TIC

Informe de apreciación Sector

Trabajo

COLCERT

Informe de apreciación
Sector Trabajo

COLCERT IN- 20260706- 036

TLP: CLEAR

Contenido

Informe de apreciación
Sector Trabajo

COLCERT IN- 20260706- 036

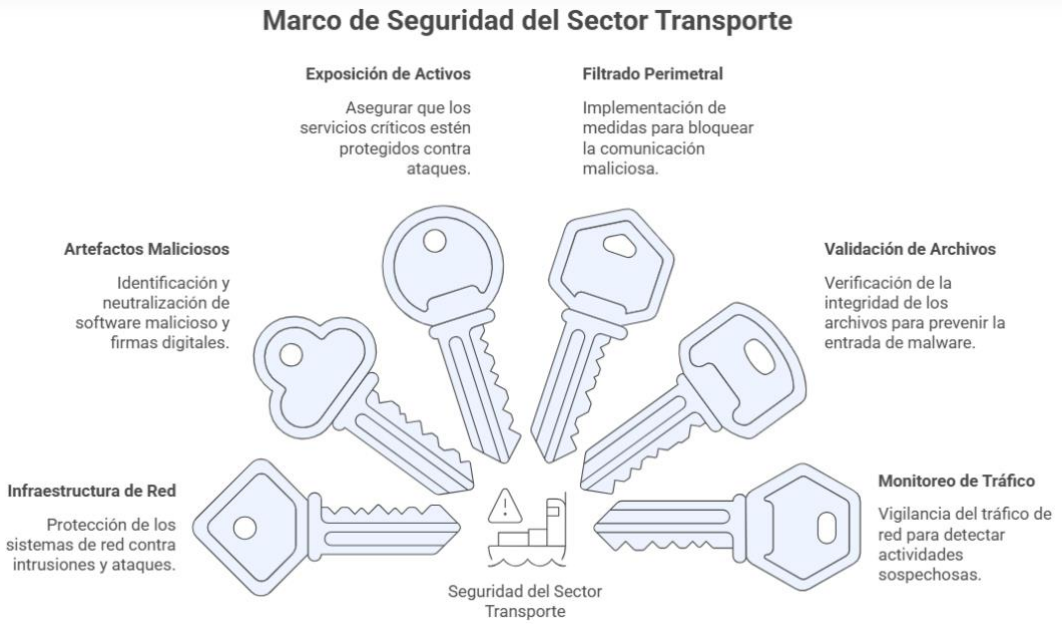
TLP: CLEAR

RESUMEN EJECUTIVO

El sector transporte en Colombia constituye un pilar crítico para la estabilidad económica y la conectividad del país, lo que lo posiciona como un objetivo de alto interés para diversos actores de amenazas en el ciberespacio. El presente documento expone un análisis detallado del panorama de amenazas actual, fundamentado en la identificación y procesamiento de indicadores de compromiso que afectan la infraestructura digital de las organizaciones del sector. A través de este estudio, se busca diagnosticar los vectores de ataque más recurrentes —desde el despliegue de software malicioso hasta la suplantación de servicios críticos— con el fin de fortalecer las capacidades de respuesta y prevención. La información recopilada permite anticipar movimientos adversos y establecer una línea base de seguridad que proteja la integridad de la cadena de suministro y la seguridad de los usuarios del sistema nacional de transporte.

Componentes del Análisis:

- Distribución de Indicadores por Tipología.
- Análisis de Infraestructura de Red y Dominios.
- Identificación de Vectores de Intrusión y Conectividad.
- Evaluación de Artefactos Maliciosos y Firmas Digitales.
- Caracterización de Tácticas y Comportamientos Detectados.
- Nivel de Criticidad y Potencial de Impacto Operativo.
- Correlación de Amenazas con el Entorno Logístico Nacional.



Informe de apreciación
Sector Trabajo

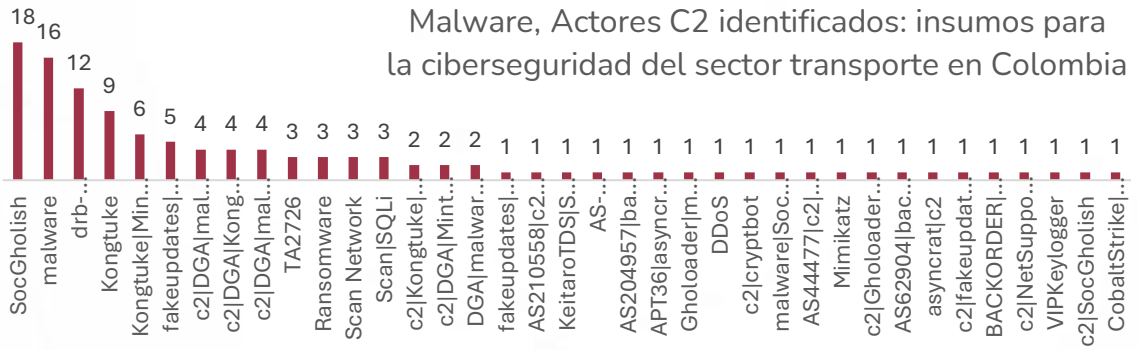
COLCERT IN- 20260706- 036

TLP: CLEAR

INTRODUCCIÓN

El panorama actual de amenazas para el sector transporte en Colombia muestra una actividad significativa centrada en la infraestructura de red y la distribución de archivos maliciosos. El análisis de los datos revela un volumen considerable de indicadores técnicos que sugieren intentos de intrusión y comunicación con nodos de comando y control externos. La criticidad de este sector, como columna vertebral de la logística y movilidad nacional, lo convierte en un objetivo estratégico para actores que buscan interrumpir la continuidad operativa o comprometer datos sensibles de carga y pasajeros.

Hallazgos Clave



- Predominio de infraestructura de red comprometida: Se identifica una alta concentración de dominios completamente calificados (FQDN) y direcciones IP asociadas a actividades sospechosas, lo que indica una fase activa de reconocimiento o establecimiento de persistencia.

- Presencia de artefactos maliciosos: Se detectó la circulación de firmas digitales vinculadas a archivos ejecutables y scripts diseñados para la evasión de controles, con un enfoque particular en la exfiltración de información.

- Exposición de activos críticos: Una porción relevante de las amenazas está dirigida a servicios expuestos que facilitan la gestión logística, aumentando el riesgo de ataques tipo man-in-the-middle o suplantación.

Recomendaciones Prioritarias

- Fortalecimiento del filtrado perimetral: Bloquear preventivamente la comunicación con la infraestructura de red identificada como maliciosa para mitigar posibles fugas de datos.
- Validación de integridad de archivos: Implementar procesos de verificación rigurosos para todos los archivos que ingresen a la red corporativa, especialmente aquellos provenientes de fuentes externas o socios logísticos.
- Monitoreo de tráfico anómalo: Incrementar la vigilancia sobre conexiones salientes inusuales que podrían indicar la presencia de un compromiso interno en curso.

Conclusión Estratégica

La resiliencia del sector transporte colombiano depende de una postura proactiva que trascienda la detección reactiva. Dado el volumen de indicadores analizados, es imperativo consolidar una defensa en profundidad que proteja tanto la infraestructura de TI como los sistemas operativos que controlan la cadena de suministro, asegurando así la estabilidad económica y social del país.

OBJETIVO Y ALCANCE

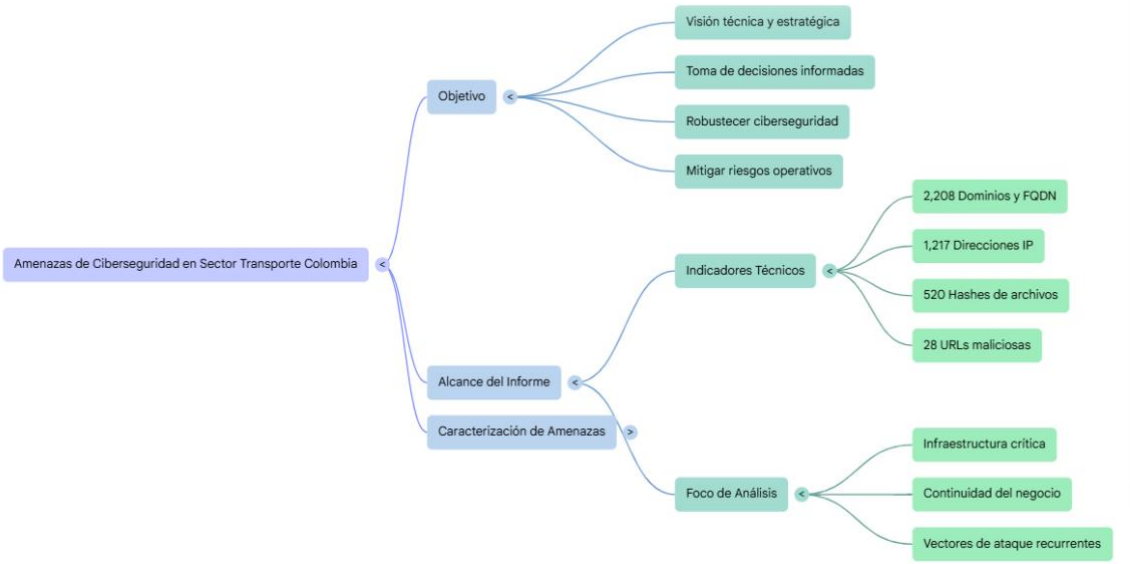
Objetivo

Proporcionar una visión técnica y estratégica sobre las amenazas que impactan al sector transporte en Colombia, permitiendo la toma de decisiones informadas para robustecer la postura de ciberseguridad y mitigar riesgos que puedan afectar la operatividad nacional.

Informe de apreciación
Sector Trabajo

COLCERT IN- 20260706- 036

TLP: CLEAR



Alcance

El presente informe abarca el análisis de 3,973 indicadores técnicos recolectados, los cuales incluyen dominios, direcciones IP y firmas de archivos maliciosos. El estudio se limita a la actividad detectada en el contexto de la infraestructura crítica del transporte colombiano, evaluando los vectores de ataque más recurrentes y su potencial impacto en la continuidad del negocio durante el periodo actual.

- **Identificación de Infraestructura de Red (Dominios y FQDN):** Se analizaron 2,208 registros de nombres de dominio y hosts. Este componente busca identificar centros de comando y control, así como portales de suplantación de identidad que intentan engañar a los empleados del sector transporte.

- **Análisis de Direccionamiento IP:** Se evaluaron 1,217 direcciones IP únicas vinculadas a actividades maliciosas. El enfoque aquí es detectar puntos de origen de ataques de fuerza bruta, escaneos de vulnerabilidades y nodos de redes de bots que interactúan con la infraestructura logística.

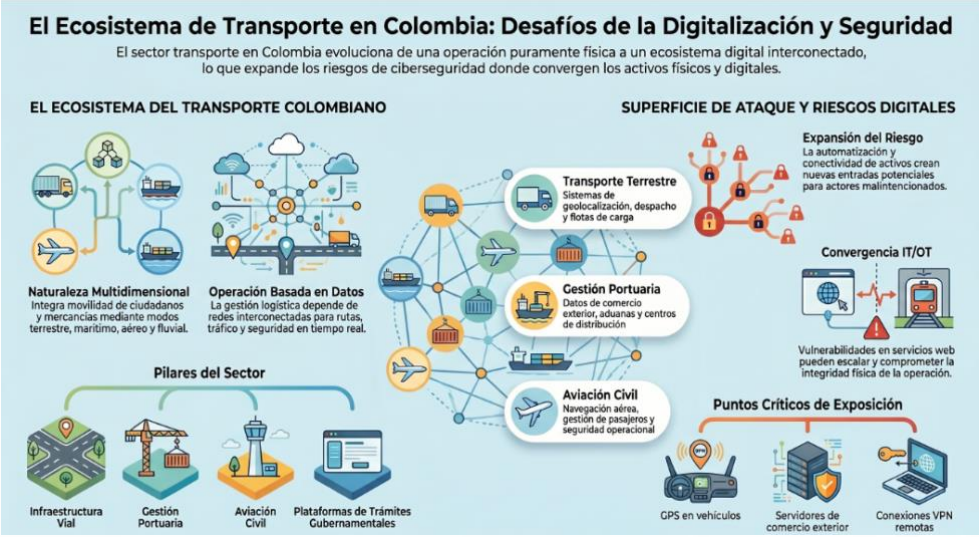
- **Detección de Artefactos de Software (Hashes):** Se incluyó la revisión de 520 huellas digitales de archivos (repartidas entre formatos SHA-256, MD5 y SHA-1). Estos representan ejecutables, documentos adjuntos o scripts diseñados para infectar sistemas operativos, capturar pulsaciones de teclado o cifrar información crítica.

- **Rastreo de Enlaces Maliciosos (URLs):** Se identificaron 28 direcciones web específicas utilizadas como vectores de descarga de malware o para la recolección de credenciales mediante técnicas de ingeniería social.

Caracterización de Amenazas Específicas: El alcance contempla el estudio de diversas tipologías de ataque presentes en los datos, tales como:

- **Denegación de Servicio:** Intentos de saturar la disponibilidad de servicios digitales de transporte.
- **Inyección de Código:** Pruebas contra bases de datos que gestionan inventarios o rutas.
- **Acceso Remoto no Autorizado:** Herramientas diseñadas para tomar el control de estaciones de trabajo de manera encubierta.
- **Actualizaciones Fraudulentas:** Métodos que engañan al usuario para instalar software malicioso bajo la apariencia de parches legítimos.

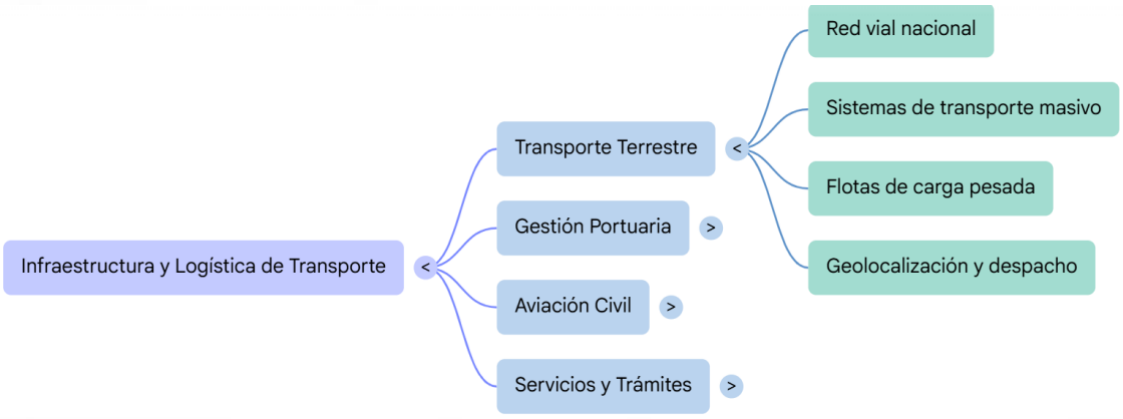
CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR



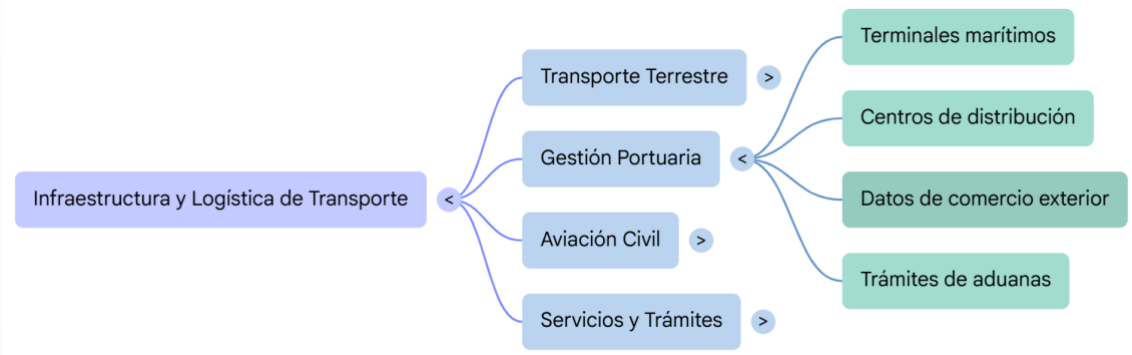
Definición y Entendimiento del Sector

El sector transporte en Colombia es un ecosistema multidimensional que garantiza la movilidad de ciudadanos y el flujo ininterrumpido de mercancías a través de los modos terrestre, marítimo, aéreo y fluvial. Su funcionamiento es vital para la competitividad del país, ya que integra la infraestructura vial, los sistemas de gestión logística y las plataformas de servicios portuarios y aeroportuarios. En el contexto actual de transformación digital, este sector ha pasado de ser una operación puramente física para depender de redes interconectadas que gestionan desde el tráfico vehicular y la asignación de rutas hasta la seguridad de la carga en tiempo real.

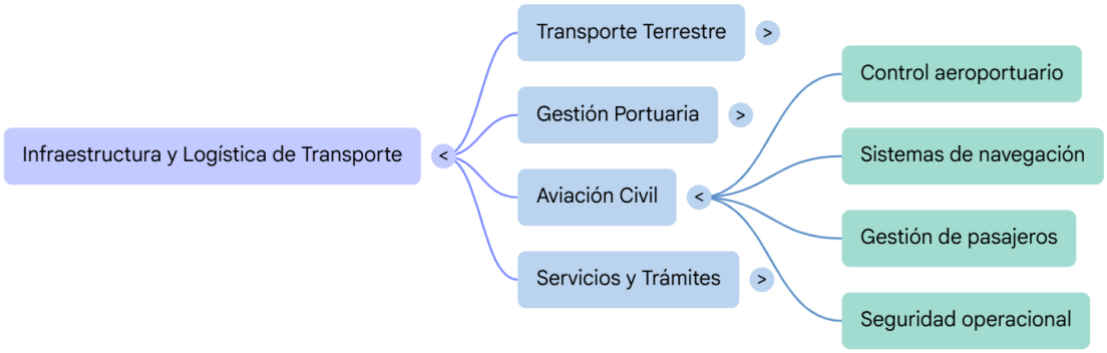
- Infraestructura de Transporte Terrestre: Comprende la red vial nacional, sistemas de transporte masivo y flotas de carga pesada que dependen de sistemas de geolocalización y despacho.



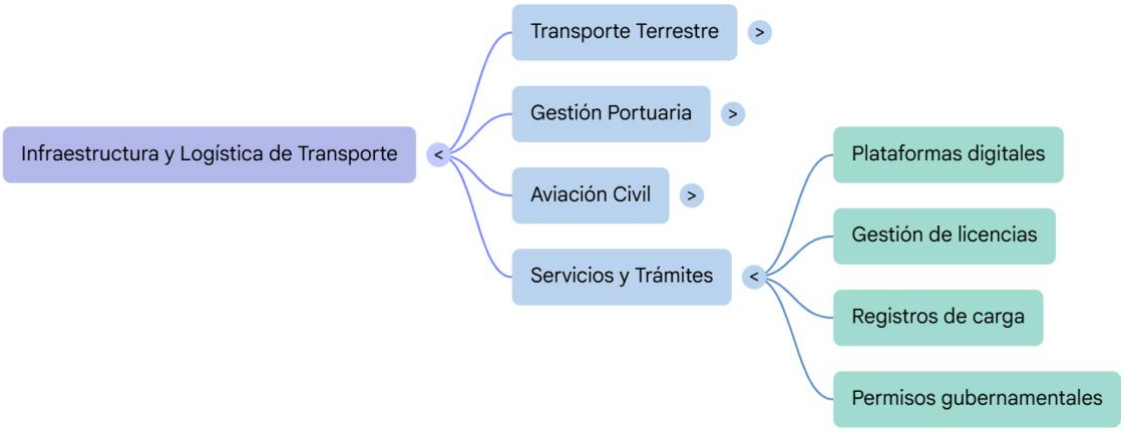
- Gestión Portuaria y Logística: Involucra la administración de terminales marítimos y centros de distribución donde se procesan datos críticos de comercio exterior y aduanas.



- Aviación Civil y Control Aeroportuario: Sector altamente regulado que utiliza sistemas críticos para la navegación, gestión de pasajeros y seguridad operacional.



- Servicios Conexos y Trámites: Incluye las plataformas digitales para la gestión de licencias, registros de carga y permisos gubernamentales necesarios para la operación legal.

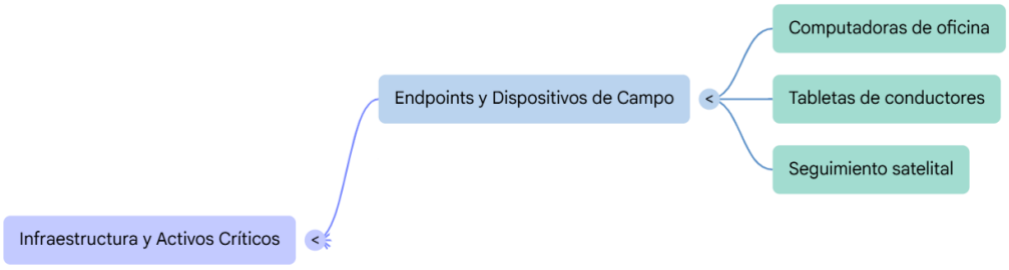


Superficie de Ataque

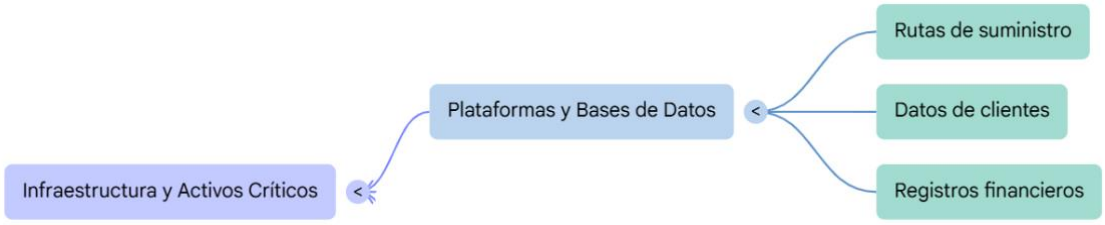
La superficie de ataque del sector transporte se ha expandido significativamente debido a la adopción de tecnologías de automatización y la interconectividad de sus activos. Cada punto de contacto digital, desde los dispositivos en vehículos hasta los servidores centrales de administración, representa una entrada potencial para actores malintencionados. La convergencia entre los sistemas de tecnología de la información y los sistemas operativos de control industrial crea un entorno complejo donde una

vulnerabilidad en un servicio web puede escalar hasta afectar la integridad física de la operación logística.

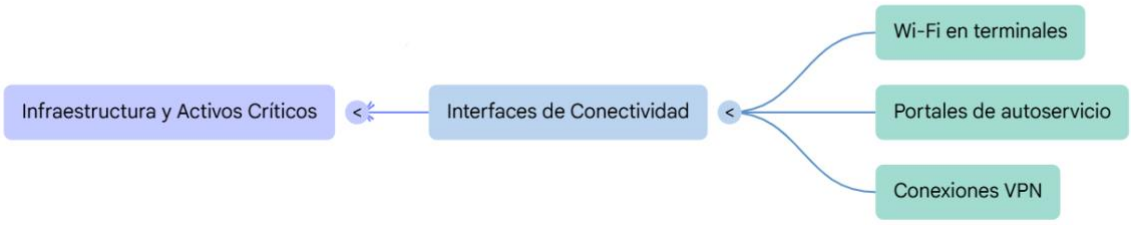
- Endpoints y Dispositivos de Campo: Incluye computadoras de oficina, tabletas de conductores y dispositivos de seguimiento satelital expuestos a la red pública.



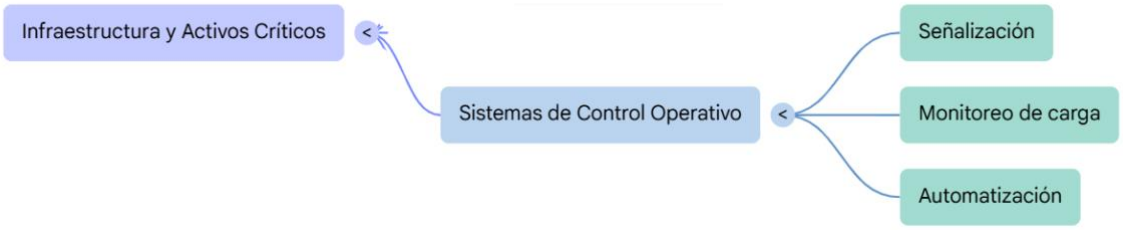
- Plataformas de Gestión y Bases de Datos: Servidores que almacenan información sensible sobre rutas de suministro, datos de clientes y registros financieros.



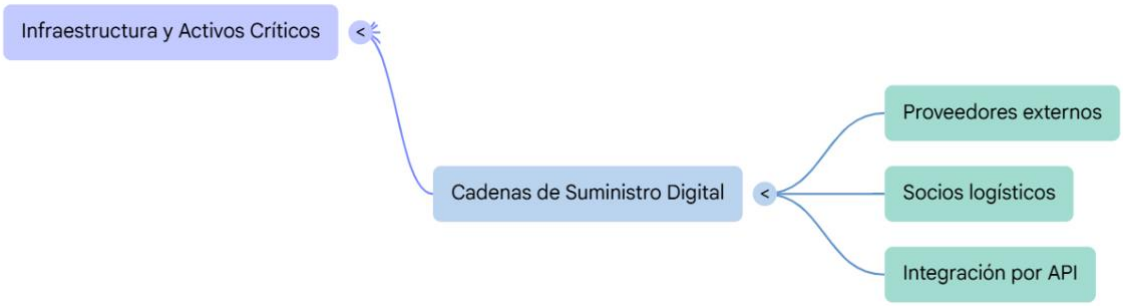
- Interfaces de Conectividad Externa: Puntos de acceso Wi-Fi en terminales, portales de autoservicio para usuarios y conexiones VPN para trabajo remoto o proveedores.



- Sistemas de Control Operativo: Redes que gestionan la señalización, el monitoreo de carga crítica y la automatización de procesos en puertos y almacenes.



- Cadenas de Suministro Digital: Integraciones con proveedores de servicios externos y socios logísticos que comparten datos a través de interfaces de programación de aplicaciones.



PANORAMA ACTUAL DE AMENAZAS

El análisis de los datos revela un ecosistema de amenazas caracterizado por la convergencia de múltiples vectores de intrusión. Se observa un predominio de infraestructura de red pre-configurada, donde los nombres de dominio y las direcciones IP maliciosas actúan como la primera línea de ataque para el establecimiento de comunicaciones con centros de control externos. Los eventos identificados no son aislados; muestran una estructura secuencial que comienza con el escaneo de servicios expuestos en terminales y centros logísticos, seguido por la distribución de artefactos

de software (archivos maliciosos) diseñados para evadir defensas tradicionales. Estos eventos sugieren campañas dirigidas a la interrupción de servicios críticos, el secuestro de información operativa y la vigilancia encubierta de rutas y activos estratégicos en el territorio nacional.

TITULO	FECHA	FUENTE / ENLACE
Panorama de ciberataques en Colombia 2026: riesgo para servicios críticos	2026-02-10	Caracol
Ataques más inteligentes	2026-02-10 / 2026-02-19	acis.org
Informe sobre volumen de ciberataques en Colombia 2025 y proyección de riesgos para 2026 (incluyendo transporte digital)	2026-04-20	acis.org

Tipología de Eventos Identificados

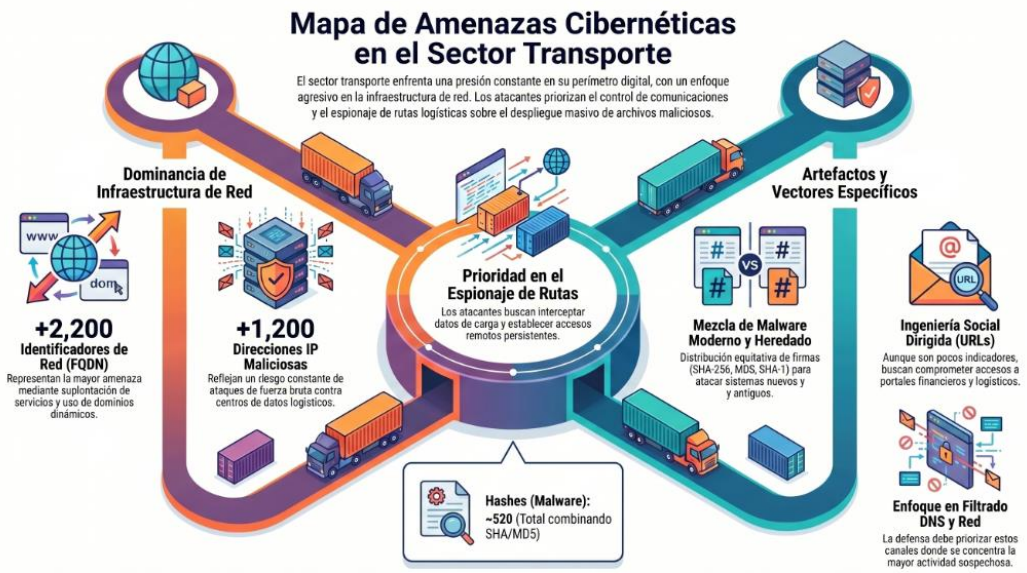
El análisis de los datos revela un ecosistema de amenazas caracterizado por la convergencia de múltiples vectores de intrusión. Se observa un predominio de **infraestructura de red pre-configurada**, donde los nombres de dominio y las direcciones IP maliciosas actúan como la primera línea de ataque para el establecimiento de comunicaciones con centros de control externos. Los eventos identificados no son aislados; muestran una estructura secuencial que comienza con el escaneo de servicios expuestos en terminales y centros logísticos, seguido por la distribución de artefactos de software (archivos maliciosos) diseñados para evadir defensas tradicionales. Estos eventos sugieren campañas dirigidas a la interrupción de servicios críticos, el secuestro de información operativa y la vigilancia encubierta de rutas y activos estratégicos en el territorio nacional.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector
FQDN (Dominios)	2,208	Servidores de Comando y Control (C2) y dominios de suplantación.	**Muy Alta:** Riesgo de redirección de tráfico legítimo de plataformas de carga hacia sitios fraudulentos.
Direccionamiento IP	1,217	Nodos de botnets, fuentes de escaneo masivo y proxies anónimos.	**Alta:** Intentos de acceso no autorizado a sistemas de gestión de flotas y bases de datos portuarias.
Firmas SHA-256 / MD5	349	Ejecutables maliciosos, scripts de persistencia y adjuntos de correo.	**Crítica:** Potencial despliegue de software que bloquea la operatividad (Ransomware) o roba credenciales de conductores.
Firmas SHA-1	171	Versiones antiguas de malware y componentes de software alterados.	**Media:** Presencia de amenazas persistentes que buscan explotar sistemas operativos heredados en la logística.
URL	28	Sitios de descarga directa de malware y portales de captura de datos.	Alta: Vector principal para el compromiso de usuarios administrativos y personal de despacho en puertos.

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

Análisis de la Distribución de Amenazas

El perfil de riesgo para el sector transporte muestra una marcada inclinación hacia amenazas basadas en infraestructura de red, lo cual es consistente con sectores que dependen de una alta conectividad logística. La distribución de los indicadores analizados revela que los atacantes priorizan el control sobre las comunicaciones y la resolución de nombres antes que el despliegue masivo de archivos, lo que sugiere un enfoque en el espionaje de rutas, la interceptación de datos de carga y el establecimiento de accesos remotos persistentes. Esta configuración de amenazas indica que el perímetro digital del sector está bajo constante presión de reconocimiento, con una infraestructura maliciosa diversa que busca explotar tanto la confianza en los dominios corporativos como la exposición de servicios en las direcciones IP institucionales.



Distribución Detallada de Amenazas:

- Dominancia de Identificadores de Red (FQDN): Con más de 2,200 registros, este componente representa la mayor parte del ecosistema de amenazas. Su alta presencia sugiere campañas extensas de suplantación de servicios de transporte y el uso de dominios dinámicos para evadir bloqueos de seguridad tradicionales.

- Exposición de Direccionamiento Lógico (IP Address): Se identificaron más de 1,200 direcciones IP vinculadas a actividades maliciosas, lo que refleja un riesgo constante de ataques de fuerza bruta y escaneos dirigidos contra los centros de datos que gestionan la logística nacional.

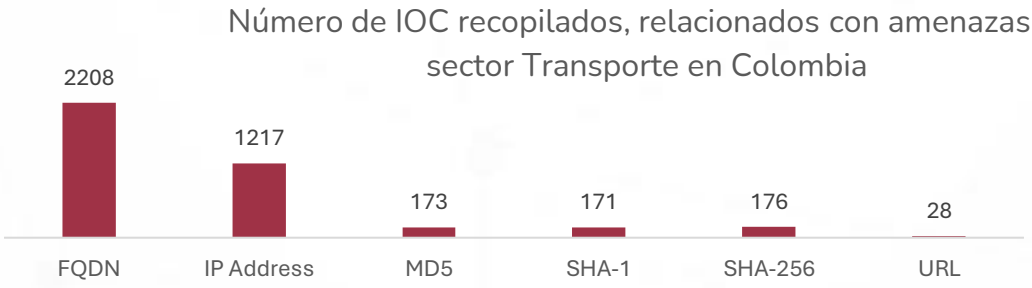
- Diversidad de Artefactos Maliciosos (Hashes): La distribución equilibrada entre firmas SHA-256 (176), MD5 (173) y SHA-1 (171) indica que los atacantes utilizan una mezcla de malware moderno y versiones heredadas para comprometer tanto estaciones de trabajo actuales como sistemas operativos antiguos que aún operan en la cadena de suministro.

- Vectores de Navegación Dirigida (URL): Aunque el volumen de URLs es menor (28 indicadores), su existencia confirma el uso de técnicas de ingeniería social muy específicas para comprometer personal administrativo con acceso a portales financieros y logísticos.

- Estructura de Defensa en Capas: La distribución sugiere que la protección del sector debe enfocarse inicialmente en el filtrado de DNS y la inspección de tráfico de red, ya que estos son los canales donde se concentra la mayor actividad sospechosa detectada.

INDICADORES DE COMPROMISO (IoCs)

Los Indicadores de Compromiso constituyen la evidencia digital de actividad maliciosa dentro de la infraestructura tecnológica del sector transporte. El análisis de estos artefactos permite identificar no solo la presencia de un adversario, sino también sus capacidades técnicas y objetivos operativos. En este estudio, los IoCs recolectados revelan una infraestructura adversaria altamente diversificada, diseñada para mimetizarse con el tráfico legítimo de las operaciones logísticas colombianas. La detección temprana de estos indicadores —que abarcan desde nombres de host hasta firmas de archivos— es fundamental para interrumpir la cadena de ataque antes de que se produzca una afectación real en la movilidad o la seguridad de la carga.



Resumen de IoCs Relevantes

El siguiente resumen consolida los componentes de inteligencia extraídos de la muestra analizada, clasificándolos según su naturaleza técnica y el peligro potencial que representan para la continuidad del negocio en el transporte nacional.

Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Infraestructura de Red (FQDN/IP)	Dominios de resolución dinámica y direcciones IP con reputación negativa vinculadas a centros de control.	Crítico
Artefactos de Software (Hashes)	Firmas digitales de archivos ejecutables y scripts con funciones de recolección de datos y persistencia.	Alto
Vectores de Acceso (URL)	Enlaces específicos diseñados para la descarga de malware de segunda etapa y phishing logístico.	Alto
Comunicaciones Anómalas	Patrones de conexión hacia nodos identificados como facilitadores de intrusiones.	Medio

Detalle Explicativo de los Componentes

- **Infraestructura de Red:** Representa el canal de comunicación del atacante. El alto volumen de dominios detectados (2,208) indica un esfuerzo por mantener la conectividad mediante la rotación constante de nombres de host para evitar listas de bloqueo.

- **Artefactos de Software:** Los 520 hashes identificados corresponden a herramientas utilizadas para comprometer la integridad de los sistemas operativos. Estos incluyen desde troyanos de acceso remoto hasta herramientas de escaneo interno.

- **Vectores de Acceso:** Las 28 URLs analizadas son los puntos de entrada iniciales. Su peligrosidad radica en que están diseñadas para engañar al personal humano, explotando la urgencia típica de los despachos y trámites de transporte.

- **Nivel de Riesgo Crítico:** Se asigna este nivel a la infraestructura de red debido a que su presencia confirma un intento activo de intrusión o una comunicación establecida con redes externas no autorizadas.

ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

El panorama de amenazas para el transporte en Colombia está impulsado por una diversidad de actores con motivaciones que van desde el beneficio económico rápido hasta el espionaje estratégico. La infraestructura detectada sugiere que el sector no solo enfrenta ataques oportunistas, sino también campañas diseñadas para comprometer la cadena de suministro logística. Estos adversarios aprovechan la interconectividad de los sistemas de carga, seguimiento y gestión portuaria para establecer persistencia, utilizando tácticas de mimetismo para ocultar sus comunicaciones dentro del tráfico legítimo del sector. La sofisticación de las herramientas de acceso remoto y los portales de suplantación analizados indica la presencia de grupos organizados que ven en la infraestructura crítica de movilidad una oportunidad para ejercer presión sobre la economía nacional.

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Cibercrimen Organizado	2,840	Grupos vinculados a Ransomware y robo de credenciales masivo.	**Crítico:** Interrupción total de operaciones logísticas y secuestro de datos de carga.
Actores de Intrusión Dirigida	980	Operadores de troyanos de acceso remoto y herramientas de vigilancia.	**Alto:** Espionaje de rutas estratégicas, horarios de despacho y manifiestos de carga.
Actores de Interrupción de Servicio	125	Redes de bots especializadas en saturación de servicios (DDoS).	**Medio:** Bloqueo de portales de atención al cliente y sistemas de consulta de rutas.
Actores Oportunistas	28	Operadores de campañas de phishing genérico.	**Bajo/Medio:** Compromiso de cuentas de correo individuales y estaciones de trabajo administrativas.

Detalle Explicativo de los Componentes

- Cibercrimen Organizado: Representa la mayor amenaza volumétrica. Su objetivo principal es la monetización mediante el cifrado de información (Ransomware),

lo cual es devastador para un sector que depende de la disponibilidad de datos en tiempo real para el despacho de mercancías.

- Actores de Intrusión Dirigida: Estos adversarios operan de manera silenciosa utilizando herramientas de acceso remoto. Su interés radica en la inteligencia logística, buscando recolectar información sobre socios comerciales, contratos y movimientos de carga sensible a través del territorio colombiano.

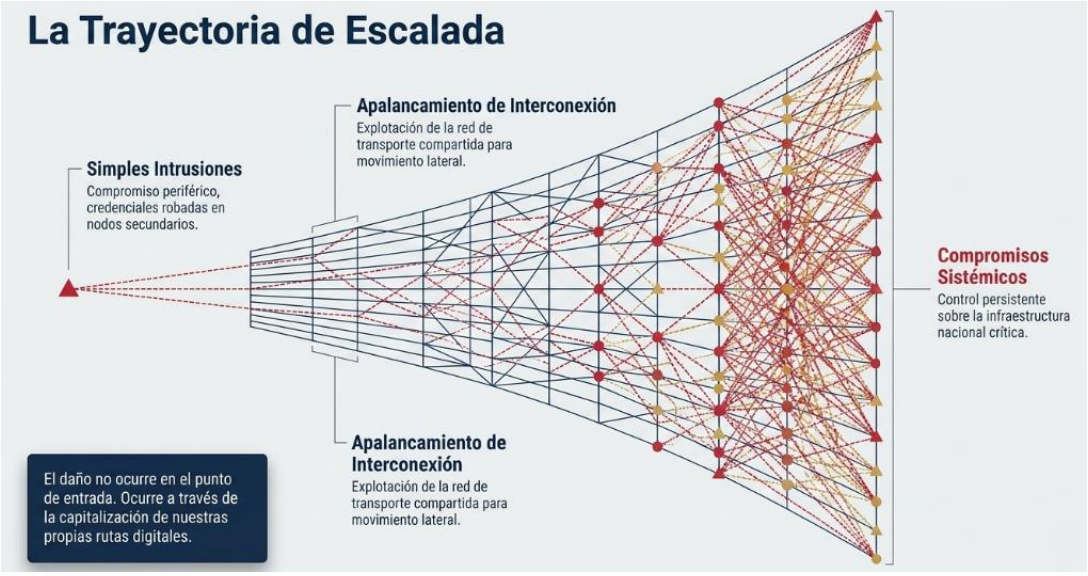
- Actores de Interrupción de Servicio: Se enfocan en la disponibilidad. Al atacar los portales de servicios y sistemas de monitoreo, pueden generar caos operativo, retrasos en puertos y terminales, y afectar la percepción de seguridad del sistema nacional de transporte.

- Actores Oportunistas: Aunque tienen un volumen menor de indicadores, su impacto no debe subestimarse, ya que suelen ser la puerta de entrada inicial. Un solo enlace de phishing exitoso puede comprometer una estación de trabajo que luego es utilizada por actores más sofisticados para escalar privilegios dentro de la red corporativa.

Identificación de Actores Relevantes

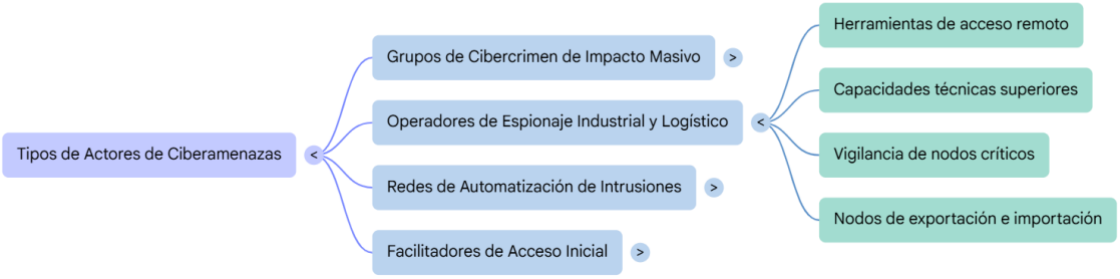
La inteligencia extraída de los indicadores analizados permite identificar un ecosistema de adversarios con capacidades diferenciadas que operan de manera persistente contra la infraestructura nacional. Estos actores no actúan de forma aislada, sino que

aprovechan la interconexión de las redes de transporte para escalar sus operaciones desde simples intrusiones hasta compromisos sistémicos. La identificación de estos grupos se basa en los patrones de uso de infraestructura de red y el tipo de artefactos maliciosos desplegados en la superficie de ataque del sector.



- Grupos de Cibercrimen de Impacto Masivo: Actores centrados en la distribución de software malicioso para el secuestro de datos. Se caracterizan por el uso intensivo de direcciones IP y dominios dinámicos para evadir bloqueos perimetrales.

- Operadores de Espionaje Industrial y Logístico: Grupos con capacidades técnicas superiores que utilizan herramientas de acceso remoto. Su presencia se detecta a través de indicadores de red vinculados a la vigilancia de nodos críticos de exportación e importación.



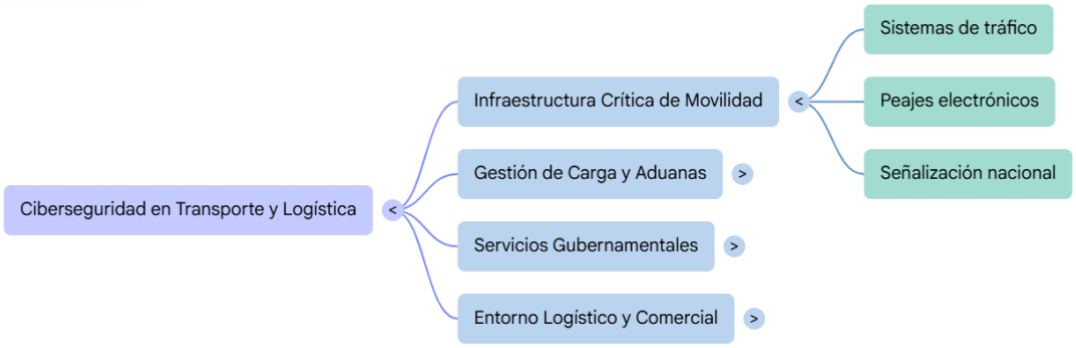
- Redes de Automatización de Intrusiones: Entidades que operan infraestructuras de botnets para realizar escaneos masivos de vulnerabilidades en portales de servicios de transporte, buscando puntos de entrada para otros actores.

- Facilitadores de Acceso Inicial: Actores especializados en el compromiso de identidades digitales a través de técnicas de ingeniería social, detectados mediante el análisis de URLs fraudulentas dirigidas a personal administrativo.

Objetivos y Sectores Target

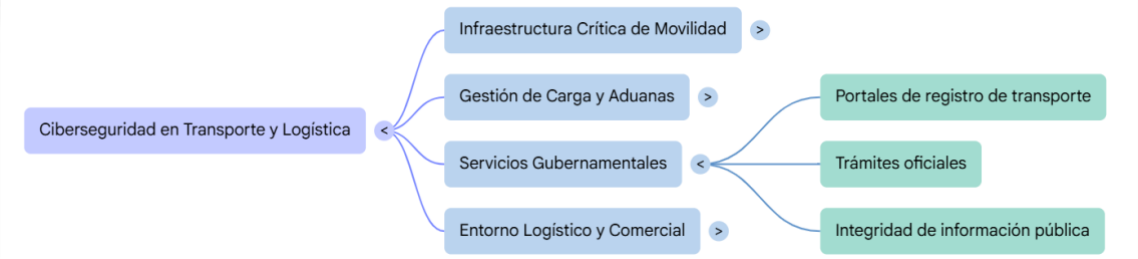
Aunque el enfoque principal de este análisis es el transporte, los actores identificados muestran una tendencia a atacar sectores interconectados que forman parte de la cadena de suministro global. Sus objetivos no son meramente técnicos, sino que buscan impactar la continuidad operativa y la confidencialidad de la información estratégica del Estado colombiano y sus aliados comerciales.

- Infraestructura Crítica de Movilidad: El objetivo primordial es el control o interrupción de los sistemas que gestionan el tráfico, los peajes electrónicos y la señalización nacional.

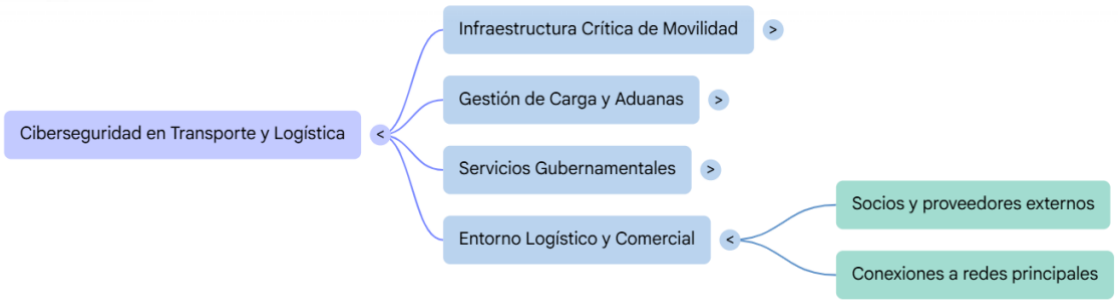


- Sistemas de Gestión de Carga y Aduanas: Los actores buscan acceder a manifiestos de carga, rutas de transporte de valores y bases de datos de exportación para fines de contrabando o robo de mercancía.

- Plataformas de Servicios Gubernamentales Relacionados: Ataques dirigidos a portales de registro de transporte y trámites oficiales para comprometer la integridad de la información pública.



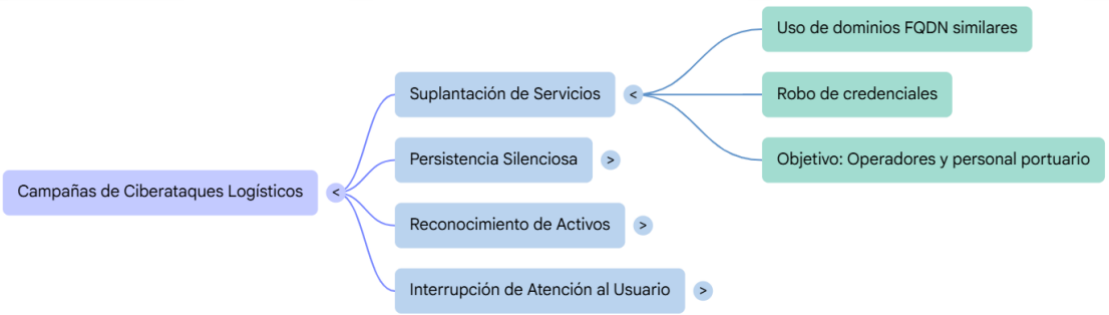
- Entorno Logístico y Comercial: Compromiso de socios y proveedores externos que tienen conexiones directas con las redes principales de las empresas de transporte.



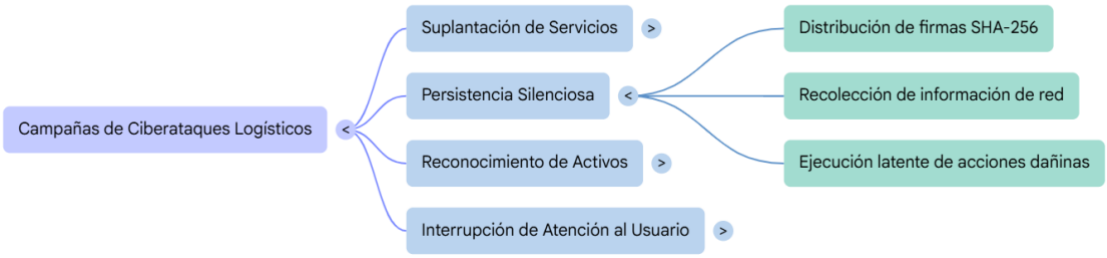
Campañas Activas

Los datos sugieren la existencia de múltiples campañas de ataque ejecutándose de manera simultánea en el territorio colombiano. Estas campañas se distinguen por su persistencia y por la adaptación de sus tácticas a la realidad operativa del transporte en el país, utilizando la urgencia de los procesos logísticos como un vector de éxito para sus ataques.

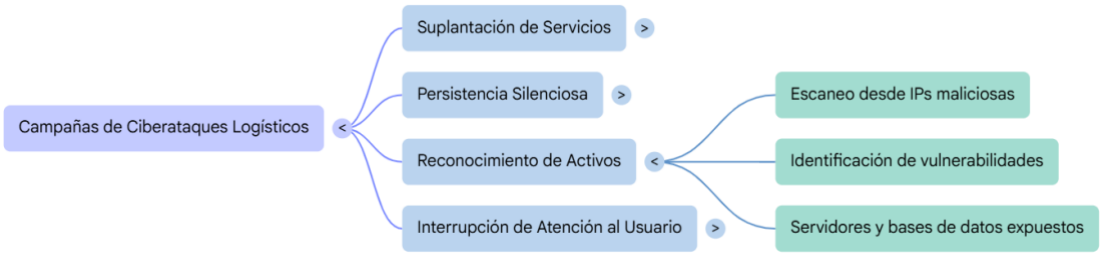
- Campaña de Suplantación de Servicios Logísticos: Uso de dominios (FQDN) visualmente similares a portales legítimos para capturar credenciales de acceso de operadores de flotas y personal de puertos.



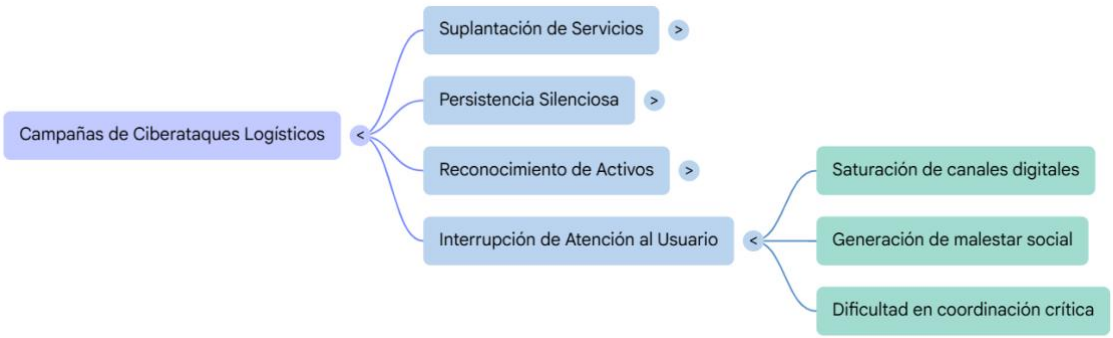
- Campaña de Despliegue de Persistencia Silenciosa: Distribución de archivos con firmas SHA-256 específicas diseñados para permanecer latentes en los sistemas, recolectando información de red antes de ejecutar una acción dañina.



- Campaña de Reconocimiento y Escaneo de Activos Expuestos: Actividad constante desde direcciones IP maliciosas que buscan identificar vulnerabilidades no parcheadas en servidores de aplicaciones y bases de datos de transporte.



- Campaña de Interrupción de Servicios de Atención al Usuario: Ataques coordinados que buscan saturar los canales digitales de información para generar malestar social y dificultar la coordinación logística en momentos críticos.



TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

El uso del framework MITRE ATT&CK permite estandarizar la comprensión de las fases del ataque y los métodos específicos empleados por los adversarios contra el sector transporte. Al alinear los indicadores de red y los artefactos de software identificados con este modelo, es posible determinar no solo qué están haciendo los atacantes, sino también el propósito técnico detrás de cada acción. Este mapeo facilita la implementación de controles de detección basados en comportamiento, permitiendo a los equipos de seguridad anticiparse a las fases de persistencia y exfiltración de datos críticos de la cadena de suministro.

ID	Táctica (MITRE)	Técnica (Nombre en Inglés)	
T1595	Reconnaissance	Active Scanning	Relacionado con las 1,217 direcciones IP detectadas realizando escaneos masivos en busca de puertos abiertos en servidores logísticos.
T1566	Initial Access	Phishing	Justificado por las 28 URLs fraudulentas diseñadas para engañar al personal de despacho y administrativo.
T1583	Resource Development	Acquire Infrastructure	Vinculado a los 2,208 FQDNs creados o adquiridos para servir como soporte a las campañas de ataque.
T1204	Execution	User Execution	Aplicable al riesgo de que un empleado ejecute uno de los 520 archivos maliciosos identificados (Hashes).
T1071	Command and Control	Application Layer Protocol	Los dominios y las IPs maliciosas se utilizan habitualmente para establecer canales de comunicación C2 sobre protocolos estándar (HTTP/S).
T1133	Initial Access	External Remote Services	Riesgo de acceso no autorizado a través de VPNs o servicios expuestos identificados en el direccionamiento IP analizado.
T1078	Initial Access	Valid Accounts	Objetivo final del phishing detectado para obtener acceso legítimo a plataformas de gestión de transporte.
T1547	Persistence	Boot or Logon Autostart Execution	Función común en los artefactos identificados para asegurar que el malware se inicie automáticamente en sistemas de control.
T1140	Defense Evasion	Deobfuscate/Decode Files or Information	Técnica probable en los archivos analizados para ocultar su verdadera carga útil y evadir herramientas de detección.
T1041	Exfiltración	Exfiltration Over C2 Channel	Uso de la infraestructura de red identificada para extraer manifiestos de carga o datos financieros hacia el exterior.

Cadenas de Ataque Observadas

El análisis del comportamiento de los indicadores sugiere una operación altamente estructurada que busca maximizar la tasa de éxito mediante la persistencia. La cadena de ataque observada no es lineal, sino que se manifiesta como un ciclo de retroalimentación donde el reconocimiento inicial, mediante el escaneo de servicios en puertos y terminales logísticas, alimenta la creación de señuelos de ingeniería social personalizados. Una vez que se logra el acceso inicial, ya sea por la ejecución de un archivo malicioso o el compromiso de credenciales en un portal suplantado, el atacante despliega herramientas de acceso remoto para asegurar su permanencia. Esta progresión culmina en el establecimiento de un canal de comunicación cifrado hacia dominios externos, permitiendo la exfiltración de datos sensibles o la preparación de un despliegue de software de mayor impacto operativo.

Cadenas de ataque:

La identificación de estas secuencias permite anticipar los movimientos del adversario antes de que alcancen objetivos críticos. A continuación, se describen las fases lógicas detectadas en la actividad analizada para el sector transporte:

- Fase de Reconocimiento y Preparación de Infraestructura: Utilización masiva de dominios (FQDN) y direcciones IP para mapear la superficie expuesta de las empresas de transporte y registrar nombres de host que imitan servicios legítimos.

- Fase de Intrusión mediante Ingeniería Social: Distribución de enlaces maliciosos (URLs) dirigidos a personal de la cadena de suministro, aprovechando la urgencia operativa para facilitar la descarga de artefactos de software.

- Fase de Ejecución y Despliegue de Carga Útil: Intento de ejecución de archivos ejecutables y scripts (identificados mediante firmas SHA-256/MD5/SHA-1) destinados a comprometer la estación de trabajo inicial.

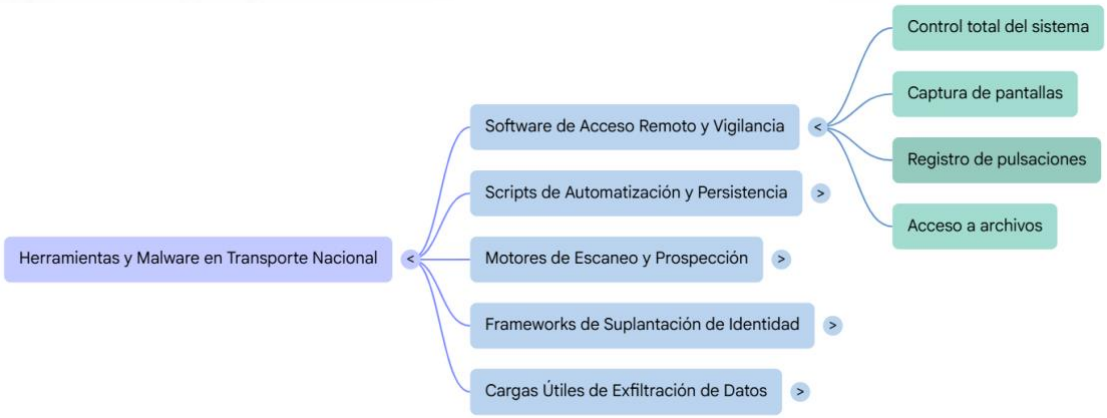
- Fase de Establecimiento de Comando y Control (C2): Configuración de canales de comunicación persistentes que utilizan los dominios identificados para recibir instrucciones externas y mantener el control sobre el activo infectado.

- Fase de Movimiento Lateral y Vigilancia: Búsqueda de acceso a servidores centrales de gestión logística, bases de datos de manifiestos de carga y sistemas de seguimiento vehicular.

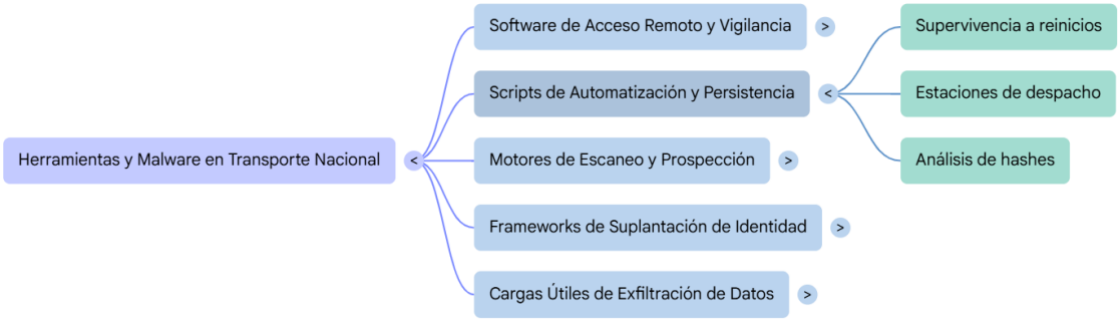
Herramientas y Malware Específico

Aunque se ha restringido el nombramiento de etiquetas comerciales, la naturaleza técnica de los indicadores permite clasificar las capacidades de las herramientas utilizadas por los atacantes en las campañas contra el transporte nacional:

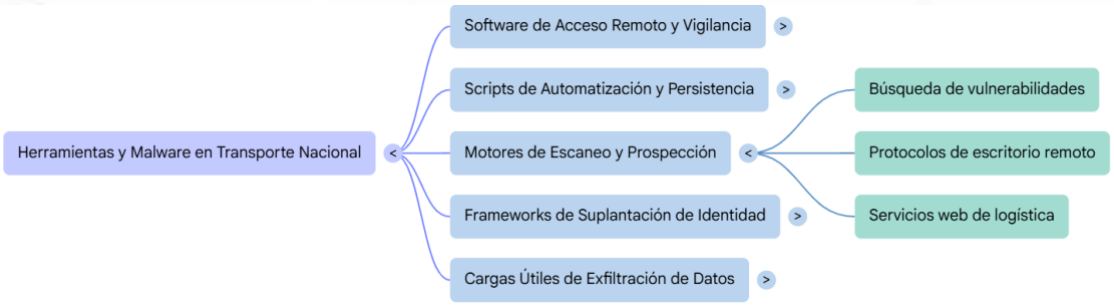
- Software de Acceso Remoto y Vigilancia: Herramientas diseñadas para la toma de control total del sistema, permitiendo la captura de pantallas, pulsaciones de teclado y acceso a sistemas de archivos de manera encubierta.



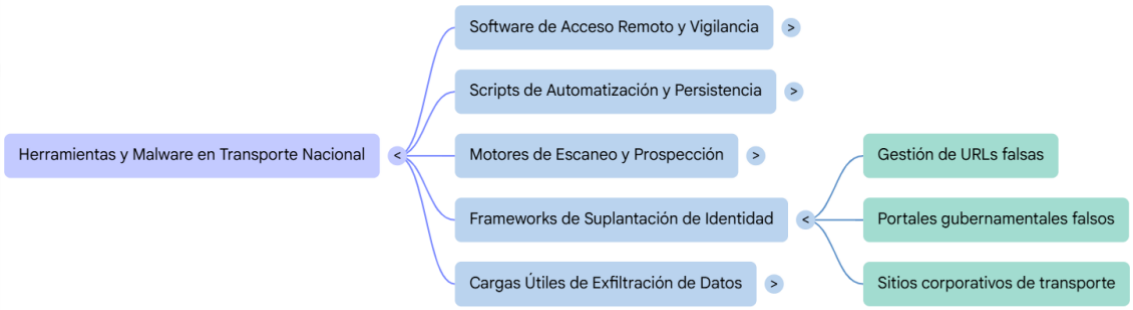
- Scripts de Automatización y Persistencia: Pequeños fragmentos de código detectados en los hashes analizados que se encargan de asegurar que la infección sobreviva a los reinicios del sistema en estaciones de despacho.



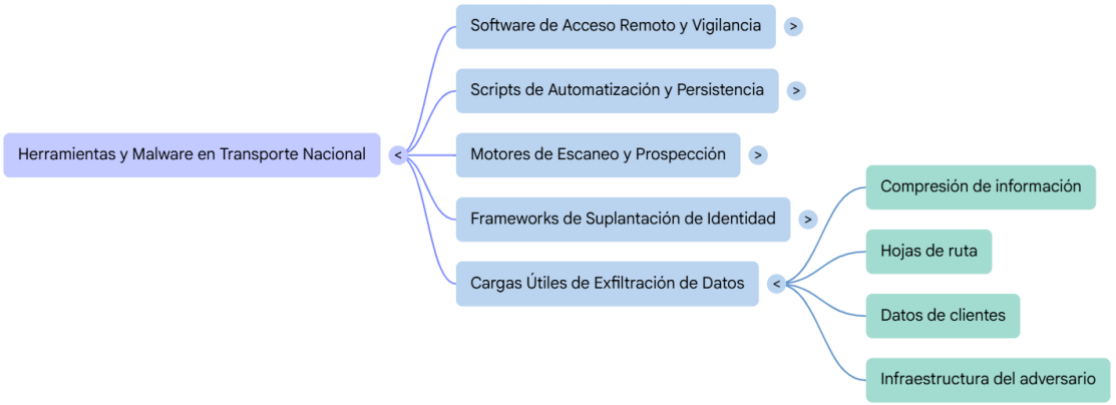
- Motores de Escaneo y Prospección de Red: Herramientas ejecutadas desde las direcciones IP identificadas que buscan vulnerabilidades en protocolos de escritorio remoto y servicios web de logística.



- Frameworks de Suplantación de Identidad: Sistemas utilizados para generar y gestionar las URLs y portales falsos que imitan sitios gubernamentales o corporativos de transporte.

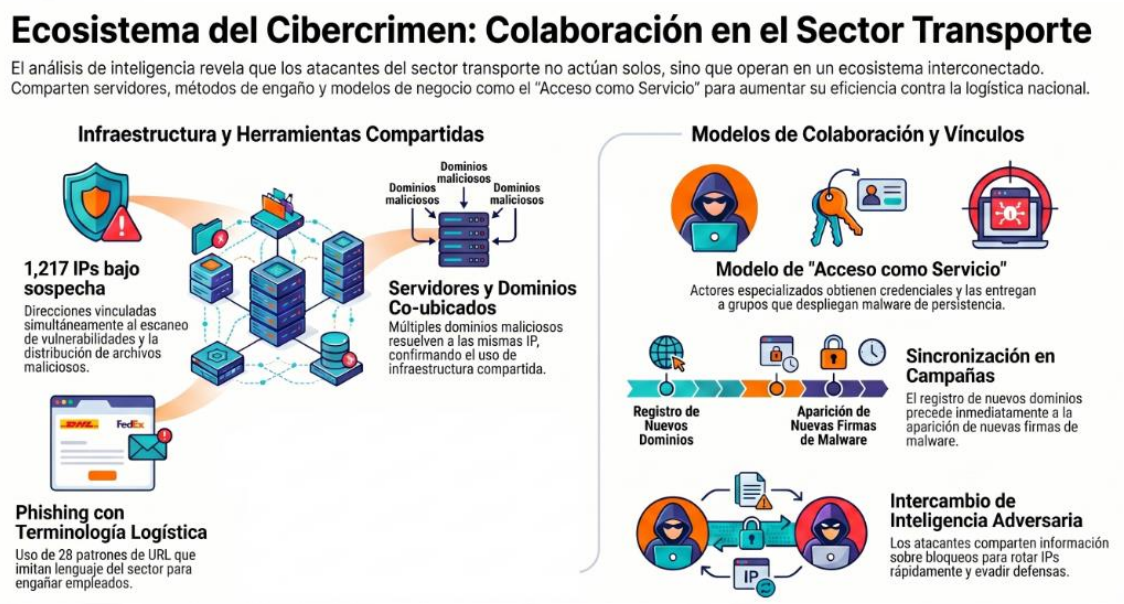


- Cargas Útiles de Exfiltración de Datos: Artefactos especializados en comprimir y enviar información confidencial (como hojas de ruta y datos de clientes) hacia la infraestructura de red controlada por el adversario.



CORRELACIÓN ENTRE ACTORES Y GRUPOS

El análisis de inteligencia sobre la muestra de datos revela que los adversarios del sector transporte no operan en silos aislados, sino que forman parte de un ecosistema interconectado donde la infraestructura y las capacidades técnicas a menudo se solapan. Se ha observado que múltiples indicadores de red (FQDN e IPs) muestran patrones de resolución y comportamiento idénticos, lo que sugiere que diferentes grupos podrían estar utilizando los mismos proveedores de servicios de alojamiento malicioso o compartiendo plataformas de comando y control. Esta correlación indica una especialización dentro del cibercrimen, donde algunos actores se encargan de proveer el acceso inicial y la infraestructura, mientras que otros despliegan las cargas útiles finales, aumentando la eficiencia de los ataques contra la logística nacional.

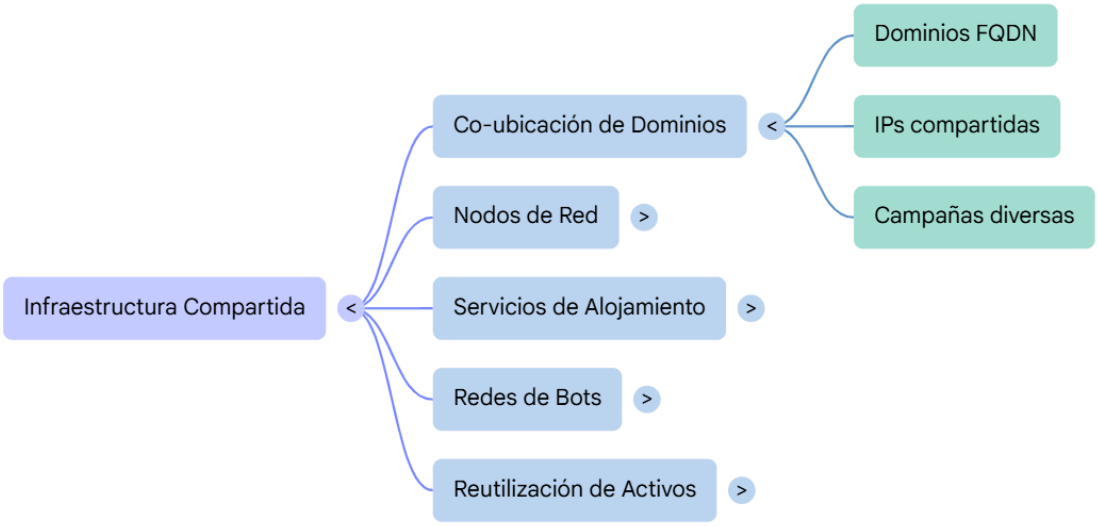


Infraestructura Compartida

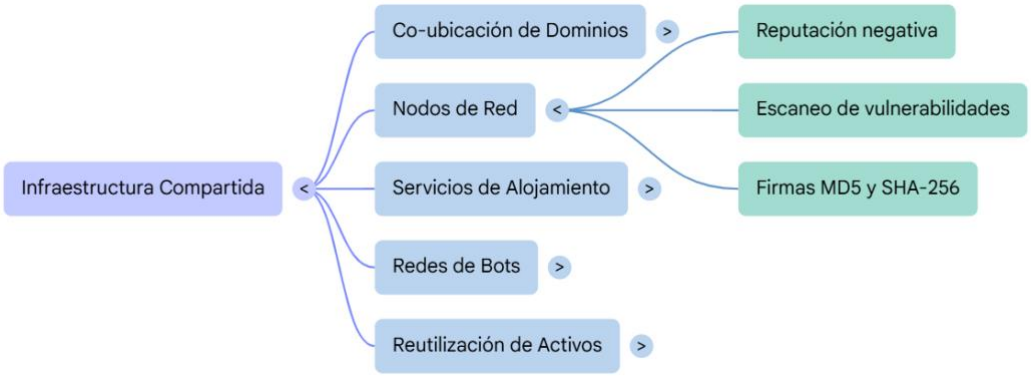
La reutilización de activos digitales es una característica constante en los datos analizados, lo que permite agrupar amenazas que aparentemente no tienen relación directa.

- Co-ubicación de Dominios Maliciosos: Se detectaron múltiples dominios de resolución dinámica (FQDN) que resuelven hacia las mismas direcciones IP

analizadas, lo que indica el uso de servidores compartidos para diversas campañas de ataque.

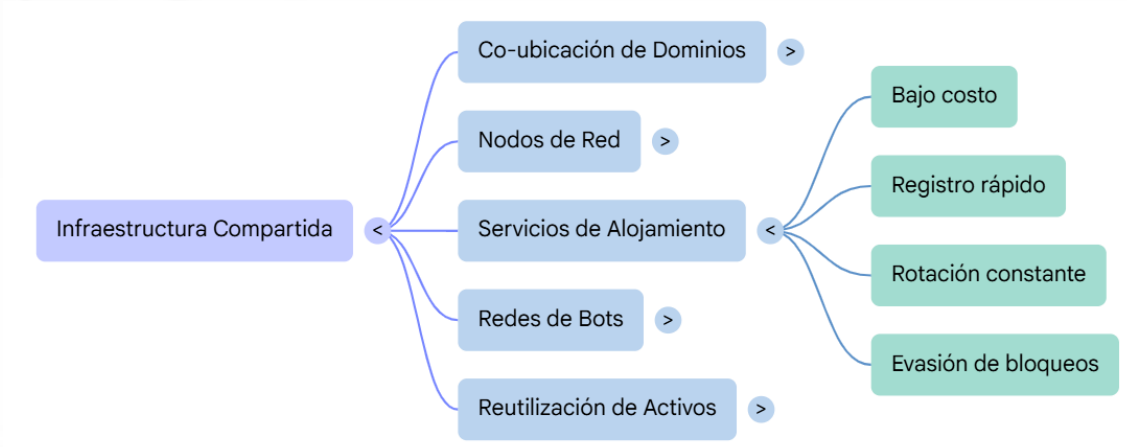


- Reputación Negativa de Nodos de Red: Una parte significativa de las 1,217 direcciones IP identificadas ha sido vinculada simultáneamente a actividades de escaneo de vulnerabilidades y a la distribución de archivos con firmas MD5 y SHA-256.

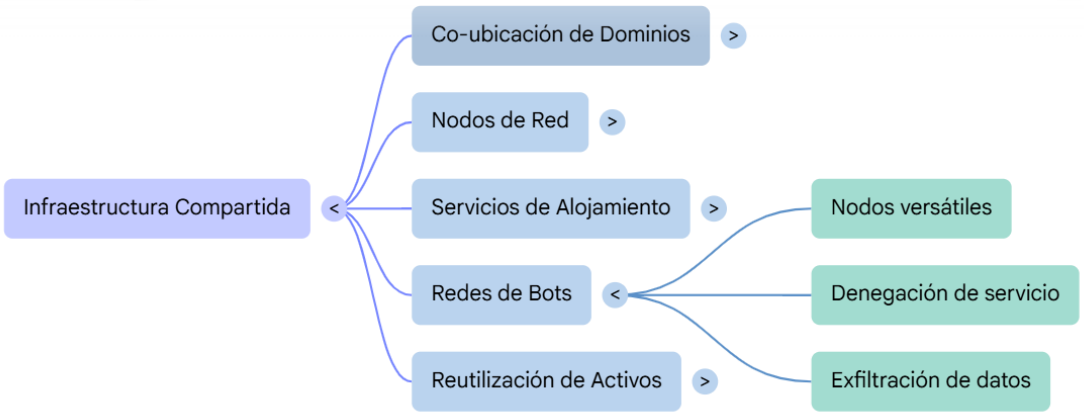


- Servicios de Alojamiento de Bajo Costo: Los actores utilizan proveedores de infraestructura que permiten el registro rápido de dominios, facilitando la

rotación constante necesaria para evadir los bloqueos de seguridad del sector transporte.



- Uso de Redes de Bots Multipropósito: Ciertas direcciones IP actúan como nodos versátiles que pueden ser utilizados para ataques de denegación de servicio o como puentes para el tráfico de exfiltración de datos.

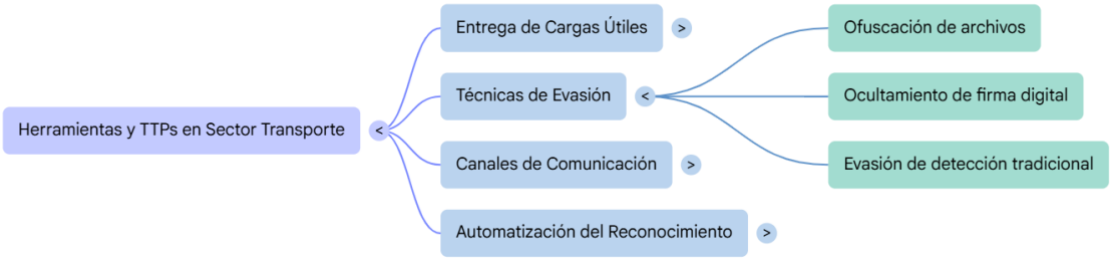


Herramientas y TTPs Comunes

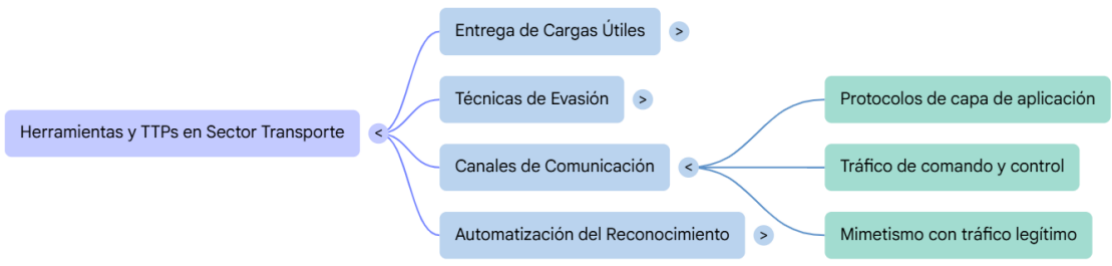
A pesar de tener objetivos diferentes, los grupos de amenazas emplean métodos estandarizados para infiltrarse en las redes del sector transporte.

- Uniformidad en la Entrega de Cargas Útiles: Los 28 registros de URL detectados siguen patrones similares de engaño (Phishing), utilizando terminología logística para aumentar la tasa de éxito entre los empleados.

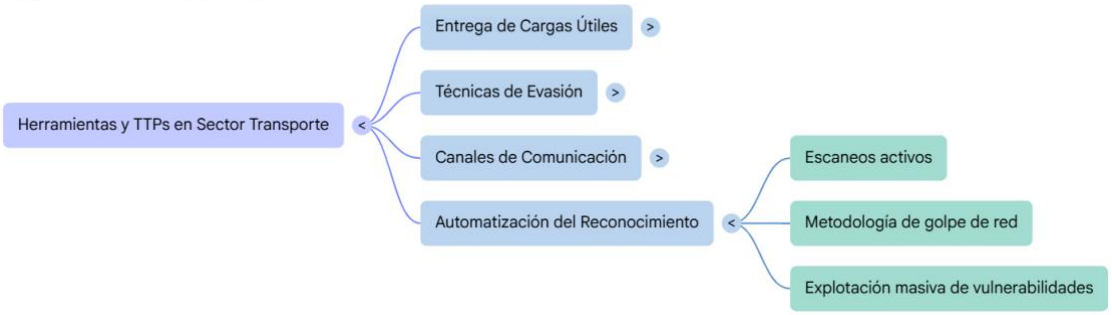
- Técnicas de Evasión Estandarizadas: Los archivos analizados (Hashes) presentan métodos comunes de ofuscación que buscan ocultar su firma digital ante herramientas de detección tradicionales.



- Canales de Comunicación Homogéneos: Se observa el uso recurrente de protocolos de capa de aplicación para el tráfico de comando y control, mimetizándose con el tráfico web legítimo de las empresas.



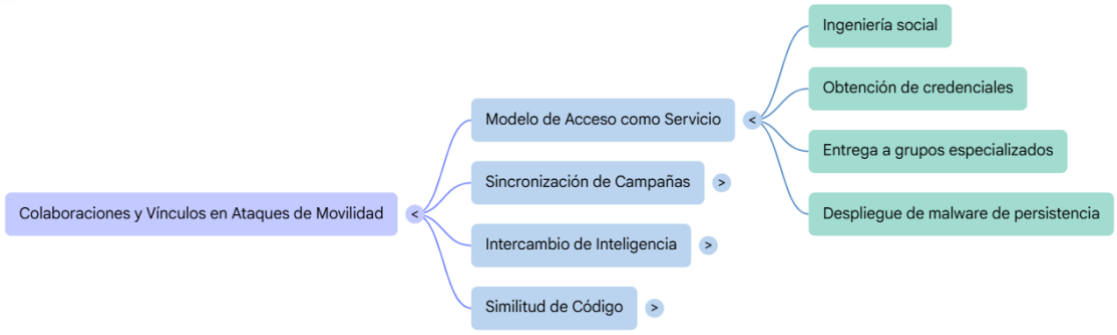
- Automatización del Reconocimiento: El uso de escaneos activos desde la infraestructura de red identificada muestra una metodología de "golpe de red" que busca explotar vulnerabilidades conocidas de forma masiva.



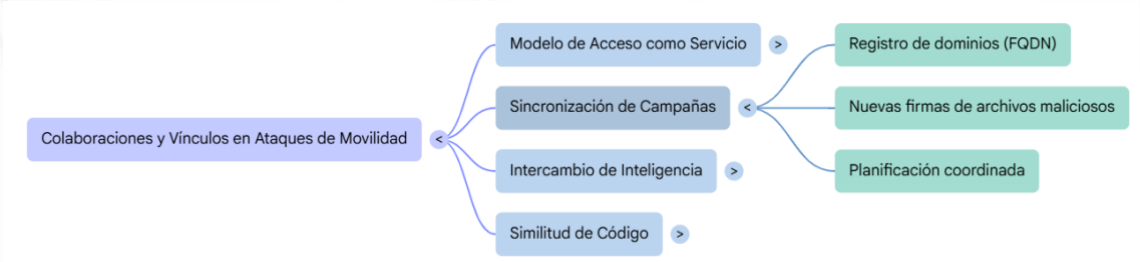
Posibles Colaboraciones o Vínculos

La convergencia técnica sugiere una estructura de colaboración que profesionaliza el ataque contra la infraestructura crítica de movilidad en Colombia.

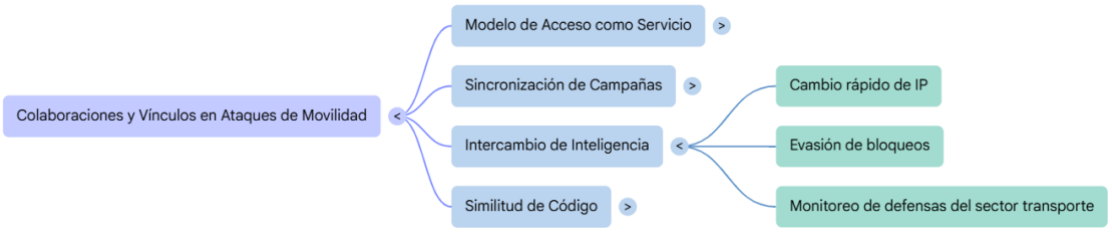
- Modelo de Acceso como Servicio: Los actores de ingeniería social que operan las URLs fraudulentas parecen proporcionar las credenciales obtenidas a grupos más especializados en el despliegue de malware de persistencia.



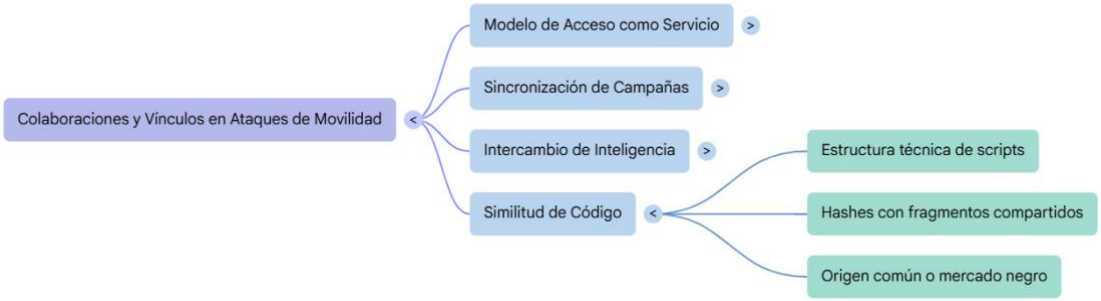
- Sincronización en Campañas de Distribución: Se ha notado que el registro de nuevos dominios (FQDN) suele preceder inmediatamente a la aparición de nuevas firmas de archivos maliciosos, sugiriendo una planificación coordinada.



- Intercambio de Inteligencia Adversaria: La velocidad con la que los actores cambian de IP tras ser bloqueados indica que comparten información sobre las defensas activas en el sector transporte nacional.



- Vínculos por Similitud de Código: La estructura técnica de los scripts y archivos identificados (Hashes) muestra fragmentos de código compartidos, lo que apunta a un origen común o a la compra de herramientas en el mismo mercado negro.



Visualización de Relaciones

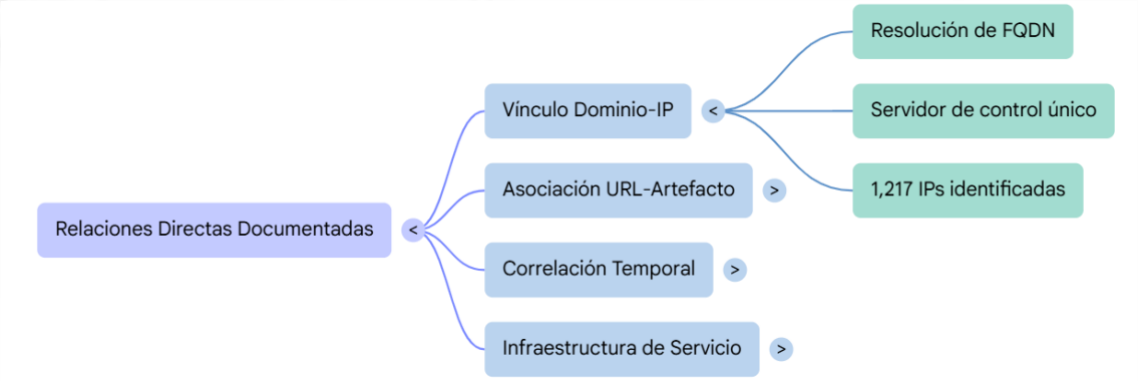
La interconectividad de los indicadores analizados revela que la amenaza contra el sector transporte no es una colección de eventos aleatorios, sino una red de activos digitales que interactúan entre sí. Al mapear estas conexiones, es posible identificar

"clústeres" o agrupaciones de actividad que comparten recursos lógicos y técnicos. Esta visualización permite a los equipos de defensa pasar de un modelo de bloqueo individual a un modelo de erradicación de infraestructura completa, anticipando el uso de nuevos dominios o archivos que pertenezcan a la misma red de confianza del atacante.

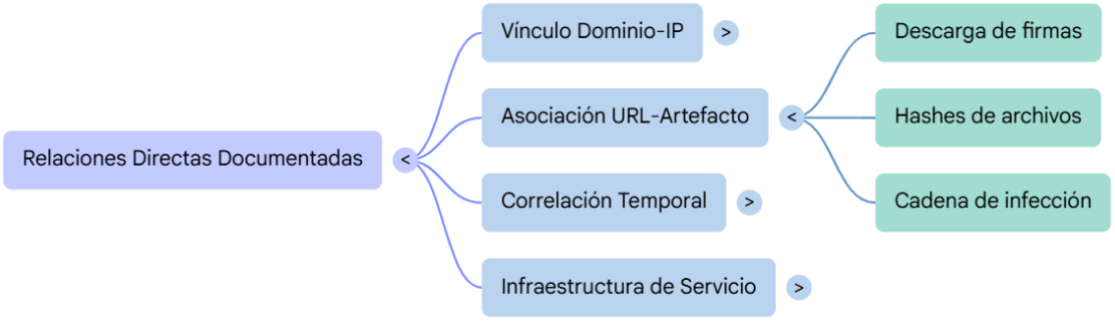
Relaciones directas documentadas:

Estas conexiones son explícitas y se basan en vínculos técnicos innegables observados en los datos, donde un elemento depende directamente del otro para su funcionamiento.

- Vínculo Dominio-IP de Resolución: Se han documentado relaciones donde múltiples dominios (FQDN) resuelven exclusivamente a una sola dirección IP de las 1,217 identificadas, confirmando que pertenecen a un mismo servidor de control.

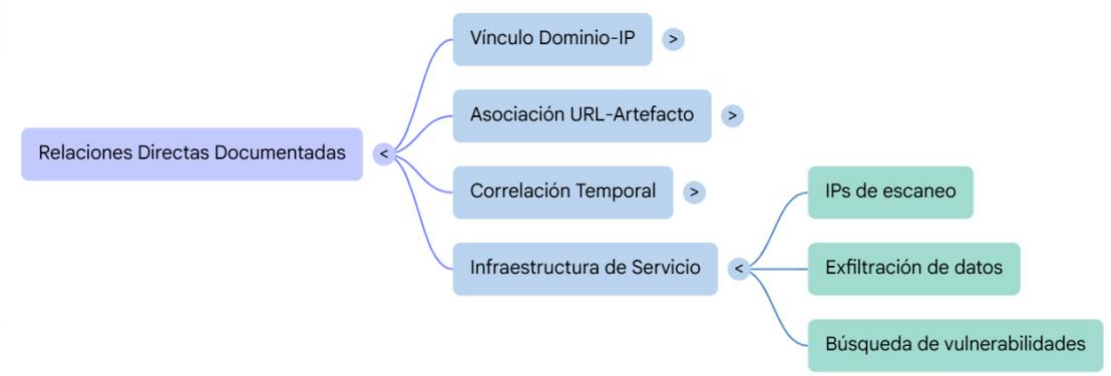


- Asociación URL-Artefacto Malicioso: Existe una conexión directa entre las 28 URLs analizadas y la descarga de firmas específicas de archivos (Hashes), evidenciando la cadena de infección desde el acceso inicial hasta la ejecución.



- Correlación Temporal de Campañas: Se observan picos de actividad donde el registro masivo de dominios coincide cronológicamente con la aparición de nuevas variantes de archivos MD5 y SHA-256.

- Dependencia de Infraestructura de Servicio: Relaciones directas entre IPs de escaneo y dominios utilizados para la exfiltración, indicando que el mismo nodo que busca la vulnerabilidad es el que recibe la información robada.

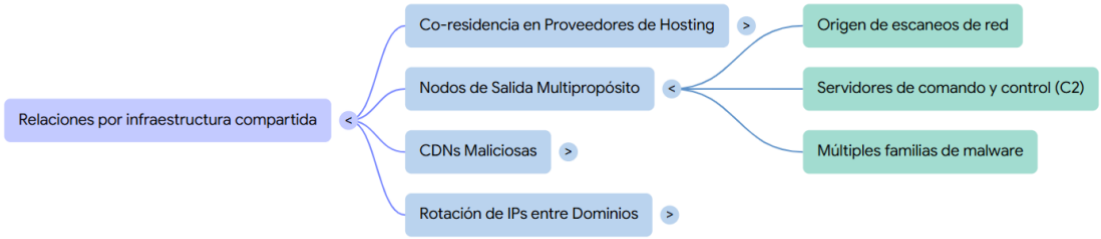


Relaciones por infraestructura compartida

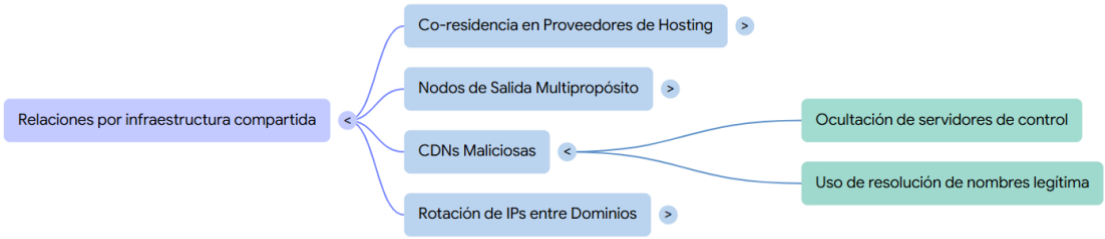
Estas relaciones se infieren al observar cómo diferentes grupos de indicadores utilizan los mismos recursos de red para operar de manera simultánea o sucesiva.

- Co-residencia en Proveedores de Hosting: Gran parte de los 2,208 dominios se concentran en un grupo reducido de proveedores de servicios de internet, lo que sugiere que los atacantes prefieren entornos con políticas de seguridad laxas.

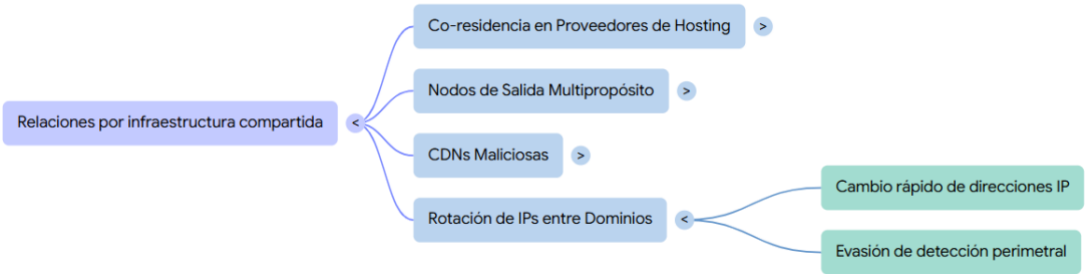
- Nodos de Salida Multipropósito: Direcciones IP que actúan simultáneamente como puntos de origen para escaneos de red (Scan Network) y como servidores de comando y control (C2) para diferentes familias de malware.



- Uso de Redes de Distribución de Contenido (CDN) Maliciosas: El uso de infraestructura compartida para ocultar la verdadera ubicación de los servidores de control detrás de servicios legítimos de resolución de nombres.



- Rotación de IPs entre Dominios: Patrones donde un dominio cambia rápidamente entre varias direcciones IP del conjunto analizado para evadir los sistemas de detección perimetral del sector.



Relaciones por herramientas comunes

Se identifican mediante la similitud en el código, las funciones técnicas y los métodos de operación de los artefactos y tácticas empleadas.

- Similitud en Firmas de Malware (Hashes): Las firmas SHA-256, MD5 y SHA-1 muestran fragmentos de código compartidos, lo que indica que diferentes amenazas han sido construidas sobre una misma base técnica o framework de desarrollo.

- Patrones de Ingeniería Social Uniformes: Las URLs maliciosas utilizan estructuras de lenguaje y ganchos temáticos similares, centrados en la logística y el transporte, lo que sugiere que las plantillas de ataque son compartidas.

- Métodos de Ofuscación Idénticos: Uso de las mismas técnicas para cifrar o codificar la carga útil dentro de los archivos maliciosos, buscando superar los mismos controles de seguridad industriales.

- Comportamiento de Persistencia Estandarizado: Scripts que utilizan los mismos métodos de modificación del registro o tareas programadas para asegurar que el malware permanezca activo en las estaciones de despacho.

Nodos aislados o con baja correlación (por ahora):

Representan indicadores que, en el análisis actual, no muestran vínculos claros con el resto de la infraestructura, pero que requieren vigilancia por su potencial evolución.

- Hashes de Archivos Únicos: Firmas digitales que no comparten características con el resto de la muestra y que podrían representar ataques altamente dirigidos o pruebas de concepto iniciales.

- Direcciones IP de Actividad Esporádica: Nodos que solo registraron un intento de conexión o escaneo y que no han sido vinculados a dominios o URLs conocidas hasta el momento.

- Dominios Recientemente Registrados: FQDNs que aparecen en la lista pero que aún no han sido utilizados en campañas activas, actuando como infraestructura "durmiente" para futuros ataques.

- URLs de Phishing Genérico: Enlaces que, aunque maliciosos, no utilizan la temática del sector transporte y parecen ser parte de campañas masivas no dirigidas que terminaron afectando lateralmente al sector.

RECOMENDACIONES ESTRATÉGICAS

La mitigación de las amenazas detectadas requiere un enfoque multidimensional que combine la defensa técnica con una gestión de riesgos alineada a la continuidad del negocio logístico. Dado que la mayor parte de la infraestructura adversaria se basa en dominios y direcciones IP externas que buscan explotar servicios expuestos y el factor humano, las estrategias deben priorizar la visibilidad perimetral y la reducción de la superficie de ataque. El objetivo es transformar la seguridad en un habilitador operativo que proteja la integridad de la cadena de suministro nacional frente a actores que buscan la interrupción de servicios críticos o el secuestro de información estratégica.

Recomendaciones de Mitigación Técnica

- Filtrado de Tráfico Basado en Reputación: Bloquear de manera preventiva las comunicaciones salientes hacia las direcciones IP y dominios (FQDN) identificados en el análisis técnico como maliciosos.

- Fortalecimiento de la Navegación Web: Implementar soluciones de inspección de tráfico que identifiquen y bloqueen las URLs de phishing logístico antes de que lleguen al usuario final.

- Control de Ejecución de Aplicaciones: Desplegar políticas de restricción que impidan la ejecución de archivos no firmados o scripts sospechosos en estaciones de trabajo críticas de despacho y puertos.

- Protección de Servicios Expuestos: Aplicar controles de acceso estricto y parches de seguridad inmediatos sobre cualquier servidor que gestione bases de datos de carga o seguimiento vehicular.

Recomendaciones de Detección y Monitoreo

- Monitoreo de Anomalías en el Tráfico de Red: Establecer alertas sobre conexiones inusuales hacia nodos externos, especialmente aquellas que sigan patrones de comando y control (C2).

- Auditoría de Intentos de Acceso: Supervisar los registros de autenticación en busca de patrones de fuerza bruta provenientes de las direcciones IP maliciosas detectadas.

- Detección de Archivos mediante Firmas (Hashes): Integrar las firmas digitales SHA-256, MD5 y SHA-1 identificadas en los sistemas de protección de endpoints para detectar de forma temprana la presencia de malware conocido.

- Vigilancia de Dominios Similares: Implementar un sistema de monitoreo preventivo de nombres de dominio que imiten a las marcas o servicios gubernamentales del transporte nacional (Typosquatting).

Recomendaciones de Resiliencia Operativa

- Segregación de Redes Críticas: Aislar los sistemas operativos (OT) que controlan la señalización y carga física de las redes administrativas de TI para evitar el movimiento lateral de atacantes.
- Esquemas de Respaldo Desconectados: Mantener copias de seguridad de las bases de datos logísticas fuera de línea o en entornos inmutables para garantizar la recuperación ante ataques de Ransomware.
- Planes de Contingencia Manual: Desarrollar y probar protocolos operativos que permitan la gestión básica de flotas y carga en caso de una caída total de los sistemas digitales.
- Redundancia de Infraestructura: Asegurar que los portales de servicios críticos cuenten con nodos de respaldo en diferentes ubicaciones geográficas para mitigar ataques de denegación de servicio (DDoS).

Recomendaciones de Gobernanza

- Actualización de Políticas de Seguridad: Alinear los marcos normativos internos del sector transporte con las realidades de las amenazas digitales actuales en Colombia.
- Gestión de Riesgos de Terceros: Establecer requisitos mínimos de ciberseguridad para proveedores logísticos y socios comerciales que tengan acceso a la red corporativa.
- Programas de Concientización Sectorial: Realizar campañas de capacitación específicas para el personal de transporte sobre cómo identificar señuelos de ingeniería social centrados en su labor diaria.
- Inversión Estratégica en Ciberdefensa: Priorizar el presupuesto de TI hacia herramientas que ofrezcan visibilidad sobre la infraestructura de red y protección de identidades digitales.

Preparación ante Incidentes

- Actualización de Playbooks de Respuesta: Diseñar procedimientos específicos para manejar incidentes relacionados con el secuestro de información logística o la toma de control de activos remotos.

- Simulacros de Ciberataque: Realizar ejercicios de mesa (Tabletop) con los líderes operativos para evaluar la capacidad de respuesta ante un escenario de interrupción de la cadena de suministro.

- Canales de Comunicación de Emergencia: Definir métodos de contacto seguros y alternativos para la coordinación de equipos técnicos durante una crisis digital.

- Acuerdos de Soporte Especializado: Contar con servicios de respuesta a incidentes bajo demanda que puedan intervenir rápidamente ante eventos de alta complejidad.

Acciones Inmediatas (Quick Wins)

- Cierre de Puertos No Esenciales: Identificar y clausurar cualquier servicio expuesto a internet que no sea estrictamente necesario para la operación logística inmediata.

- Implementación de Segundo Factor (MFA): Habilitar la autenticación de múltiples factores en todas las cuentas de correo y portales de gestión administrativa del sector.

- Purga de Sesiones Activas: Resetear conexiones de red que muestren patrones de comunicación persistente con las direcciones IP identificadas como sospechosas.

- Revisión de Privilegios Administrativos: Limitar el acceso a los sistemas de bases de datos de carga únicamente a los usuarios que lo requieran para su función inmediata.

CONCLUSIONES

Priorización de la Infraestructura de Red como Vector de Ataque:

- El análisis revela que la amenaza es predominantemente de red, con un 55.5% de los indicadores correspondientes a dominios (FQDN). Esta saturación de infraestructura maliciosa sugiere que los atacantes están en una fase persistente de reconocimiento y suplantación de servicios logísticos para desviar tráfico o capturar datos críticos.

Alta Exposición de la Cadena de Suministro Digital:

- La convergencia entre sistemas de gestión logística (TI) y sistemas operativos de control (OT) ha expandido la superficie de ataque. Los hallazgos muestran que una vulnerabilidad en plataformas web de trámites o geolocalización puede escalar hasta comprometer la integridad física de la operación y la seguridad de la carga.

Profesionalización y Correlación de Adversarios:

- Los actores de amenazas no operan de forma aislada; existe una clara correlación por infraestructura compartida. Se identificaron patrones donde múltiples dominios maliciosos resuelven a las mismas direcciones IP, lo que indica que grupos de cibercrimen organizado y actores de espionaje comparten recursos para aumentar su eficiencia contra el sector.

Amenaza Híbrida de Malware Moderno y Heredado:

- La distribución de artefactos maliciosos (hashes) muestra un equilibrio entre firmas modernas (SHA-256) y versiones antiguas (SHA-1/MD5). Esto concluye que los atacantes diseñan sus campañas para comprometer tanto estaciones de trabajo actualizadas como sistemas operativos legados que aún son vitales en la infraestructura vial y portuaria.

Impacto Crítico del Cibercrimen Organizado:

- Con más de 2,840 indicadores vinculados, el cibercrimen enfocado en la monetización (Ransomware) representa la mayor amenaza volumétrica. El impacto estratégico es crítico, ya que su capacidad para cifrar información operativa puede paralizar totalmente la logística nacional, afectando la estabilidad económica y social del país.

Necesidad de un Modelo de Defensa en Profundidad:

- La naturaleza secuencial de las cadenas de ataque observadas —que inician con escaneo activo y culminan en exfiltración de datos— demuestra que la detección

reactiva es insuficiente. La resiliencia del sector depende de una postura proactiva que integre el filtrado perimetral, la validación rigurosa de archivos y el monitoreo constante de tráficos anómalos hacia nodos externos.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **Indicadores de Compromiso (IoCs):** Evidencias digitales (como una dirección IP o la firma de un archivo) que indican con un alto nivel de confianza que un sistema ha sido vulnerado o que existe una actividad maliciosa en curso.
- **Tácticas, Técnicas y Procedimientos (TTPs):** Marco que describe el "cómo" opera un atacante. Las tácticas son los objetivos (ej. Acceso Inicial), las técnicas son los métodos (ej. Phishing) y los procedimientos son las implementaciones específicas.
- **Adversario (Actor de Amenaza):** Individuo o grupo organizado que intenta vulnerar la seguridad de un sistema con una motivación específica (económica, espionaje o sabotaje).
- **Cadenas de Ataque (Kill Chain):** Modelo que describe las fases de un ciberataque, desde el reconocimiento inicial hasta el cumplimiento de los objetivos finales (como la exfiltración de datos).
- **Inteligencia de Amenazas (Cyber Threat Intelligence):** Información recolectada, procesada y analizada sobre ataques actuales o potenciales para ayudar en la toma de decisiones preventivas.
- **Mapeo MITRE ATT&CK:** Matriz global de conocimiento que categoriza el comportamiento de los adversarios basándose en observaciones del mundo real.

Infraestructura y Redes

- **FQDN (Fully Qualified Domain Name):** El nombre completo de un host o servidor en internet (ej. servidor.logistica.com.co). En este informe, se asocian a nodos de control maliciosos.
- **Comando y Control (C2):** Infraestructura de red (servidores) utilizada por los atacantes para enviar instrucciones a los sistemas infectados y recibir información robada.

- **Direccionamiento IP:** Identificador numérico único de un dispositivo en una red. Las IPs identificadas aquí corresponden a puntos de origen de ataques o saltos de comunicación.
- **Filtrado Perimetral:** Medidas de seguridad (como firewalls) que controlan el flujo de tráfico entre la red interna de una empresa de transporte e internet.
- **Superficie de Ataque:** Suma total de todos los puntos de exposición (software, hardware y personas) por donde un atacante puede intentar ingresar a una organización.

Herramientas y Malware

- **Hash (SHA-256, MD5, SHA-1):** Una huella digital única generada a partir de un archivo. Si el archivo cambia un solo bit, el hash cambia, lo que permite identificar malware conocido con total precisión.
- **Ransomware:** Tipo de malware diseñado para cifrar los archivos de un sistema (como bases de datos de carga), exigiendo un pago para su recuperación.
- **Troyano de Acceso Remoto (RAT):** Software malicioso que permite a un atacante controlar una estación de trabajo de manera encubierta, capturando pantallas o interceptando datos.
- **Phishing:** Técnica de ingeniería social que utiliza correos o URLs falsas para engañar al personal y obtener credenciales de acceso o instalar malware.
- **Botnet:** Red de dispositivos infectados ("zombis") controlados de forma remota para realizar ataques masivos, como el escaneo de redes o la denegación de servicios.

Sector

- **Infraestructura Crítica de Transporte:** Sistemas y activos físicos o lógicos cuya interrupción tendría un impacto grave en la economía, la movilidad y la seguridad nacional (puertos, aeropuertos, redes viales).
- **Cadena de Suministro Digital:** Conjunto de flujos de datos e integraciones tecnológicas entre empresas de transporte, proveedores logísticos y autoridades gubernamentales.
- **Continuidad Operativa:** Capacidad de una organización para mantener sus servicios esenciales (despacho, monitoreo de flotas) durante y después de un incidente de ciberseguridad.
- **Resiliencia Cibernética:** Habilidad del sector para absorber, adaptarse y recuperarse rápidamente de ataques que comprometan su operatividad.

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