

Cíber Seguridad y Cooperación Regional



Carlos Álvarez
Sr. Manager, Security Engagement
carlos.alvarez@icann.org
@isitreallysafe
Septiembre de 2015

– Actores y papeles

- Reportes de abuso
- El papel de cada cual
- CERTs / WARP / Agencias de Policía
- Comunidades de confianza

– Reflexión, amplificación, DDoS

- BCP 38
- BCP 140

– Conclusiones

¿Quiénes son los actores relevantes en el mundo de la ciber seguridad? ¿Cuál es su papel?

- Usuarios finales (individuales, corporativos, educacionales, gobiernos)
- ISPs
- Desarrolladores de software/hardware
- Registradores/registros de dominios
- Comunidad de seguridad (sector privado)
- Agencias de policía

Usuarios finales (individuales, corporativos, educacionales, gobiernos): reportar casos de potencial abuso

- Reportar a quién?
 - Botón de 'esto es phishing en su correo'
 - Registrador de dominios, proveedor de hosting, empresas de anti-malware
 - ICANN
 - ic3.gov, agencias de policía

Actores y papeles

- ISPs: pueden hacer uso de listas negras para proteger a sus usuarios bloqueando conexiones a dominios y direcciones IP que se sabe son maliciosas (malware, phishing, botnets)
- Comunidad de seguridad (sector privado): detecta amenazas en tiempo real, investiga, perfila modus operandi, comparte información
- Registradores/registros de dominios: reciben reportes de abuso, pueden suspender o cancelar dominios
- Agencias de policía: reciben denuncias de actividad presuntamente delictiva, investigan, identifican, capturan, judicializan, protegen

Actores y papeles

- CERTs en la región: 25
- Punto de coordinación: WARP de LACNIC
- Unidades cibernéticas en la región: diferentes estados de evolución, capacidades van desde alta sofisticación hasta nivel básico
- Compartir entre sector privado (incluyendo CERTs) y con agencias de policía? Es necesario!

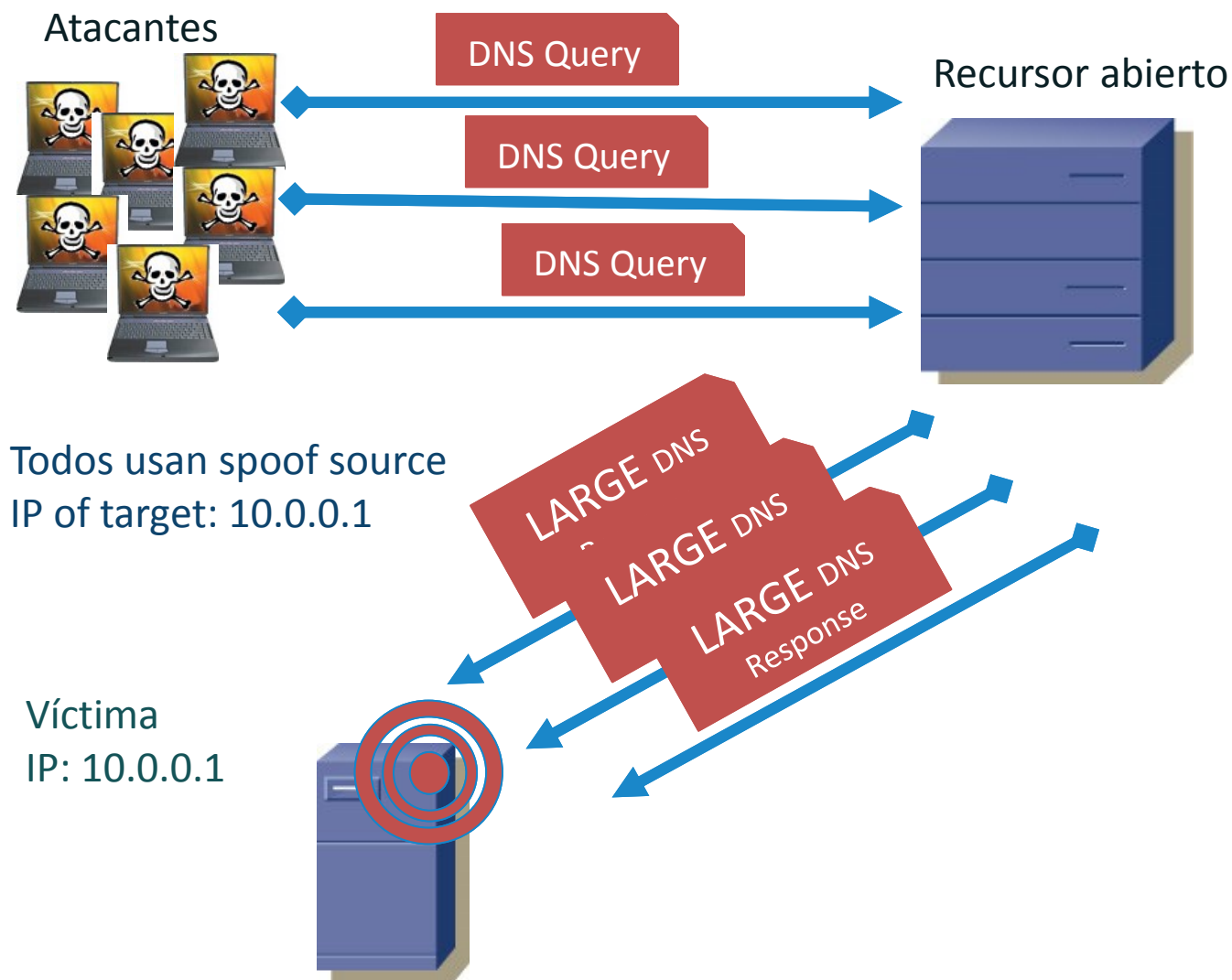
Actores y papeles

- No todos comparten.
 - Desconfianza
 - Celos
 - Posiciones políticas
 - Razones legales
- Comunidades de confianza:
 - Única forma de compartir información de forma efectiva
 - Dentro de ley aplicable y políticas corporativas
 - Compartir qué? Dominios, direcciones IP, nameservers, muestras de malware, muestras de spam.
 - Qué no se comparte? PII – Excepción: remediación de infecciones – ejemplo DNS Changer.

Objetivos

- Proteger:
 - Evitar que delincuentes alcancen dispositivos de usuarios (spam, phishing, contenido malicioso vía web)
 - Si los dispositivos son alcanzados, evitar que se conecten con servidores maliciosos (consultas de DNS interrumpidas en red corporativa o a nivel de ISP)
- Disrumpir infraestructura criminal:
 - Suspender dominios, incluir dominios e IPs en listas de bloqueo, acabar comando y control
- Individualizar:
 - Agencias de policía interesadas en individualizar responsables de actividad criminal
- Judicializar:
 - Algunas veces, no siempre es posible

Ataque distribuido con reflexión y amplificación



- Dirigen ataque desde miles de orígenes
- **Reflexión** vía recursos abiertos
- Envío de miles de grandes respuestas a víctima **(amplificación)**

Engage with ICANN



Thank You and Questions

Reach us at:

Email: engagement@icann.org

Website: icann.org



twitter.com/icann



[gplus.to/icann](https://plus.google.com/icann)



facebook.com/icannorg



weibo.com/ICANNorg



linkedin.com/company/icann



flickr.com/photos/icann



youtube.com/user/icannnews



slideshare.net/icannpresentations