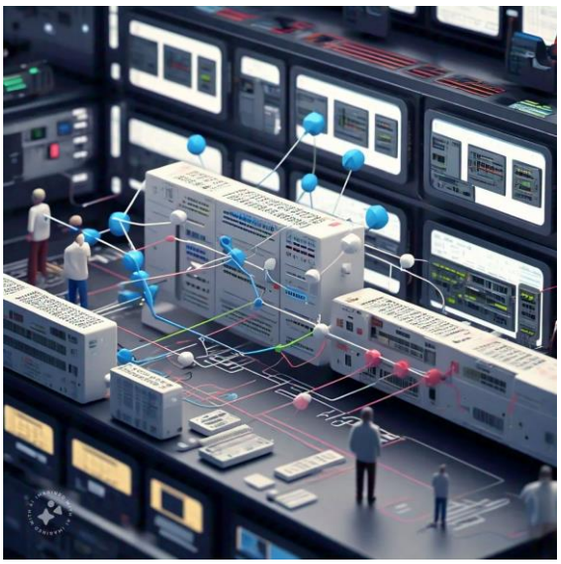
TIC

ALERTA

Guía Endurecimiento Equipo de Comunicación Telcos

COLCERT AL-0612-060



TLP:CLEAR

Las infraestructuras de comunicaciones se ven amenazadas por una campaña de ciberespionaje atribuida a actores afiliados a la República Popular China (RPC). Según los reportes emitidos por las agencias de ciberseguridad de Estados Unidos, Australia, Canadá y Nueva Zelanda, es altamente probable que las redes de telecomunicaciones de importantes proveedores globales se encuentren comprometidas.

ELEMENTOS DE INFORMACIÓN DISPONIBLES

Los principales vectores de ataque se centran en configuraciones de dispositivos de red inseguras, protocolos débiles o desactualizados, falta de segmentación de red y gestión inadecuada de accesos y autenticación. Esto representa un llamado de atención global sobre la fragilidad de las infraestructuras de comunicaciones; para Colombia, significa una oportunidad para fortalecer la ciberseguridad en un escenario de crecientes tensiones geopolíticas.

- **La campaña se centra en infiltrar y obtener información estratégica, exponiendo las vulnerabilidades críticas en infraestructuras de comunicaciones.**
- **Se evidencia un escenario tendiente a una guerra de quinta generación, donde los actores estatales buscan penetrar sistemas de comunicación críticos para obtener ventajas geopolíticas**

RECOMENDACIONES

El endurecimiento de dispositivos y la arquitectura de red es una estrategia de defensa en profundidad para limitar los posibles puntos de entrada. Las prácticas clave de endurecimiento incluyen:

- **Usar una red de administration fuera de Banda físicamente separada de la red operativa.**
- **Implementar una estrategia estricta de lista de control de acceso (ACL) de denegación por defecto.**
- **Emplear una fuerte segmentación de red utilizando VLAN, firewalls y DMZ.**
- **Asegurar el cifrado de extremo, al extremo del tráfico.**
- **Deshabilitar protocolos y servicios de descubrimiento innecesarios.**
- **Configurar TLS v1.3 y opciones criptográficas sólidas.**

NIVEL DE RIESGO

MEDIO

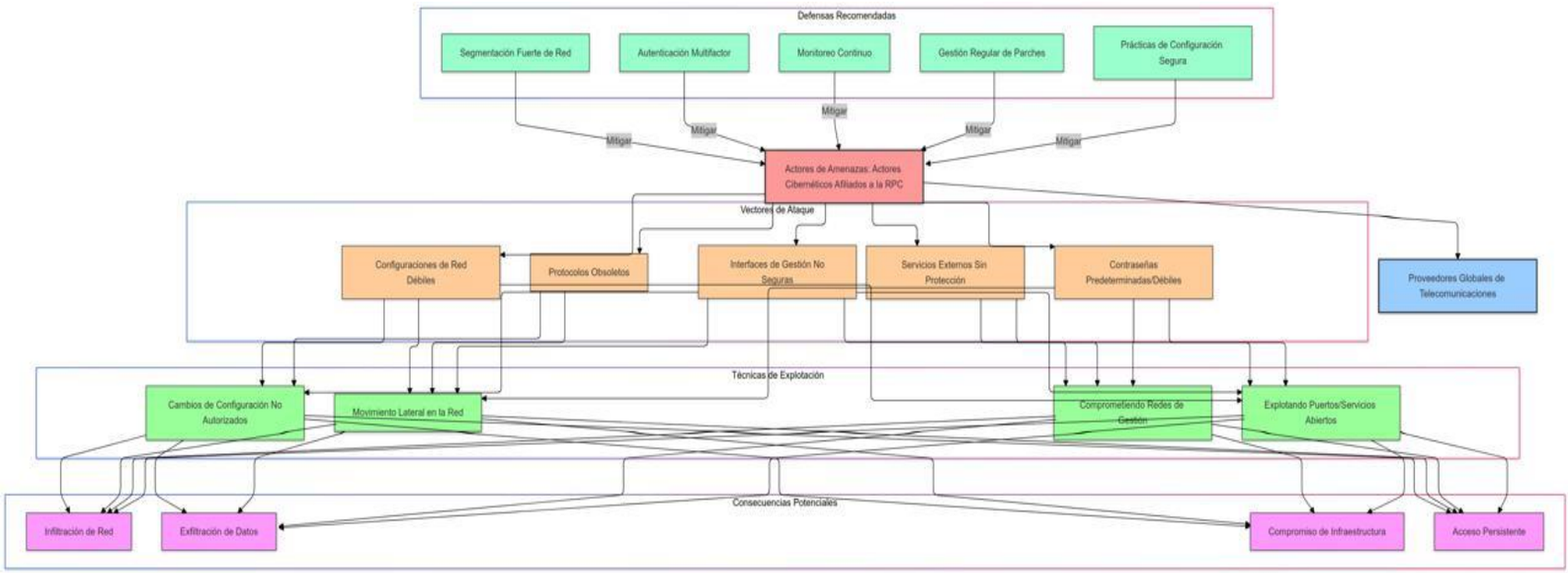
COLCERT

ANEXO

Guía Endurecimiento Equipo de Comunicación Telcos

COLCERT AL-0612-060

El siguiente gráfico resume los diferentes aspectos clave en la ciberseguridad de infraestructuras de comunicaciones, mostrando los vectores de ataque, recomendaciones, técnicas de explotación, impactos y consecuencias potenciales.



Fuente: ColCERT

IMPACTO PARA COLOMBIA Y LA REGIÓN

Las agencias de ciberseguridad consideran que las amenazas evidenciadas no son actividades novedosas, sino que aprovechan vulnerabilidades existentes y críticas en infraestructuras de comunicaciones, centrándose en configuraciones de dispositivos de red inseguras, protocolos débiles o desactualizados, falta de segmentación de red y gestión inadecuada de accesos y autenticación.

Para Colombia y Latinoamérica, esto implica una necesidad urgente de:

- **Modernización de la infraestructura tecnológica.**
- **Desarrollo de capacidades de defensa cibernética.**
- **Construcción de resiliencia digital.**
- **Cooperación internacional en ciberseguridad.**

En un escenario de crecientes tensiones geopolíticas, fortalecer la ciberseguridad es crucial para proteger la integridad y disponibilidad de las comunicaciones.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure

COLCERT