Análisis de impacto LACNIC 31

Mayo, 2019

Gianina Pensky, LACNIC

31 lacnic
06/10 DE MAYO 2019
REPÚBLICA DOMINICANA

id indotel
Instituto Dominicano de las Telecomunicaciones

lacnic

Los secuestros BGP constituyen una violación de las políticas (1)

(Versión anterior)

Aplicación: ante un reporte sobre un secuestro de rutas.

Modificación del texto actual: nueva sección en el manual.

Comentarios

- ¿Qué sucede con los secuestradores que no son miembros?
- Es muy difícil adjudicar intencionalidad de un anuncio no autorizado, por lo cual estos temas se gestionan en CSIRTs especializados en buenas prácticas.
- El WARP (Warning Advice and Reporting Point) recibe este tipo de reportes (anuncios no autorizados)
  - 2019: 3 reportes resueltos.
  - 2018: 6 reportes resueltos.
  - 2017: 11 reportes resueltos y 1 dejó de anunciar.

Los secuestros BGP constituyen una violación de las políticas (2)

Impacto legal

- No existen pruebas absolutas para determinar un secuestro de rutas, sino indicios.
- Para iniciar un proceso de revocación, se debe contar con prueba fehaciente. Puede traer consecuencias muy graves para LACNIC, en caso de que se actué en base a indicios en lugar de certezas.
- Casos de falsos positivos, que al revocar recursos implicaría una mayor responsabilidad jurídica y financiera para el grupo de expertos y para LACNIC.

Los secuestros BGP constituyen una violación de las políticas (3)

Recomendaciones

- Se reconoce que el secuestro de rutas debe ser indicado como un incidente de seguridad.
- Sin embargo, la política entra en detalles del procedimiento que deberían ser manejados por un CSIRT.
- LACNIC gestiona este tipo de incidentes a través del WARP, basado en las buenas prácticas establecidas por CSIRTs.
- Ser cuidadosos en los aspectos que se definen como responsabilidad de un RIR como parte de su administración de los recursos numéricos y no del ruteo. Es importante tener claro donde se establecen las fronteras.

lacnic warp

Warning Advice and Reporting Point

Home > Reportar Incidente

Reportar Incidente

Ingrese su nombre

Ingrese el nombre de su organización

email del contacto

País

Teléfono de contacto

- ✓ ---
- DOS
- DDOS
- Email Abuse
- Fuerza Bruta
- Intrusion attempt
- MALWARE
- PHARMING
- PHISHING
- Otros
- Unauthorized Prefix Advertising
- REDIRECT

Contacto:
info-warp@lacnic.net

Los secuestros BGP constituyen una violación de las políticas (4)

- **En la sección 4.0 Líneas de acción:**
  - Un aspecto importante a destacar es que los Centros de Respuesta tienen como principio básico la reserva de la información en forma confidencial para la correcta gestión del incidente.
- **En la sección 6.0 Grupo de expertos:**
  - Ya existe una red de confianza de CSIRTs que trabajan de una forma establecida a nivel internacional. El WARP puede escalar estos incidentes a otros CSIRTs.
  - No queda claro como LACNIC podría evaluar la experiencia de los expertos mundiales en el tema.
- **En la sección 7. Procedimiento**
  - No permite a LACNIC tomar alguna acción en caso de que lo considere pertinente.

Los secuestros BGP constituyen una violación de las políticas (5)

- **En la sección 8.0 Posibles objeciones**
  - "(...) el secuestrador, dispondrá de un máximo de cuatro semanas para objetar (...)" contradice uno de los principios básicos de la gestión de incidentes *"The speed with which an organization can recognize, analyze, and respond to an incident will limit the damage and lower the cost of recovery*" Cert.org
  - "el informe se hará público" podría ser tomado como una acusación y podría abrir una posible demanda.
- **En la sección 11.0 Apelaciones**
  - Los tiempos propuestos no concuerdan con la gravedad de este tipo de incidentes.
  - La demora significa un gran impacto en la estabilidad y la seguridad de Internet.