Abuso del DNS: Experiencias desde .CL

José Urzúa
jose@nic.cl

nic chile
SOMOS EL PUNTO CL

NIC Chile

- Centro de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile
- Administrador del ccTLD .CL, rol de Registro y Agente Registrador
  - Agente registrador que administra el 90% de los dominios .CL
- Modificaciones a la reglamentación el 14 de julio de 2020:

NIC Chile se encuentra ahora autorizado para suspender temporal o definitivamente la operación de cualquier dominio en caso de constatarse que éste ha sido inscrito con la finalidad de realizar phishing, distribuir malware, operar botnets u otra que a juicio de NIC Chile constituya alguna práctica que sea considerada como abuso técnico de DNS.

https://www.nic.cl/anuncios/20200714-modifica-reglamentacion.html

nic chile
SOMOS EL PUNTO CL

Protocolo de suspensión de dominios

- “Suspensión de dominio”:
  - Nombre de dominio sigue inscrito pero no está incluido en la zona de .CL
    - No se puede usar técnicamente en Internet
- NIC Chile conformó un comité de análisis:
  - Comité multidisciplinario
  - Revisa antecedentes reportados
  - Formaliza solicitud de suspender funcionamiento técnico de dominio

nic chile
SOMOS EL PUNTO CL

Protocolo de suspensión de dominios

- Análisis
  - Descartar si dominio sufrió *hackeo*
    - Cambios no autorizados por explotación de vulnerabilidades o accesos no autorizados
  - Identificar si dominio fue creado con el propósito de abuso técnico
  - Analizar:
    - Tiempo de vida del dominio
    - Similitud del nombre con otros existentes
    - Información de Titular y contactos del dominio
    - Información de Agente Registrador que inscribió el dominio

nic chile
SOMOS EL PUNTO CL

Protocolo de suspensión de dominios

- Clasificación de abuso del DNS
  - Phishing, Malware, Pharming, Botnet, Medio de SPAM, BEC (Business Email Compromise)
- Registro del caso en un sistema que permite:
  - Determinar cantidad de casos en periodo de tiempo
  - Generar estadísticas por clasificación
  - Derivar casos para ser analizados por otro punto de reglamentación

Ejecución protocolo

1. Clasificación del Caso en la(s) categoría(s)
2. Al menos 3 miembros del comité deben votar
3. Decisión de desactivar debe ser unánime
    - Ante la duda no se desactiva
4. Desactivación del dominio
5. Registro del caso
6. Información a contactos del dominio

nic chile
SOMOS EL PUNTO CL

Incidentes comunes

- Phishing a instituciones financieras, públicas y privadas
- 2024:
  - 1058 casos reportados
  - 143 corresponden a Abuso del DNS
    - 61 dominios suspendidos (artículo 6.d de Reglamentación)
  - 53 casos procesados por datos incompletos o inexactos (artículo 17 de Reglamentación)
    - 41 dominios suspendidos (datos de Titular incompletos o inexactos)

nic chile
SOMOS EL PUNTO CL

Desafíos para mitigar abuso del DNS

- Atacantes conocen los mecanismos, procedimientos y facultades legales de ccTLD
- Necesidad de validar identidad para descartar un usuario ilegítimo
  - Documento de identidad nacional
  - ¿Cómo validar documento internacional de identidad de forma interoperable y consensuada?
- Identificar denuncias equívocas:
  - Basadas solo en nombre de dominio pretenden impactar en contenido
  - Identificar usos legítimos que podrían incomodar pero no vulnerar
  - Evitar que procedimiento sea una vía de *lawfare*

nic chile
SOMOS EL PUNTO CL

Equilibrio: protección ccTLD vs apertura y accesibilidad

- En NIC Chile tenemos inscripción libre sin restricciones locales
- Procedimiento para tratar Abuso del DNS posterior a la denuncia
  - Denuncias se canalizan por medio de correo electrónico: abuse@nic.cl
  - Sistema de seguimiento de casos
  - Herramientas para recopilar información de casos a analizar

nic chile
SOMOS EL PUNTO CL

Abuso del DNS: Experiencias desde .CL

José Urzúa
jose@nic.cl

nic chile
SOMOS EL PUNTO CL