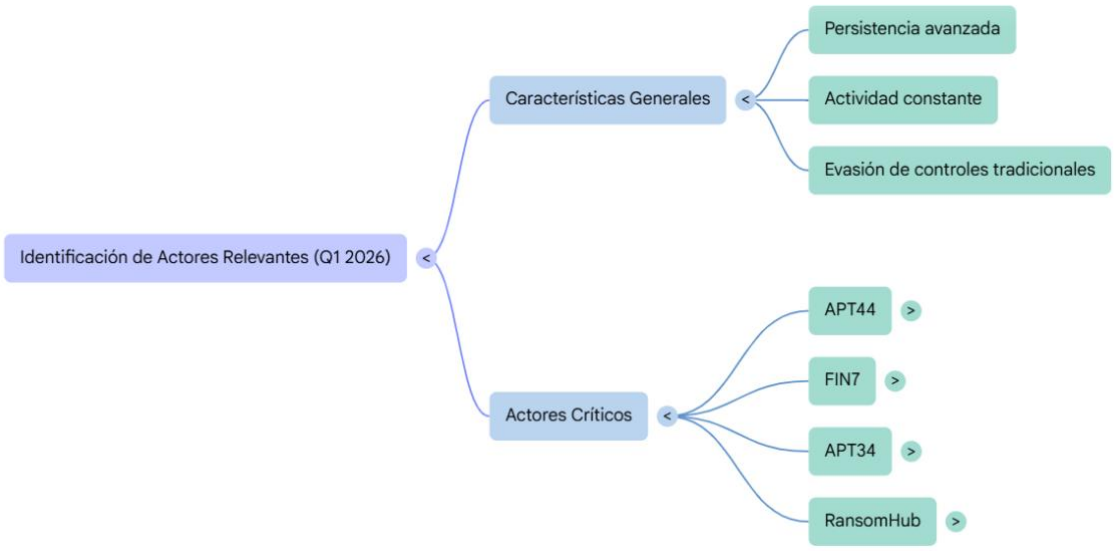
- **Rutas de Acceso:** 21 URLs específicas vinculadas a campañas de suplantación y descarga de contenido no autorizado.

ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Grupos de Espionaje (APT)	3	APT44, APT34, APT19	Exfiltración de investigaciones médicas y datos sensibles de ciudadanos.
Cibercrimen Financiero	1	FIN7	Secuestro de activos financieros y extorsión mediante bloqueo de sistemas.
Actores No Clasificados (UNC)	7	UNC1543, UNC3512, UNC5736, UNC2053, UNC3840, UNC5537, UNC3559	Infiltración oportunista y despliegue de diversas variantes de malware.
Operadores de Ransomware	1	RansomHub	Interrupción total de servicios asistenciales y compromiso de integridad de datos.

Identificación de Actores Relevantes

El monitoreo ha permitido identificar actores con capacidades avanzadas de persistencia, cuya actividad en la región se ha mantenido constante durante el primer cuatrimestre de 2026. Estos grupos destacan por su especialización en evadir controles de seguridad tradicionales.

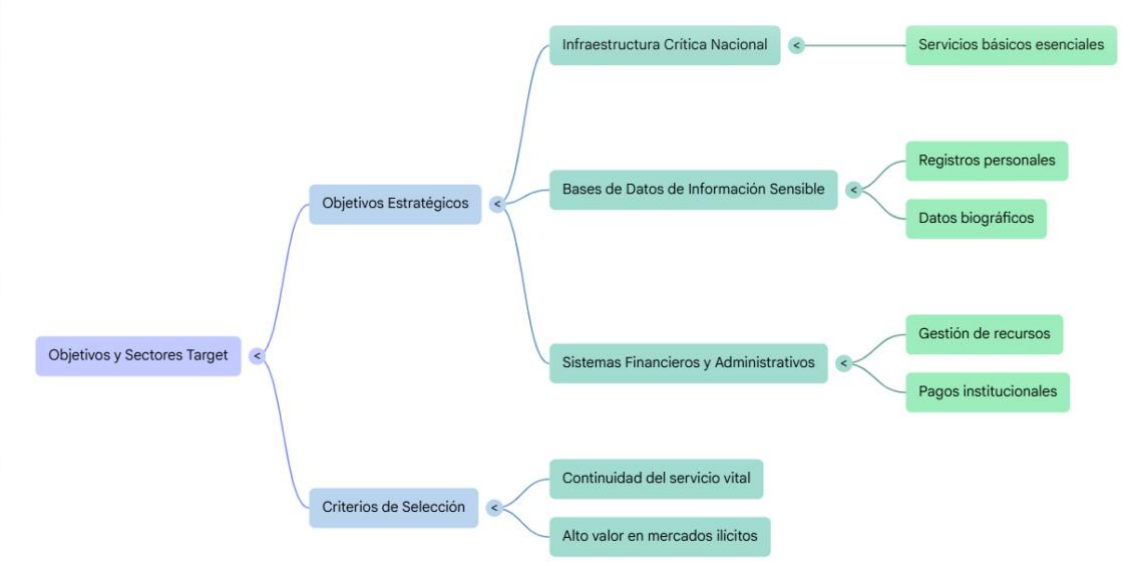


Actores Críticos:

- APT44: Reconocido por operaciones de alto impacto que pueden comprometer la integridad de infraestructuras críticas.
- FIN7: Grupo altamente organizado con un enfoque en la explotación de sistemas de procesamiento de datos y activos financieros.
- APT34: Especializado en el compromiso de infraestructuras de comunicación y sistemas de información estratégica.
- RansomHub: Actor enfocado en operaciones de doble extorsión que representan una amenaza directa a la disponibilidad de las historias clínicas.

Objetivos y Sectores Target

Aunque estos adversarios operan globalmente, sus tácticas están diseñadas para afectar sectores donde la continuidad del servicio es vital y la información almacenada posee un alto valor en mercados ilícitos.

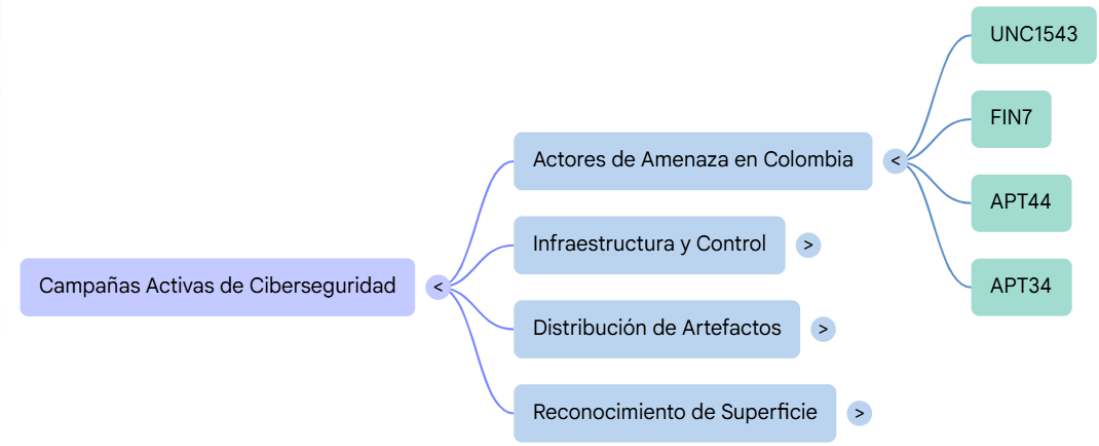


Objetivos Estratégicos:

- Infraestructura Crítica Nacional: Entidades que soportan servicios básicos esenciales para la población.
- Bases de Datos de Información Sensible: Repositorios de registros personales y datos biográficos.
- Sistemas Financieros y Administrativos: Plataformas de gestión de recursos y pagos institucionales.

Campañas Activas

La inteligencia recopilada muestra que los adversarios no cesan sus operaciones, manteniendo infraestructuras de comando y control actualizadas recientemente.



Campañas e Iniciativas:

- Explotación de Infraestructura en Colombia: Actores como UNC1543, FIN7, APT44 y APT34 registran actividad específica dirigida al país.
- Distribución de Artefactos de Intrusión: Uso de botnets y cargadores de malware para establecer acceso inicial en redes corporativas.
- Reconocimiento de Superficie de Red: Campañas masivas de escaneo de dominios y direcciones IP para identificar vulnerabilidades en portales de salud.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

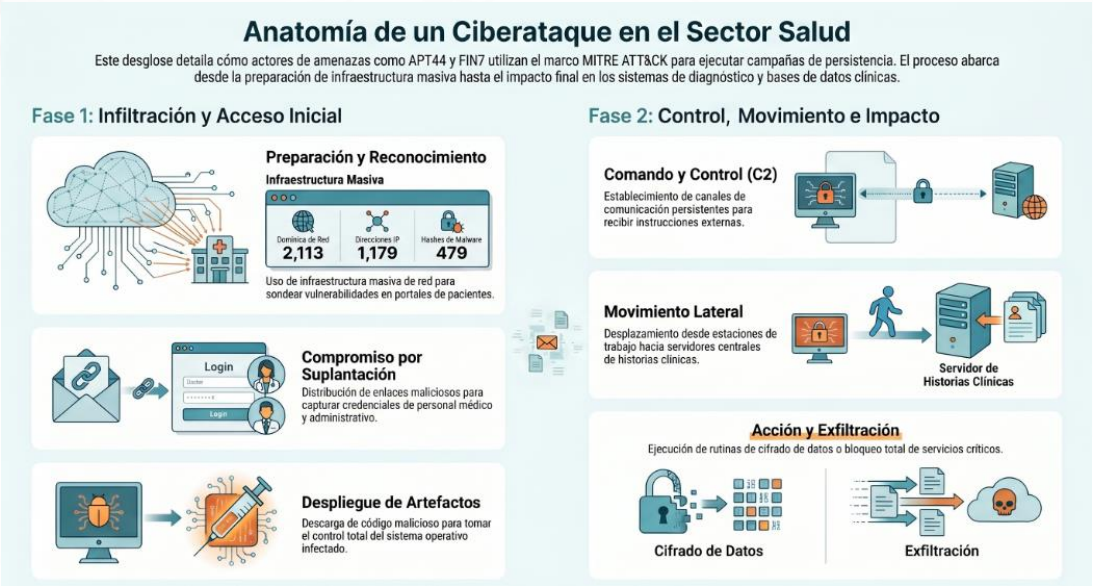
Mapeo a MITRE ATT&CK Framework

El comportamiento de los actores identificados, como APT44, FIN7 y diversos grupos UNC, se alinea con el marco de referencia MITRE ATT&CK, evidenciando una especialización en la persistencia y la evasión de defensas. En el sector salud, estas tácticas se traducen en el uso de dominios legítimos suplantados para engañar al personal asistencial y el despliegue de artefactos que buscan deshabilitar soluciones de seguridad antes de proceder con el cifrado o la extracción de historias clínicas. La alta presencia de indicadores de red sugiere que la fase de "Comando y Control" es crítica, permitiendo a los atacantes mantener acceso remoto a sistemas de diagnóstico y bases de datos sensibles durante periodos prolongados.

Táctica	ID Técnica	Técnica (Nombre en Inglés)	Técnica (Nombre en Inglés)
Reconnaissance	T1594	Search Open Technical Databases	Los actores analizan los 2,113 dominios y bases de datos públicas para identificar vulnerabilidades en portales de salud.
Resource Development	T1583	Acquire Infrastructure	Proceso de obtención de las 1,179 direcciones IP y dominios utilizados para alojar contenido malicioso.
Initial Access	T1566	Phishing	Uso de correos dirigidos a personal médico para obtener acceso inicial a la red interna.
Execution	T1059	Command and Scripting Interpreter	Ejecución de los 479 artefactos maliciosos (hashes) para tomar control de estaciones de trabajo.
Persistence	T1133	External Remote Services	Mantenimiento del acceso mediante VPNs o servicios remotos comprometidos de la entidad de salud.
Defense Evasion	T1027	Obfuscated Files or Information	Uso de técnicas para que los archivos maliciosos no sean detectados por antivirus tradicionales.
Discovery	T1082	System Information Discovery	Identificación de sistemas operativos en equipos de diagnóstico para planear ataques específicos.
Command and Control	T1071	Application Layer Protocol	Comunicación entre el malware instalado y los servidores externos de los atacantes (C2).
Exfiltration	T1041	Exfiltration Over C2 Channel	Extracción de historias clínicas y datos sensibles hacia la infraestructura controlada por el adversario.
Impact	T1486	Data Encrypted for Impact	Acción final de cifrado de datos (Ransomware) que impide la prestación de servicios médicos.

Cadenas de Ataque Observadas

El comportamiento de los actores identificados, como APT44, FIN7 y diversos grupos UNC, se alinea con el marco de referencia MITRE ATT&CK, evidenciando una especialización en la persistencia y la evasión de defensas. En el sector salud, estas tácticas se traducen en el uso de dominios legítimos suplantados para engañar al personal asistencial y el despliegue de artefactos que buscan deshabilitar soluciones de seguridad antes de proceder con el cifrado o la extracción de historias clínicas. La alta presencia de indicadores de red sugiere que la fase de "Comando y Control" es crítica, permitiendo a los atacantes mantener acceso remoto a sistemas de diagnóstico y bases de datos sensibles durante periodos prolongados.

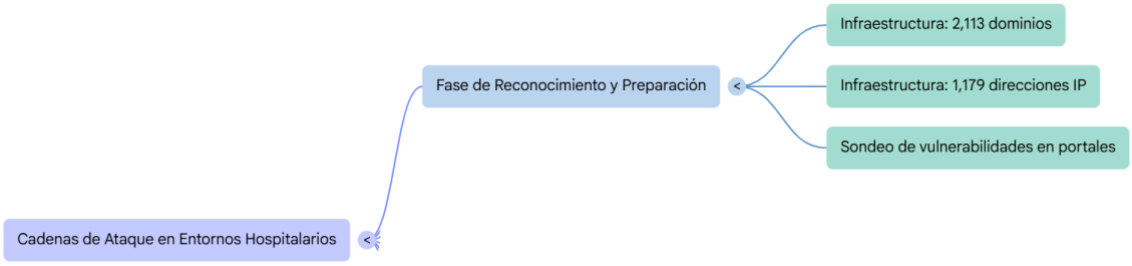


Cadenas de ataque:

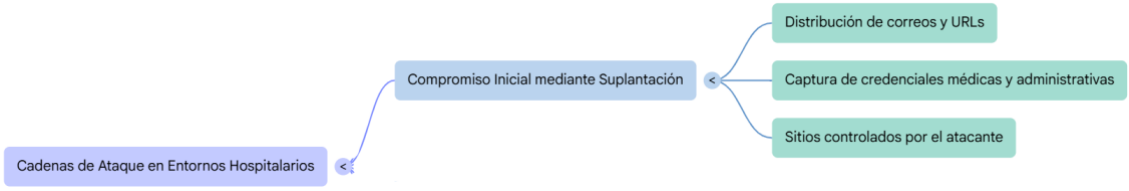
Las cadenas de ataque identificadas en el monitoreo reflejan una metodología altamente estructurada, donde los adversarios priorizan la estabilidad del acceso inicial antes de proceder con acciones de impacto. En el contexto hospitalario, se observa un patrón donde la infraestructura de red masiva (dominios y direcciones IP) sirve como soporte para campañas de engaño que buscan depositar artefactos de ejecución en estaciones de trabajo. Una vez que el código malicioso se ejecuta, los atacantes establecen canales de comunicación persistentes para navegar por la red interna, identificar servidores de historias clínicas y proceder con la extracción o el cifrado de la información.

Cadenas de ataque:

- Fase de Reconocimiento y Preparación: Los actores utilizan la amplia base de 2,113 dominios y 1,179 direcciones IP para sondear vulnerabilidades en servicios web y portales de pacientes.

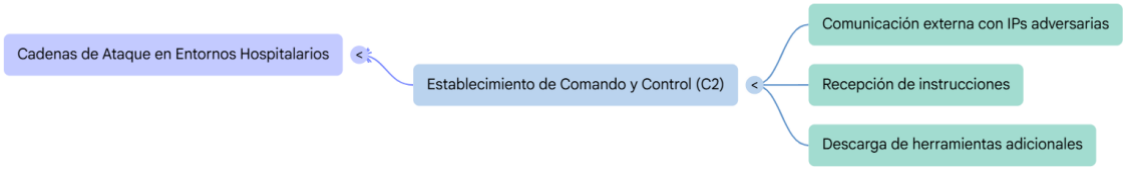


- Compromiso Inicial mediante Suplantación: Se distribuyen correos o enlaces (URLs) que dirigen a sitios controlados por el atacante para capturar credenciales de acceso de personal administrativo o médico.

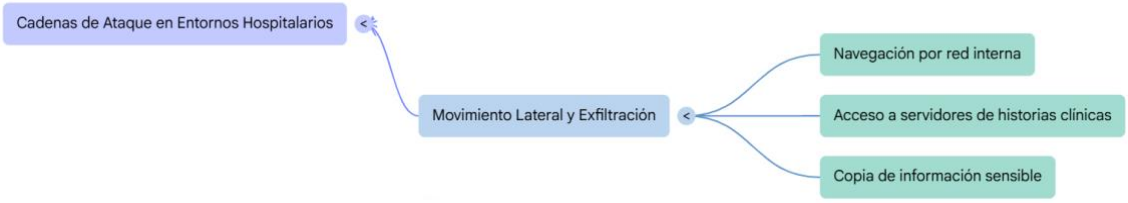


- Despliegue de Artefactos Maliciosos: Tras el acceso inicial, se descargan archivos identificados mediante los 479 hashes analizados, los cuales permiten tomar control del sistema operativo infectado.

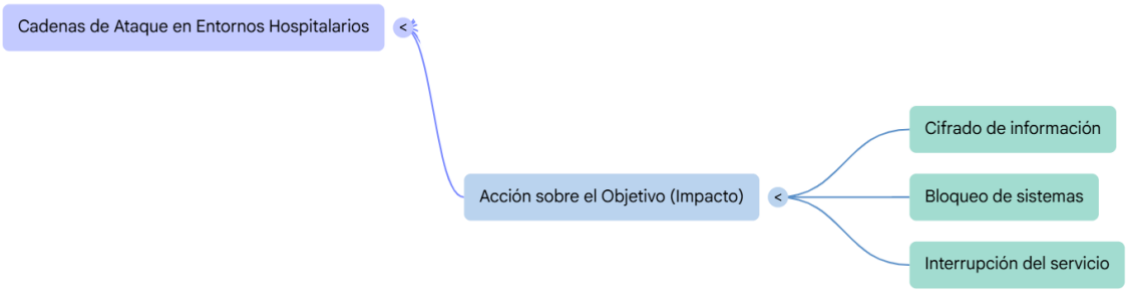
- Establecimiento de Comando y Control (C2): El malware se comunica de forma externa con las direcciones IP de los adversarios para recibir instrucciones y herramientas adicionales.



- Movimiento Lateral y Exfiltración: Los atacantes se desplazan desde la estación de trabajo inicial hacia los servidores centrales de bases de datos para copiar información sensible.

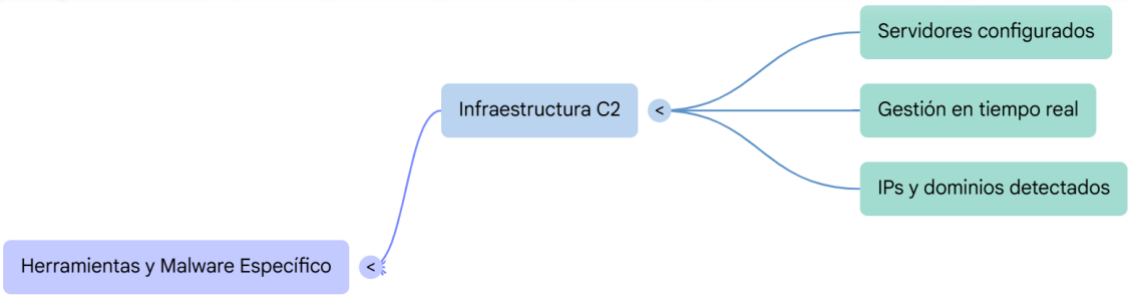


- Acción sobre el Objetivo (Impacto): Ejecución de rutinas de cifrado o bloqueo de sistemas, como se observa en las operaciones de grupos enfocados en la interrupción del servicio.



Herramientas y Malware Específico

- Infraestructura de Comando y Control (C2): Servidores configurados en las direcciones IP y dominios detectados que gestionan la actividad del malware en tiempo real.

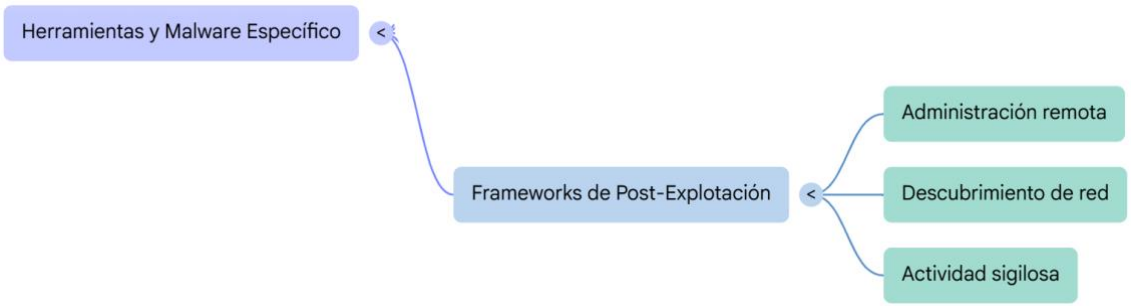


- Cargadores de Malware (Loaders): Archivos ligeros diseñados para evadir la detección inicial y descargar componentes más pesados y dañinos.

- Software de Exfiltración de Datos: Herramientas personalizadas o scripts utilizados para comprimir y enviar grandes volúmenes de registros médicos fuera de la red.

- Variantes de Ransomware: Código especializado en el cifrado de archivos a gran escala, utilizado para paralizar la operación asistencial y exigir rescates.

- Frameworks de Post-Explotación: Conjuntos de herramientas que permiten a los atacantes realizar tareas de administración remota y descubrimiento de red de manera sigilosa.



CORRELACIÓN ENTRE ACTORES Y GRUPOS

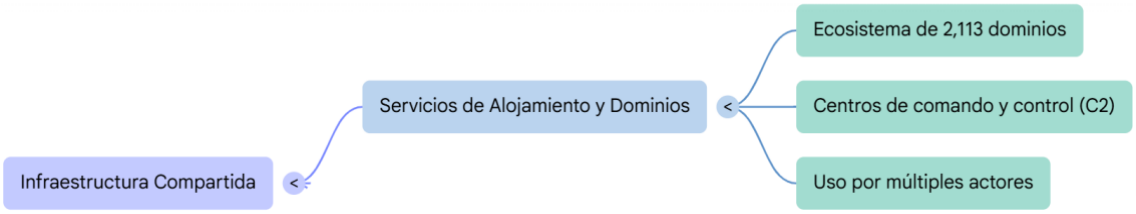
El análisis de la inteligencia recopilada revela que los adversarios no operan de forma aislada, sino que existe una superposición significativa en el uso de infraestructuras y metodologías de ataque. Actores como FIN7, APT44 y diversos grupos UNC (como UNC1543 y UNC2053) muestran patrones de actividad que sugieren un ecosistema de colaboración indirecta o el uso de los mismos proveedores de servicios ilícitos.

En el sector salud, esta correlación se manifiesta cuando diferentes grupos utilizan los mismos dominios o direcciones IP para lanzar campañas dirigidas, lo que indica una economía del cibercrimen donde el acceso a las redes médicas es un activo que se

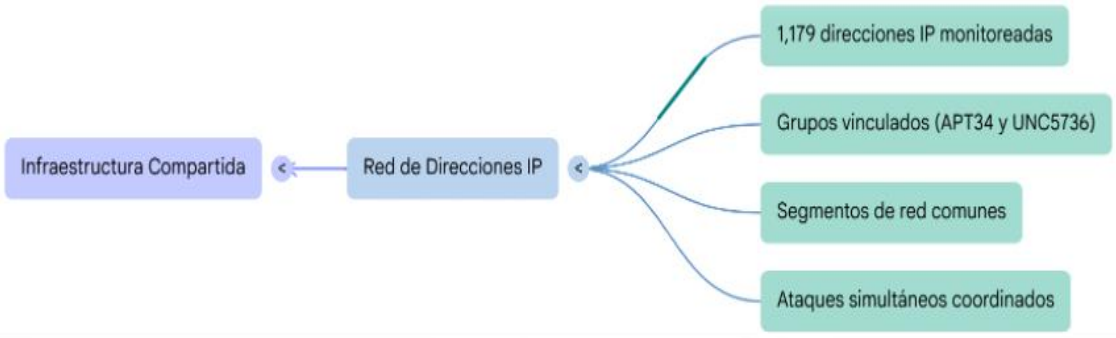
intercambia o se explota de manera coordinada para maximizar el impacto operativo y financiero.

Infraestructura Compartida

- Servicios de Alojamiento y Dominios: Se observa que múltiples actores hacen uso del ecosistema de 2,113 dominios (FQDN) identificados para alojar sus centros de comando y control.

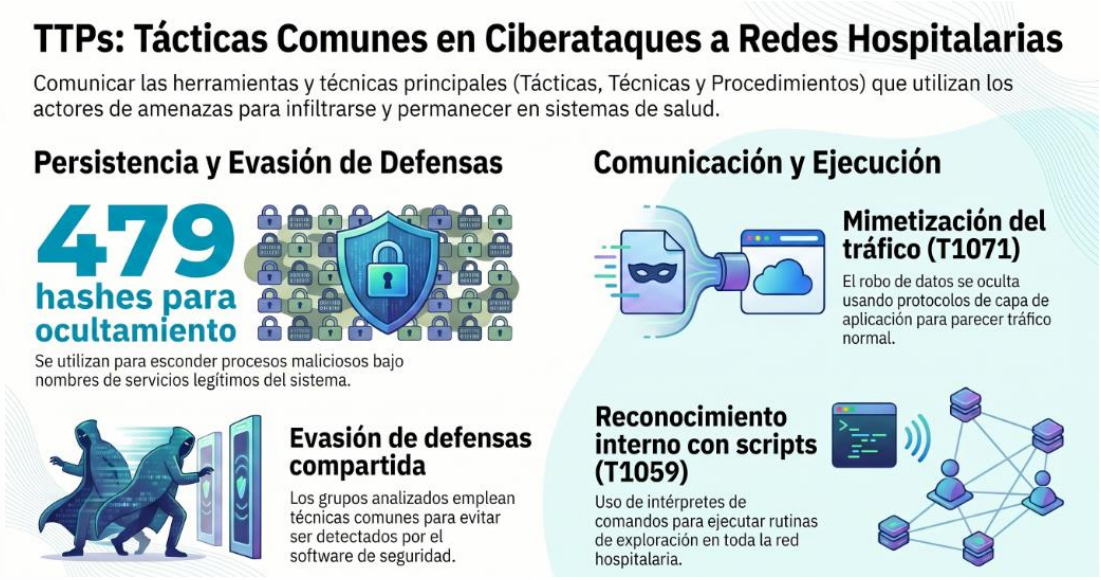


- Red de Direcciones IP: Grupos como APT34 y UNC5736 han sido vinculados a segmentos de red comunes dentro de las 1,179 direcciones IP monitoreadas, facilitando ataques simultáneos desde los mismos puntos de origen.

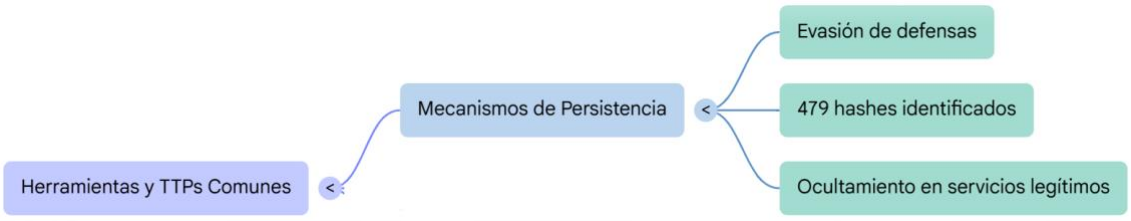


- Plataformas de Distribución: El uso de infraestructuras de importación masiva sugiere que los adversarios aprovechan canales de distribución de malware ya establecidos para depositar sus artefactos en las instituciones de salud.

Herramientas y TTPs Comunes

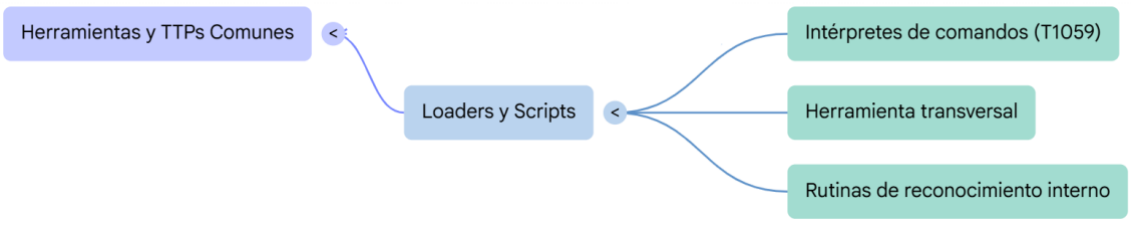


- Mecanismos de Persistencia: Los grupos analizados comparten técnicas de evasión de defensas, utilizando los 479 hashes identificados para ocultar procesos maliciosos bajo nombres de servicios legítimos del sistema.

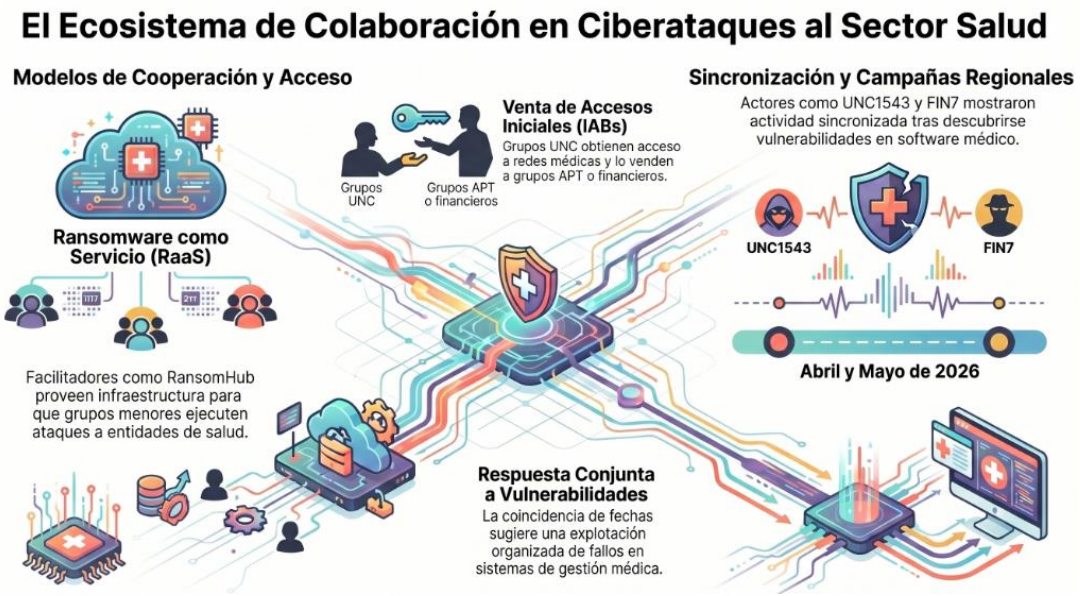


- Protocolos de Comunicación: El uso extensivo de protocolos de capa de aplicación (T1071) es una constante entre actores como APT19 y FIN7 para mimetizar el tráfico de robo de datos con el tráfico normal de la red hospitalaria.

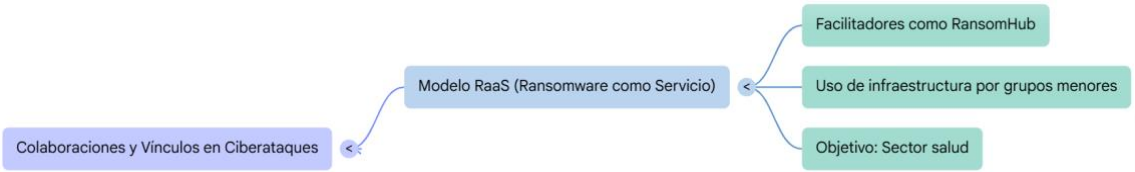
- Uso de Loaders y Scripts: La implementación de intérpretes de comandos (T1059) es una herramienta transversal para la ejecución de rutinas de reconocimiento interno en todas las categorías de actores identificados.



Posibles Colaboraciones o Vínculos



- Modelo de Ransomware como Servicio (RaaS): Actores como RansomHub actúan como facilitadores, permitiendo que otros grupos menores utilicen su infraestructura para atacar entidades del sector salud.



- Venta de Accesos Iniciales (IABs): Grupos clasificados como UNC (Unclassified) suelen actuar como la primera fase de la cadena, vendiendo el acceso obtenido en redes médicas a grupos APT o financieros para ataques de mayor envergadura.

- Sincronización en Campañas Regionales: La coincidencia de fechas de modificación de indicadores en abril y mayo de 2026 para actores como UNC1543 y FIN7 sugiere una coordinación o una respuesta conjunta a vulnerabilidades recientemente descubiertas en software de gestión médica.

Visualización de Relaciones

El análisis de la red de amenazas revela un grafo complejo donde la mayoría de los adversarios no operan de manera estanca, sino que convergen en puntos críticos de la infraestructura digital. Se observa una alta densidad de conexiones en torno a los servicios de comando y control alojados en las direcciones IP y dominios monitoreados, lo que sugiere que grupos con objetivos distintos (espionaje vs. financiero) utilizan los mismos canales de despliegue.

Para el sector salud, esto implica que el bloqueo de un solo nodo de infraestructura compartida puede neutralizar simultáneamente vectores de ataque de múltiples grupos de amenazas identificados en este informe.

Relaciones directas documentadas:

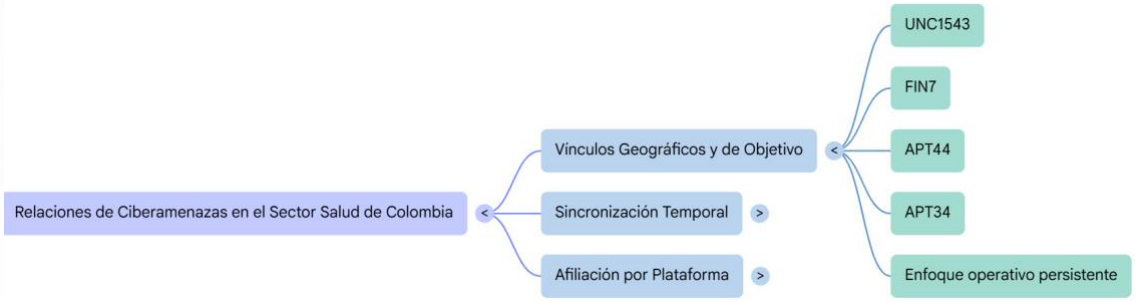
- Vínculos Geográficos y de Objetivo: Actores como UNC1543, FIN7, APT44 y APT34 muestran una relación directa por su enfoque operativo persistente sobre objetivos en el sector salud de Colombia.

- Sincronización Temporal: Se identifican vínculos operativos por fechas de actividad reciente (abril y mayo de 2026) entre grupos como UNC3512, UNC5736 y UNC2053, sugiriendo una ventana de explotación coordinada, al sector salud colombiano.

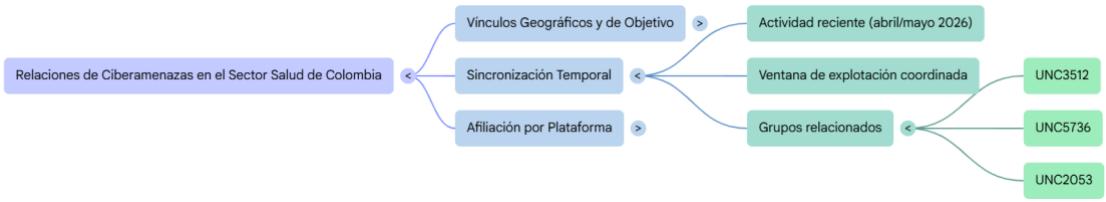
- Afiliación por Plataforma: Grupos como APT44 y APT34 comparten orígenes de inteligencia y reporte en plataformas de análisis de amenazas globales y malware especializado.

Relaciones por infraestructura compartida

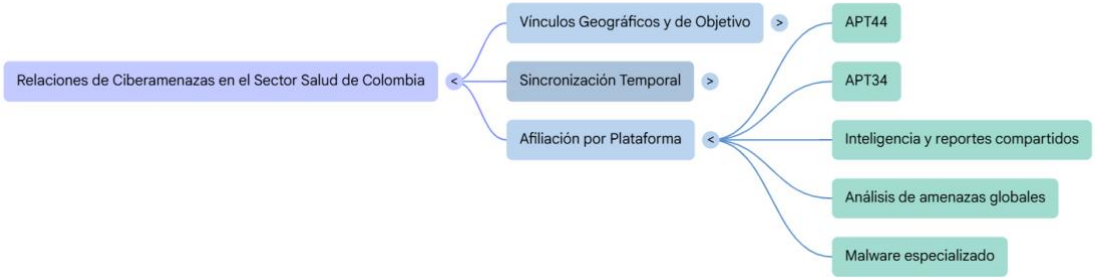
- Convergencia de Red: Los 2,113 dominios (FQDN) identificados actúan como nodos centrales donde diversos grupos UNC y APT coinciden para el alojamiento de sus campañas de suplantación.



- Nodos de Comunicación (IPs): Las 1,179 direcciones IP registradas sirven como puntos de contacto transversales para el tráfico de exfiltración de datos utilizado por actores financieros como FIN7 y grupos de espionaje como APT19.

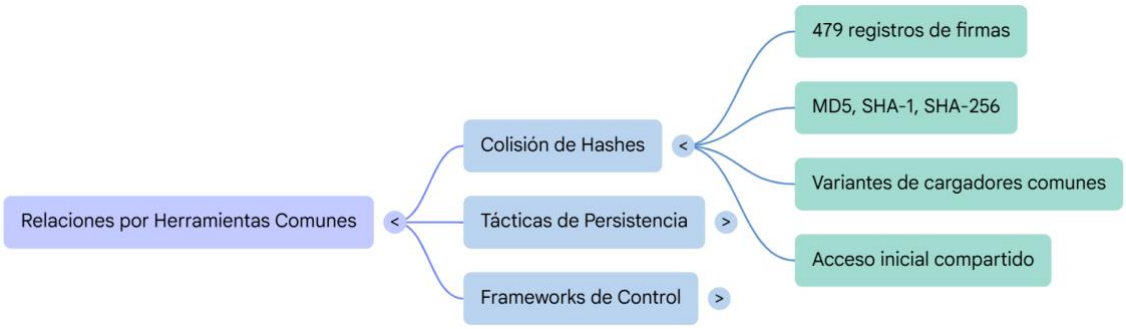


- Puertos de Acceso Web: Las 21 URLs monitoreadas muestran una relación de uso para la descarga de diversos artefactos, conectando la infraestructura de red con la fase de ejecución de los atacantes.

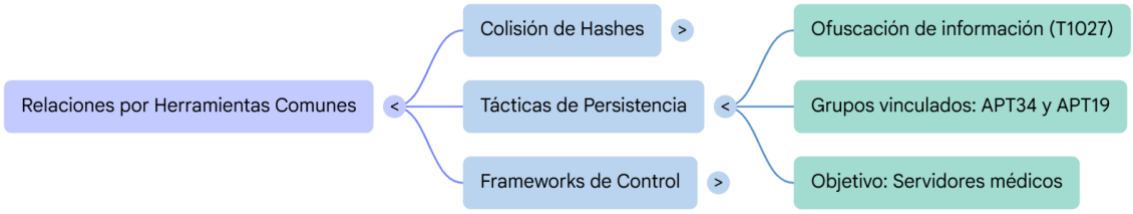


Relaciones por herramientas comunes

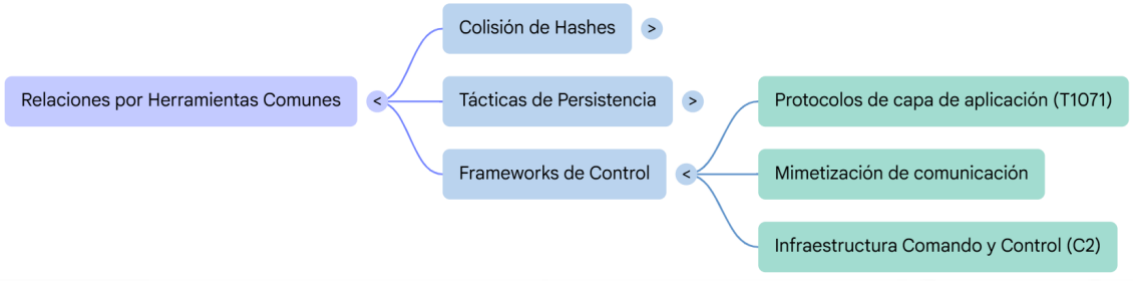
- Colisión de Hashes: El análisis de los 479 registros de firmas de archivos (MD5, SHA-1, SHA-256) revela que diferentes actores utilizan las mismas variantes de cargadores de malware para ganar acceso inicial.



- Tácticas de Persistencia: Existe una correlación en el uso de mecanismos de ofuscación de información (T1027) entre grupos como APT34 y APT19 para proteger su presencia en servidores médicos.

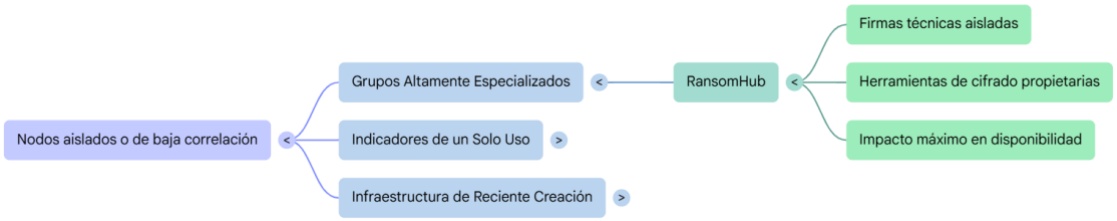


- Frameworks de Control: Se detecta una dependencia común en protocolos de capa de aplicación (T1071) para mimetizar la comunicación con la infraestructura externa de comando y control.

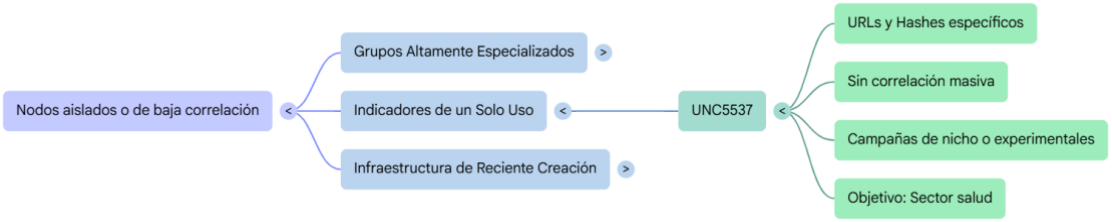


Nodos aislados o con baja correlación (por ahora):

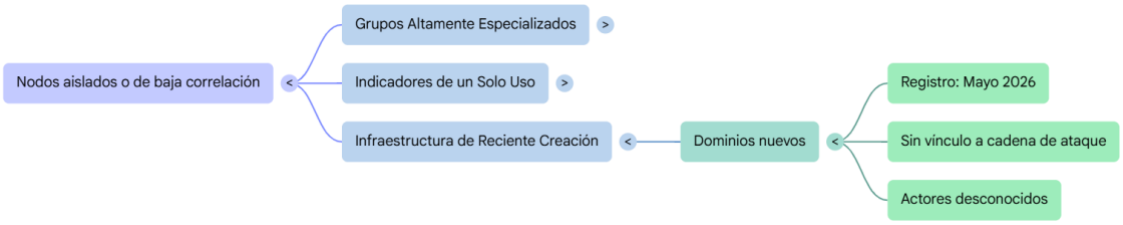
- Grupos Altamente Especializados: Actores como RansomHub presentan firmas técnicas más aisladas debido al uso de herramientas de cifrado propietarias, aunque su impacto en la disponibilidad de servicios es máximo.



- Indicadores de un Solo Uso: Ciertas URLs y Hashes específicos vinculados a UNC5537 no muestran por ahora una correlación masiva con otros grupos, lo que podría indicar campañas de nicho o experimentales hacia el sector salud.



- Infraestructura de Reciente Creación: Dominios registrados en las últimas semanas de mayo de 2026 que aún no han sido vinculados a una cadena de ataque completa de los actores conocidos.

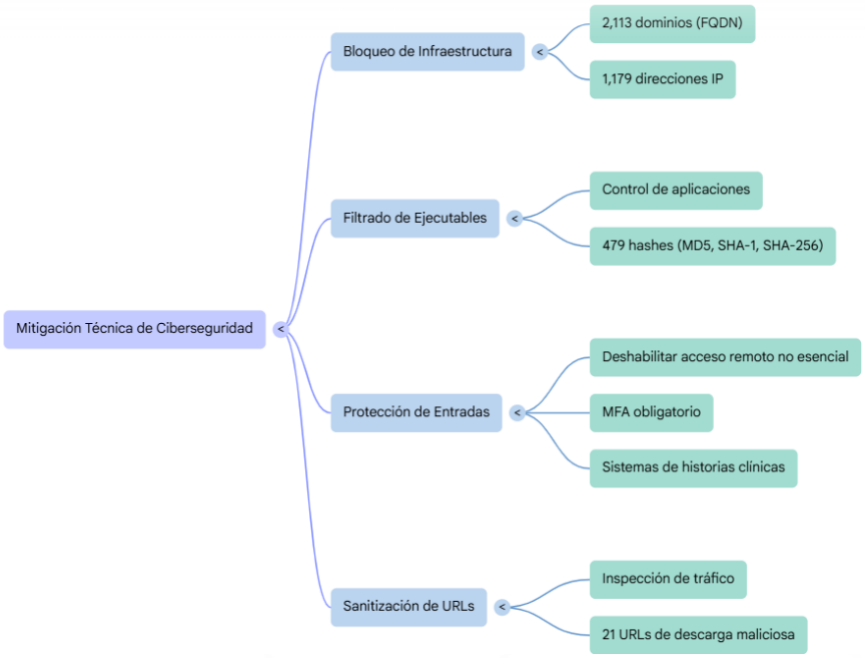


RECOMENDACIONES ESTRATÉGICAS

La defensa del sector salud ante los 12 grupos de amenazas identificados debe trascender la simple implementación de herramientas tecnológicas. Se requiere una estrategia integral que priorice la protección de la información del paciente y la continuidad de los sistemas críticos de soporte vital.

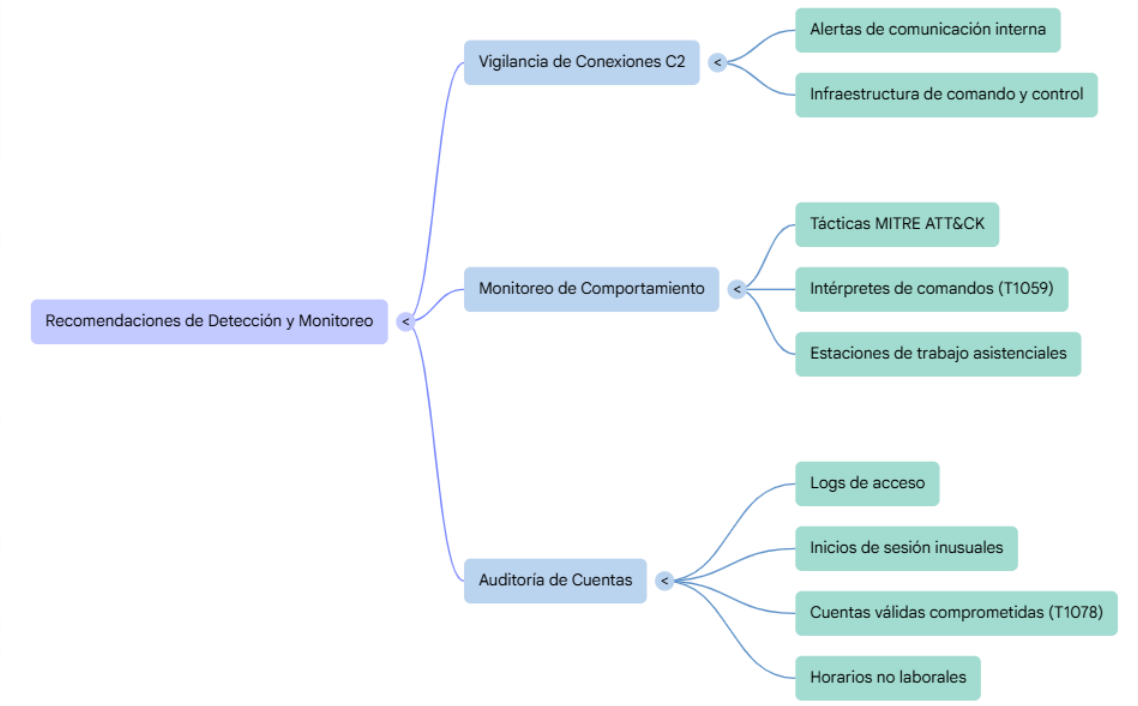
Dado que actores como RansomHub y FIN7 han demostrado una alta capacidad para explotar la superficie de red (específicamente a través de los dominios e IPs analizados), la estrategia debe centrarse en la reducción de la visibilidad de los activos críticos y en la segmentación estricta de las redes médicas para evitar que una infección en un puesto de trabajo comprometa el núcleo de datos hospitalarios.

Recomendaciones de Mitigación Técnica



- Bloqueo de Infraestructura Maliciosa: Implementar en los perímetros de red listas de denegación para los 2,113 dominios (FQDN) y las 1,179 direcciones IP identificadas en este análisis.
- Filtrado de Ejecutables: Configurar políticas de control de aplicaciones que bloqueen la ejecución de archivos cuyos hashes coincidan con los 479 registros (MD5, SHA-1, SHA-256) detectados.
- Protección de Puntos de Entrada: Deshabilitar servicios de acceso remoto no esenciales y aplicar autenticación multifactor (MFA) obligatoria para todo el personal que acceda a sistemas de historias clínicas.
- Sanitización de URLs: Utilizar sistemas de inspección de tráfico para bloquear el acceso a las 21 URLs de descarga maliciosa identificadas.

Recomendaciones de Detección y Monitoreo

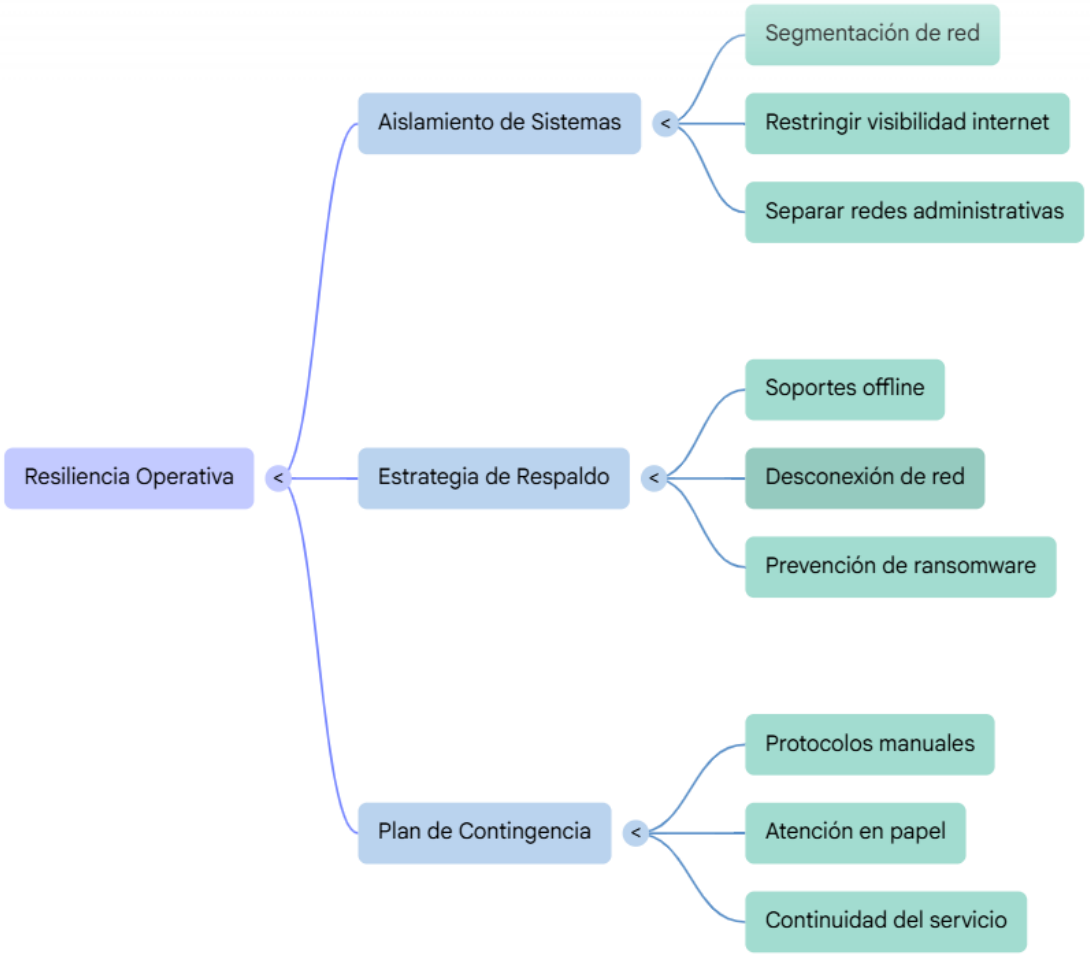


- Vigilancia de Conexiones C2: Configurar alertas de detección para identificar cualquier intento de comunicación interna hacia la infraestructura de comando y control vinculada a los adversarios monitoreados.

- Monitoreo de Comportamiento: Establecer reglas de detección basadas en las tácticas MITRE ATT&CK analizadas, especialmente sobre el uso de intérpretes de comandos (T1059) en estaciones de trabajo asistenciales.

- Auditoría de Cuentas: Supervisar logs de acceso en busca de inicios de sesión inusuales o en horarios no laborales que sugieran el uso de cuentas válidas comprometidas (T1078).

Recomendaciones de Resiliencia Operativa

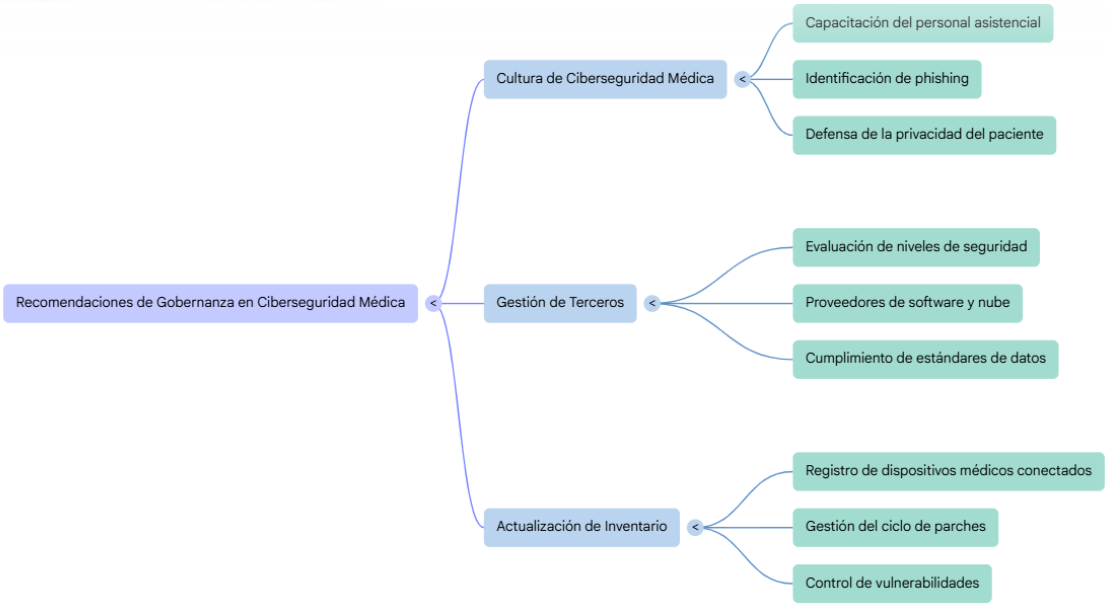


- Aislamiento de Sistemas de Diagnóstico: Ejecutar la segmentación de red para que equipos como tomógrafos o monitores fetales no tengan visibilidad directa hacia internet o redes administrativas.

- Estrategia de Respaldo Offline: Garantizar que las copias de seguridad de las bases de datos de pacientes se encuentren en soportes desconectados de la red para evitar su cifrado por ataques de ransomware.

- Plan de Contingencia Manual: Desarrollar y practicar protocolos de atención médica en papel para asegurar la continuidad del servicio en caso de caída total de los sistemas digitales.

Recomendaciones de Gobernanza



- Cultura de Ciberseguridad Médica: Capacitar al personal asistencial en la identificación de campañas de phishing, subrayando que su rol es la primera línea de defensa de la privacidad del paciente.

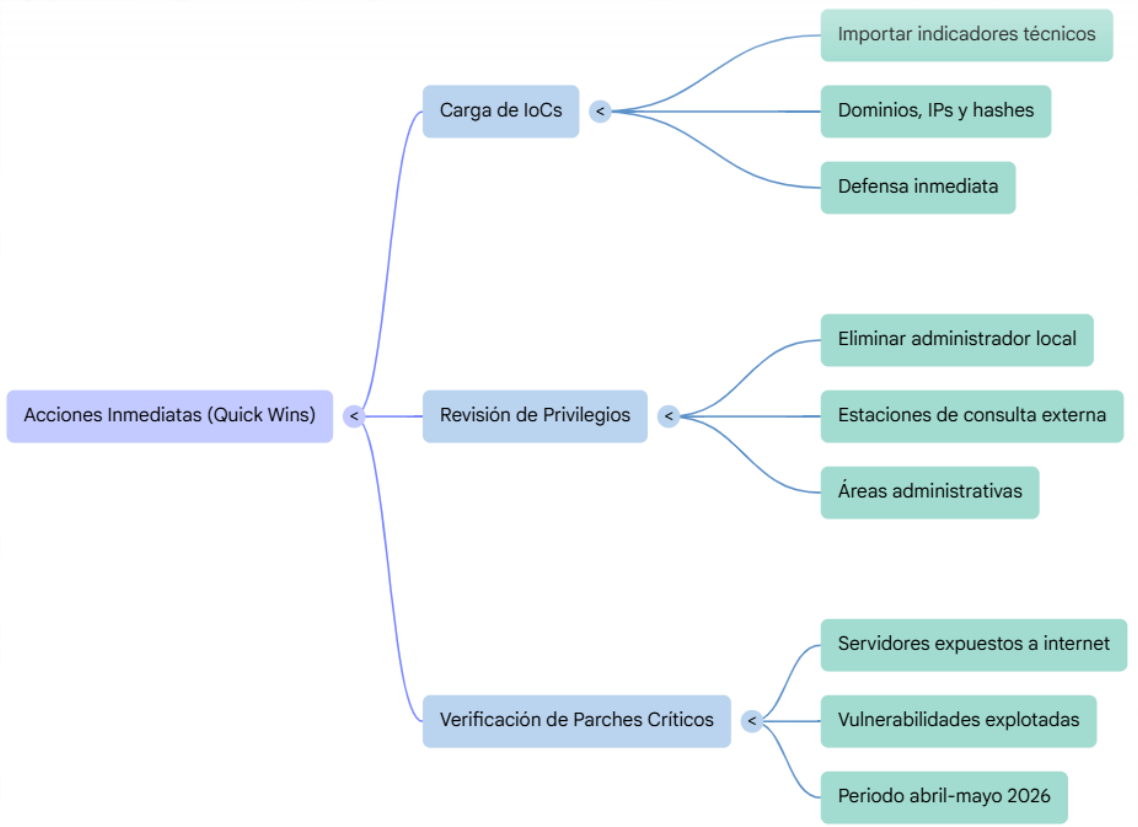
- Gestión de Terceros: Evaluar los niveles de seguridad de proveedores de software médico y servicios en la nube, exigiendo cumplimiento con estándares de protección de datos.

- Actualización de Inventario: Mantener un registro riguroso de todos los dispositivos médicos conectados para gestionar oportunamente su ciclo de parches y vulnerabilidades.

Preparación ante Incidentes

- Simulacros de Ataque: Realizar ejercicios de mesa (Tabletop) donde se simule el compromiso de los sistemas por parte de actores identificados como APT44 o RansomHub.
- Canales de Comunicación Alternos: Establecer medios seguros de coordinación para el equipo de respuesta ante incidentes que no dependan de la infraestructura corporativa principal.
- Alianzas con el Sector: Participar en redes de intercambio de información de amenazas específicas del sector salud en Colombia para anticipar tendencias de ataque regionales.

Acciones Inmediatas (Quick Wins)



- Carga de IoCs: Importar los indicadores técnicos de este informe (dominios, IPs y hashes) en los sistemas de protección actuales para una defensa inmediata.
- Revisión de Privilegios: Eliminar permisos de administrador local en todas las estaciones de trabajo de consulta externa y áreas administrativas.
- Verificación de Parches Críticos: Priorizar la actualización de servidores expuestos a internet que presenten vulnerabilidades conocidas explotadas por los actores analizados en abril y mayo de 2026.

CONCLUSIONES

1. Estado de Vulnerabilidad Crítica y Sistémica
   - El sector salud en Colombia se encuentra bajo un periodo de exposición extrema. Con más de 23 millones de intentos de ataque registrados en un solo mes y incidentes reales de descarga masiva de datos en entidades regulatorias, la amenaza no es teórica, sino una realidad operativa que afecta la soberanía de la información clínica nacional.

2. Predominio de la Infraestructura de Red como Vector
   - La estrategia de los atacantes se centra masivamente en el control de la red externa. El 55.7% de los hallazgos (2,113 registros) corresponden a nombres de dominio (FQDN), lo que demuestra que los adversarios priorizan el uso de sitios web fraudulentos y centros de comando y control (C2) para orquestar la exfiltración de datos médicos.

3. Sofisticación y Persistencia de los Actores
   - Se han identificado 12 grupos de amenazas activos en la región, incluyendo actores de espionaje avanzado (APT44, APT34) y cibercrimen financiero (FIN7, RansomHub). Estos grupos no solo buscan lucro económico, sino que mantienen una persistencia técnica capaz de evadir controles tradicionales para acceder a investigaciones médicas y datos sensibles.

4. Ciclo de Vida de las Amenazas en Tiempo Real
   - Existe una vigencia operativa alarmante; los registros muestran actualizaciones de infraestructura maliciosa tan recientes como abril y mayo de 2026. Esto indica que los adversarios están en una fase de operación activa, adaptando sus tácticas y herramientas (como el uso de IA para explotar vulnerabilidades) de manera casi simultánea a las defensas actuales.

5. Convergencia y Colaboración entre Atacantes
   - El análisis revela que los actores no operan de forma aislada. Existe una superposición significativa en el uso de los mismos dominios y direcciones IP. Esto sugiere una economía del cibercrimen donde los accesos iniciales a redes hospitalarias se intercambian o venden, permitiendo que grupos de ransomware ejecuten ataques finales sobre brechas abiertas por otros grupos.

6. Necesidad de un Modelo de Defensa Proactiva
   - Dada la alta disponibilidad de indicadores técnicos y la interconexión de dispositivos médicos (IoMT), la prevención reactiva es insuficiente. La conclusión estratégica es que la seguridad debe integrarse en la continuidad asistencial: si los sistemas digitales caen, la atención médica se detiene. Es imperativo transicionar hacia la resiliencia operativa y la segmentación estricta de redes críticas.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **Ciberinteligencia de Amenazas (CTI):** Proceso de recopilación, análisis y difusión de información sobre ataques e intenciones de adversarios para la toma de decisiones proactivas.
- **Actor de Amenaza (Threat Actor):** Individuo o grupo (como **APT44** o **RansomHub**) que realiza acciones maliciosas contra sistemas digitales con objetivos de espionaje o lucro.
- **Amenaza Persistente Avanzada (APT):** Grupos de atacantes altamente capacitados que mantienen una presencia prolongada y encubierta en una red específica.
- **Indicadores de Compromiso (IoC):** Evidencias técnicas de una intrusión, como direcciones IP, hashes de archivos o nombres de dominio maliciosos.
- **Tácticas, Técnicas y Procedimientos (TTPs):** Descripción del comportamiento y los métodos operativos que caracterizan a un grupo de ataque específico.

Infraestructura y Redes

- **Nombre de Dominio Completamente Calificado (FQDN):** Nombre único que identifica un host exacto en internet; constituye el **55.7%** de los hallazgos en este informe.

- **Centro de Comando y Control (C2):** Servidor controlado por un atacante que se utiliza para enviar instrucciones a sistemas comprometidos y recibir datos exfiltrados.
- **Dirección IP (Internet Protocol):** Identificador numérico de un dispositivo en la red; representa el **44.3%** de los indicadores analizados en el periodo.
- **Exfiltración de Datos:** Transferencia no autorizada de información sensible desde el interior de una red hacia una ubicación externa controlada por el atacante.
- **Segmentación de Red:** Práctica de dividir una red en subredes más pequeñas para limitar el movimiento lateral de un atacante y proteger activos críticos.

Herramientas y Malware

- **Ransomware:** Software malicioso que cifra los datos de una organización y exige un rescate para su liberación; grupos como **FIN7** son expertos en su despliegue.
- **Exploit:** Fragmento de software o secuencia de comandos que aprovecha una vulnerabilidad (como errores de seguridad en software de salud) para causar un comportamiento no deseado.
- **Prueba de Concepto (PoC):** Código diseñado para demostrar que una vulnerabilidad existe y es explotable antes de que se convierta en un ataque a gran escala.
- **Infostealer:** Tipo de malware diseñado específicamente para recolectar y robar credenciales, cookies y datos de formularios de los navegadores de las víctimas.
- **Malware Information Sharing Platform (MISP):** Plataforma de código abierto utilizada para compartir y almacenar indicadores de amenazas de forma colaborativa.

Sector Salud y Normativa

- **Internet de las Cosas Médicas (IoMT):** Ecosistema de dispositivos médicos conectados (bombas de infusión, monitores) que generan y transmiten datos clínicos, aumentando la superficie de ataque.
- **Resiliencia Operativa:** Capacidad de una entidad de salud para resistir, absorber y recuperarse de incidentes cibernéticos sin interrumpir la atención al paciente.
- **Datos Sensibles de Salud:** Información relacionada con el estado de salud físico o mental de un individuo; es el objetivo principal de la descarga masiva de datos en entidades regulatorias.
- **Continuidad Asistencial:** La garantía de que los procesos médicos y de cuidado no se vean interrumpidos por fallos tecnológicos o ataques informáticos.
- **Vulnerabilidad Crítica:** Fallo de seguridad que, de ser explotado, permite un control total sobre el sistema afectado, representando un riesgo extremo para la soberanía de la información nacional.

COLCERT

El **ColCERT** tiene la misión de liderar y coordinar la gestión de incidentes, la identificación de vulnerabilidades, riesgos y amenazas contra la seguridad digital nacional. Actuamos como punto central de contacto y colaboración entre entidades públicas, privadas y la comunidad internacional, fortaleciendo la resiliencia del Estado mediante el intercambio de información, el desarrollo de capacidades, la difusión de lineamientos, la identificación de infraestructuras críticas y la promoción de una cultura de seguridad, a través de la cooperación nacional e internacional.

Más allá de la gestión ante amenazas, el **ColCERT** fortalece la seguridad digital del país mediante acciones de prevención, orientación y generación de capacidades dirigidas a entidades públicas, privadas y ciudadanía, contribuyendo a una transformación digital más segura y resiliente en Colombia.

Conéctate con el ColCERT

Reporte de incidentes:
csirtgob@mintic.gov.co
Entidades de Gobierno

contacto@colcert.gov.co
Privados

icc@colcert.gov.co
Temas de ICC

Sitio web
https://www.colcert.gov.co
Alertas y boletines

@colCERT

Línea directa:
+57 601 344 2222