lacnic mentoreo

Programa de Mentoreo IT Women
2024-2025

Detección de ataques en un IXP

Resumen del trabajo técnico

En los últimos 8 años se han intensificado los ataques en Nicaragua. Es de vital importancia para los ISP (Proveedores de Servicio de Internet) tomar medidas para la protección. En este sentido, el trabajo técnico sugiere a los operadores de servicios activar NetFlow en sus equipos. Parte del trabajo se centró en el procesamiento de la información recopilada para identificar todos los tipos de ataques en el punto de intercambio de tráfico. Fueron observados anuncios de prefijos específicos /26, /27, /29 y /30. Adicionalmente, se encontraron bloques IP que aún no hacen uso de RPKI. Como conclusión, todos los miembros se beneficiarían al adoptar las medidas de seguridad de enrutamiento establecidas a nivel global.

Introducción: antecedentes, descripción y resultados

En Nicaragua se cuenta con 1 IXP (Punto de Intercambio de Internet). La función del IXP es brindar interconexión de redes con un mejor rendimiento en latencia y *jitter*. Se encuentra conformado por 10 ISPs, cada uno de ellos conectado con fibra óptica monomodo en interfaces de 10 Gigabit ethernet, convergiendo en un switch.

El equipo cuenta con redundancia de energía, la debida climatización y acceso de alta seguridad, dado que se encuentra resguardado en un centro de datos de uno de los ISPs desde finales del 2024. Cada miembro tiene acuerdos bilaterales, genera una sesión BGP para cada necesidad.

Los miembros del IXP de Nicaragua son: CLARO, TIGO, TECOMUNICA, ALFANUMERIC, IBW, XINWEI (ITEL), YOTA, CASAVISION, UFINET, TELEFONICA. De acuerdo a los datos recabados en este trabajo, ENATREL aún no cuenta con conexión directa, pero utiliza a XINWEI como intermediario.

Wireshark · Información especializada · Wi-Fi

Gravedad	Informe	Grupo	Protocolo	Recuento
Chat	Connection establish request (SYN)	Sequence	TCP	
42	4480 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
149	4495 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
298	4507 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
372	4516 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
740	4556 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
771	4561 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
962	4577 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
1016	4594 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
1018	4595 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
1043	4596 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
1061	4597 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
1066	4598 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
1070	4599 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W...	Sequence	TCP	
1124	4600 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	
1173	4605 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 ...	Sequence	TCP	

Metodología

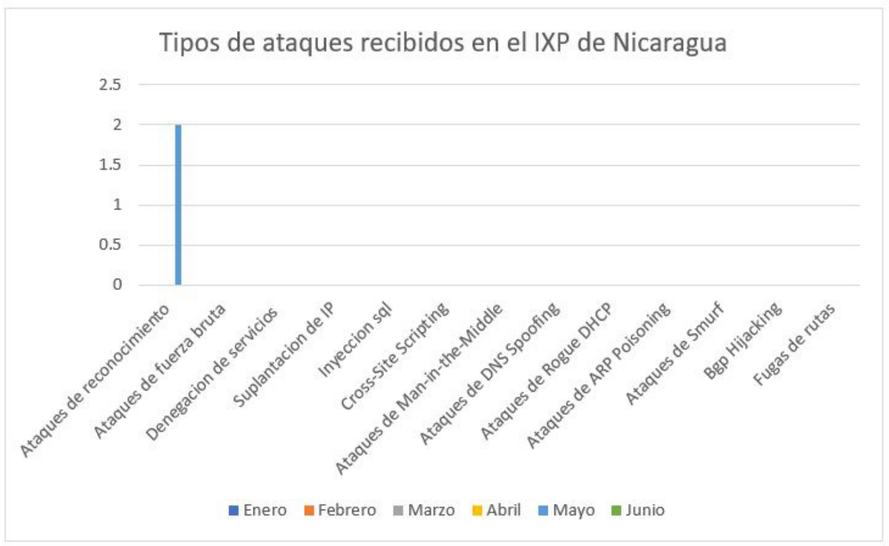
A modo de estructurar el análisis, se adoptaron dos marcos de referencias ampliamente reconocidos: MITRE ATT&CK y NIST SP 800-30, y se investigaron las herramientas gratuitas para la detección de ataques.

Una vez extraída la información durante el periodo establecido, se identificaron anomalías en algunos prefijos y se analizaron los flujos de tráfico recopilados del IXP.

Cifras, datos y resultados principales

A partir de la información extraída, fueron identificados prefijos del segmento 165.98.1.0-165.98.250.0. Dichos prefijos del segmento podrían ser interpretados como *Hijacking*. Esto se debe a su anuncio por varios proveedores locales, de los cuales algunos no cuentan con un ASN (Número de Sistema Autónomo) propio.

Se aplicaron varios filtros en las herramientas Suricata y Wireshark con el objetivo de sensar el tráfico del IXP. Sin embargo, solamente se logró identificar ataques de reconocimiento dentro de su clasificación (escaneo de puertos).



Relevancia del trabajo técnico

La detección de ataques en un Punto de Intercambio de Internet (IXP) reviste una importancia técnica crítica. Esto se debe a que estas infraestructuras concentran un volumen masivo de tráfico entre múltiples redes autónomas, lo cual las convierte en blancos atractivos para actividades maliciosas como ataques de denegación de servicio distribuido (DDoS), suplantación de direcciones IP (*spoofing*) o intentos de interceptación de datos.

Implementar mecanismos de monitoreo avanzado como el análisis del comportamiento del tráfico BGP y el uso de sensores de detección de anomalías en tiempo real, resultan esenciales para identificar y mitigar rápidamente incidentes que podrían comprometer la estabilidad y seguridad de las redes.

Además, la colaboración entre los miembros del IXP para compartir inteligencia sobre amenazas, junto al despliegue de tecnologías como NetFlow o sFlow contribuyen a fortalecer la resiliencia operativa, asegurando un intercambio eficiente y confiable para todos los participantes.

Este análisis puede proveer una base para futuras regulaciones o políticas operativas.

Conclusiones, retos y oportunidades

Algunos clientes de los proveedores miembros del IXP de Nicaragua cuentan con su propio prefijo /24. Al no contar con un ASN propio, al momento de enviar sus prefijos utilizan 1 o 2 proveedores, generando la impresión de que se confirme un *Hijacking*. Por otro lado, el presente trabajo también detectó una carencia en el uso de RPKI por parte de usuarios de los sectores privado o gubernamental que se encuentran utilizando un prefijo /24 de los ISPs miembros.

En base a esto, se recomiendan los siguientes aspectos:

- Mantener el monitoreo continuo mediante equipos con sistemas de detección de intrusos o de prevención (IDS/IPS).
- Bloquear el tráfico no autorizado mediante *firewalls* o listas de acceso en los routers. Cambiar puertos predeterminados en aplicaciones o servicios.
- Aplicar políticas de sanción temporal en servidores que brindan servicios críticos después de determinada cantidad de intentos de autenticación o conexión erróneos. Por ejemplo herramientas como: fail2ban o Nginx.
- Promover el uso de RPKI y la adquisición de un ASN público en los clientes que tienen bloques /24.

Referencias

KENTIK (2025). *BGP ROUTE VIEWS*. Disponible en: https://portal.kentik.com/v4/core/quick-views/tcp-traffic
[Consultado: 3 de junio de 2025]

Bitag (2022, 11 de febrero). *Seguridad de enrutamiento*. Bitag.org. Disponible en: https://www.bitag.org/documents/BITAG_Routing_Security.pdf
[Consultado: 3 de junio de 2025]

Attack.mitre (2025). *Matriz de ataques*. Attack.mitre.org. Disponible en: https://attack.mitre.org
[Consultado: 3 de mayo de 2025]

Manrs.org (2025). *Seguridad IXP*. Disponible en: https://manrs.org/netops/actions
[Consultado: 28 de mayo de 2025]

Autora

Ing. Erika Garay

Mentora

Lic. Marcela Orbiscay

Contactos

erika.garay@ibw.com.ni

morbiscay@gmail.com

Perfil Profesional

Ing. en sistemas y tecnologías de la información con mención en redes y comunicaciones.

Desde hace 9 años ha estado involucrada en el ecosistema de los ISPs. Ha llevado adelante cursos de ciberseguridad, redes y fibra óptica.

Adicionalmente, ha trabajado en soporte técnico, Ingeniera de red y actualmente se desempeña como Ing. Core IP en un ISP de Centroamérica.

Agradecimientos

Agradezco profundamente a LACNIC durante este periodo por el acompañamiento brindado en el **Programa de Mentoreo de IT Women (LACNIC)**.

Estoy enormemente agradecida con mi mentora por su orientación y conocimientos para el desarrollo de este trabajo técnico.

Citación de esta publicación

E. Garay. “Detección de ataques en un IXP” [Presentación de póster]. Presentado en: LACNIC 44-LACNOG 2025, 6-10 de octubre de 2025, San Salvador, El Salvador.