TIC

Informe de apreciación Sector

Energético

COLCERT

Contenido

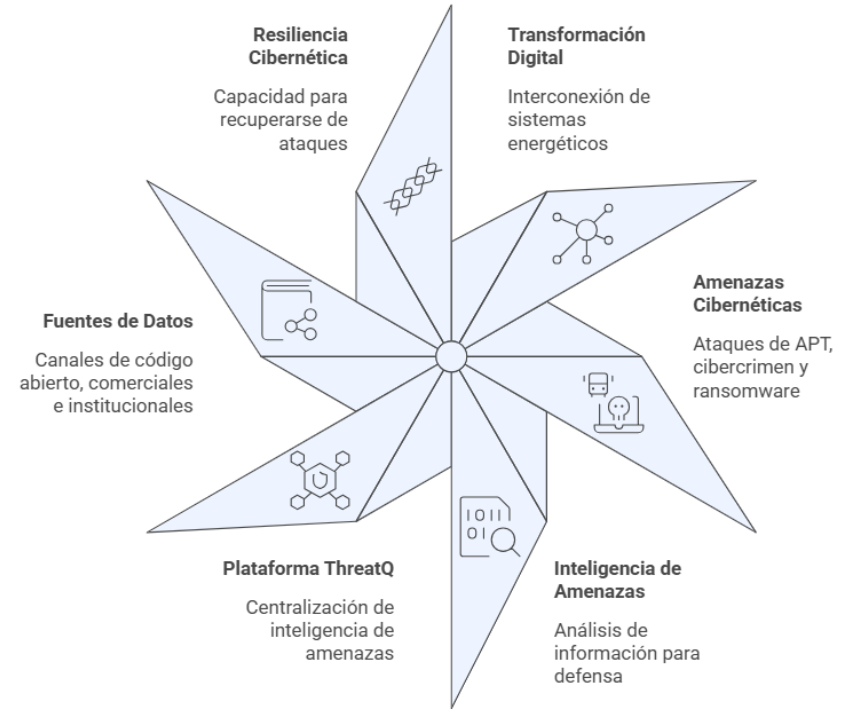
RESUMEN EJECUTIVO

En el sector energético colombiano, la transformación digital ha ampliado la exposición a ciberamenazas. Actores APT, cibercrimen y ransomware atacan infraestructuras críticas buscando afectar la operación y los servicios esenciales.

Este informe usa inteligencia de amenazas para hacer seguimiento al comportamiento de actores que afectan el sector, a partir de información recopilada. Se priorizan fuentes (abiertas, comerciales, institucionales) que aporten visibilidad sobre amenazas relevantes para infraestructuras críticas nacionales.

Lineamientos

- Seguimiento a actores que afectan el sector energético colombiano.
- Uso de inteligencia de amenazas.
- Priorización de fuentes de ciberinteligencia aplicables al país.
- Enfoque en infraestructuras críticas nacionales.
- Reducción de tiempos de detección y respuesta.
- Fortalecimiento de la resiliencia cibernética del sector.



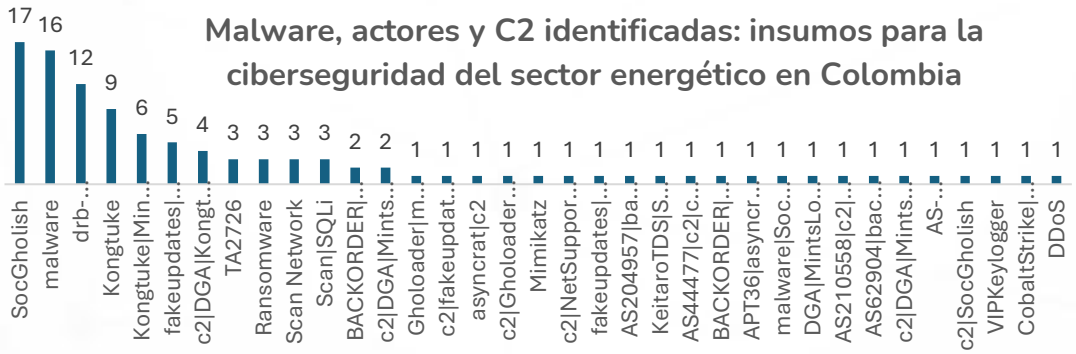
INTRODUCCIÓN

El presente informe se enfoca en fortalecer la ciberinteligencia del sector energético colombiano mediante el seguimiento al comportamiento de actores que lo afectan. Se fundamenta en la revisión de fuentes de inteligencia (OSINT, comerciales e institucionales) para la detección y respuesta ante incidentes en infraestructuras críticas.

Aspectos clave

- Fortalecer la ciberinteligencia en el sector energético colombiano.
- Seguimiento al comportamiento de actores que afectan el sector.
- Revisión de fuentes OSINT, comerciales e institucionales.
- Detección y respuesta ante incidentes.
- Protección de activos de generación, transmisión y control operativo.

Hallazgos Clave

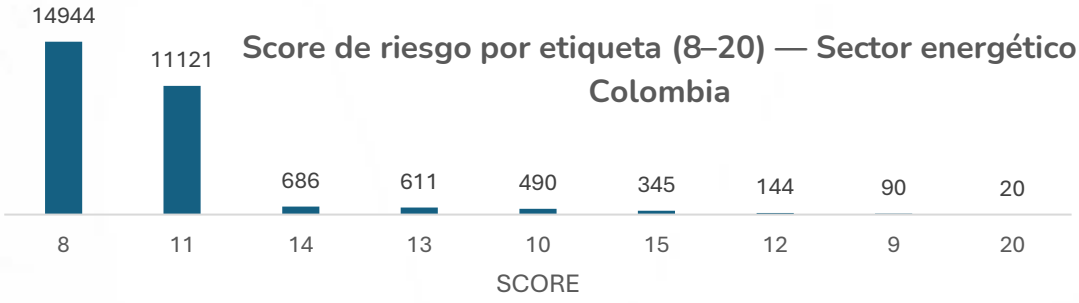


- **Actores de Amenaza Identificados:** Se ha detectado actividad persistente de 15 grupos de adversarios de alto perfil, destacando la presencia de APT44 (Sandworm), APT34 (OilRig) y FIN7. Estos grupos poseen capacidades avanzadas para el sabotaje de infraestructura crítica y el fraude financiero a gran escala.

- **Volumen de Indicadores:** Se analizaron 3,070 indicadores activos, con una predominancia de FQDNs (1,406) e Direcciones IP (1,200), lo que sugiere una infraestructura de comando y control (C2) externa altamente distribuida.

- **Aparición de Amenazas Híbridas:** Se observa una convergencia entre grupos de espionaje estatal (APT44) y actores de ransomware (RansomHub, SocGholish), aumentando el riesgo de ataques de "Doble Extorsión" contra empresas generadoras y distribuidoras de energía en Colombia.

- **Severidad de los Indicadores:** Más de 11,000 registros presentan un score de criticidad superior a 11, lo que indica una alta probabilidad de compromiso si no se aplican medidas correctivas inmediatas.



Recomendaciones Prioritarias

- **Bloqueo de Infraestructura C2:** Implementar de manera inmediata el bloqueo en el perímetro de las 1,200 direcciones IP y 1,406 dominios identificados en este análisis.

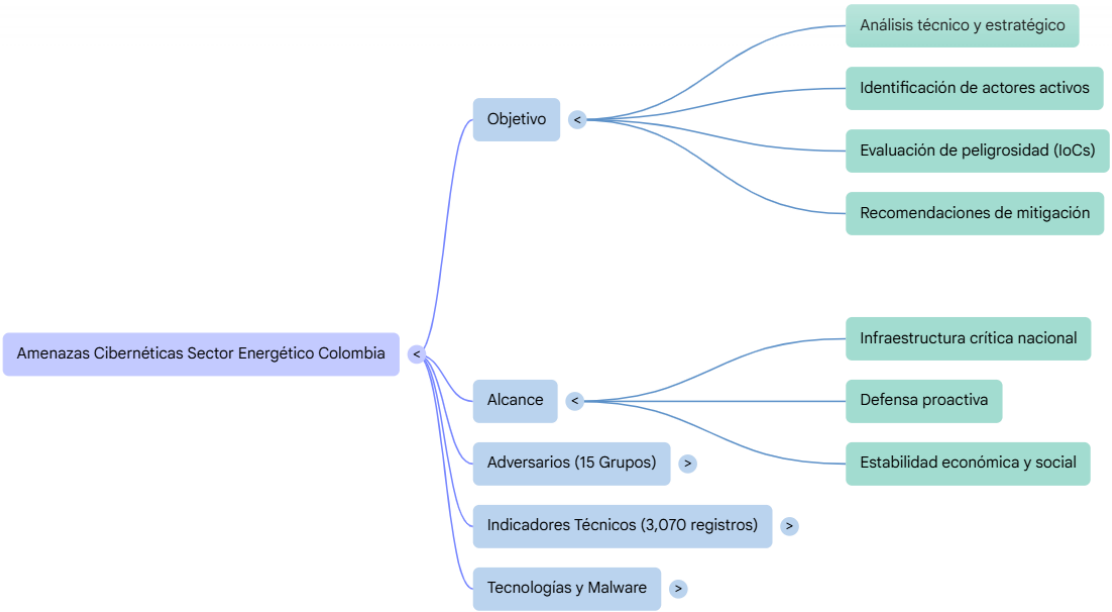
- **Monitoreo de Movimiento Lateral:** Dado el registro de herramientas como Mimikatz y CobaltStrike, es crítico reforzar la vigilancia sobre el uso de credenciales administrativas y la segmentación entre las redes IT y las redes de control industrial (OT).

- **Protección contra Ransomware:** Reforzar las defensas contra los vectores de SocGholish y RansomHub, los cuales están utilizando activamente técnicas de Fake Updates para infiltrarse en las estaciones de trabajo de los analistas.

Conclusión Estratégica

El sector energético colombiano se encuentra bajo el radar de grupos APT con historial de ataques a infraestructuras críticas globales (especialmente Sandworm). La postura de seguridad debe evolucionar de un modelo reactivo a uno basado en Inteligencia de Amenazas (CTI), donde la detección temprana de indicadores con score elevado sea la prioridad para garantizar la continuidad del flujo en el sector energético nacional.

OBJETIVO Y ALCANCE



Objetivo

Proveer un análisis técnico y estratégico sobre el panorama de amenazas cibernéticas dirigidas al sector energético en Colombia durante el periodo actual. El informe busca identificar a los actores de amenazas activos, evaluar su peligrosidad mediante el análisis de indicadores de compromiso (IoCs) y proporcionar recomendaciones accionables para mitigar el riesgo de interrupción operativa o exfiltración de datos sensibles.

Alcance

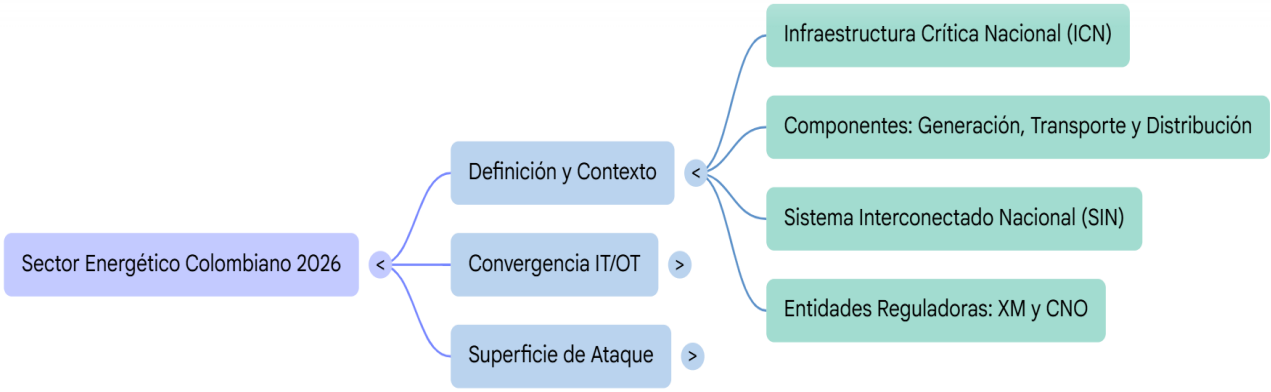
El presente análisis se fundamenta en la correlación de inteligencia estratégica y datos operativos para identificar vectores de ataque dirigidos específicamente a la infraestructura crítica nacional. Dado que el sector energético es el eje de la estabilidad económica y social de Colombia, este alcance define el marco de monitoreo sobre los actores de amenazas más persistentes, permitiendo transformar los indicadores técnicos en una defensa proactiva contra el sabotaje digital y la interrupción del servicio. Este informe abarca:

- **Adversarios**: Análisis de 15 grupos APT y financieros (incluyendo APT44, APT34, FIN7, FIN11 y UNC5736) con actividad registrada o interés en activos colombianos.
- **Indicadores Técnicos**: Evaluación de 3,070 registros activos desglosados en FQDN, IPs, URLs y hashes de malware (MD5, SHA-1, SHA-256).
- **Tecnologías** y **Malware**: Identificación de herramientas de ataque detectadas (AsyncRAT, CobaltStrike, Mimikatz, SocGholish, RansomHub).
- **Geografía**: Enfocado exclusivamente en el impacto sobre la infraestructura crítica del territorio nacional colombiano.

CONTEXTO ESTRATÉGICO Y DEFINICIÓN DEL SECTOR

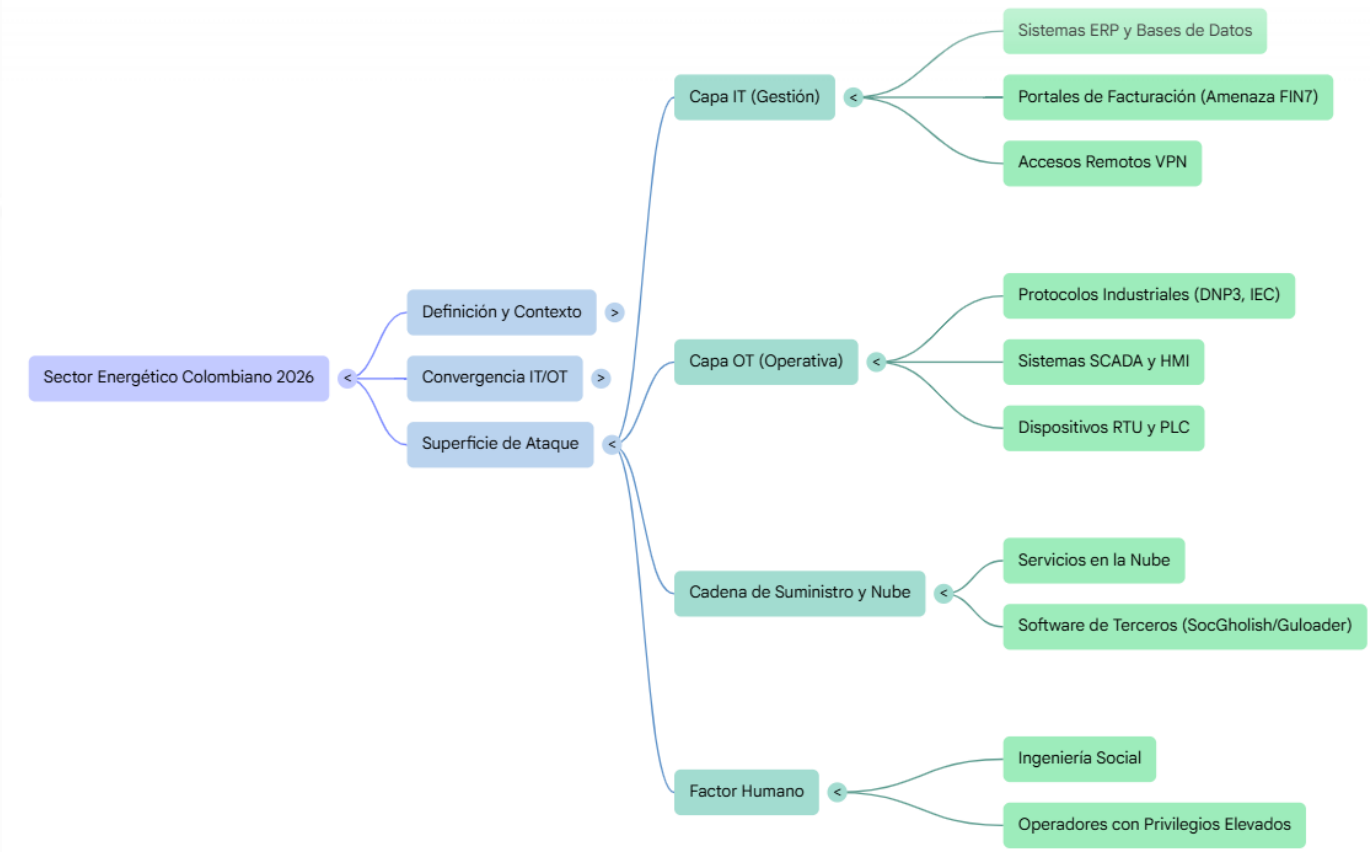
Definición y Entendimiento del Sector

El sector energético colombiano se define como un ecosistema de Infraestructura Crítica Nacional (ICN), cuya operatividad es vital para la seguridad, la economía y el orden público. Este sector no solo comprende la generación (hidráulica, térmica y renovables no convencionales), sino también el transporte y la distribución de energía a través del Sistema Interconectado Nacional (SIN).



Estratégicamente, el sector está regido por una estricta jerarquía normativa donde la XM (operador del mercado) y el CNO establecen los parámetros de seguridad. En 2026, el entendimiento del sector ha evolucionado hacia la convergencia IT/OT, donde la digitalización de las subestaciones y el uso de redes inteligentes (Smart Grids) han eliminado el "aislamiento físico" tradicional, convirtiendo la disponibilidad del servicio en un objetivo directamente dependiente de la integridad ciberespacial.

Superficie de Ataque



La superficie de ataque en el sector energético colombiano se ha expandido de manera multidimensional, exponiendo puntos críticos en tres niveles principales:

Capa de Gestión y Administración (IT):

- Sistemas ERP y bases de datos corporativas.
- Portales de atención al cliente y facturación, frecuentemente atacados por grupos como FIN7 para exfiltración de datos financieros.
- Puntos de acceso remoto (VPN) utilizados por contratistas y personal de mantenimiento.

Capa de Control Operativo (OT):

- Protocolos industriales (DNP3, IEC 60870-5-104 y IEC 61850) que, en muchos casos, carecen de cifrado nativo.
- Interfaces Hombre-Máquina (HMI) y sistemas SCADA que gestionan el flujo de carga en tiempo real.
- Unidades Terminales Remotas (RTU) y Controladores Lógicos Programables (PLC) situados en zonas geográficamente aisladas.

Cadena de Suministro y Nube:

- Interconexiones con proveedores de servicios en la nube para el análisis de datos de red.
- Actualizaciones de software de terceros, identificadas como un vector crítico dado el registro de amenazas tipo SocGholish y Guloader observadas en el análisis de adversarios.
- Punto Crítico: La superficie de ataque no es solo tecnológica; incluye el factor humano mediante técnicas de Social Engineering dirigidas a operadores de centros de control con privilegios elevados.

PANORAMA ACTUAL DE AMENAZAS

El panorama de ciberseguridad para el sector energético en Colombia durante 2025 y 2026 se ha tornado crítico, marcado por incidentes de alto impacto como el ataque de ransomware contra la empresa Air-e, que evidenció la vulnerabilidad de la infraestructura de servicios públicos ante la extorsión digital. Con un registro alarmante de 35 millones de intentos de ransomware en el país al cierre de abril de 2026, la estabilidad del Sistema Interconectado Nacional depende hoy más que nunca del cumplimiento estricto del Acuerdo CNO 1960. Este marco normativo busca blindar la operación energética frente a un ecosistema de amenazas que ya no solo busca el lucro económico, sino el sabotaje directo a la continuidad de la infraestructura vital colombiana.

TITULO	FECHA	FUENTE / ENLACE
Acuerdo CNO cumplimiento para el sector eléctrico	30/10/2025	Internexa
Ciberseguridad en Colombia 2025: amenazas y estrategias clave	30/10/2025	impactotic
Ciberseguridad y Acuerdo 1960: garantizando estabilidad energética	6/10/2025	ey.com
El ciberataque contra Air-e planta un nuevo obstáculo	23/10/2024	elpais.com
Ransomware en Colombia: 35 Millones de ataques	21/04/2026	ransomwarehelp

Tipología de Eventos Identificados

El análisis detallado de los indicadores de compromiso (IoCs) permite categorizar las amenazas según su naturaleza técnica y su potencial de afectación en la cadena de valor energética. Esta tipología no solo clasifica el volumen de los eventos detectados, sino que prioriza aquellos hallazgos que, por su origen en fuentes de inteligencia global como Google Threat Intelligence y CISA, representan un riesgo inminente para la integridad de los activos críticos en Colombia.

Tipo de IOC	Volumen Estimado	Fuentes Principales	Relevancia para Sector Energético
Malware (hashes SHA-1, SHA-256, MD5)	Alto	Google Threat Intelligence, AllenVault OTX, MISP Import	Crítica – Puede indicar presencia de ransomware o backdoors en sistemas TI/TO
C2 y Exfiltración (FQDN, IP Address)	Muy Alto	Google Threat Intelligence, MISP Import, ThreatFox	Crítica – Identifica servidores de comando y control para APIs y botnets
Phishing y Suplantación (FQDN, URL)	Alto	Google Threat Intelligence, MISP Import	Alta – Dirigido a robo de credenciales de operadores y personal administrativo
Infraestructura Maliciosa (IP Address, FQDN)	Medio	MISP Import, Google Threat Intelligence, CISA	Alta – Hosting de payloads, paneles de administración maliciosa
Redes de Distribución de Malware (FQDN, URL)	Medio	Abuse.ch URLs, Google Threat Intelligence	Media-Alta – Descarga de malware actualizado a equipos del sector
Dominios DGA y Acortadores (FQDN)	Bajo	MISP Import	Media – Asociado a malware avanzado que evade listas estáticas
Posible Explotación Activa (IP Address, URL)	Bajo	MISP Import, CISA KEV, Abuse.ch	Crítica – Requiere verificación inmediata por posible compromiso

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

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

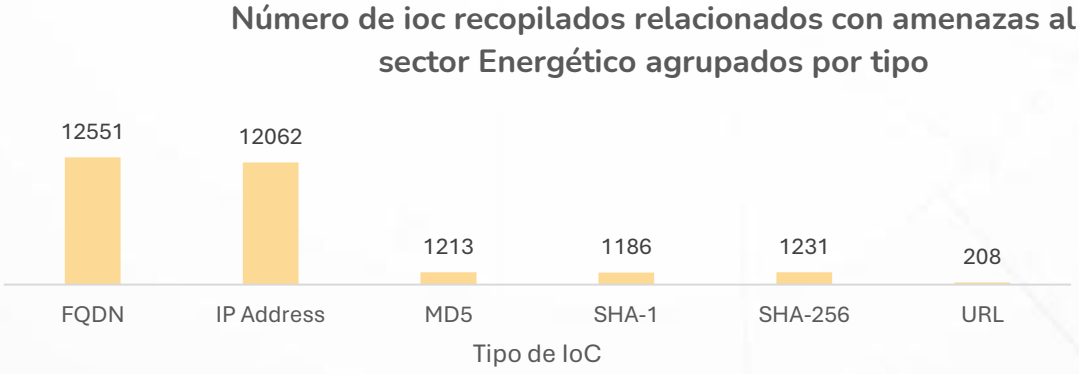
- **Predominancia de Infraestructura C2:** El volumen "Muy Alto" de indicadores de Comando y Control (C2) sugiere que existen intentos persistentes de establecer persistencia dentro de las redes del sector para futuras fases de ataque.
- Convergencia de Riesgos TI/TO: Los hallazgos de malware con criticidad alta indican una amenaza directa hacia la disponibilidad de los sistemas de control industrial, donde un compromiso puede derivar en fallas físicas de suministro.

- **Sofisticación en la Evasión:** La presencia de dominios DGA y acortadores resalta la necesidad de contar con sistemas de detección dinámica, ya que los atacantes están utilizando infraestructuras efímeras para evadir listas negras estáticas tradicionales.

- **Enfoque en el Robo de Identidad:** El alto volumen de phishing y suplantación confirma que el eslabón humano (operadores y personal administrativo) sigue siendo el vector preferido para obtener acceso inicial a las redes corporativas.

INDICADORES DE COMPROMISO (IoCs)

El análisis de los Indicadores de Compromiso (IoCs) constituye la base táctica para la detección y mitigación de amenazas en el sector energético colombiano. Estos datos, recopilados y correlacionados a partir de múltiples fuentes de inteligencia de amenazas, permiten identificar las huellas digitales de los adversarios, desde la infraestructura de red utilizada para el comando y control hasta las firmas específicas de los artefactos maliciosos desplegados. La visibilidad detallada de estos indicadores es fundamental para robustecer los controles preventivos y acelerar los tiempos de respuesta ante posibles incidentes en la infraestructura crítica.



Análisis Cuantitativo de Inteligencia

- **Predominancia de Infraestructura de Red:** Los FQDN (12,551) e IP Addresses (12,062) constituyen la mayoría de los hallazgos, reflejando un despliegue masivo de nodos para comunicaciones de comando y control (C2) y exfiltración de datos.
- **Identificación de Malware:** Se han catalogado más de 3,600 hashes únicos (repartidos entre MD5, SHA-1 y SHA-256), permitiendo la detección exacta de variantes de ransomware, troyanos de acceso remoto (RATs) y cargadores detectados en el entorno.
- **Focalización en Vectores Web:** Aunque el número de URLs (208) es menor, estas representan puntos específicos de infección mediante descargas dirigidas (drive-by downloads) o portales de suplantación de identidad para el robo de credenciales.
- **Capacidad de Correlación:** El alto volumen de indicadores recopilados permite una detección temprana, facilitando el bloqueo proactivo en el perímetro antes de que se establezca una conexión exitosa con los sistemas críticos.

Resumen de IoCs Relevantes

Esta sección sintetiza los hallazgos técnicos más críticos extraídos del análisis masivo de datos. A diferencia de la visión cuantitativa general, aquí se priorizan aquellos indicadores que, por su elevado puntaje de riesgo (Score) y su asociación directa con familias de malware y campañas activas, representan una amenaza inmediata de compromiso para las redes del sector energético. Estos IoCs han sido validados por múltiples fuentes de inteligencia y requieren una atención prioritaria en los esquemas de monitoreo y bloqueo del SOC.

Componente de Inteligencia	Descripción Técnica	Nivel de Riesgo
Adversarios Detectados	Identificación de 15 grupos (APTs y Financieros) con interés en infraestructura crítica.	Crítico
Infraestructura C2	Dominios y direcciones IP configurados para el control remoto de activos comprometidos.	Muy Alto
Familias de Malware	Presencia de agentes como AsyncRAT, SocGholish y RansomHub en la cadena de ataque.	Alto
Evasión de Defensas	Uso de algoritmos de generación de dominios (DGA) para ocultar comunicaciones maliciosas.	Medio-Alto
Severidad de Alertas	Concentración masiva de indicadores con puntuación de riesgo (Score) superior a 11/15.	Crítico

A continuación, se detallan los indicadores más relevantes identificados dentro del monitoreo de afectación al sector energético.

Dominios de Alta Criticidad (Score 15-20)

- drive.google.com/uc (Asociado a: APT36, AsyncRAT, Guloader, Raccoon)
- virtual.urban-orthodontics.com (Asociado a: SocGholish, FakeUpdates)
- sponsor.sewacanada.org (Asociado a: SocGholish)
- zone.ebuilderssource.com (Asociado a: SocGholish)
- order.buyanemostatonline.com (Asociado a: SocGholish)
- nevada.mandros.us (Asociado a: SocGholish)

Infraestructura DGA y C2 (Familia Kongtuke/MintsLoader)

- imfiejalbhhgijl.top
- ikhgijabfnkajem.top
- dckhgjimeghemhl.top
- kmaealcfcalhcac.top
- kjalcimbfaaddff.top
- kffgkjmjangegkg.top
- gnmdjjckbgddaie.top
- poubnxu3jubz.top

Indicadores de Red y Malware (Nivel de Riesgo 8-14)

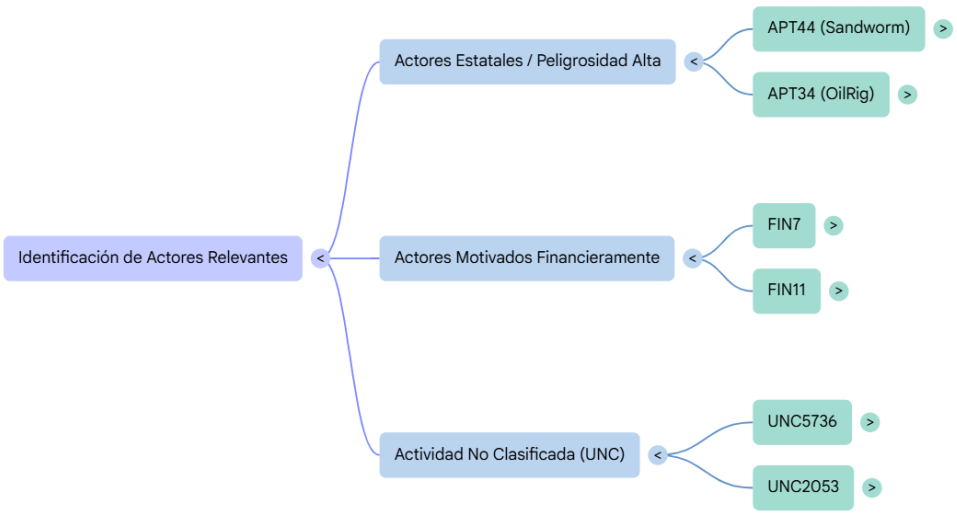
- IP 213.164.204.152
- IP 198.98.59.35
- Hash SHA-256: 61cddbce89b545fc61eb63948d305d68e8632ef5afc3c9040bc11f81be65f0c
- Hash SHA-1: a64f895cb6f3b4a47e0ba02109ba52740557cb9a
- Hash MD5: 3c92aa984b250d8545f23e74d2f0dd9b

ANÁLISIS DE ACTORES DE AMENAZAS (ADVERSARIES)

Categoría de Actor	Cantidad	Actores Identificados	Impacto Estratégico en el Sector
Gubernamentales (APT)	3	APT44 (Sandworm), APT34 (OilRig), APT19	**Crítico:** Sabotaje de infraestructura crítica y espionaje de activos estratégicos nacionales.
Cibercrimen Financiero	3	FIN7, FIN11, FIN6	**Alto:** Interrupción operativa mediante ransomware y exfiltración de datos corporativos.
Acceso Inicial y Soporte	2	UNC1543, UNC3840 (Raspberry Robin)	**Medio-Alto:** Infección masiva y venta de accesos a grupos de ransomware de mayor impacto.
Acceso Inicial y Soporte	7	UNC5736, UNC2053, UNC5487, UNC5537, UNC3559, UNC4515, UNC5111	**Bajo-Medio:** Actividades de reconocimiento, escaneo de vulnerabilidades y persistencia silenciosa.

Identificación de Actores Relevantes

El monitoreo de inteligencia ha permitido identificar 15 grupos de amenazas con actividad persistente que impactan el ecosistema financiero. Entre los más críticos se encuentran:



- **APT44 (Sandworm):** Actor estatal de altísima peligrosidad, reconocido globalmente por ejecutar ataques destructivos contra redes eléctricas. Su presencia en los datos recopilados es el hallazgo más alarmante para la estabilidad del SIN.
-

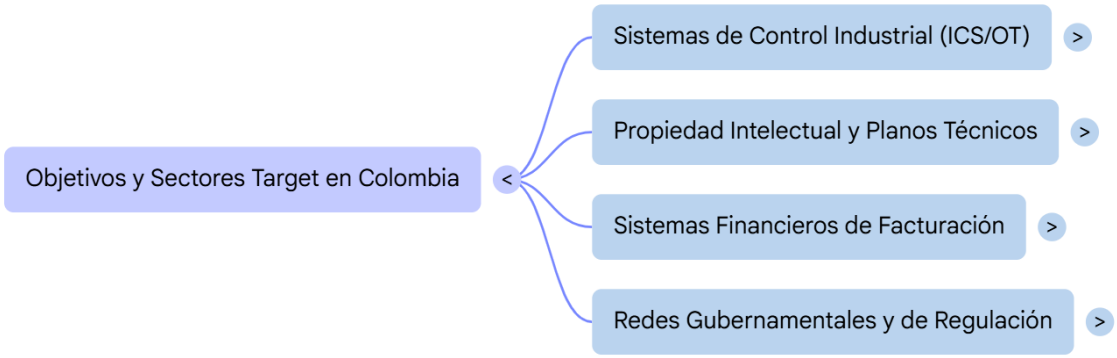
- **APT34 (OilRig):** Grupo especializado en operaciones de ciber espionaje de largo aliento, con un enfoque documentado en infraestructura crítica y sectores gubernamentales.

- **FIN7 y FIN11:** Actores motivados financieramente que han evolucionado de ataques bancarios tradicionales a operaciones de ransomware de "caza mayor", dirigidas a corporaciones que gestionan servicios públicos.

- **UNC5736 y UNC2053:** Grupos de actividad no clasificada que utilizan herramientas de acceso remoto (RATs) para el reconocimiento y la exfiltración de datos técnicos sensibles.

Objetivos y Sectores Target

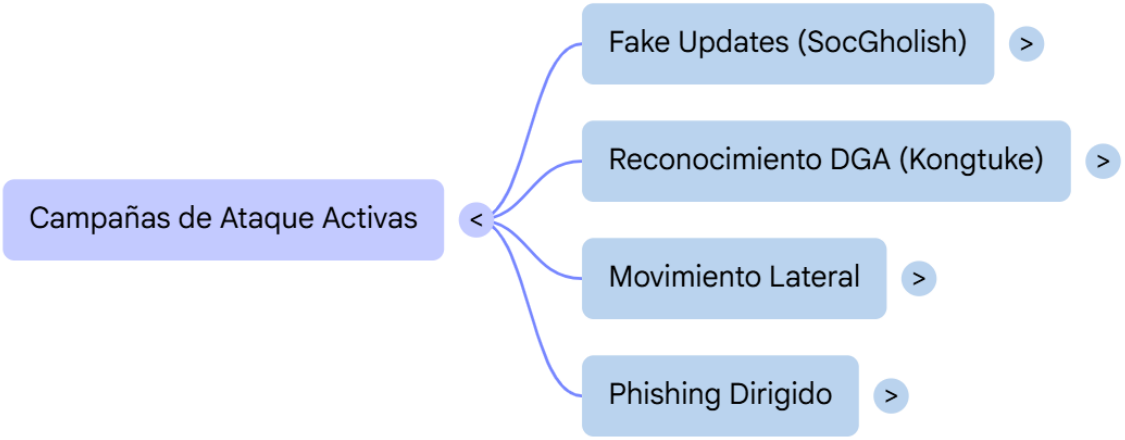
Los adversarios identificados comparten un interés estratégico en sectores que manejan activos físicos y económicos de gran escala. En el contexto colombiano, sus objetivos principales son:



- **Sistemas de Control Industrial (ICS/OT):** Interrupción de procesos de generación y distribución de energía para causar impacto social o político.
- **Propiedad Intelectual y Planos Técnicos:** Obtención de diagramas de red de subestaciones y manuales de configuración de sistemas SCADA.
- **Sistemas Financieros de Facturación:** Secuestro de bases de datos de clientes y sistemas de recaudo para extorsión mediante ransomware.
- **Redes Gubernamentales y de Regulación:** Monitoreo de las decisiones estratégicas de entes como la CREG y XM para anticipar cambios en la política energética nacional.

Campañas Activas

Se han detectado múltiples campañas de ataque en curso que utilizan los siguientes métodos:



- **Campaña de Distribución de "Fake Updates":** Utilización de infraestructuras como SocGholish para engañar a operadores y técnicos del sector, instalando backdoors bajo la apariencia de actualizaciones de software necesarias.
- **Operaciones de Reconocimiento DGA:** Uso intensivo de algoritmos de generación de dominios (identificados en la familia Kongtuke) para mantener comunicaciones ocultas con servidores de comando y control sin ser detectados por filtros estáticos.
- **Campañas de Movimiento Lateral:** Uso de herramientas de post-explotación como CobaltStrike y Mimikatz para saltar desde redes administrativas (IT) hacia redes de operación (OT) una vez obtenido el acceso inicial.
- **Infraestructura de Phishing Dirigido:** Despliegue de URLs y dominios fraudulentos diseñados para capturar credenciales de acceso remoto (VPN) de personal crítico y contratistas del sector eléctrico.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTPs)

Mapeo a MITRE ATT&CK Framework

A partir de la evidencia recolectada y correlacionada por el equipo de CTI —incluyendo IOCs de phishing, hashes de malware, IPs de C2, dominios DGA y etiquetas como Scan Network, SQLi, Ransomware y DDoS—, se han identificado las siguientes tácticas y técnicas del marco MITRE ATT&CK que aplican a las cadenas de ataque observadas contra el sector energético colombiano.

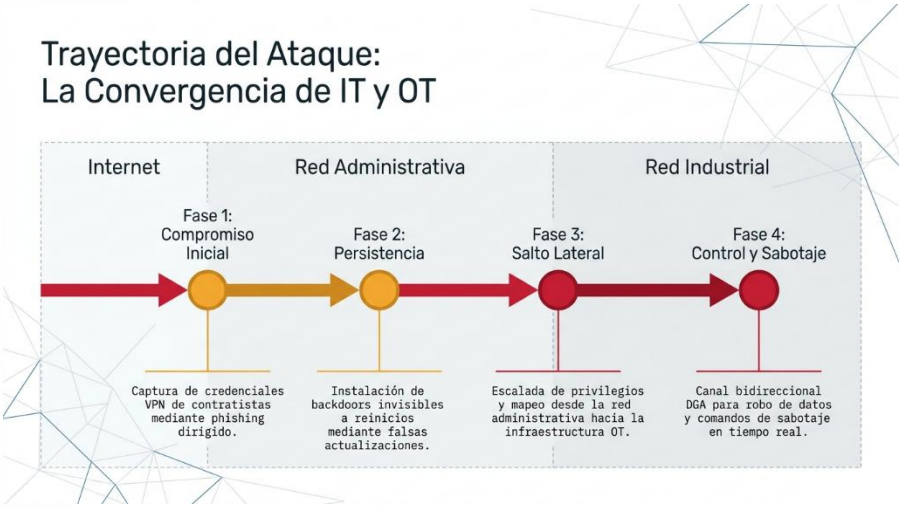
ID Táctica	Nombre	Justificación
TA0043	Reconnaissance	Evidencia de IPs con etiquetas Scan Network y Scan en MISP Import (ej. 23.129.64.143)
TA0001	Initial Access	Dominios de suplantación (microsoft-um.xyz, adobeprotect.com) y URLs de descarga de malware
TA0002	Execution	Hashes de malware (SHA-256, SHA-1, MD5) que requieren ejecución para desplegar carga maliciosa
TA0003	Persistence	Malware como DanBot (APT34) y GreyEnergy (APT44) diseñados para mantener acceso
TA0005	Defense Evasion	Técnicas de ofuscación, uso de DGA (k6j.pw, 4j5.xyz) y loaders como Raspberry Robin
TA0006	Credential Access	Presencia de Mimikatz en feeds de ThreatFox y MISP Import para robo de credenciales
TA0007	Discovery	IPs etiquetadas como Scan Network y SQLi para mapeo de activos y vulnerabilidades
TA0008	Lateral Movement	Uso de PsExec, Cobalt Strike y etiquetas malware en IPs reportadas por MISP Import
TA0011	Command and Control	IPs y FQDN de C2 activos (uz3.me, api-us.thenycmeetings.com, 109.70.100.1 con score 14)
TA0040	Impact	Etiquetas Ransomware, DDoS y malware Industroyer2 dirigido a disponibilidad de ICS/SCADA

ID	Nombre	Justificación
T1490	Inhibit System Recovery	Ransomware que elimina copias de seguridad y puntos de restauración.
T1210	Exploitation of Remote Services	Movimiento lateral con PsExec y Cobalt Strike.
T1547	Boot or Logon Autostart Execution	Persistencia mediante tareas programadas (relacionado con Raspberry Robin).
T1055	Process Injection	Técnica común en loaders como DanBot y GreyEnergy.
T1070	Indicator Removal	Limpieza de logs posterior al despliegue de ransomware.
T1036	Masquerading	Dominios suplantando a Microsoft, Adobe y Google.
T1041	Exfiltration Over C2 Channel	Exfiltración de datos a través de canales C2 establecidos.
T1046	Network Service Discovery	IPs etiquetadas como Scan Network en MISP Import.
T1190	Exploit Public-Facing Application	Vulnerabilidades escaneadas (etiqueta SQLi) en activos expuestos.
T1566	Phishing	Dominios de suplantación (microsoft-um.xyz, adobeprotect.com).
T1204	User Execution	Documentos maliciosos descargados desde URLs como cloudpromo.xyz.
T1059	Command and Scripting Interpreter	Malware como JSSLOADER y DICELOADER basados en scripts.
T1027	Obfuscated Files or Information	Hashes de malware ofuscado y dominios DGA.
T1003	OS Credential Dumping	Presencia de Mimikatz en ThreatFox y MISP Import.
T1071	Application Layer Protocol	C2 sobre HTTP/HTTPS en IPs como 45.154.98.176.
T1102	Web Service	Uso de acortadores de URL (uz3.me, k6j.pw) como redireccionamiento.
T1568	Dynamic Resolution	Dominios DGA (4j5.xyz, k6j.pw) para evadir listas estáticas.
T1573	Encrypted Channel	C2 sobre TLS/SSL en FQDN como api-us.thenycmeetings.com.
T1486	Data Encrypted for Impact	Ransomware LockBit y BlackCat (etiqueta Ransomware).
T1498	Network Denial of Service	IP etiquetada como DDoS (141.255.162.218).

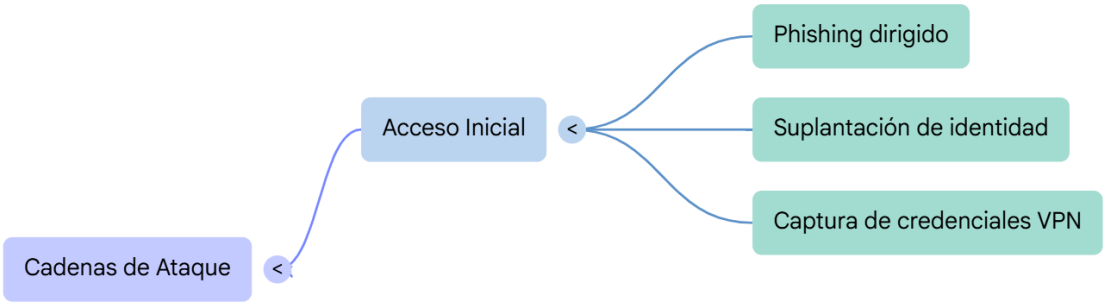
Cadenas de Ataque Observadas

Esta sección describe la progresión táctica empleada por los adversarios para infiltrarse en la infraestructura energética. Las cadenas de ataque observadas no son lineales; representan un esfuerzo coordinado que comienza con el compromiso de activos periféricos y evoluciona hacia el control profundo de la red, aprovechando tanto vulnerabilidades técnicas como el factor humano. El análisis permite identificar los puntos de quiebre donde las medidas de detección pueden interceptar la operación antes de que se alcance el objetivo final.

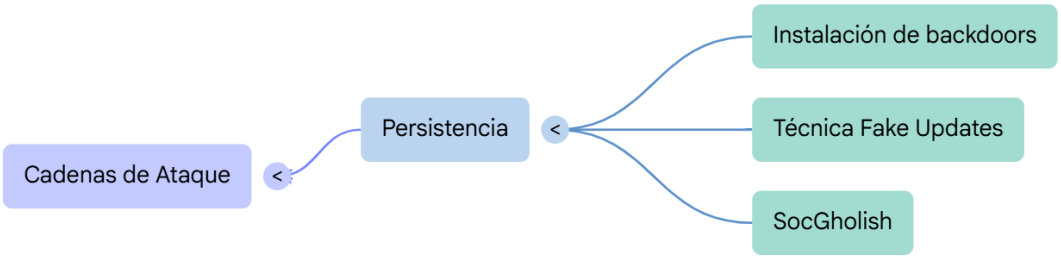
Cadenas de ataque:



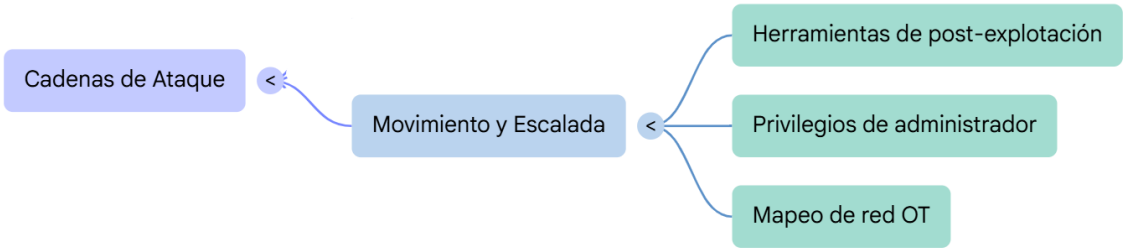
- **Compromiso de Acceso Inicial:** Uso intensivo de campañas de phishing dirigido y técnicas de suplantación de identidad para capturar credenciales de acceso remoto (VPN) de contratistas y personal operativo.



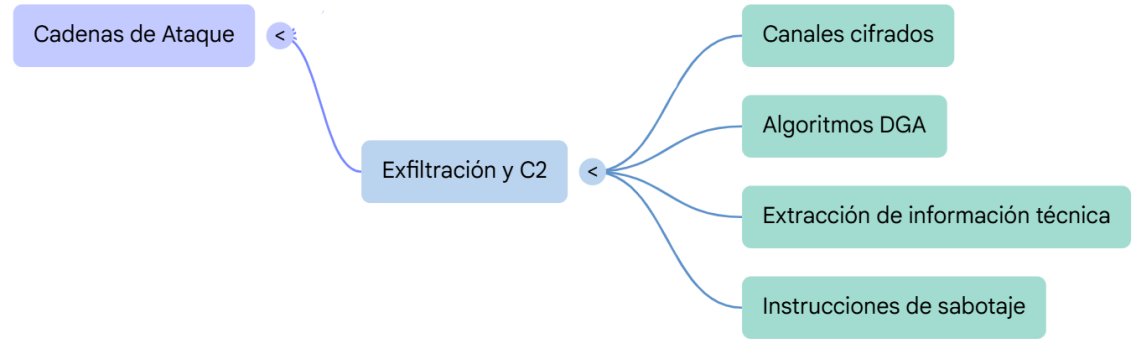
- **Despliegue de Balizas de Persistencia:** Instalación de puertas traseras (backdoors) mediante la técnica de "Fake Updates" (SocGholish), asegurando que el atacante mantenga el acceso incluso tras reinicios de sistema.



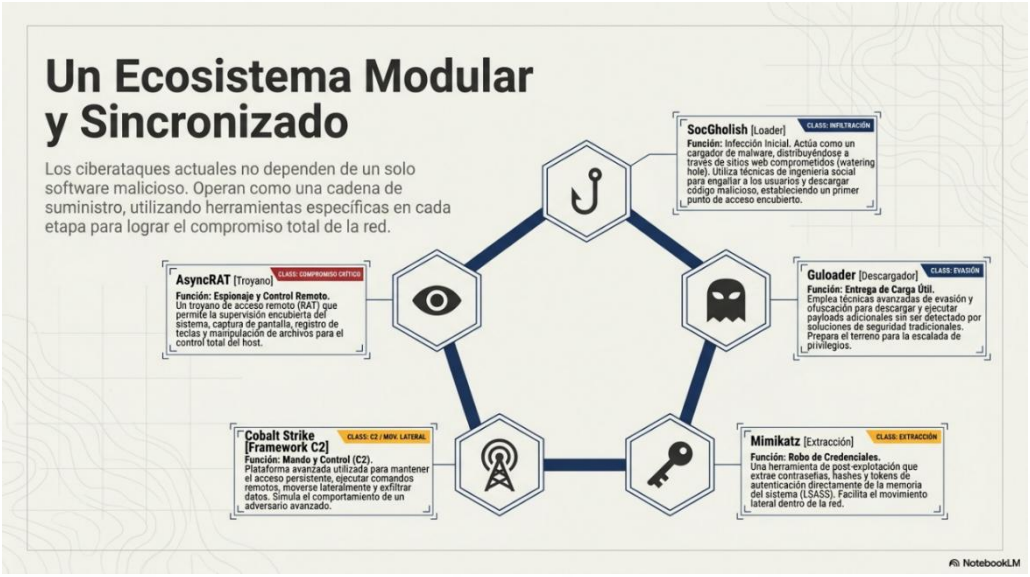
- **Movimiento Lateral y Escalada de Privilegios:** Una vez dentro de la red administrativa, los actores utilizan herramientas de post-explotación para obtener privilegios de administrador y mapear la topología hacia la red de control industrial (OT).



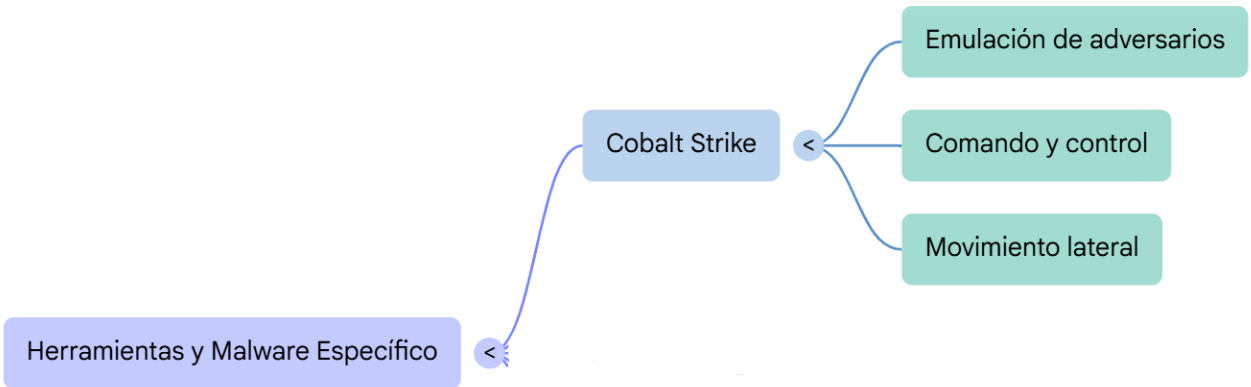
- **Exfiltración y Comando y Control (C2):** Establecimiento de canales de comunicación cifrados mediante algoritmos DGA para extraer información técnica sensible y recibir instrucciones de sabotaje en tiempo real.



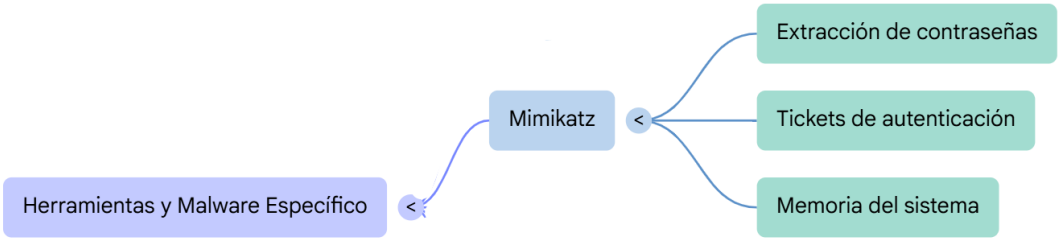
Herramientas y Malware Específico



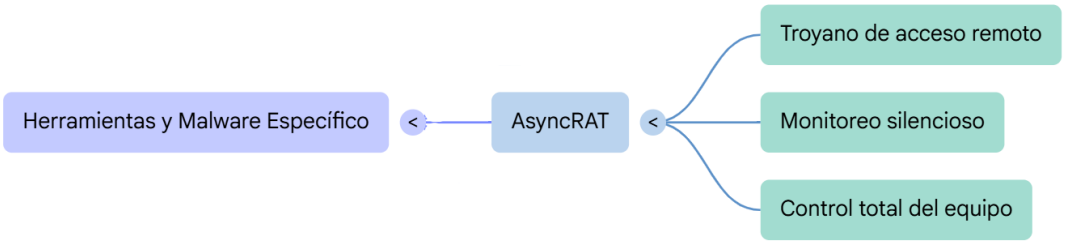
- **Cobalt Strike:** Framework de emulación de adversarios utilizado para el comando y control de sistemas comprometidos y el movimiento lateral dentro de la red.



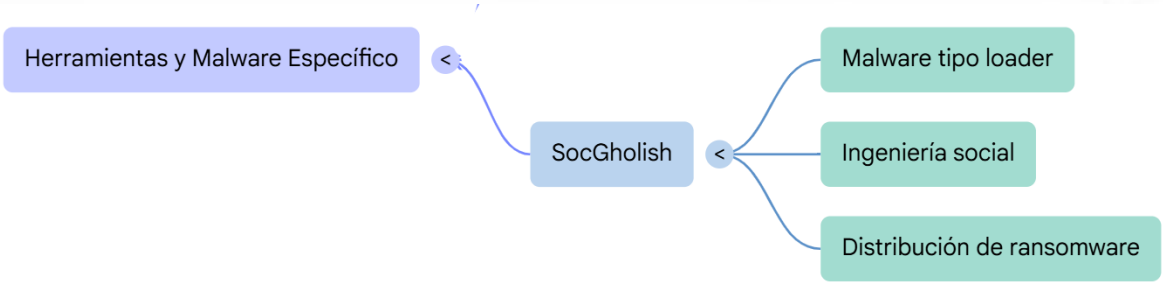
- **Mimikatz:** Herramienta crítica empleada para la extracción de contraseñas y tickets de autenticación almacenados en la memoria de los sistemas operativos.



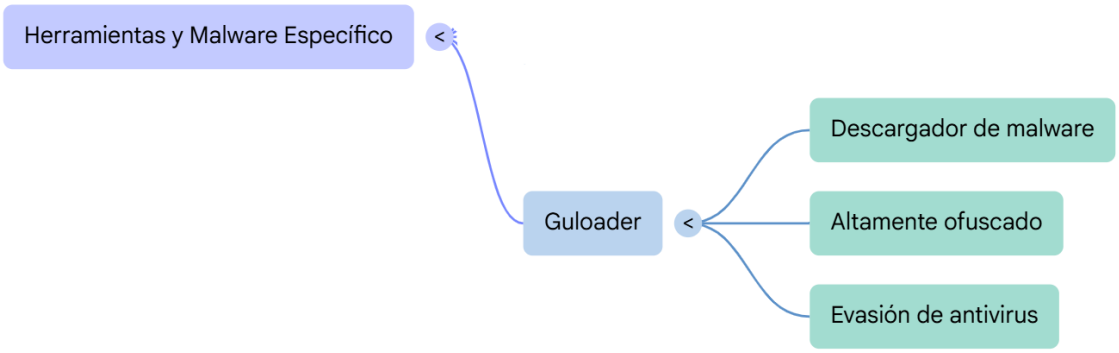
- **AsyncRAT:** Troyano de acceso remoto detectado en múltiples alertas, diseñado para el monitoreo silencioso y el control total del equipo de la víctima.



- **SocGholish:** Malware de tipo loader que utiliza ingeniería social para distribuir cargas útiles adicionales, sirviendo como el primer eslabón en ataques de ransomware.



- **Guloader:** Descargador de malware altamente ofuscado que facilita la entrada de amenazas más complejas sin ser detectado por soluciones antivirus tradicionales.

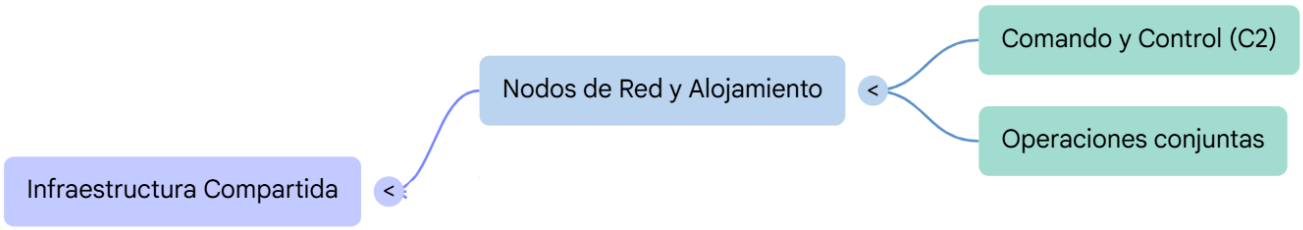


CORRELACIÓN ENTRE ACTORES Y GRUPOS

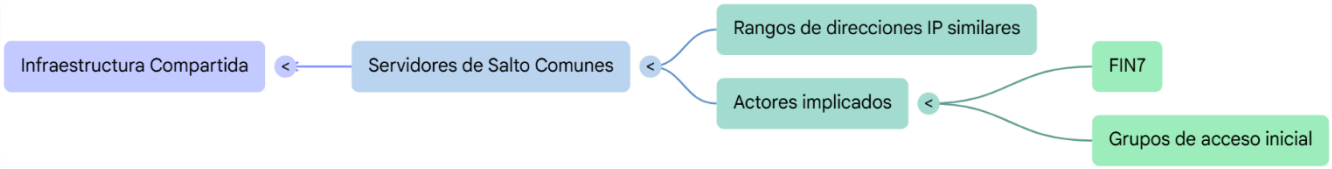
Esta sección analiza las interconexiones técnicas y operativas entre los diferentes grupos de amenazas identificados. La correlación permite entender cómo el ecosistema del cibercrimen no opera de forma aislada, sino mediante el uso de recursos compartidos y tácticas transversales que buscan maximizar la eficiencia del ataque contra el sector energético colombiano.

Infraestructura Compartida

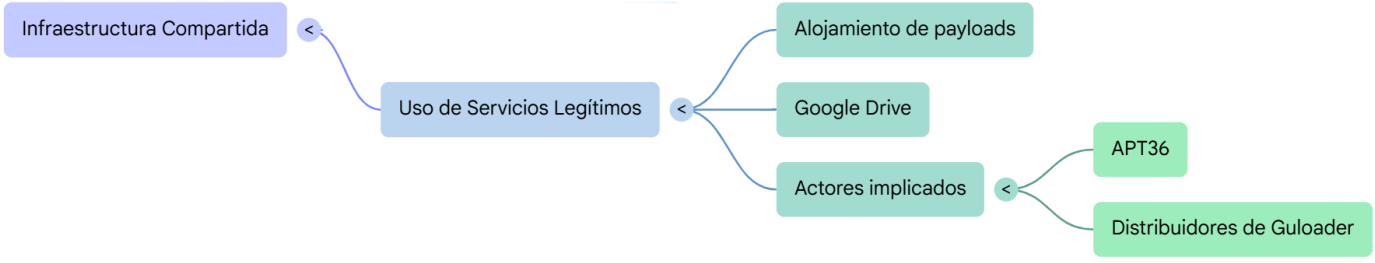
- Varios grupos utilizan los mismos nodos de red y servicios de alojamiento para sus operaciones de comando y control.

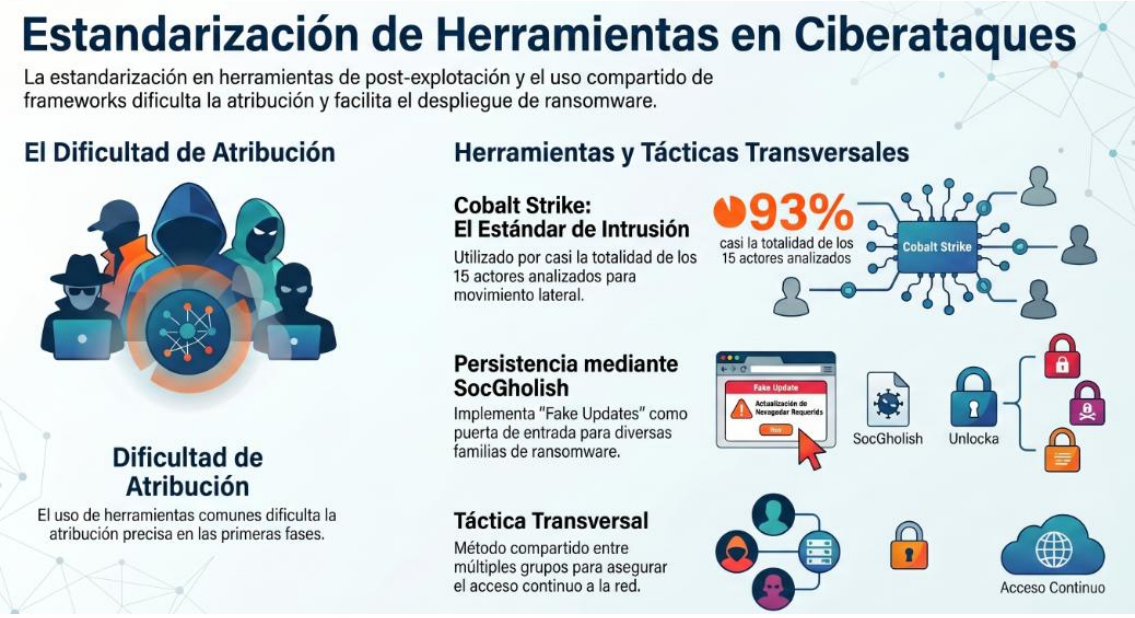


- **Servidores de Salto Comunes:** Se ha detectado que diferentes adversarios, como FIN7 y grupos de acceso inicial, utilizan rangos de direcciones IP similares para el despliegue de infraestructuras C2.

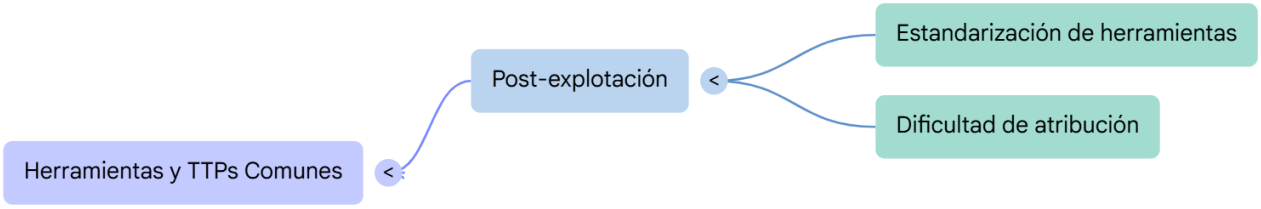


- **Uso de Servicios Legítimos:** El uso de plataformas como Google Drive para el alojamiento de payloads es una constante entre múltiples actores, incluyendo APT36 y distribuidores de Guloader.

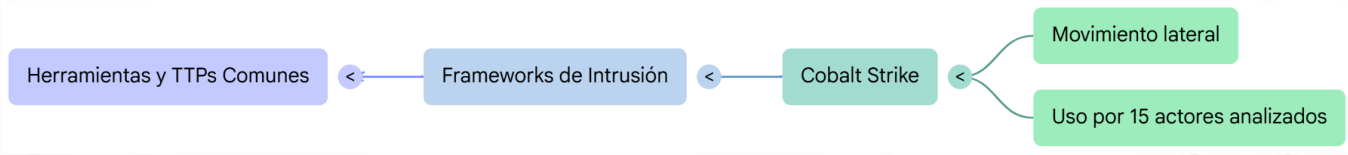




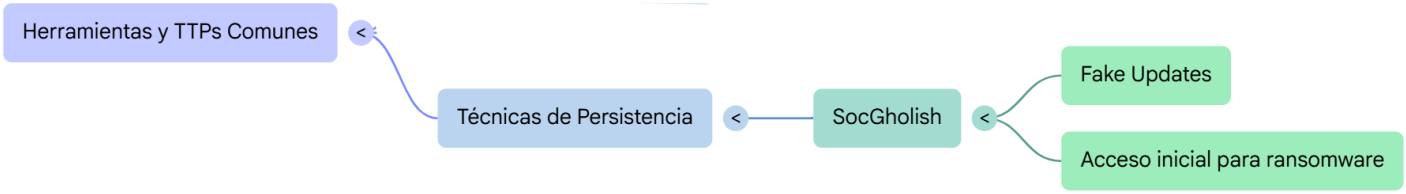
- Existe una estandarización en el uso de herramientas de post-explotación que dificulta la atribución precisa en las primeras fases del ataque.



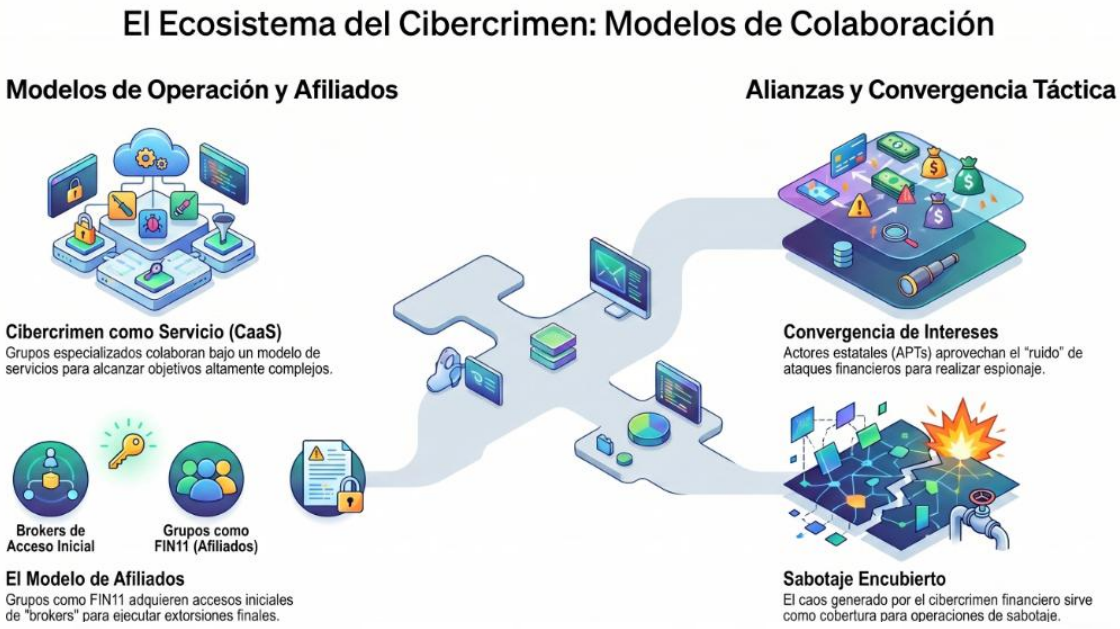
- **Frameworks de Intrusión:** El uso de Cobalt Strike es un estándar compartido por casi la totalidad de los 15 actores analizados para el movimiento lateral.



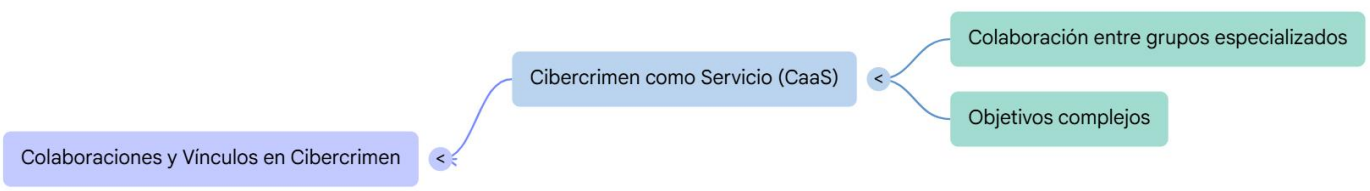
- **Técnicas de Persistencia: La** implementación de Fake Updates mediante SocGholish es una táctica transversal utilizada para abrir la puerta a diversas familias de ransomware.



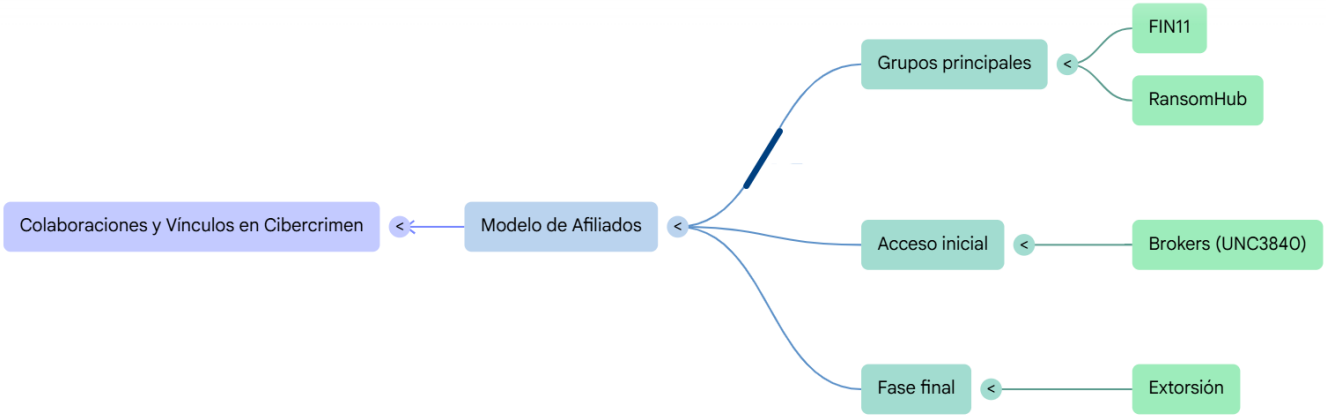
Posibles Colaboraciones o Vínculos



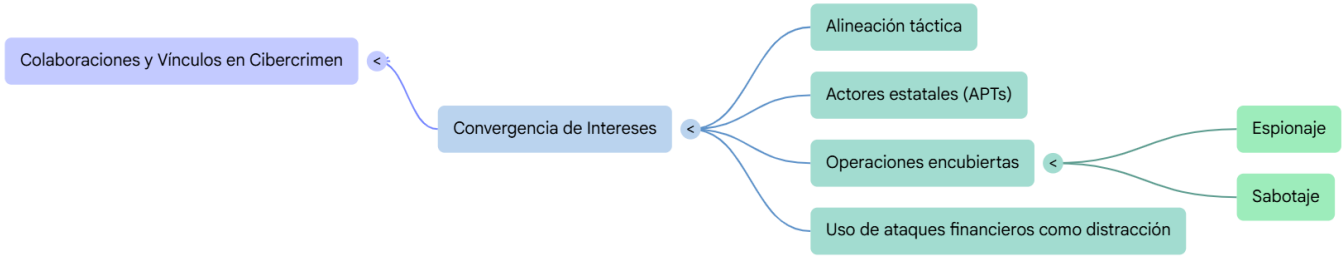
- La evidencia sugiere un modelo de "Cibercrimen como Servicio" (CaaS) donde grupos especializados colaboran para alcanzar objetivos complejos.



- Modelo de Afiliados: Grupos como FIN11 y RansomHub suelen adquirir accesos iniciales de "brokers" (como los identificados en las campañas de UNC3840) para ejecutar la fase final de extorsión.



- Convergencia de Intereses: Se observa una alineación táctica donde actores estatales (APTs) pueden aprovechar el "ruido" generado por ataques financieros para ejecutar operaciones de espionaje o sabotaje de forma encubierta.

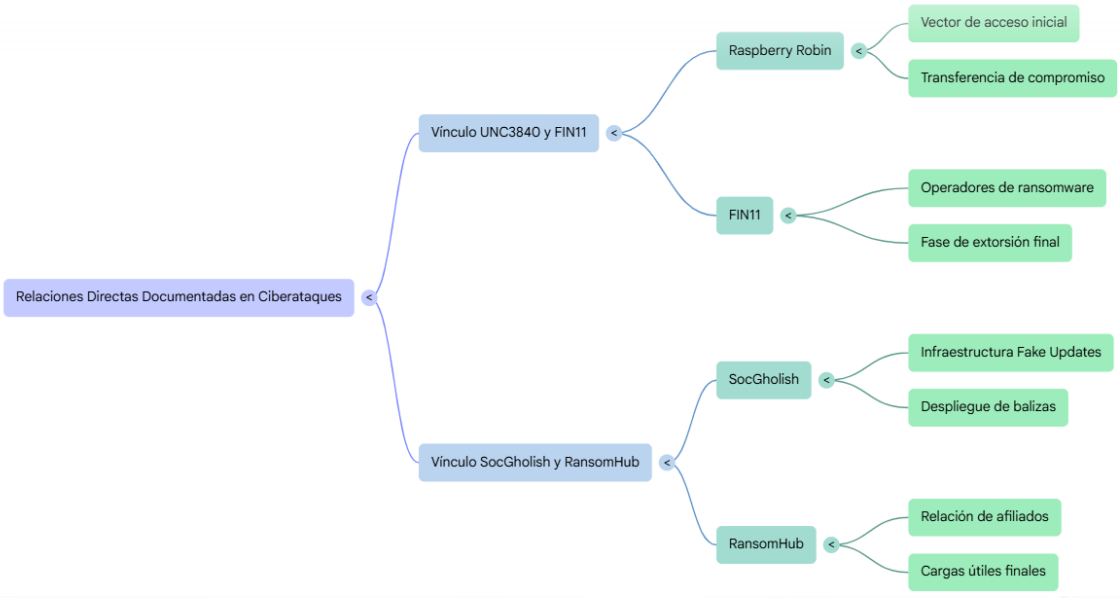


Visualización de Relaciones

Esta sección permite visualizar cómo los 15 adversarios identificados no operan en un vacío, sino que forman una red interconectada de capacidades técnicas y recursos digitales. Al mapear estas relaciones, el equipo de seguridad puede anticipar que la detección de un indicador asociado a un "nodo" específico (como un acceso inicial) es, con alta probabilidad, el preludio de una intrusión por parte de un actor de mayor impacto (como un grupo de ransomware o sabotaje).

Relaciones directas documentadas:

Existen vínculos confirmados donde un actor entrega explícitamente el control de una brecha a otro grupo para completar la operación.

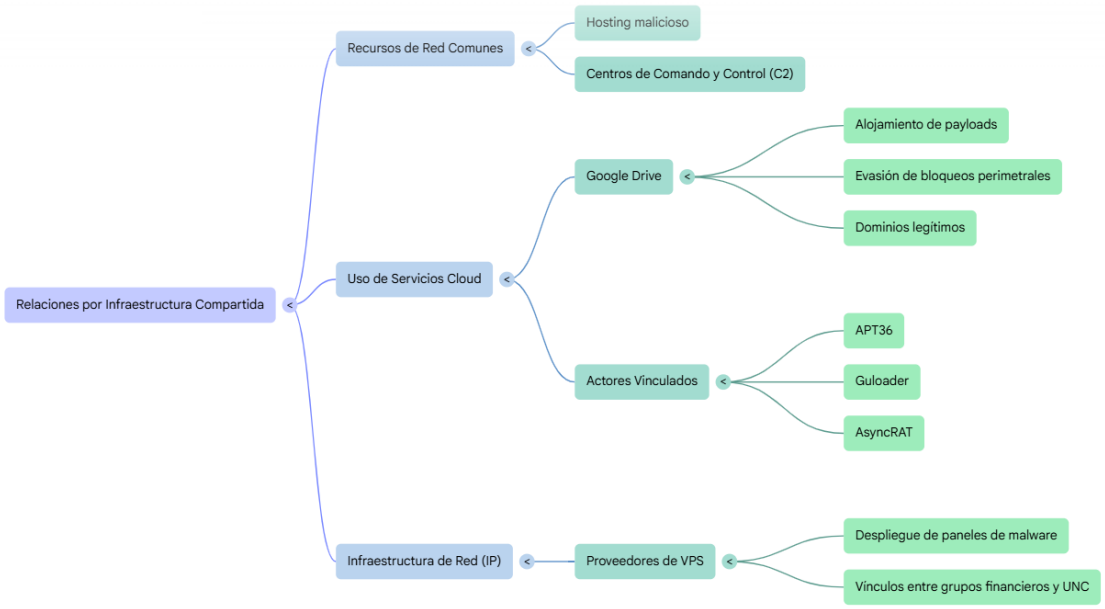


- **Vínculo UNC3840 (Raspberry Robin) y FIN11**: Se ha documentado que el malware Raspberry Robin actúa como un vector de acceso inicial que suele "vender" o transferir el compromiso a operadores de ransomware como FIN11 para la fase de extorsión final.

- **Vínculo SocGholish y RansomHub:** La infraestructura de Fake Updates de SocGholish se utiliza frecuentemente para desplegar balizas que culminan en el despliegue de cargas útiles de RansomHub, consolidando una relación directa de "afiliados".

Relaciones por infraestructura compartida

Diferentes actores utilizan los mismos recursos de red, lo que sugiere el uso de proveedores comunes de servicios de hosting malicioso o centros de comando y control (C2) compartidos.

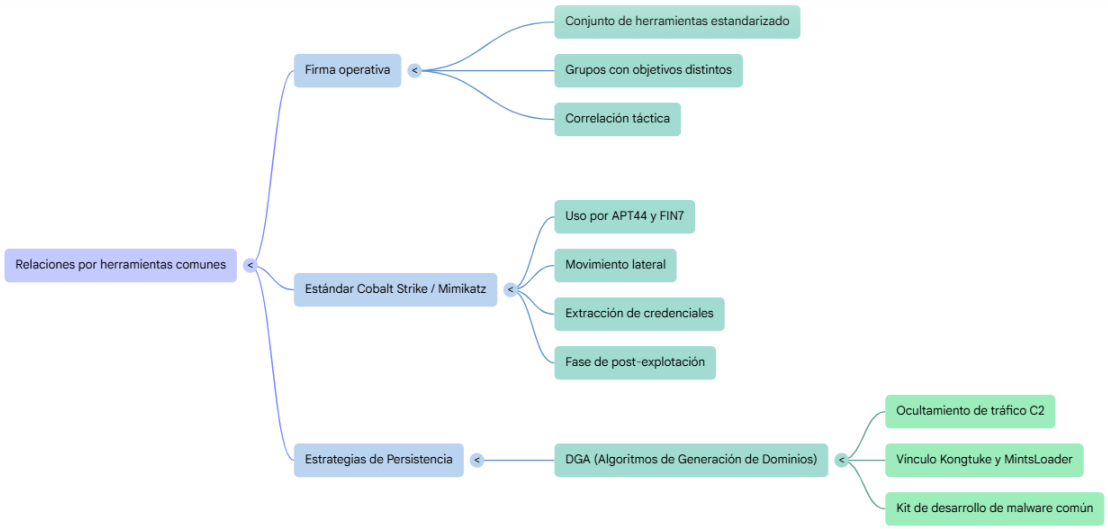


- **Uso de Servicios Cloud (Google Drive):** Actores como APT36, Guloader y AsyncRAT comparten el uso de URLs de drive.google.com/uc para el alojamiento de sus payloads, buscando evadir bloqueos perimetrales mediante el uso de dominios legítimos.
    - **Coincidencia en Rangos de IP:** Se observa una correlación en el uso de proveedores de VPS específicos para el despliegue de paneles de

administración de malware, vinculando tácticas de grupos financieros con actores no clasificados (UNC).

Relaciones por herramientas comunes

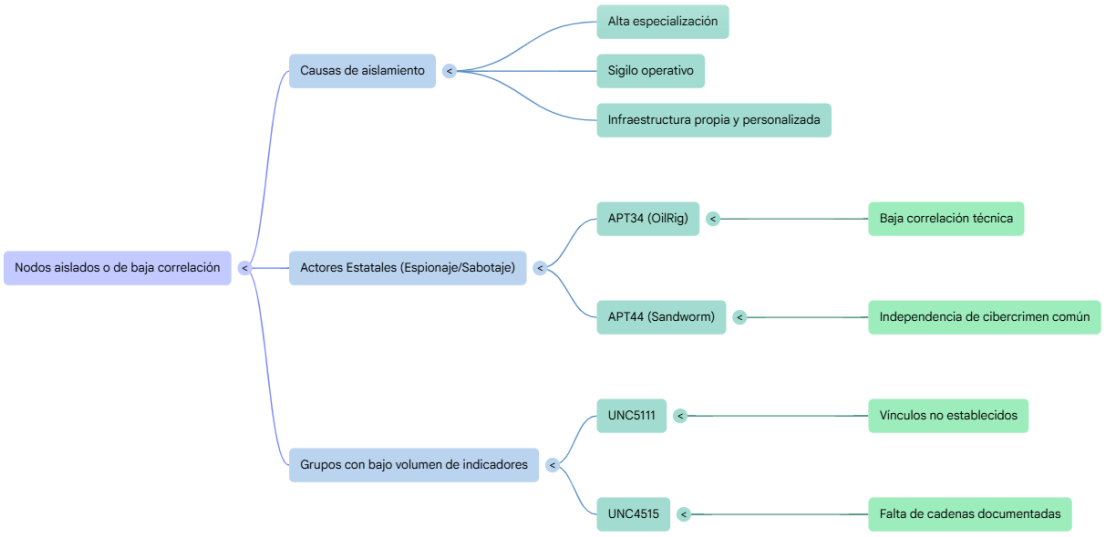
El uso de un conjunto de herramientas estandarizado genera una "firma operativa" similar entre grupos con objetivos distintos.



- **El Estándar Cobalt Strike / Mimikatz:** Prácticamente todos los grupos detectados, desde APT44 hasta FIN7, utilizan estas herramientas para el movimiento lateral y la extracción de credenciales, lo que crea una correlación táctica en la fase de post-explotación.

- **Estrategias de Persistencia:** El uso de DGA (Algoritmos de Generación de Dominios) para ocultar el tráfico C2 vincula las campañas de Kongtuke y MintsLoader, sugiriendo el uso de un mismo kit de desarrollo de malware.

Nodos aislados o con baja correlación (por ahora):

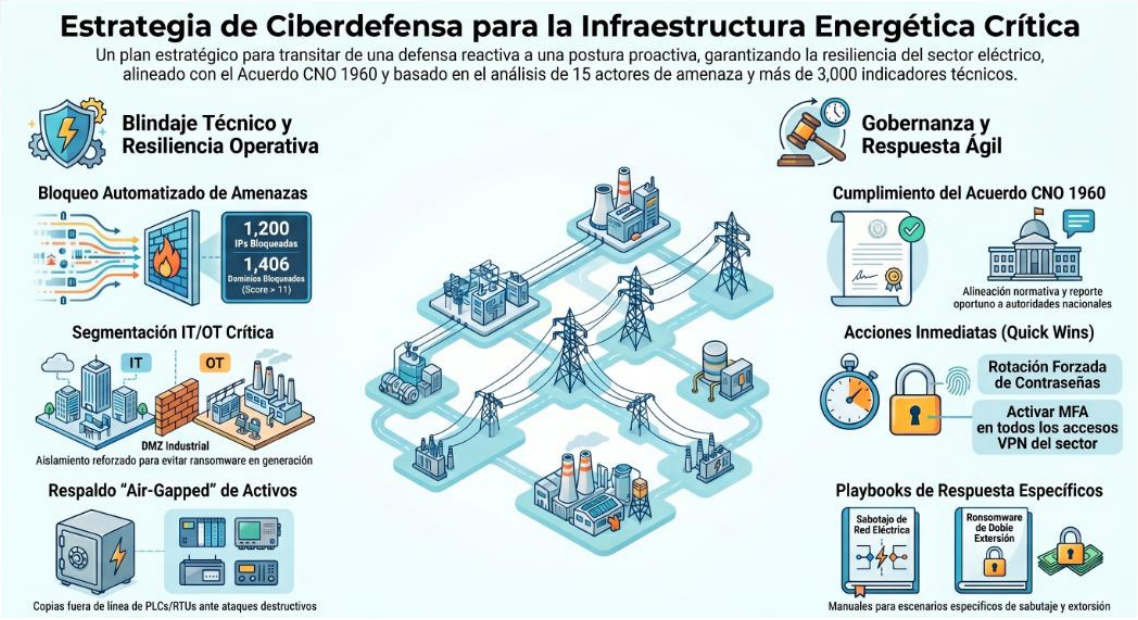


Existen actores que, debido a su alta especialización o sigilo, muestran pocos vínculos con el resto del ecosistema detectado.

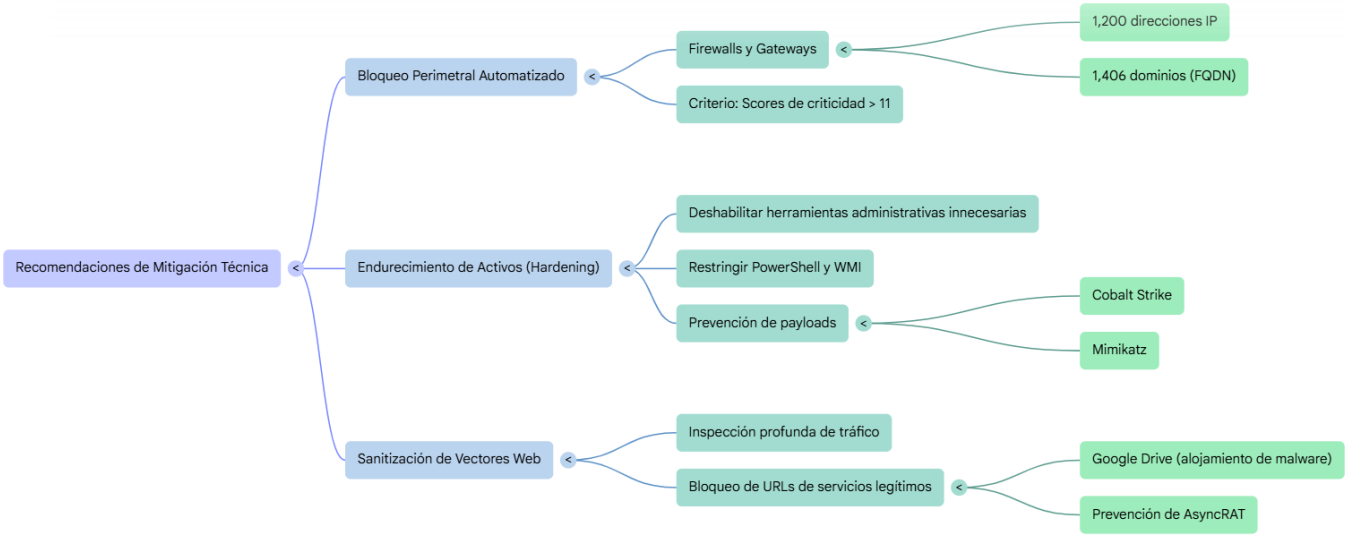
- **APT34 (OilRig) y APT44 (Sandworm):** Al ser actores estatales con objetivos de espionaje y sabotaje altamente específicos, suelen utilizar infraestructura propia y personalizada (custom-made), lo que los mantiene como nodos independientes con baja correlación técnica respecto a los grupos de cibercrimen común.
- **UNC5111 y UNC4515**: Estos grupos presentan un volumen bajo de indicadores en el periodo analizado, lo que impide por el momento establecer vínculos sólidos con otras cadenas de ataque documentadas.

RECOMENDACIONES ESTRATÉGICAS

Las recomendaciones presentadas a continuación surgen del análisis detallado de los 15 actores de amenaza y los más de 3,000 indicadores técnicos recolectados. Este plan estratégico busca transitar de una defensa reactiva a una postura proactiva, alineada con el cumplimiento del Acuerdo CNO 1960 y la protección de la infraestructura crítica energética nacional.

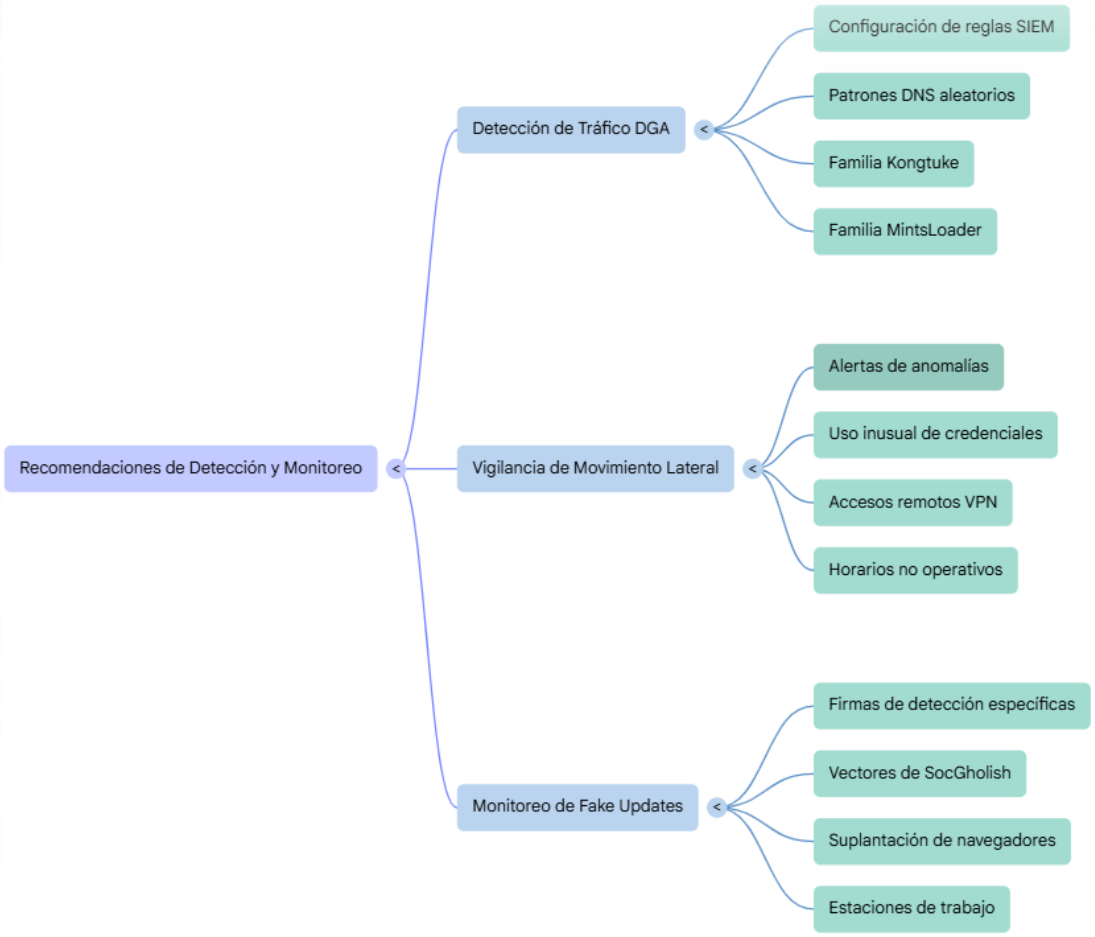


Recomendaciones de Mitigación Técnica



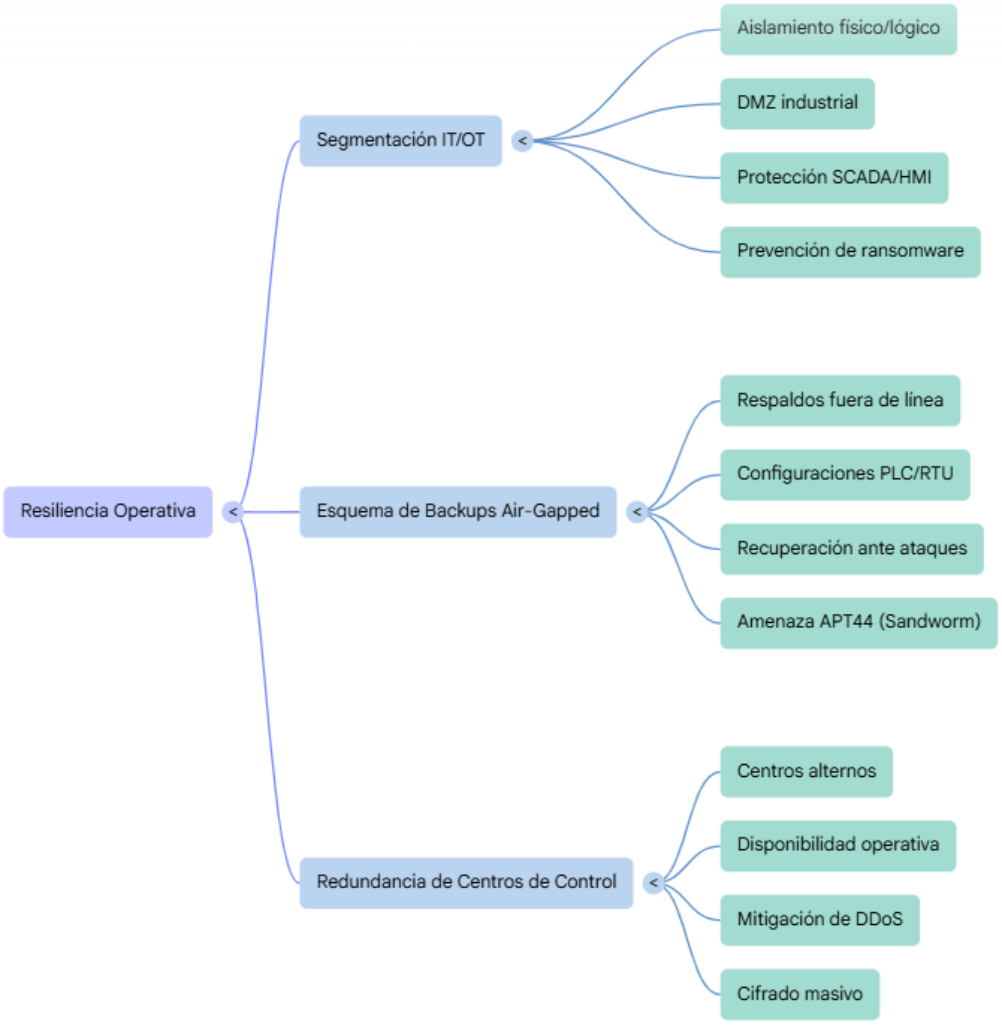
- **Bloqueo Perimetral Automatizado:** Ejecutar el bloqueo inmediato en firewalls y gateways de las 1,200 direcciones IP y 1,406 dominios (FQDN) identificados.
- **Endurecimiento de Activos (Hardening):** Deshabilitar herramientas administrativas innecesarias y restringir el uso de PowerShell y WMI para prevenir la ejecución de payloads de Cobalt Strike y Mimikatz.
- **Sanitización de Vectores Web:** Implementar inspección profunda de tráfico para bloquear el acceso a URLs de servicios legítimos (como Google Drive) que estén siendo utilizadas para el alojamiento de malware como AsyncRAT.

Recomendaciones de Detección y Monitoreo



- **Detección de Tráfico DGA:** Configurar reglas en el SIEM para identificar patrones de consulta DNS aleatorios asociados a las familias Kongtuke y MintsLoader.
- **Vigilancia de Movimiento Lateral:** Implementar alertas de detección de anomalías ante el uso inusual de credenciales administrativas y accesos remotos (VPN) fuera de horarios operativos.
- **Monitoreo de "Fake Updates":** Establecer firmas de detección específicas para los vectores de SocGholish que intentan suplantar actualizaciones de navegadores en estaciones de trabajo.

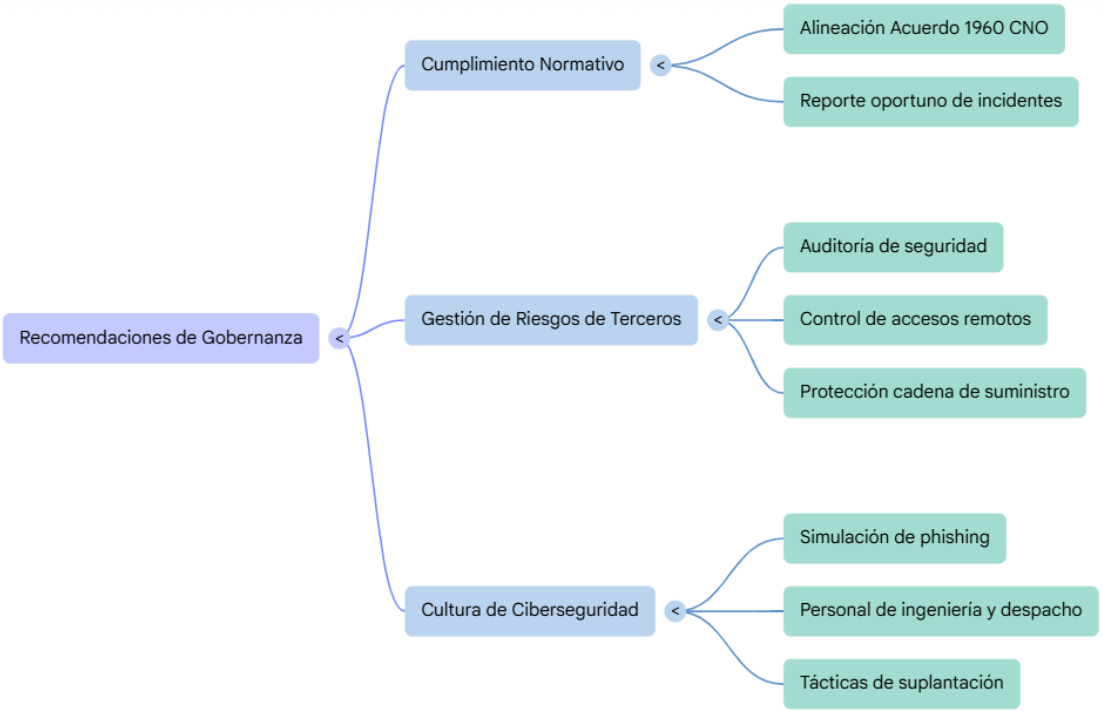
- **Segmentación IT/OT:** Reforzar el aislamiento físico o lógico (DMZ industrial) entre las redes corporativas y los sistemas de control (SCADA/HMI) para evitar que un ransomware en la capa administrativa afecte la generación.



- **Esquema de Backups "Air-Gapped":** Garantizar que los respaldos de configuraciones de PLCs y RTUs se mantengan fuera de línea para asegurar la recuperación ante ataques destructivos de actores como APT44 (Sandworm).

- **Redundancia de Centros de Control:** Validar la capacidad de operación desde centros alternos ante eventos de indisponibilidad por ataques de denegación de servicio (DDoS) o cifrado masivo.

Recomendaciones de Gobernanza



- **Cumplimiento Normativo:** Asegurar la alineación total con los lineamientos de ciberseguridad del CNO (Acuerdo 1960) y el reporte oportuno de incidentes a las autoridades nacionales.

- **Gestión de Riesgos de Terceros:** Auditar los niveles de seguridad y los accesos remotos de contratistas, dado que actores como UNC3840 utilizan la cadena de suministro como vector inicial.

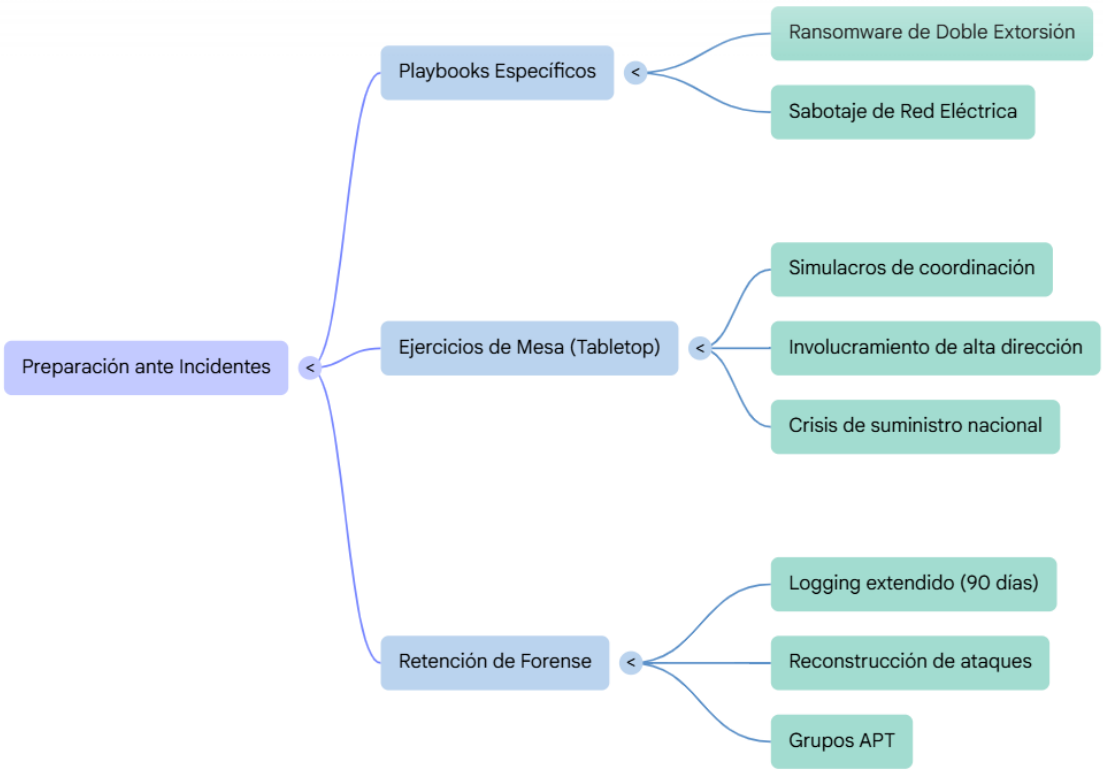
- **Cultura de Ciberseguridad:** Implementar programas de simulación de phishing específicos para personal de ingeniería y despacho, enfocados en las tácticas de suplantación detectadas en este informe.

Preparación ante Incidentes

- **Playbooks Específicos:** Desarrollar manuales de respuesta detallados para escenarios de Ransomware de Doble Extorsión y Sabotaje de Red Eléctrica.

- **Ejercicios de Mesa (Tabletop):** Realizar simulacros que involucren tanto al equipo técnico como a la alta dirección para coordinar la comunicación ante una crisis nacional de suministro.

- **Retención de Forense:** Configurar políticas de logging extendido (mínimo 90 días) para permitir la reconstrucción de ataques persistentes llevados a cabo por grupos APT.

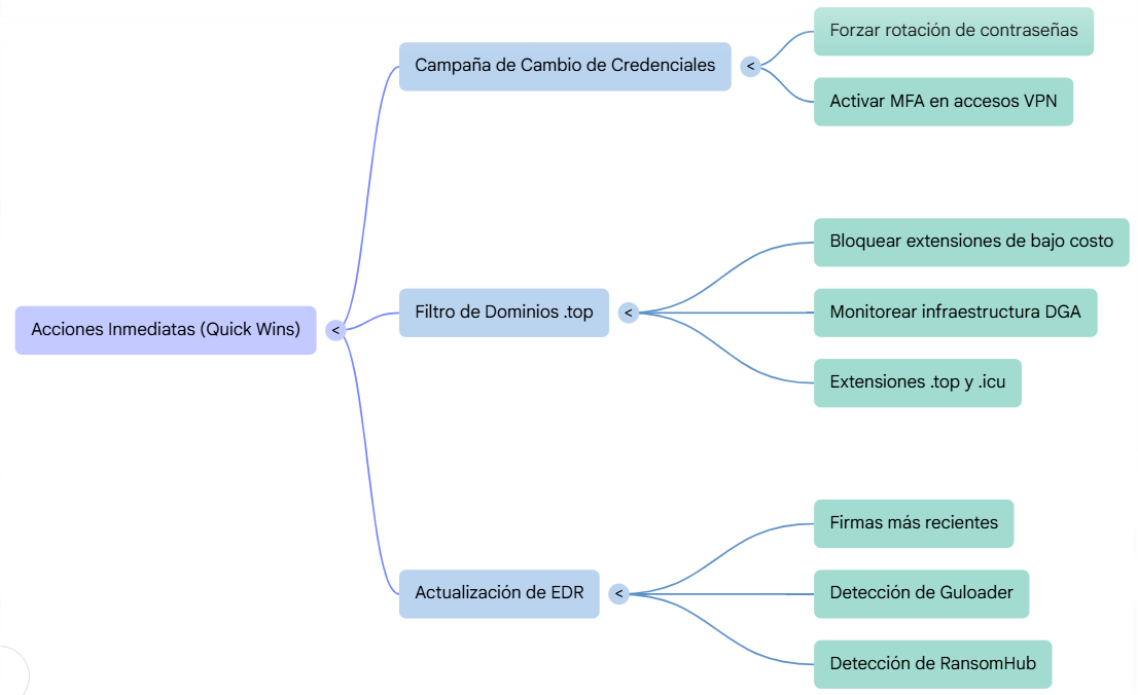


Acciones Inmediatas (Quick Wins)

- **Campaña de Cambio de Credenciales:** Forzar la rotación de contraseñas y activar el Doble Factor de Autenticación (MFA) en todos los accesos VPN del sector.

- **Filtro de Dominios .top:** Bloquear o monitorear preventivamente dominios con extensiones de bajo costo (como .top y .icu) que concentran gran parte de la infraestructura DGA.

- **Actualización de EDR:** Asegurar que todos los endpoints tengan las firmas más recientes para la detección de Guloader y variantes de RansomHub.



CONCLUSIONES

1. **Elevada Exposición de Infraestructura Crítica**: El análisis confirma que el sector energético colombiano es un objetivo prioritario y activo para 15 grupos de amenazas, destacando actores estatales como APT44 (Sandworm). Esta concentración de adversarios especializados en sabotaje indica que la infraestructura nacional no enfrenta ataques aleatorios, sino campañas dirigidas con el potencial de interrumpir el suministro eléctrico del país.

2. **Crecimiento Exponencial del Riesgo de Ransomware:** Con un registro de 35 millones de ataques de ransomware en Colombia al cierre de abril de 2026 y el precedente crítico de Air-e, la extorsión digital se consolida como la principal amenaza a la estabilidad financiera y operativa de las empresas prestadoras de servicios públicos.

3. **Magnitud de la Infraestructura de Ataque:** La detección de más de 12,000 IPs y 12,500 dominios maliciosos vinculados al sector evidencia un despliegue masivo de capacidades de Comando y Control (C2). Este volumen técnico sugiere que los atacantes mantienen una presencia latente y persistente, buscando evadir controles tradicionales mediante el uso de algoritmos dinámicos (DGA).

4. **Convergencia de Amenazas TI/TO:** Se observa una preocupante pérdida del aislamiento en las redes de control. El uso de herramientas como Cobalt Strike y Mimikatz demuestra que los atacantes están logrando saltar de la capa administrativa (IT) a los sistemas de operación (OT), poniendo en riesgo directo el control de subestaciones y plantas de generación.

5. **Evolución del Modelo de Agresión:** La correlación de datos muestra una colaboración entre "brokers" de acceso inicial (como SocGholish) y grupos de ransomware de alto impacto. Este modelo de "Cibercrimen como Servicio" permite que actores con motivaciones económicas faciliten la entrada a grupos de sabotaje, escalando rápidamente la severidad de cualquier intrusión inicial.

6. **Urgencia de Cumplimiento Regulatorio:** La seguridad del Sistema Interconectado Nacional (SIN) ya no es opcional, sino una obligación vinculada al Acuerdo CNO 1960. La adopción de una postura basada en Inteligencia de Amenazas (CTI) es la única vía efectiva para reducir los tiempos de detección y garantizar la resiliencia operativa que el Estado colombiano exige al sector.

GLOSARIO

Conceptos de Inteligencia y Amenazas

- **APT (Advanced Persistent Threat):** Grupos de atacantes, generalmente respaldados por Estados, que ejecutan campañas de ciberespionaje o sabotaje de manera prolongada y sofisticada.

- **Adversario (Adversary):** Individuo o grupo que realiza acciones maliciosas contra una organización o infraestructura.

- **IoC (Indicador de Compromiso):** Evidencia digital (como una IP, un dominio o un hash de archivo) que indica que un sistema ha sido vulnerado.

- **Score de Criticidad:** Valor numérico que determina la peligrosidad de un indicador basado en su historial y relación con ataques conocidos.

- **TTPs (Tácticas, Técnicas y Procedimientos):** Metodología de ataque que describe "cómo" opera un adversario de principio a fin.

- **MITRE ATT&CK:** Marco global que clasifica y describe el comportamiento de los atacantes basándose en observaciones del mundo real.

Infraestructura y Redes

- **IT (Information Technology):** Sistemas informáticos orientados a la gestión de datos, administración y procesos corporativos.
- **OT (Operational Technology):** Hardware y software que detecta o causa cambios mediante el monitoreo y control directo de dispositivos físicos (como generadores o subestaciones).
- **C2 (Command and Control):** Servidores externos utilizados por los atacantes para enviar instrucciones a los sistemas infectados.
- **FQDN (Fully Qualified Domain Name):** Nombre completo de un dominio en internet (ej. malicious-site.top) que apunta a una dirección IP específica.
- **DGA (Domain Generation Algorithm):** Técnica donde el malware genera miles de nombres de dominio aleatorios para ocultar su comunicación y evadir bloqueos.

Herramientas y Malware

- **Ransomware:** Tipo de malware que cifra la información de la víctima y exige un rescate económico para su liberación.
- **RAT (Remote Access Trojan):** Herramienta que permite al atacante controlar un equipo de forma remota y silenciosa.
- **Payload:** La carga útil o código malicioso final que ejecuta la acción dañina (robo de datos, cifrado, etc.).
- **Hash (SHA-1, SHA-256, MD5):** Huella digital única de un archivo que permite identificar malware sin importar si se le cambia el nombre.
- **Phishing:** Técnica de ingeniería social para engañar a los usuarios y robar sus credenciales de acceso.

Sector

- **SIN (Sistema Interconectado Nacional):** Red de líneas de transmisión, subestaciones y plantas que suministran energía a todo el territorio colombiano.
- **CNO (Consejo Nacional de Operación):** Organismo encargado de acordar los aspectos técnicos para garantizar la operación segura del SIN.
- **SCADA:** Sistema de control y adquisición de datos utilizado para monitorear procesos industriales a distancia.
- **Acuerdo CNO 1960:** Normativa que establece los requisitos mínimos de ciberseguridad que deben cumplir las empresas del sector eléctrico en Colombia.

COLCERT

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

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

Conéctate con el ColCERT

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

contacto@colcert.gov.co
Privados

icc@colcert.gov.co
Temas de ICC

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

@colCERT

Línea directa:
+57 601 344 2222