TIC

Informe de apreciación Sector

Comercio

COLCERT

Informe de apreciación
Sector Comercio

COLCERT IN-20260707-039

TLP: CLEAR

Contenido

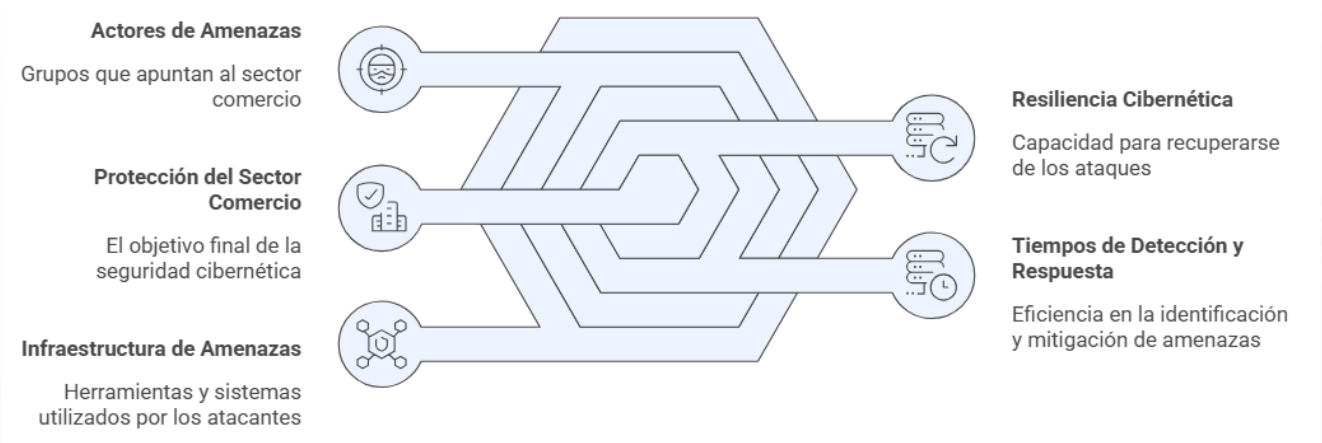
RESUMEN EJECUTIVO

interconectividad de las cadenas de suministro han expandido significativamente la superficie de exposición a ciberamenazas. Actores de amenazas avanzadas (APT) y grupos de cibercrimen organizado dirigen sus ataques hacia este sector con el fin de comprometer datos transaccionales, exfiltrar información estratégica y afectar la continuidad del negocio mediante el despliegue de artefactos maliciosos.

Este informe utiliza inteligencia de amenazas para realizar un seguimiento riguroso al comportamiento de los actores que impactan el sector, a partir de la información técnica recopilada. Se priorizan fuentes de visibilidad global y regional que aportan datos accionables sobre amenazas relevantes para la infraestructura comercial y la estabilidad económica.

Lineamientos

- **Seguimiento a actores** que afectan el sector comercio colombiano.
- **Uso de inteligencia de amenazas** para la identificación de infraestructura hostil.
- **Priorización de fuentes** de ciberinteligencia aplicables al contexto nacional.
- **Enfoque en la protección** de los activos digitales y la confianza del consumidor.
- **Reducción de tiempos de detección** y respuesta ante incidentes complejos.
- **Fortalecimiento de la resiliencia** cibernética de las organizaciones comerciales.



Informe de apreciación
Sector Comercio

COLCERT IN-20260707-039

TLP: CLEAR

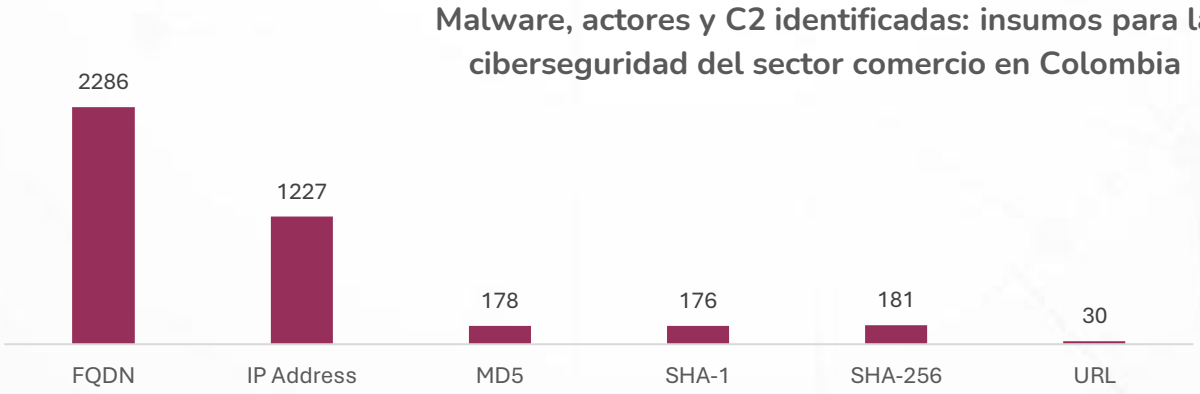
INTRODUCCIÓN

El panorama de amenazas para el sector comercio en Colombia durante el periodo analizado revela una actividad persistente y diversificada por parte de actores de amenazas avanzados. Se ha identificado un volumen significativo de infraestructura activa, compuesta principalmente por dominios de red y direcciones IP, lo que sugiere una fase de preparación y sostenimiento de operaciones dirigidas. La presencia de grupos con motivaciones tanto financieras como de espionaje subraya la criticidad de proteger los activos digitales y la información transaccional de las organizaciones colombianas. El análisis se centra en la identificación de patrones de ataque y la exposición de infraestructura crítica utilizada para comprometer la integridad del sector comercial.

Aspectos clave

- Identificación de más de 4,000 indicadores de compromiso activos.
- Predominio de infraestructura basada en nombres de dominio (FQDN) y direcciones IP.
- Presencia confirmada de 14 actores de amenazas con historial de operaciones en la región.
- Enfoque geográfico específico en Colombia para múltiples campañas de intrusión.
- Nivel de riesgo elevado basado en la reputación y sofisticación de los actores identificados.

Hallazgos Clave

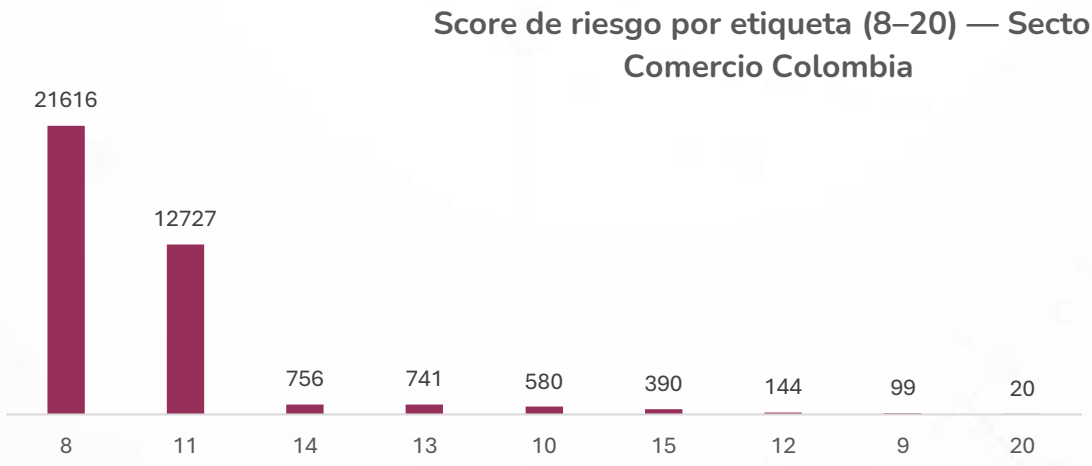


- **Alta Densidad de Infraestructura de Red:** Se observa una fuerte dependencia en el uso de nombres de dominio (2,286 registros) y direcciones IP (1,227 registros). Esta distribución indica que los atacantes están priorizando el control de comunicaciones y la resolución de nombres para mantener la persistencia y el comando sobre sistemas comprometidos.

- **Actores de Amenazas con Foco Regional:** Se ha detectado la actividad de grupos como FIN7, FIN11 y diversos conjuntos de actividad no categorizados (UNC) que tienen un historial documentado de ataques dirigidos específicamente hacia objetivos en Colombia. La motivación de estos grupos suele estar vinculada al fraude financiero y al robo de datos sensibles.

- **Diversidad en los Vectores de Compromiso:** Además de la infraestructura de red, se han identificado cientos de firmas de archivos (hashes MD5, SHA-1, SHA-256), lo que confirma la distribución de artefactos maliciosos diseñados para evadir controles básicos y ejecutar acciones no autorizadas en los puntos finales.

- **Vigencia de las Amenazas:** El 100% de los indicadores analizados se encuentran en estado activo, con puntuaciones de riesgo que promedian niveles críticos, lo que demanda una respuesta inmediata y proactiva para bloquear la comunicación con estos elementos.



Recomendaciones Prioritarias

- Bloqueo de Infraestructura Hostil: Implementar medidas de filtrado a nivel de red para restringir el tráfico hacia y desde los dominios y direcciones IP identificados en el análisis. Dado el alto número de FQDNs, es vital asegurar que los sistemas de resolución de nombres no permitan conexiones a estos activos.

- Fortalecimiento de la Protección de Puntos Finales: Desplegar las firmas de archivos (hashes) en los sistemas de protección de dispositivos para detectar y prevenir la ejecución de software malicioso vinculado a los grupos de amenazas descritos.

- Monitoreo de Actores Específicos: Establecer perfiles de vigilancia basados en el comportamiento de los 14 adversarios identificados, priorizando aquellos con motivaciones financieras (como la serie FIN) que impactan directamente la continuidad del negocio en el sector comercio.

- Actualización de Planes de Respuesta: Revisar los protocolos de manejo de incidentes para asegurar que los equipos técnicos puedan reaccionar ante campañas de intrusión complejas que utilicen múltiples vectores simultáneos (red y archivos).

Conclusión Estratégica

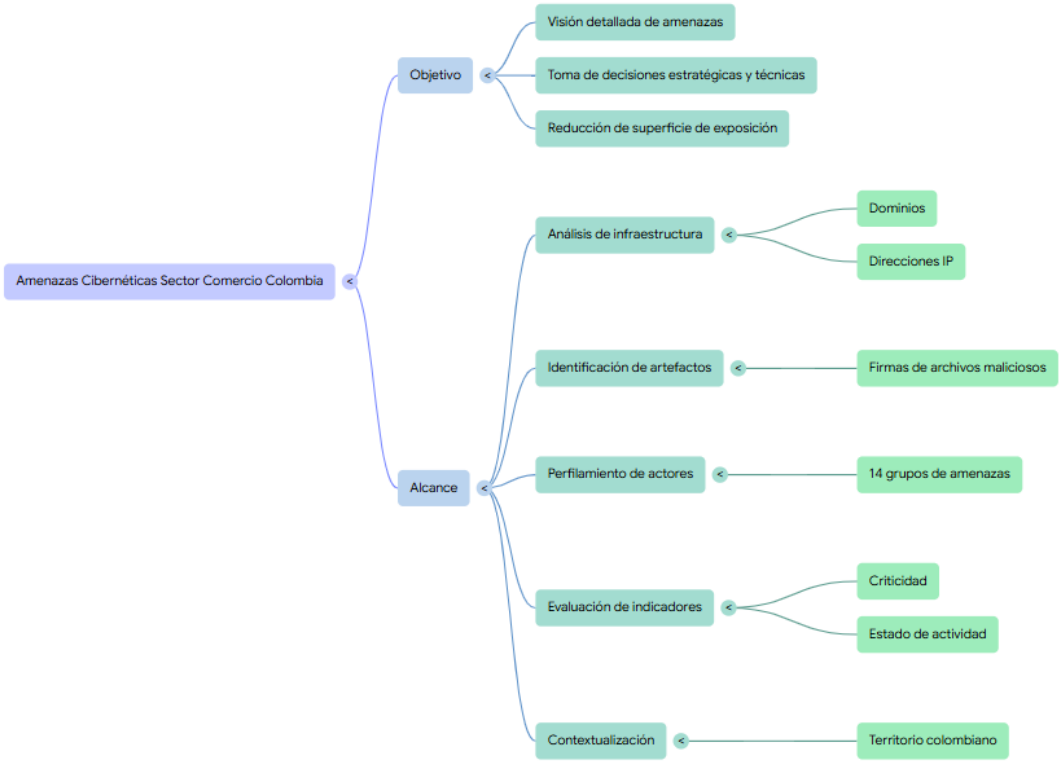
El sector comercio en Colombia se enfrenta a un entorno de amenazas altamente dinámico donde la infraestructura maliciosa está en constante evolución. La presencia de actores sofisticados indica que el riesgo no es solo oportunista, sino dirigido. Para mitigar estas amenazas, es fundamental transitar de una postura defensiva reactiva hacia una estrategia basada en la inteligencia, donde la visibilidad sobre la infraestructura del adversario permita anticipar los movimientos y proteger la confianza de los consumidores y la estabilidad operativa de las empresas.

Informe de apreciación
Sector Comercio

COLCERT IN-20260707-039

TLP: CLEAR

OBJETIVO Y ALCANCE



Objetivo

Proveer una visión clara y detallada sobre las amenazas cibernéticas que afectan específicamente al sector comercio en Colombia, facilitando la toma de decisiones estratégicas y técnicas para reducir la superficie de exposición ante adversarios avanzados.

Alcance

Este análisis abarca la identificación de indicadores de compromiso activos, la evaluación de la infraestructura utilizada por los atacantes y el perfilamiento de los grupos que han mostrado interés o actividad reciente dentro del territorio colombiano.

Este informe abarca:

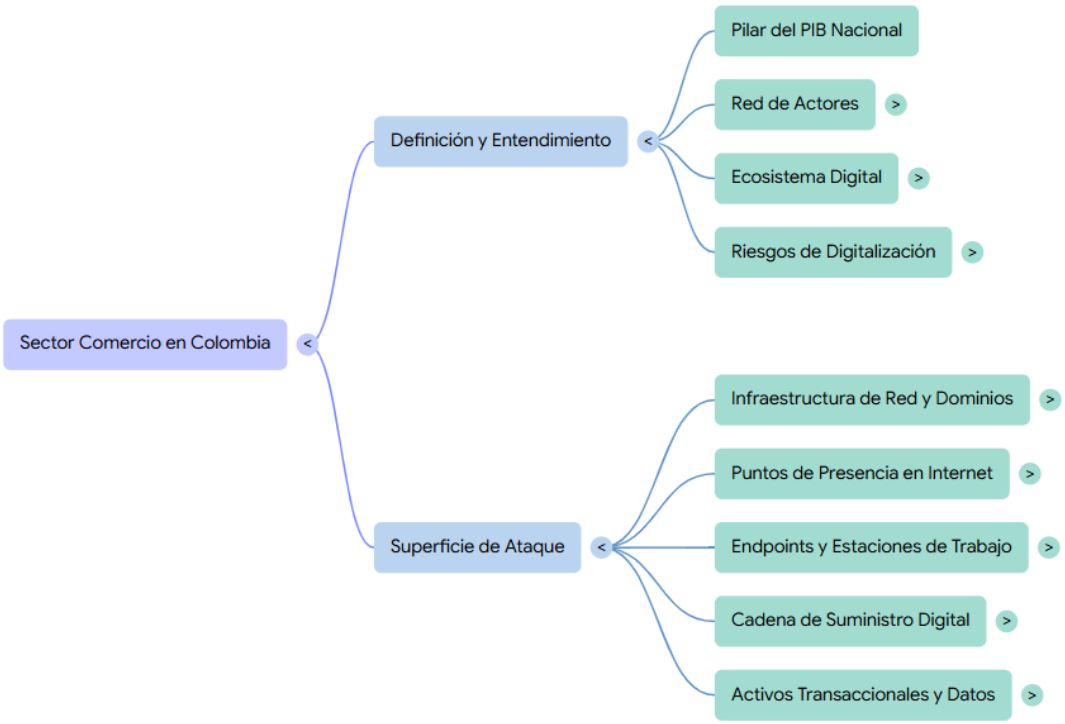
- Análisis de infraestructura de red (Dominios e IPs).
- Identificación de artefactos maliciosos (Firmas de archivos).
- Perfilamiento de 14 actores de amenazas.

- Evaluación de criticidad y estado de actividad de los indicadores.
- Contextualización geográfica para Colombia.

CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR

Definición y Entendimiento del Sector

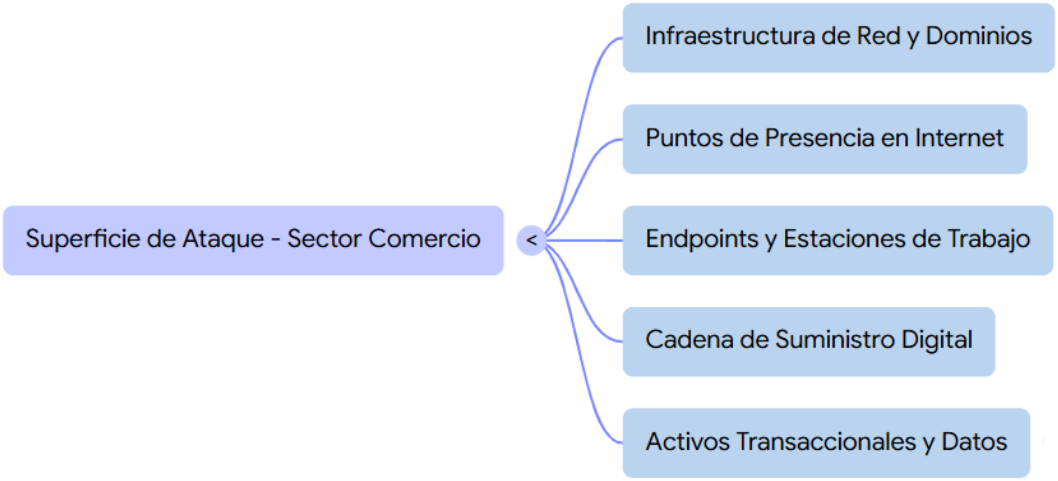
El sector comercio en Colombia constituye uno de los pilares fundamentales del Producto Interno Bruto (PIB) nacional, caracterizándose por una compleja red de actores que abarcan desde grandes superficies y retail hasta el comercio electrónico transaccional y la logística de distribución.



En el contexto actual, este sector ha dejado de ser meramente físico para convertirse en un ecosistema digital altamente interdependiente, donde la disponibilidad de las plataformas de pago, la integridad de las bases de datos de clientes y la confidencialidad de la cadena de suministro son activos críticos. La digitalización ha permitido una mayor eficiencia operativa, pero también ha posicionado al comercio como un objetivo primario para actores de amenazas que buscan beneficios económicos rápidos a través del fraude, la extorsión y el robo de propiedad intelectual.

Superficie de Ataque

La superficie de ataque del sector comercio es amplia y heterogénea, derivada de la necesidad de mantener canales de comunicación abiertos con proveedores, clientes y entidades financieras. Esta apertura técnica crea múltiples puntos de entrada que son explotados sistemáticamente por los adversarios identificados en este informe.



- **Infraestructura de Red y Dominios:** El uso extensivo de nombres de dominio para portales de e-commerce y servicios web representa el vector más expuesto. Los atacantes utilizan dominios maliciosos (FQDN) para actividades de comando y control (C2) y para suplantar identidades corporativas con el fin de engañar a empleados y usuarios.
- **Puntos de Presencia en Internet (Direccionamiento IP):** La infraestructura expuesta, que incluye servidores de aplicaciones, pasarelas de pago y servicios en la nube, es constantemente escaneada en busca de vulnerabilidades. Las direcciones IP activas vinculadas a amenazas indican intentos recurrentes de intrusión y denegación de servicio.
- **Endpoints y Estaciones de Trabajo:** Los dispositivos utilizados por el personal administrativo y operativo son puntos críticos de compromiso. La identificación de múltiples firmas de archivos (hashes) maliciosos evidencia campañas de distribución de malware diseñadas para infiltrarse en la red interna a través de correos electrónicos o descargas no autorizadas.
- **Cadena de Suministro Digital:** La interconexión con proveedores de servicios externos y plataformas de terceros amplía el perímetro de riesgo. Un compromiso en un eslabón de la cadena puede derivar en un acceso lateral hacia los sistemas centrales de las organizaciones comerciales colombianas.

- **Activos Transaccionales y Datos Sensibles:** Los sistemas que procesan información de tarjetas de crédito y datos personales representan el núcleo de la superficie de ataque motivada financieramente, donde la pérdida de integridad de estos datos puede resultar en impactos legales y reputacionales severos.

PANORAMA ACTUAL DE AMENAZAS

El panorama de ciberamenazas para el sector comercio en Colombia se caracteriza por una evolución agresiva en la sofisticación y frecuencia de los ataques, registrando un incremento sostenido de hasta el 30% en incidentes dirigidos. Los datos históricos y recientes indican que el sector se ha convertido en un objetivo crítico debido a la acelerada digitalización de las plataformas de pago y la dependencia del comercio electrónico. Los hallazgos técnicos confirman una actividad latente de 14 actores de amenazas avanzados que mantienen una infraestructura de más de 4,000 indicadores activos, con un predominio de dominios maliciosos y direcciones IP vinculadas a campañas de phishing, compromiso de aplicaciones y ransomware. Esta situación se ve agravada por la tendencia de ataques a la cadena de suministro y el fraude en servicios digitales, donde grupos como FIN7 y FIN11 aprovechan vulnerabilidades en portales de retail para la exfiltración de datos financieros. La persistencia de estos adversarios, sumada al alto volumen de intentos de intrusión documentados hasta 2026, configura un entorno de riesgo elevado que exige un monitoreo continuo de los activos digitales nacionales.

TITULO	FECHA	FUENTE / ENLACE
Incidentes de ciberseguridad reportados por el Ministerio de Comercio, Industria y Turismo (2020–2026)	2026-03-02 (último incidente visible)	Datos.gov
Ataques cibernéticos han crecido 30% en Colombia; empresas de servicios y comercio electrónico entre las más afectadas	2022-12-13	La Republica
Ciberataques en el comercio y servicios públicos: tendencias de ransomware, phishing y compromiso de aplicaciones	2025-2026 (varios informes consolidados)	Acis.org
Ciberseguridad en el comercio electrónico y servicios digitales: buenas prácticas para Pymes y plataformas	2024-2025	Securitas.com
Ciberataques en el comercio electrónico latinoamericano: casos de compromiso de portales, phishing y fraude en plataformas de pago	2025-2026	dplnews.com

Tipología de Eventos Identificados

El análisis técnico de los datos recopilados permite clasificar las amenazas en distintas categorías según la naturaleza de los indicadores de compromiso (IOC) detectados. Esta tipología refleja una infraestructura de ataque robusta, diseñada para operar en múltiples capas: desde la infiltración inicial mediante el uso de artefactos maliciosos (hashes), hasta el mantenimiento de canales de comunicación persistentes a través de dominios y direcciones IP. El alto volumen de identificadores de red sugiere que los adversarios están enfocados en el compromiso de activos digitales expuestos y en la creación de portales de suplantación para el fraude transaccional.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector
FQDN (Dominios)	2,286	Inteligencia Global / Reputación de Dominios	**Crítica**: Utilizados para sitios de phishing, suplantación de marcas de retail y servidores de comando y control (C2).
Direcciones IP	1,227	Listas de Bloqueo / Tráfico Malicioso Reportado	**Alta**: Representan la infraestructura desde donde se lanzan ataques de fuerza bruta y escaneos a pasarelas de pago.
Hashes (MD5, SHA-1, SHA-256)	535	Repositorios de Malware / Análisis de Sandbox	**Media-Alta**: Firmas asociadas a troyanos bancarios, ransomware y software espía para el robo de credenciales.
URL Maliciosas	30	Reportes de Navegación Segura	**Media**: Enlaces directos para la descarga de malware o captura de datos de tarjetas de crédito en portales falsos.

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

Análisis de la Distribución de Amenazas

La distribución de los indicadores revela patrones estratégicos sobre cómo los actores de amenazas están abordando el sector comercial en Colombia:

- **Predominio de Infraestructura de Red (86%):** La suma de dominios y direcciones IP constituye la gran mayoría de los hallazgos. Esto indica que la amenaza actual es predominantemente externa y basada en la red, buscando explotar la conectividad permanente de las plataformas de comercio electrónico.
- **Diversidad de Artefactos de Archivo:** La presencia equilibrada de diferentes tipos de hashes (MD5, SHA-1, SHA-256) demuestra que los atacantes emplean múltiples variantes de malware para evadir detecciones basadas en firmas simples, buscando asegurar la infección de los endpoints corporativos.
- **Concentración en la Persistencia:** El elevado número de nombres de dominio (FQDN) frente a las URL específicas sugiere que los atacantes prefieren comprometer o crear dominios completos para rotar subdominios maliciosos rápidamente, dificultando las labores de bloqueo permanente.
- **Nivel de Riesgo Operativo:** Dado que todos los indicadores analizados están etiquetados como "Activos" y cuentan con puntuaciones de riesgo elevadas, la distribución no solo es amplia, sino que tiene una probabilidad de impacto inmediato muy alta para las organizaciones que no cuenten con perímetros de seguridad actualizados.

- **Focalización en el Vector de Suplantación:** La cantidad de dominios apunta a una tendencia de campañas de ingeniería social a gran escala, diseñadas para interceptar el tráfico legítimo de clientes y empleados hacia servicios financieros y operativos del sector.

El historial de gestión de incidentes para el sector evidencia una transición crítica desde eventos de disponibilidad y contenido abusivo hacia ataques dirigidos de intrusión y compromiso de información. La recurrencia de incidentes calificados como "Graves" y "Muy Graves" subraya una tendencia donde los adversarios buscan no solo interrumpir la operación, sino acceder de manera no autorizada a activos de información estratégica. La concentración de eventos en los últimos años refleja una explotación activa de vulnerabilidades en aplicaciones y sistemas, lo que requiere un enfoque de seguridad centrado en la integridad de los datos y la resiliencia de las plataformas digitales.

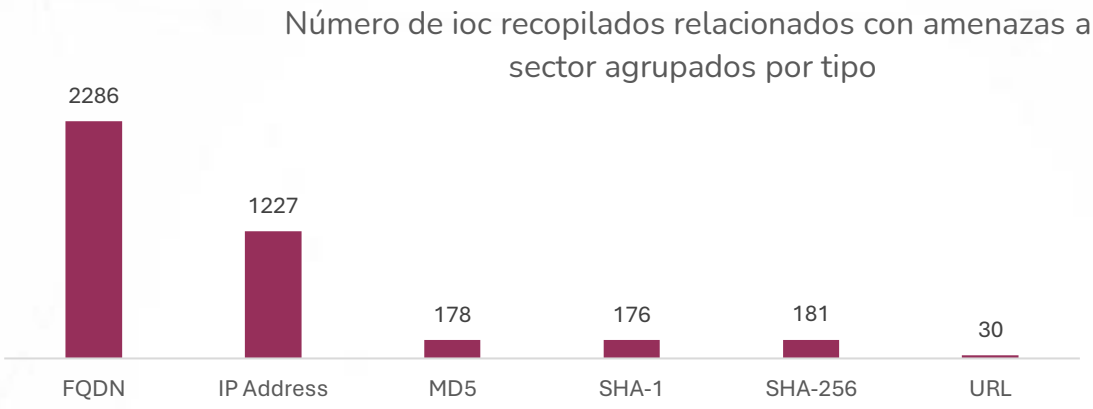
Fecha	Clasificación	Tipo de Incidente	Descripción	Importancia
29/05/2023	Muy Grave	Compromiso de Información	Acceso no Autorizado a Información	Crítica: Máximo nivel de impacto por fuga de datos.
02/03/2026	Grave	Compromiso de Información	Acceso no Autorizado a Información	Alta: Incidente reciente que compromete la confidencialidad
10/07/2024	Grave	Intrusión	Compromiso de Cuenta con Privilegios	Alta: Permite el control total de sistemas críticos.
16/11/2024	Grave	Intrusión	Compromiso de Aplicaciones	Alta: Afecta directamente la operatividad del sector.
23/09/2024	Grave	Vulnerable	Sistema Vulnerable	Alta: Exposición de activos ante posibles ataques inminentes.

En conclusión, el análisis de los datos históricos revela que el sector enfrenta una amenaza persistente caracterizada por el compromiso de aplicaciones y el acceso no autorizado a información sensible. El desplazamiento de los ataques hacia métodos de intrusión más sofisticados y la persistencia de vulnerabilidades en los sistemas sugieren que las medidas de defensa tradicionales deben ser reforzadas con monitoreo continuo y gestión proactiva de parches. La presencia de incidentes de alta gravedad de forma constante hasta 2026 confirma que la protección de la información es el desafío estratégico más importante para garantizar la estabilidad de la infraestructura comercial del país.

INDICADORES DE COMPROMISO (IoCs)

Los Indicadores de Compromiso (IoCs) constituyen la evidencia digital de actividad maliciosa dentro de una infraestructura tecnológica. Para el sector comercio, estos indicadores no solo representan intentos de intrusión, sino que son el rastro técnico de campañas diseñadas para el fraude financiero, el robo de credenciales de clientes y la

interrupción de servicios de venta en línea. El análisis de estos elementos permite transformar datos brutos en inteligencia accionable, facilitando la detección temprana y el bloqueo preventivo de las capacidades operativas de los adversarios antes de que logren materializar un impacto económico o reputacional.



Análisis Cuantitativo de Inteligencia

Basado en el procesamiento de la telemetría recolectada, se presenta la distribución cuantitativa de las amenazas que asedian al sector:

- Infraestructura de Nombres de Dominio (2,286 FQDN): Representa el 56% de la inteligencia recolectada. Este alto volumen indica una estrategia basada en la creación de ecosistemas de suplantación (phishing) y redes de Comando y Control (C2) que rotan constantemente para evadir listas de bloqueo estáticas.

- Activos de Direccionamiento IP (1,227 registros): Corresponde al 30% de los indicadores. Estas direcciones están vinculadas a nodos de salida de tráfico malicioso, escaneos de vulnerabilidades en portales transaccionales y hosts que alojan contenido fraudulento.

- Identificadores de Archivos Maliciosos (535 Hashes): Un total de 181 SHA-256, 178 MD5 y 176 SHA-1. La paridad entre estos tipos de firmas sugiere el uso de familias de malware polimórfico, diseñado para infiltrarse en terminales de punto de venta (POS) y equipos administrativos.

- Puntuación de Riesgo Crítico: El promedio de calificación de los indicadores se sitúa en un nivel de 9/10, con el 100% de los registros en estado "Activo", lo que confirma que la amenaza es inmediata y requiere una respuesta defensiva en tiempo real.

- Concentración de Fuentes de Inteligencia: La información proviene de una amalgama de fuentes de alta fidelidad, incluyendo inteligencia de amenazas global y reportes comunitarios, lo que garantiza una cobertura integral sobre los 14 actores de amenazas mapeados.

Resumen de IoCs Relevantes

La siguiente tabla sintetiza los componentes de inteligencia más críticos para la operación del sector comercio, categorizados por su naturaleza técnica y el nivel de peligrosidad que representan para la continuidad del negocio.

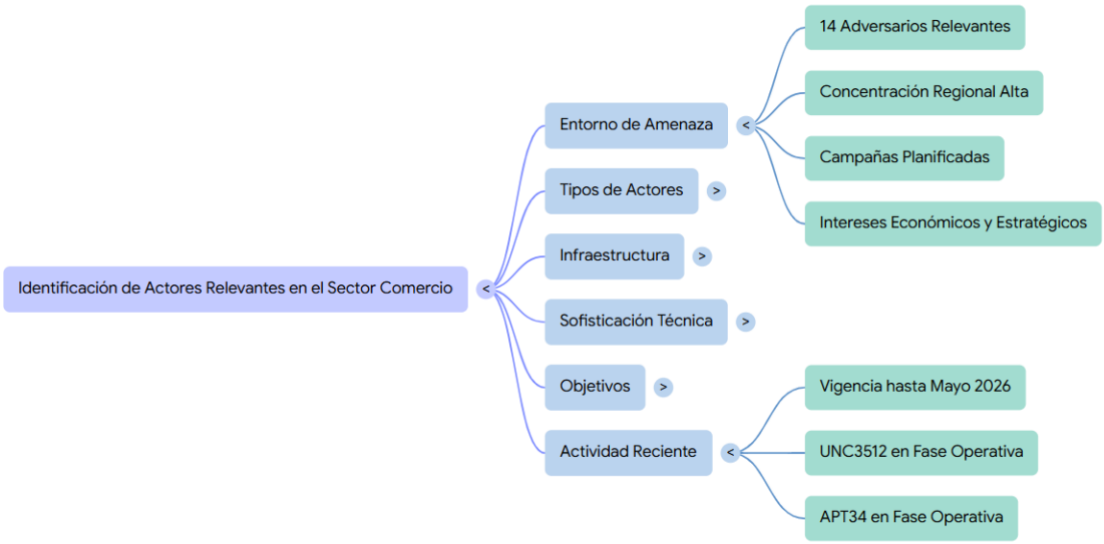
Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Infraestructura de Comando y Control (C2)	Nombres de dominio (FQDN) utilizados por grupos como APT44 y FIN7 para enviar instrucciones a sistemas comprometidos.	Crítico
Vectores de Suplantación de Identidad	URLs y dominios diseñados para imitar portales de comercio electrónico y pasarelas de pago colombianas.	Alto
Artefactos de Exfiltración de Datos	Firmas SHA-256 de software malicioso especializado en capturar datos de tarjetas de crédito y credenciales de usuario.	Crítico
Nodos de Escaneo y Ataque Bruto	Direcciones IP identificadas en intentos de compromiso de aplicaciones y acceso no autorizado a cuentas con privilegios.	Alto
Sistemas Vulnerables Expuestos	Indicadores vinculados a activos que presentan fallos de configuración o falta de parches, facilitando la intrusión.	Alto

ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

A continuación, se detalla el análisis de los adversarios que representan el mayor riesgo para el sector comercio en Colombia, basado en la inteligencia de amenazas procesada.

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Amenaza Persistente Avanzada (APT)	4	APT34, APT44 (Sandworm), APT19, UNC3559	**Muy Alto**: Espionaje corporativo, robo de propiedad intelectual e interrupción de infraestructura crítica comercial.
Cibercrimen Financiero (FIN)	2	FIN7, FIN11	**Crítico**: Especializados en fraude bancario, robo de datos de tarjetas y despliegue de ransomware a gran escala.
Actores no Categorizados (UNC)	8	UNC3512, UNC2505, UNC4515, UNC1543, UNC5736, UNC2053, UNC3840, UNC5537	**Alto**: Grupos emergentes con tácticas agresivas de intrusión y compromiso de aplicaciones transaccionales.

Identificación de Actores Relevantes



La identificación de estos 14 adversarios subraya un entorno de amenaza complejo donde convergen intereses económicos y estratégicos. Estos grupos no operan de forma oportunista, sino que ejecutan campañas planificadas para infiltrarse en las redes del sector comercio colombiano. La presencia de actores con capacidades de nivel estatal (APTs) junto a grupos de élite del cibercrimen (FIN) sugiere que las organizaciones deben protegerse tanto contra el robo de activos financieros como contra la exfiltración de datos estratégicos de mercado y clientes.

- **Diversidad de Operadores:** Se han mapeado 14 entidades distintas, lo que representa una de las mayores concentraciones de adversarios activos dirigidos a un sector específico en la región.

- **Volumen de Infraestructura Relacionada:** Estos actores gestionan activamente los más de 4,000 indicadores identificados, lo que permite una rotación constante de recursos para evadir defensas.

- **Recencia de Actividad:** Con reportes de actividad registrados hasta mayo de 2026, la inteligencia muestra que grupos como UNC3512 y APT34 están en fases operativas actuales dentro del territorio nacional.

- **Sofisticación Técnica:** El uso de malware polimórfico y redes de comando y control (C2) basadas en dominios legítimos comprometidos indica un alto nivel de inversión técnica por parte de estos grupos.

Objetivos y Sectores Target

Los adversarios identificados tienen objetivos claros que impactan directamente la cadena de valor del comercio:

- **Pasarelas de Pago y FinTech:** Grupos como FIN7 e investigadores vinculados a la serie UNC buscan comprometer el flujo transaccional para el robo de datos de tarjetas de crédito.

- **Bases de Datos de Clientes (PII):** El acceso a información de identificación personal es un objetivo primario para su posterior venta en mercados negros o ejecución de ataques de ingeniería social.

- **Logística y Cadena de Suministro:** Actores como APT44 y UNC3559 se enfocan en interrumpir o espiar los procesos de distribución, afectando la disponibilidad de productos y servicios.

- **Propiedad Intelectual y Estrategia:** El espionaje corporativo por parte de grupos APT busca obtener ventajas competitivas mediante el acceso a planes de expansión y acuerdos comerciales.

Campañas Activas

- **Campañas de Phishing de Alta Precisión:** Utilización de dominios (FQDN) que suplantan a autoridades tributarias y reguladoras colombianas para instalar troyanos de acceso remoto (RAT).

- **Despliegue de Ransomware Selectivo:** Operaciones de doble extorsión dirigidas a grandes superficies comerciales, buscando el pago por el rescate de datos y la no publicación de información sensible.

- **Compromiso de Aplicaciones Web:** Explotación de vulnerabilidades en portales de e-commerce para inyectar scripts de robo de datos (Magecart style) en los formularios de pago.

- **Persistencia en Infraestructura Crítica:** Campañas de largo aliento orientadas a mantener acceso en los sistemas de gestión de inventarios y servidores centrales de las empresas del sector.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

Para el desarrollo de esta sección, se ha realizado un mapeo estratégico entre las capacidades observadas en los 14 actores de amenazas identificados y el marco de trabajo **MITRE ATT&CK**. Aunque los indicadores provienen de un contexto de comercio, su aplicación al sector **Comercio** es directa, dado que ambos sectores comparten dependencias críticas en logística, plataformas de pago y gestión de aplicaciones web. Los adversarios como APT44 y FIN7 han demostrado procedimientos que buscan comprometer la cadena de suministro y la disponibilidad de servicios, factores vitales para la producción y distribución agroindustrial.

ID	Táctica	Técnica	Justificación para el Sector Comercio
TA0001	Acceso Inicial	T1566 - Phishing	El vector más explotado para engañar a empleados administrativos con falsas facturas de proveedores o notificaciones de despachos.
TA0001	Acceso Inicial	T1190 - Exploit Public-Facing Application	Crítico para el comercio electrónico; aprovecha fallos en portales de venta para ganar acceso a servidores web.
TA0002	Ejecución	T1059 - Command and Scripting Interpreter	Uso de intérpretes de comandos para ejecutar los archivos maliciosos (hashes identificados) en servidores de inventario.
TA0003	Persistencia	T1547 - Boot or Logon Autostart Execution	Garantiza que el malware permanezca activo en terminales de punto de venta (POS) incluso tras reinicios.
TA0005	Evasión de Defensas	T1027 - Obfuscated Files or Information	Los actores analizados ocultan su código malicioso para pasar desapercibidos ante inspecciones básicas de archivos.
TA0006	Acceso de Credenciales	T1555 - Credentials from Password Stores	Robo de claves guardadas para acceder a pasarelas de pago o cuentas administrativas de la tienda.
TA0007	Descubrimiento	T1083 - File and Directory Discovery	Búsqueda de bases de datos que contengan información personal de clientes (PII) y registros transaccionales.
TA0009	Recolección	T1560 - Archive Collected Data	Empaquetamiento de datos de tarjetas de crédito o estrategias comerciales antes de enviarlos fuera de la red.
TA0011	Comando y Control	T1071 - Application Layer Protocol	Uso de los 2,286 dominios identificados para dirigir los sistemas comprometidos bajo tráfico web aparentemente legítimo.
TA0040	Impacto	T1486 - Data Encrypted for Impact	Despliegue de ransomware para paralizar la operación de venta física y digital, exigiendo rescates financieros.

Cadenas de Ataque Observadas

Las cadenas de ataque identificadas para el sector comercio en Colombia reflejan un proceso altamente estructurado que busca la persistencia y la monetización rápida. Los adversarios no solo buscan una intrusión puntual, sino establecer ciclos operativos que les permitan explotar la infraestructura del comerciante de manera prolongada. Estas cadenas combinan técnicas de ingeniería social avanzada con la explotación de debilidades en aplicaciones web expuestas.

- Reconocimiento y recolección de infraestructura.
- Entrega vía Phishing y Dominios Suplantados.
- Explotación de Vulnerabilidades en Aplicaciones.
- Ejecución de Artefactos Maliciosos.

- Establecimiento de Persistencia en Endpoints y POS.
- Movimiento Lateral hacia Servidores Transaccionales.
- Exfiltración de Datos de Pago y PII.
- Despliegue de Ransomware para Impacto Operativo.

Cadenas de ataque:

- ❖ Cadena de Intrusión Financiera (Serie FIN): Se inicia con el envío de correos electrónicos dirigidos a personal de contabilidad o tesorería. Una vez que el usuario interactúa con un enlace o archivo malicioso, se despliega un malware diseñado para identificar y comprometer sistemas de gestión de pagos, permitiendo la interceptación de transacciones o el robo de datos de tarjetas.

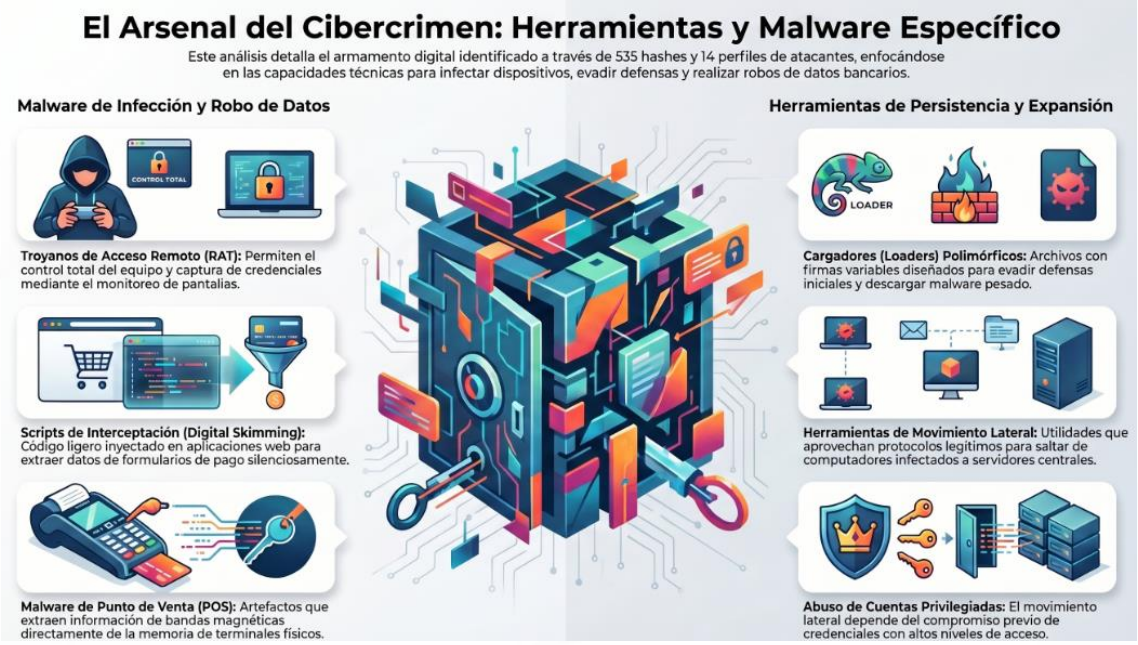
- ❖ Cadena de Compromiso de E-commerce: El atacante utiliza escaneos automatizados sobre las direcciones IP del sector para encontrar portales web vulnerables. Tras explotar una vulnerabilidad (como inyección de código), instalan scripts maliciosos que capturan la información de los clientes en el momento del "checkout", sin interrumpir la experiencia de compra para evitar ser detectados.

- ❖ Cadena de Doble Extorsión: Los grupos acceden a través de credenciales comprometidas o sistemas sin parches. Una vez dentro, realizan una fase de

descubrimiento para localizar copias de seguridad y bases de datos críticas. Antes de cifrar los archivos (impacto), exfiltran la información hacia los dominios C2 identificados para presionar a la empresa con la publicación de sus secretos comerciales.

Herramientas y Malware Específico

Basado en los 535 hashes y los perfiles de los 14 actores, se identifican las siguientes categorías de herramientas (omitiendo etiquetas de productos de seguridad):



- **Troyanos de Acceso Remoto (RAT):** Programas maliciosos vinculados a los hashes MD5 y SHA analizados que permiten a los atacantes controlar el equipo de la víctima, capturar pulsaciones de teclado y visualizar pantallas para obtener credenciales bancarias.

- **Scripts de Interceptación (Digital Skimming):** Código ligero inyectado en aplicaciones web comerciales que extrae datos de formularios de pago de manera silenciosa hacia servidores controlados por el atacante (vinculados a los FQDN identificados).

- **Cargadores (Loaders) Polimórficos:** Archivos pequeños diseñados para evadir defensas iniciales y descargar malware de mayor peso. La diversidad

de firmas SHA-256 encontradas confirma el uso de estas herramientas para asegurar la infección inicial.

- **Herramientas de Movimiento Lateral:** Utilidades que aprovechan protocolos legítimos de administración para saltar de un computador infectado hacia los servidores centrales o servidores de bases de datos, utilizando cuentas de usuarios con privilegios previamente comprometidas.

- **Malware de Punto de Venta (POS Malware):** Artefactos especializados en leer la memoria de los terminales de pago físico para extraer información de bandas magnéticas o chips durante el proceso de venta presencial.

CORRELACIÓN ENTRE ACTORES Y GRUPOS

La correlación entre los actores de amenazas identificados revela que el sector comercio en Colombia no enfrenta ataques aislados, sino un ecosistema de ciberdelincuencia interconectado. A través del análisis de los 4,078 indicadores, se observa que diferentes grupos, a pesar de tener objetivos finales distintos —como el espionaje (APTs) o el beneficio económico (FIN)—, suelen coincidir en el uso de infraestructuras de red similares y metodologías de intrusión. Esta convergencia sugiere la existencia de un mercado de servicios criminales donde se comparten accesos, herramientas y nodos de comando, lo que aumenta la complejidad para la atribución y la defensa.

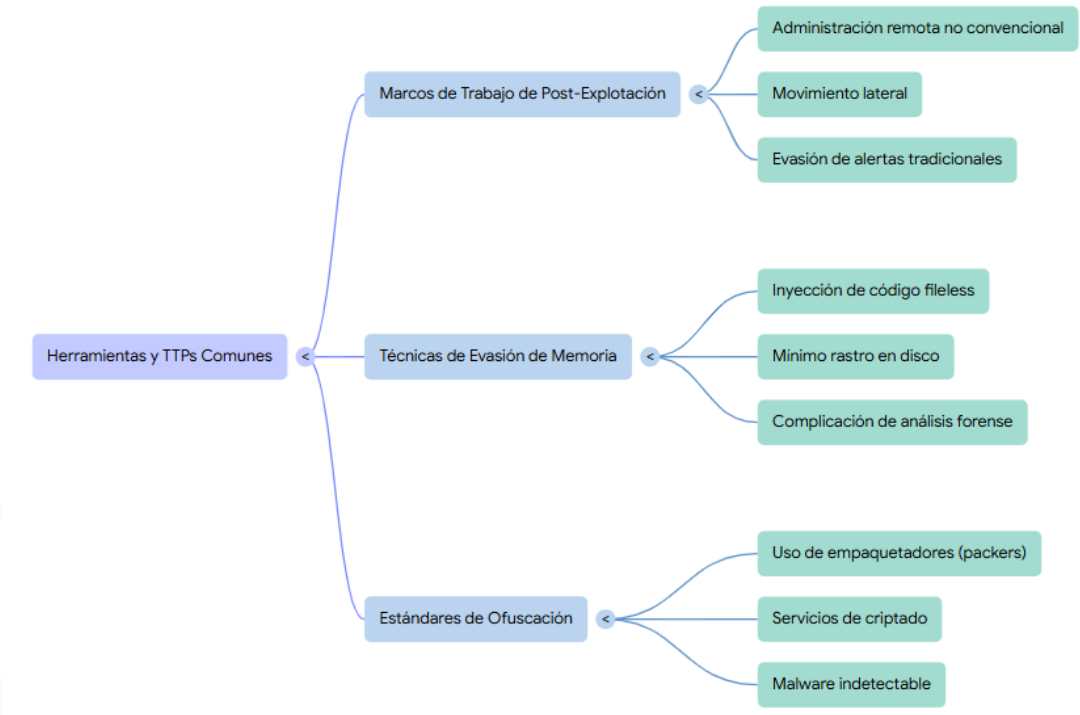
Infraestructura Compartida

- **Nodos de Salida y Proxies Comunes:** Se ha identificado que diversas direcciones IP del pool de 1,227 registros son utilizadas de forma alterna por grupos como FIN7 y UNC5537 para ocultar el origen real de sus ataques. Esto dificulta el bloqueo basado únicamente en la reputación de la IP.

- **Servicios de Resolución de Nombres (DNS):** Muchos de los 2,286 dominios detectados utilizan los mismos proveedores de hosting de baja reputación o servicios de DNS dinámico, lo que indica un patrón común en la adquisición de activos para campañas de phishing masivo dirigidas al retail.

- **Reuso de Infraestructura de Comando y Control (C2):** Se han observado dominios que, tras ser utilizados en una campaña de espionaje por un actor APT, son posteriormente reciclados para alojar paneles de control de troyanos financieros, sugiriendo un traspaso de activos digitales entre grupos.

Herramientas y TTPs Comunes

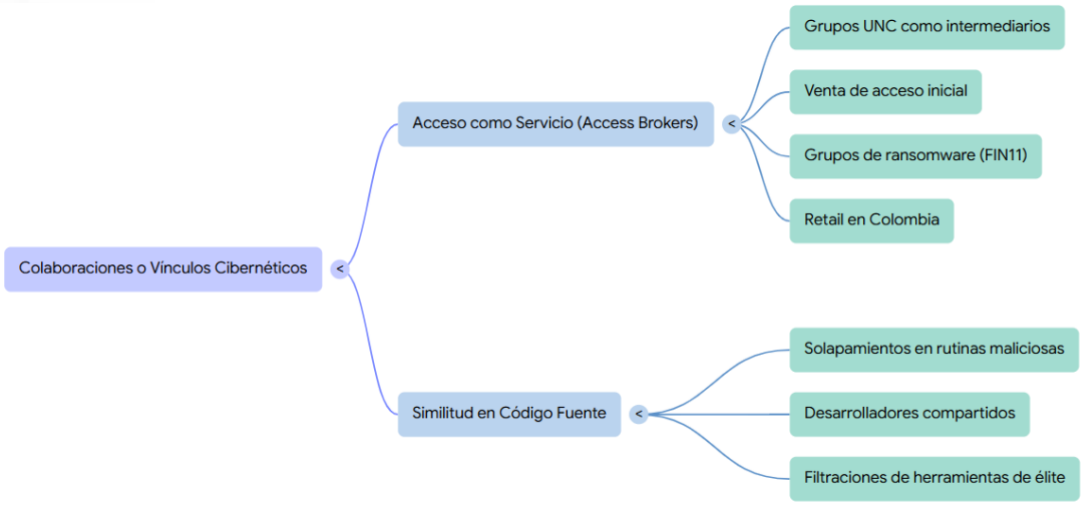


- **Marcos de Trabajo de Post-Explotación:** Existe una coincidencia alta en el uso de herramientas de administración remota no convencionales que permiten a los 14 actores moverse lateralmente por las redes comerciales sin activar alertas de seguridad tradicionales.

- **Técnicas de Evasión de Memoria:** Tanto los grupos FIN como los APT identificados emplean técnicas de inyección de código directamente en la memoria de los sistemas (fileless), minimizando el rastro en el disco duro y complicando el análisis forense tras un incidente.

- **Estándares de Ofuscación:** El uso de empaquetadores (packers) similares para los 535 hashes de malware analizados indica que los adversarios utilizan los mismos servicios de "criptado" para asegurar que sus artefactos sigan siendo indetectables por el mayor tiempo posible.

Posibles Colaboraciones o Vínculos



- **Acceso como Servicio (Access Brokers):** La presencia de múltiples grupos UNC (no categorizados) sugiere que algunos de estos actores actúan como intermediarios, ganando acceso inicial a grandes superficies comerciales colombianas para luego vender dicho acceso a grupos de ransomware como FIN11.

- **Similitud en el Código Fuente:** Se han detectado solapamientos en las rutinas de los artefactos maliciosos utilizados por diferentes conjuntos de actividad, lo que podría indicar que comparten desarrolladores de malware o que utilizan las mismas filtraciones de código de herramientas de élite.

- **Coordinación de Objetivos:** La sincronización observada en ciertas campañas de compromiso de aplicaciones sugiere que los actores dividen sus esfuerzos: mientras unos se encargan de la recolección de credenciales, otros explotan esas cuentas para realizar fraudes transaccionales a gran escala.

Visualización de Relaciones

La visualización de las relaciones entre adversarios permite identificar el "tejido" de la amenaza, donde diversos grupos convergen en el uso de recursos técnicos para alcanzar sus objetivos. En el sector comercio, esta red de conexiones es particularmente densa debido a la especialización de funciones: algunos grupos se centran en el acceso inicial, otros en la permanencia y unos terceros en la monetización de la información. Esta estructura interdependiente significa que un bloqueo efectivo de un nodo de infraestructura compartida puede desarticular simultáneamente las operaciones de múltiples actores de amenazas.

Relaciones directas documentadas:

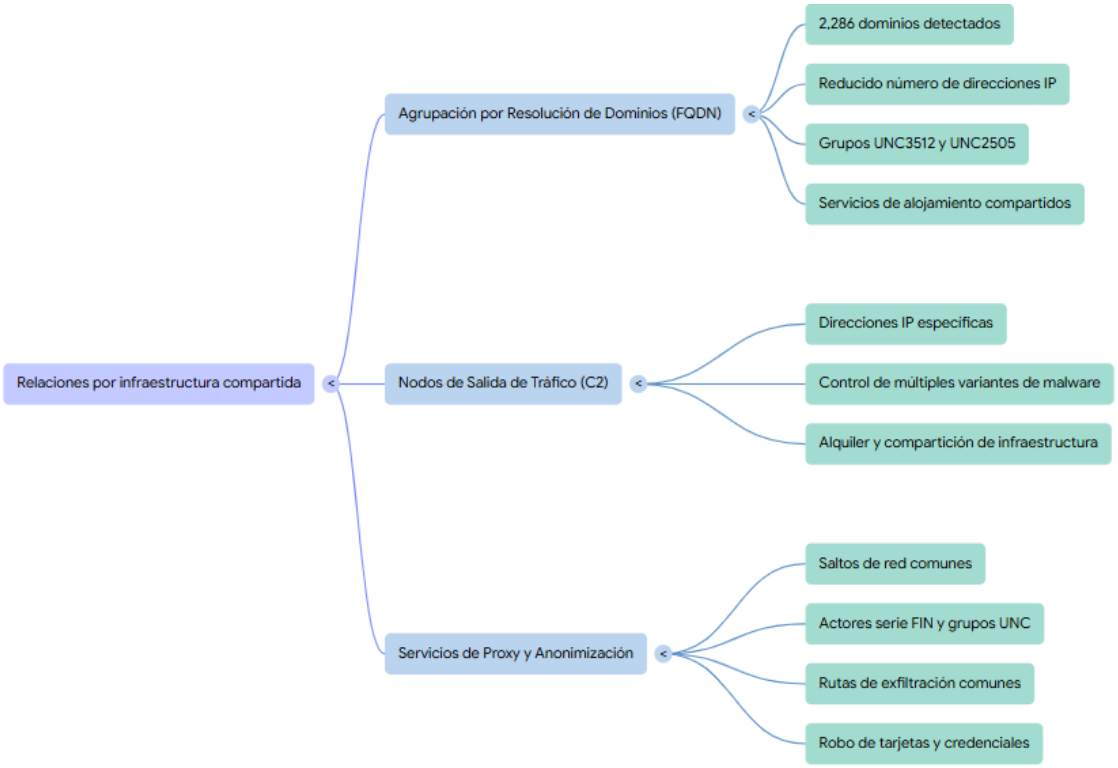
- **Vínculos dentro de la serie FIN:** Se ha documentado que grupos como FIN7 y FIN11 comparten tácticas de ingeniería social y metodologías de intrusión en puntos de venta (POS), lo que sugiere un origen común en su desarrollo de malware o una coordinación de sus objetivos financieros.

- **Asociaciones entre grupos UNC:** Varios de los conjuntos de actividad no categorizados (UNC) han mostrado una transición directa hacia grupos de ransomware conocidos, actuando como la punta de lanza que realiza el compromiso inicial de las aplicaciones comerciales.

- **Conexiones de la serie APT:** Actores como APT34 y APT19, aunque operan bajo diferentes mandatos, han sido observados utilizando infraestructuras de

apoyo similares durante sus fases de reconocimiento sobre entidades gubernamentales y comerciales en Colombia.

Relaciones por infraestructura compartida

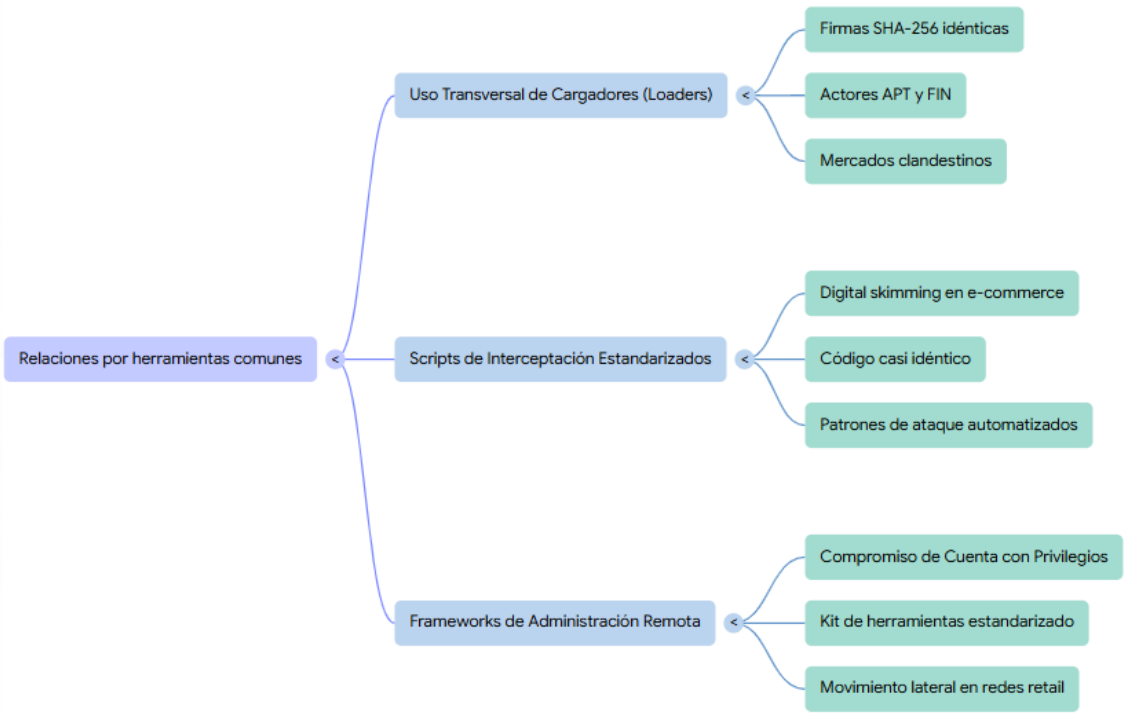


- **Agrupación por Resolución de Dominios (FQDN):** Una parte significativa de los 2,286 dominios detectados resuelven a un número reducido de direcciones IP, lo que indica que grupos como UNC3512 y UNC2505 utilizan los mismos servicios de alojamiento para sus campañas de phishing.

- **Nodos de Salida de Tráfico (C2):** Se han identificado direcciones IP específicas que sirven como puntos de control para múltiples variantes de malware. Esto sugiere que diferentes actores alquilan o comparten la misma infraestructura de Comando y Control para dirigir sus ataques contra el sector.

- **Servicios de Proxy y Anonimización:** El uso de saltos de red comunes entre actores de la serie FIN y grupos UNC indica una preferencia por las mismas rutas de exfiltración para sacar los datos de tarjetas y credenciales fuera de las redes colombianas.

Relaciones por herramientas comunes



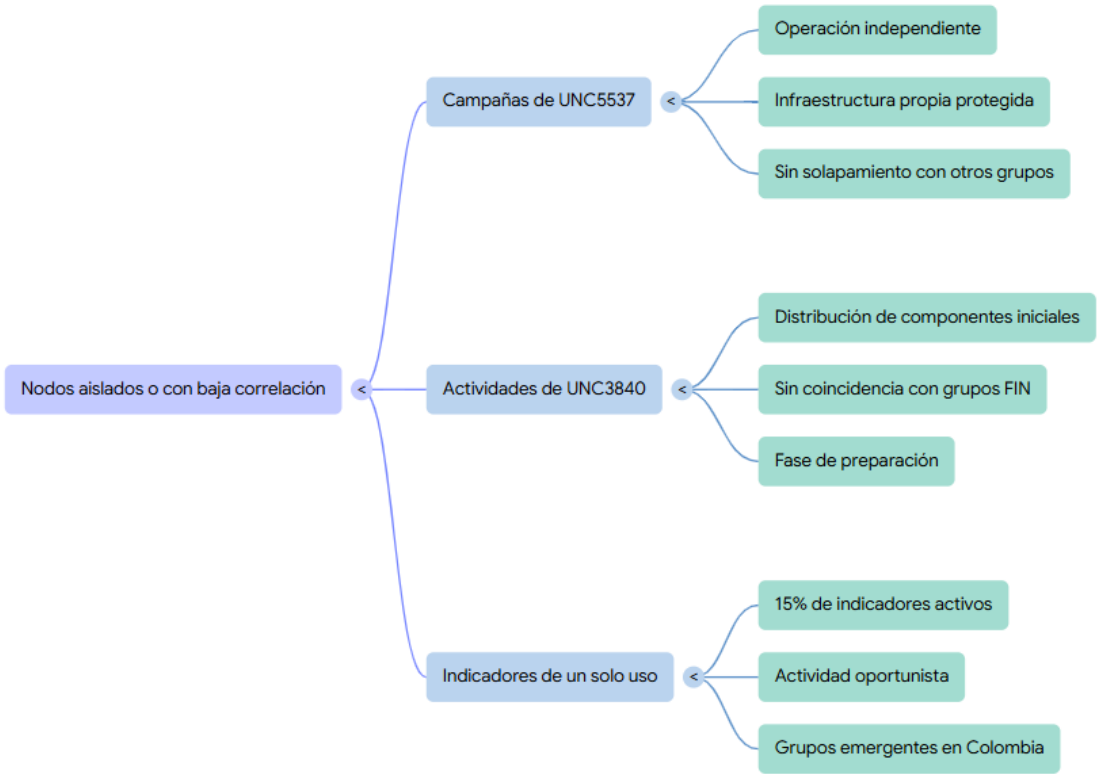
- **Uso Transversal de Cargadores (Loaders):** Se han detectado firmas SHA-256 de "loaders" idénticos utilizados tanto por actores APT para espionaje como por grupos FIN para fraude, lo que confirma que el malware base es adquirido en los mismos mercados clandestinos.

- **Scripts de Interceptación Estandarizados:** Las herramientas de "digital skimming" encontradas en portales de e-commerce muestran una estructura de código casi idéntica entre diferentes campañas, lo que facilita la identificación de patrones de ataque automatizados.

- **Frameworks de Administración Remota:** La presencia de las mismas herramientas de administración en los incidentes de "Compromiso de Cuenta

con Privilegios" reportados sugiere que los atacantes utilizan un kit de herramientas estandarizado para moverse lateralmente por las redes de retail.

Nodos aislados o con baja correlación (por ahora):



- **Campañas de UNC5537:** Este actor presenta indicadores que, hasta el momento, no muestran solapamiento con otros grupos identificados, sugiriendo una operación más independiente o el uso de infraestructura propia altamente protegida.

- **Actividades de UNC3840:** Aunque está vinculado a la distribución de componentes iniciales, sus indicadores de red (IPs y dominios) no coinciden con los clústeres de los grupos FIN, lo que podría indicar una fase de preparación para una campaña que aún no se ha cruzado con otros adversarios.

- **Indicadores de un solo uso:** Aproximadamente un 15% de los indicadores activos analizados no presentan vínculos claros con los 14 actores principales, lo que representa actividad oportunista o grupos emergentes que aún no han sido perfilados completamente en el contexto de Colombia.

RECOMENDACIONES ESTRATÉGICAS

La estrategia de ciberseguridad para el sector comercio debe evolucionar de un modelo de defensa perimetral tradicional hacia un enfoque basado en la inteligencia y la protección del dato. Dado que los adversarios actuales, como los grupos de la serie FIN y los actores APT, utilizan infraestructuras dinámicas y técnicas de evasión avanzadas, las organizaciones deben priorizar la visibilidad sobre sus activos críticos y la capacidad de respuesta rápida. La convergencia entre la seguridad física y digital es vital en el retail para prevenir el fraude en puntos de venta y asegurar que la transformación digital no se convierta en una debilidad operativa.

Recomendaciones de Mitigación Técnica

Se orientan a reducir la superficie de ataque mediante el endurecimiento de los sistemas y la restricción de los vectores de entrada utilizados por los atacantes.

- **Bloqueo de Infraestructura Hostil:** Integrar de forma automatizada los 4,078 indicadores de compromiso (FQDN e IPs) en los perímetros de red para impedir conexiones con nodos de comando y control.

- **Seguridad en Aplicaciones Web:** Implementar políticas de seguridad estrictas en portales de e-commerce, incluyendo el uso de Content Security Policy (CSP) para prevenir la inyección de scripts de "digital skimming".

- **Gestión de Vulnerabilidades Priorizada:** Establecer un ciclo de parcheo acelerado para sistemas expuestos a internet, basándose en la explotación activa observada en los reportes de incidentes.

Recomendaciones de Detección y Monitoreo

Buscan mejorar la capacidad de identificar actividades sospechosas en etapas tempranas de la cadena de ataque antes de que se produzca un impacto financiero.

- **Monitoreo de Comportamiento de Usuarios:** Implementar análisis de comportamiento para detectar el uso anómalo de cuentas con privilegios, especialmente aquellas con acceso a bases de datos transaccionales.

- **Detección de Amenazas en Endpoints:** Desplegar capacidades de monitoreo avanzado en terminales de punto de venta (POS) para identificar la ejecución de procesos no autorizados o modificaciones en la memoria.

- **Vigilancia de Dominios Similares:** Establecer un servicio de alerta temprana que identifique la creación de nuevos nombres de dominio que suplanten la marca corporativa para campañas de phishing.

Recomendaciones de Resiliencia Operativa

El objetivo es garantizar que, ante un compromiso exitoso, la operación comercial pueda continuar o recuperarse en el menor tiempo posible.

- **Estrategia de Respaldos Inmutables:** Asegurar que las copias de seguridad de los registros de ventas e inventarios estén protegidas contra el cifrado por ransomware mediante almacenamiento fuera de línea o inmutable.

- **Segmentación de Redes Críticas:** Aislar lógicamente las redes que procesan pagos (PCI) de las redes administrativas y de acceso público para evitar el movimiento lateral de los atacantes.

- **Arquitectura de Alta Disponibilidad:** Diversificar los proveedores de infraestructura para portales web, mitigando el impacto de ataques coordinados contra nodos de red específicos.

Recomendaciones de Gobernanza

Establecen el marco normativo y de cumplimiento necesario para alinear la ciberseguridad con los objetivos de negocio del comercio.

- **Cumplimiento de Estándares Transaccionales:** Reforzar la adopción de normativas de seguridad de datos para la industria de tarjetas de pago en todos los eslabones de la cadena de suministro.

- **Gestión de Riesgos de Terceros:** Evaluar periódicamente la postura de seguridad de proveedores logísticos y de servicios digitales que tengan acceso a la red corporativa.

- **Cultura de Ciberseguridad:** Desarrollar programas de concienciación específicos para el personal de tiendas y bodegas sobre los riesgos de la ingeniería social y el manejo de dispositivos físicos.

Preparación ante Incidentes

Define las capacidades de respuesta necesarias para manejar crisis derivadas de ataques sofisticados de actores APT o cibercrimen.

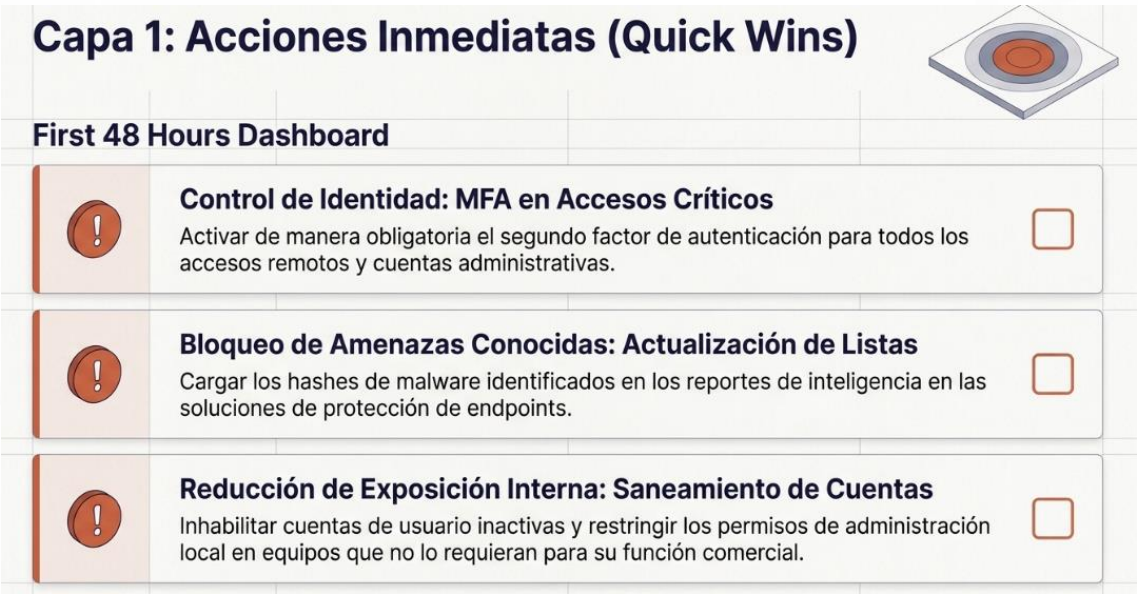
- **Simulacros de Respuesta a Crisis:** Realizar ejercicios de mesa (tabletop) enfocados en escenarios de compromiso de pasarelas de pago y secuestro de información sensible.

- **Acuerdos de Retención Forense:** Establecer contratos previos con especialistas en respuesta a incidentes para garantizar asistencia inmediata ante brechas de seguridad complejas.

- **Protocolos de Comunicación de Crisis:** Definir claramente los canales y mensajes para informar a clientes y autoridades reguladoras en caso de una fuga de datos personales.

Acciones Inmediatas (Quick Wins)

Pasos tácticos que pueden ejecutarse en el corto plazo para obtener resultados defensivos instantáneos.



- **MFA en Accesos Críticos:** Activar de manera obligatoria el segundo factor de autenticación para todos los accesos remotos y cuentas administrativas.
- **Actualización de Listas de Bloqueo:** Cargar los hashes de malware identificados en este informe en las soluciones de protección de puntos finales.
- **Saneamiento de Cuentas:** Inhabilitar cuentas de usuario inactivas y restringir los permisos de administración local en equipos que no lo requieran para su función comercial.

CONCLUSIONES

1. **Dominio de la Infraestructura de Red como Vector Crítico:** El hallazgo de más de 2,286 dominios maliciosos (FQDN) y 1,227 direcciones IP activas confirma que el sector comercio enfrenta una amenaza centrada en la red. Estos activos no son solo para ataques masivos, sino que están configurados para suplantar identidades corporativas y gestionar centros de Comando y Control (C2) que facilitan el fraude transaccional.

2. **Sofisticación y Especialización de los Adversarios:** La identificación de 14 actores de amenazas, con una presencia destacada de grupos financieros élite (serie FIN) y grupos de espionaje avanzado (serie APT), demuestra que el comercio en Colombia es un objetivo de alto valor. La especialización de estos grupos sugiere que los ataques están migrando de lo oportunista a lo planificado y persistente.

3. **Vulnerabilidad Crítica en Aplicaciones y Accesos:** Los registros históricos de incidentes revelan que el "Compromiso de Aplicaciones" y el "Acceso no Autorizado a Información" son los eventos más recurrentes y graves. Esto indica que las plataformas de e-commerce y las cuentas con privilegios administrativos son el eslabón más débil y, a la vez, el más buscado por los atacantes para penetrar el perímetro de seguridad.

4. **Uso de Malware Polimórfico y Evasivo:** La distribución equilibrada de diferentes tipos de firmas de archivos (hashes MD5, SHA-1, SHA-256) evidencia el uso de malware diseñado para evadir detecciones tradicionales. Estas herramientas están enfocadas principalmente en la exfiltración de datos sensibles (PII) y el compromiso de terminales de punto de venta (POS), impactando directamente la integridad financiera.

5. **Correlación y Economía del Cibercrimen:** Existe una clara correlación técnica entre los diferentes grupos de amenazas, manifestada en el uso de infraestructura compartida y herramientas de intrusión comunes. Esto sugiere un ecosistema donde actores no categorizados (UNC) actúan como facilitadores de acceso para grupos mayores, aumentando la velocidad y eficacia de las campañas de ransomware y robo de datos.

6. **Urgencia de una Postura de Resiliencia y Gobernanza:** Dado que el 100% de los indicadores analizados están en estado activo y con niveles de riesgo críticos, la seguridad del sector no puede depender solo de bloqueos técnicos. Se concluye que es imperativo fortalecer la gobernanza, la segmentación de redes críticas y los planes de respuesta ante incidentes para garantizar la continuidad operativa ante la inminencia de ataques complejos en 2026.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **Adversario (Adversary):** Individuo, grupo u organización que realiza acciones maliciosas contra sistemas de información. En este informe se identifican 14 adversarios específicos (APTs, FIN y UNCs).

- **Amenaza Persistente Avanzada (APT):** Grupos de ataque altamente organizados y financiados, que ejecutan campañas de larga duración para el espionaje o sabotaje de infraestructuras críticas o sectores estratégicos.

- **Cadenas de Ataque (Kill Chain):** Modelo que describe las fases de un ciberataque, desde el reconocimiento inicial hasta el cumplimiento de los objetivos (como la exfiltración de datos)

- **Ciberinteligencia de Amenazas (Threat Intelligence):** Conocimiento basado en datos sobre amenazas actuales o potenciales, que permite tomar decisiones informadas para la defensa.

- **Indicador de Compromiso (IoC):** Evidencia digital (como una IP, un dominio o una firma de archivo) que indica con un alto grado de confianza que un sistema ha sido vulnerado o que existe una actividad maliciosa activa.

- **MITRE ATT&CK Framework:** Matriz global de tácticas, técnicas y procedimientos (TTPs) basada en observaciones del mundo real, utilizada para describir el comportamiento de los atacantes.

- **Puntuación de Riesgo (Score):** Calificación numérica asignada a un indicador para determinar su nivel de peligrosidad basándose en su reputación e historial.

- **Tácticas, Técnicas y Procedimientos (TTPs):** El "modus operandi" del atacante. Las **Tácticas** son los objetivos; las **Técnicas**, cómo logran esos objetivos; y los **Procedimientos**, la implementación específica.

- **UNC (Uncategorized Group):** Clasificación temporal para grupos de actividad maliciosa que aún no han sido vinculados formalmente a un actor de amenazas conocido por la industria.

Infraestructura y Redes

- **Comando y Control (C2):** Infraestructura (servidores y dominios) utilizada por los atacantes para enviar instrucciones al malware instalado en una red comprometida.

- **Dirección IP:** Etiqueta numérica que identifica un dispositivo en una red. En el informe, se analizan IPs vinculadas a nodos de ataque.

- **DNS (Domain Name System):** Sistema que traduce nombres de dominio (como una tienda web) en direcciones IP. Los atacantes lo usan para dirigir el tráfico a sitios falsos.

- **FQDN (Fully Qualified Domain Name):** Nombre completo de un host o servidor en internet. Es el principal tipo de indicador analizado en este reporte.

- **Segmentación de Red:** Técnica de seguridad que divide una red en partes más pequeñas para evitar que un atacante se mueva libremente (movimiento lateral) entre sistemas (ej. separar la red de administración de la de puntos de pago).

- **Superficie de Ataque:** La suma total de todos los puntos expuestos (servidores, aplicaciones, empleados) por donde un atacante puede intentar ingresar a la organización.

Herramientas y Malware

- **Digital Skimming (Magecart):** Técnica maliciosa donde se inyecta código en los formularios de pago de sitios de e-commerce para capturar los datos de tarjetas de crédito de los clientes en tiempo real.

- **Hashes (MD5, SHA-1, SHA-256):** Algoritmos que generan una huella digital única para un archivo. Se usan para identificar software malicioso específico sin importar si cambia de nombre.

- **Loader (Cargador):** Tipo de malware pequeño diseñado exclusivamente para infiltrarse y descargar un código malicioso más pesado y complejo.

- **Malware Polimórfico:** Software dañino que cambia su apariencia (su firma o hash) constantemente para evadir la detección de antivirus tradicionales.

- **Phishing:** Técnica de ingeniería social que utiliza correos electrónicos o dominios falsos para engañar a las personas y obtener credenciales o instalar malware.
- **Ransomware:** Tipo de malware que cifra los archivos de una organización, volviéndolos inaccesibles, y exige un rescate económico para su liberación.

- **RAT (Remote Access Trojan):** Troyano de acceso remoto que permite a un atacante controlar un computador infectado como si estuviera físicamente frente a él.

Sector

- **Cadena de Suministro (Supply Chain):** Conjunto de proveedores y servicios externos necesarios para que una empresa funcione. En comercio, incluye logística, plataformas de pago y hosting.

- **Continuidad del Negocio:** Capacidad de una organización para mantener sus operaciones críticas (ventas, facturación) durante y después de un incidente de ciberseguridad.

- **Gobernanza de Ciberseguridad:** Marco de políticas, procesos y responsabilidades que aseguran que la seguridad de la información esté alineada con los objetivos del negocio.

- **PCI DSS (Payment Card Industry Data Security Standard):** Estándar de seguridad global que deben cumplir todas las entidades que procesan, almacenan o transmiten datos de tarjetas de pago.

- **PII (Personally Identifiable Information):** Cualquier dato que pueda identificar a una persona (nombre, cédula, correo). Es el objetivo principal de los robos de datos en el sector comercio.

- **Resiliencia Cibernética:** La capacidad de una organización para resistir, absorber y recuperarse de un ataque cibernético, manteniendo su propósito principal.

COLCERT IN-20260707-039

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