



# Seguridad en .cl una mirada desde NIC Chile

Fermin Uribe  
Octubre 2009



## NIC Chile

- Organismo de la Universidad de Chile
- DNS: servicio de nombres de dominio  
[www.clcert.cl](http://www.clcert.cl) ↔ 146.83.7.21
- .cl al día de hoy
  - 267.740 dominios inscritos
  - 210.944 dominios activos



## Temario

- Phishing en Chile
- Virus – Conficker
- Spam y DDoS
- DNS Kaminsky
- Infraestructura de NIC Chile



## Phishing

- Se le envía un mensaje a la víctima induciéndole a entregar
  - Datos personales
  - Credenciales de acceso
- Tipos de ataque
  - Genérico: puddle phishing
  - Dirigido: spear phishing



## Phishing - Estadísticas

- Porcentaje de éxito de un phishing
  - comenzó en 35% de efectividad
  - hoy está en torno al 20%
  - primeras 2 horas 67%
- Si se usa información de redes sociales
  - 72% éxito
- Usando “Power relationships” del email
  - 80% éxito
    - uso de “cadenas” de email y publicación de casillas



# Phishing

- Motivación \$\$\$
  - ganar dinero usando la información
  - ganar dinero vendiendo la información para que alguien más la use
- Objetivo
  - tarjetas de crédito y PIN
  - cada vez más pagos en línea
  - identidad online



# Phishing

- la industria del phishing
  - entre 5 y 45 USD cada millón de email
  - proxies anónimos 40 a 300 USD/mes
  - se pueden comprar kits con templates para distintos sitios
- quien lo reporta
  - 69% terceros
  - 24% interno pasivo
  - 7% interno activo



## Phishing en .cl

- no hay fast flux
  - cambios en de DNS se demoran como máximo y duran como mínimo 30 minutos
- no hay domain tasting
  - hay que pagar \$20.170 para activar el dominio y poder usarlo



## Phishing en .cl

- que hace NIC Chile
  - avisa al contacto técnico del dominio
- ranking de APWG
  - Chile 6° lugar 116 phishing (antes 227 5° lugar)
  - son casi todos sitios hackeados
  - caso peypal.cl



## Conficker

- primera aparición: 28 de Noviembre de 2008
- 9 a 15 millones de equipos infectados (enero de 2009 - Mikko Hypponen, F-Secure)
- 208.182 en Chile (marzo 2009 - sri.com)
- mayor infección desde SQL Slammer en 2003



## Conficker

- Vectores de infección
  - NetBIOS exploit MS08-067
  - ataque de diccionario sobre carpeta compartida ADMIN\$
  - dll auto ejecutable en unidades removibles



# Conficker

- Update
  - HTTP pull baja actualización
    - Conficker.A 250 dominios en 5 TLD
    - Conficker.B 250 dominios en 8 TLD
    - Conficker.C 500 de 50.000 en 8 TLD
    - Conficker.D 500 de 50.000 en 110 TLD
  - NetBIOS push parcha vulnerabilidad
  - P2P push/pull se actualiza y actualiza a otros equipos



## Conficker

- Bloquea DNS lookup a algunos sitios
- Deshabilita AutoUpdate
- Deshabilita Safe Mode (D)
- Mata anti-malware
- Instala un spambot
- Instala SpyProtect 2009 (scareware)



# Conficker

- contramedidas
  - ICANN solicita el bloqueo de estos dominios
  - los dominios se usan durante un mes
  - 26.684 dominios conficker bloqueados
  - 120 dominios conficker legales
- sinkhole
  - ns.0xc0f1c3a5.org
  - ns.0xc0f1c3a5.com
  - ns.0xc0f1c3a5.net



## Conficker

- ¿debemos hacer algo?
  - no es nuestro problema
  - quien asume los costos
- Mapping the Mal Web - McAfee
  - 0.64% probabilidad de bajar algún contenido malicioso en .cl



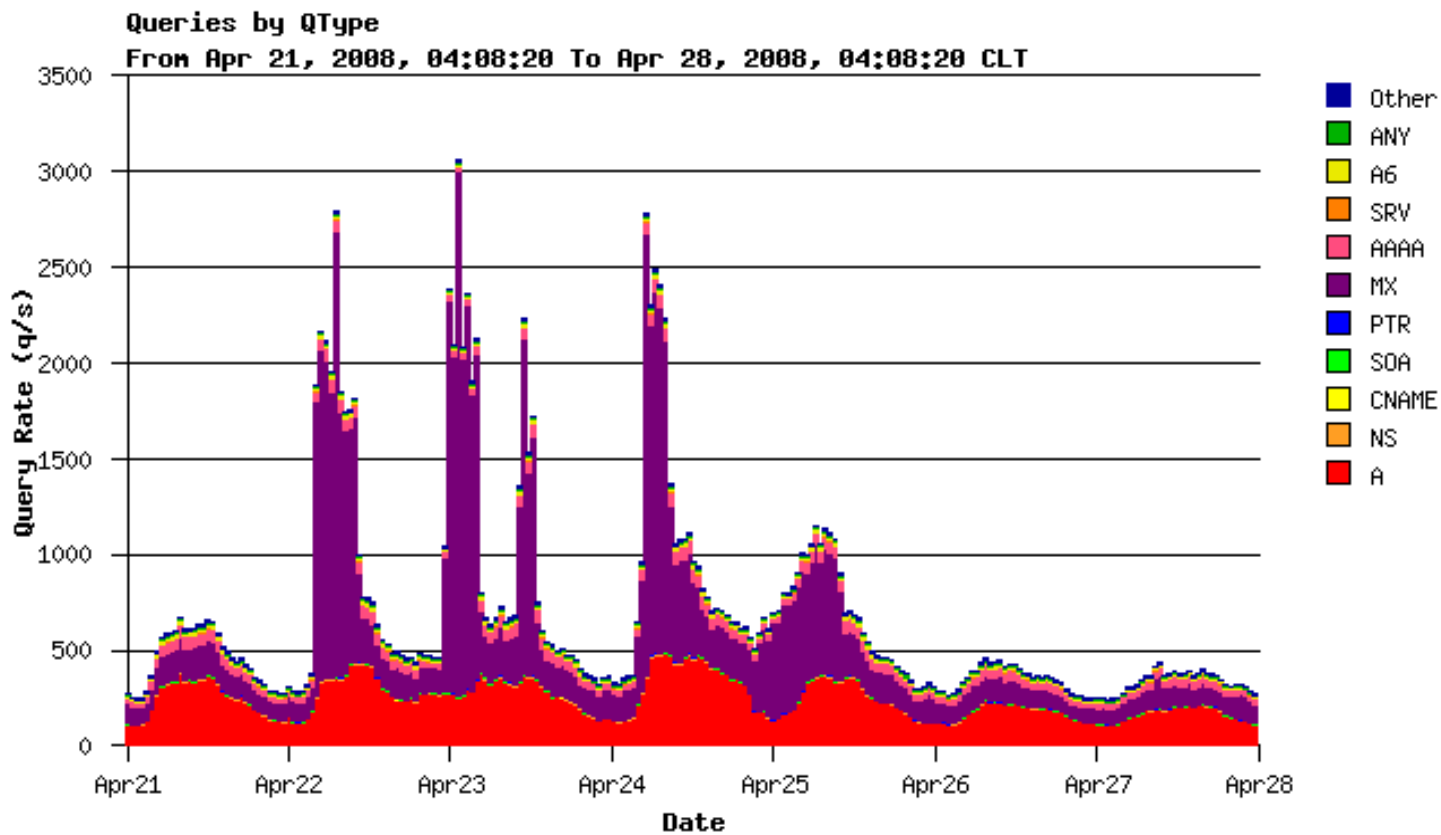
## Spam

- hoy en día el el 90% del correo es spam
  - V14GR4
  - swine flu
  - 1 line spam
- Chile genera el 1.6% del spam mundial (con un 0.25% de la población mundial)



# Spam

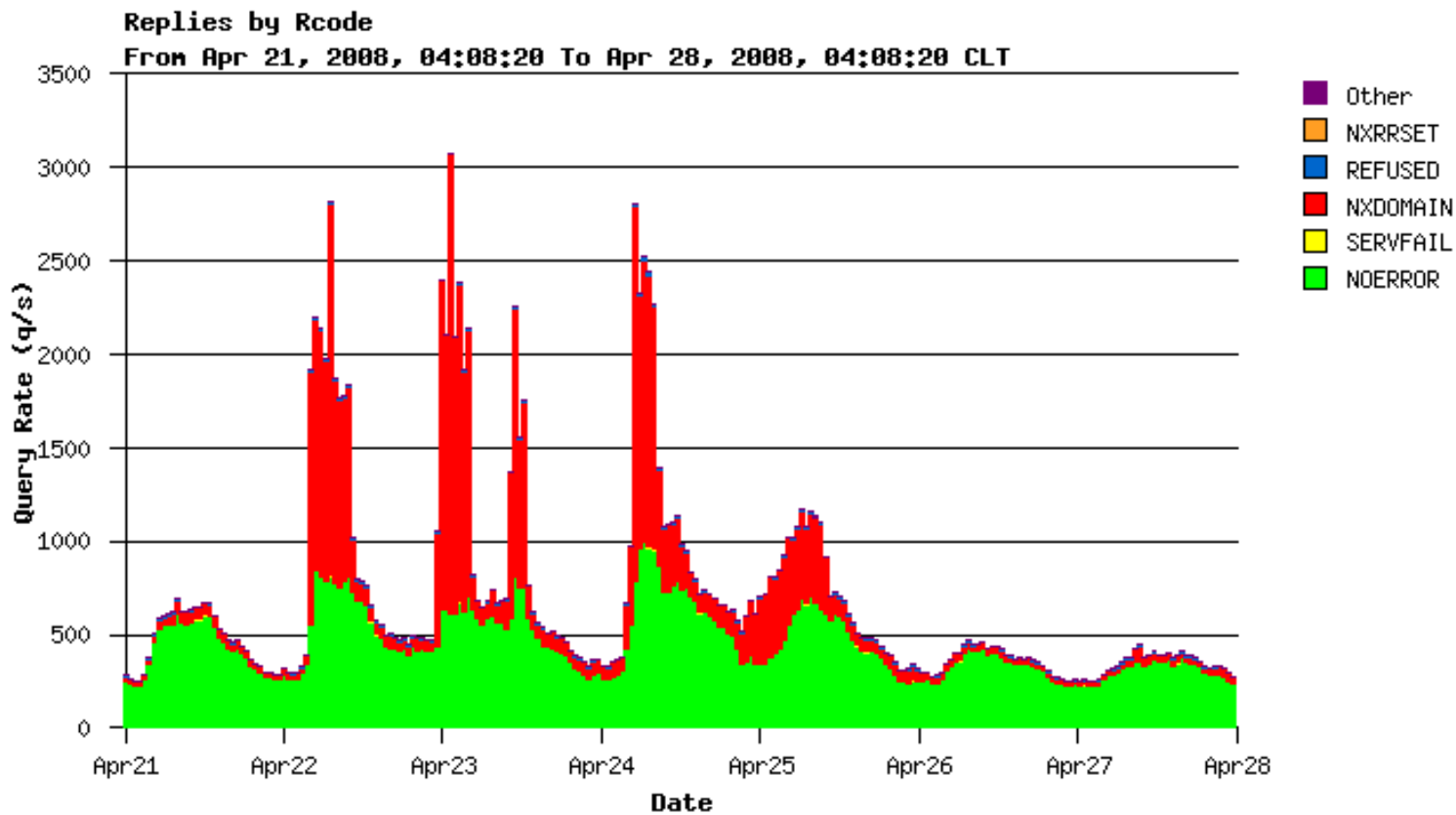
Seguridad en .cl





# Spam

Seguridad en .cl



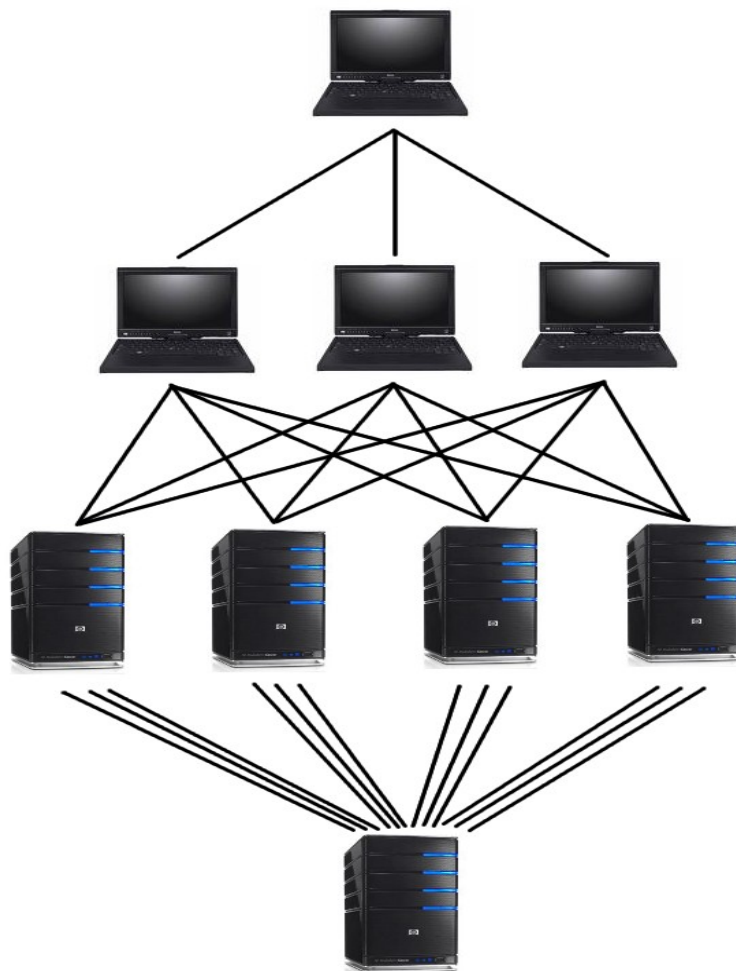


## Spam

- consultas
  - registros MX Mail Exchange
  - bit RD recursion desired
- origen
  - muchas IP
  - botnet
- destino
  - muchos dominios inexistentes



# DDoS por reflexión





## Spam DRDoS

- mail especialmente diseñado
  - To: noexiste@dominio.tld
  - From: cualquiercosa@victima
- funcionamiento
  - botnet hace el envío del mail
  - SMTP de dominios devuelven los mail porque la casilla no existe
  - víctima recibe una avalancha de correos
    - 3000 conexiones concurrentes
    - 10 Mbit/s durante 4 horas
    - catch-all



## DNS - Kaminsky

- resolver vulnerables a cache poisoning
  - ISC Bind 67%
  - Microsoft Windows DNS 10%
- el porque del revuelo
  - se iba a publicar el exploit 30 días después de los parches
  - se filtró antes de lo previsto



# DNS - Kaminsky

- cache poisoning
  - additional section

```
$ dig @ns1.example.com www.example.com
;; ANSWER SECTION:
www.example.com.      120      IN      A      192.168.1.10

;; AUTHORITY SECTION:
example.com.          86400    IN      NS     ns1.example.com.
example.com.          86400    IN      NS     ns2.example.com.

;; ADDITIONAL SECTION:
ns1.example.com.     604800  IN      A      192.168.2.20
ns2.example.com.     604800  IN      A      192.168.3.30
```

- UDP y Query ID

$2^{16}$  0..65536



# DNS - Kaminsky

- exploit
  - carrera por inyectar una respuesta
  - trata de adivinar el Query ID, no es tan difícil
  - solo el atacante sabe que sabe que es un carrera

```
;; ANSWER SECTION:
doesnotexist.example.com. 120 IN A 10.10.10.10

;; AUTHORITY SECTION:
example.com. 86400 IN NS www.example.com.

;; ADDITIONAL SECTION:
www.example.com. 604800 IN A 10.10.10.20
```



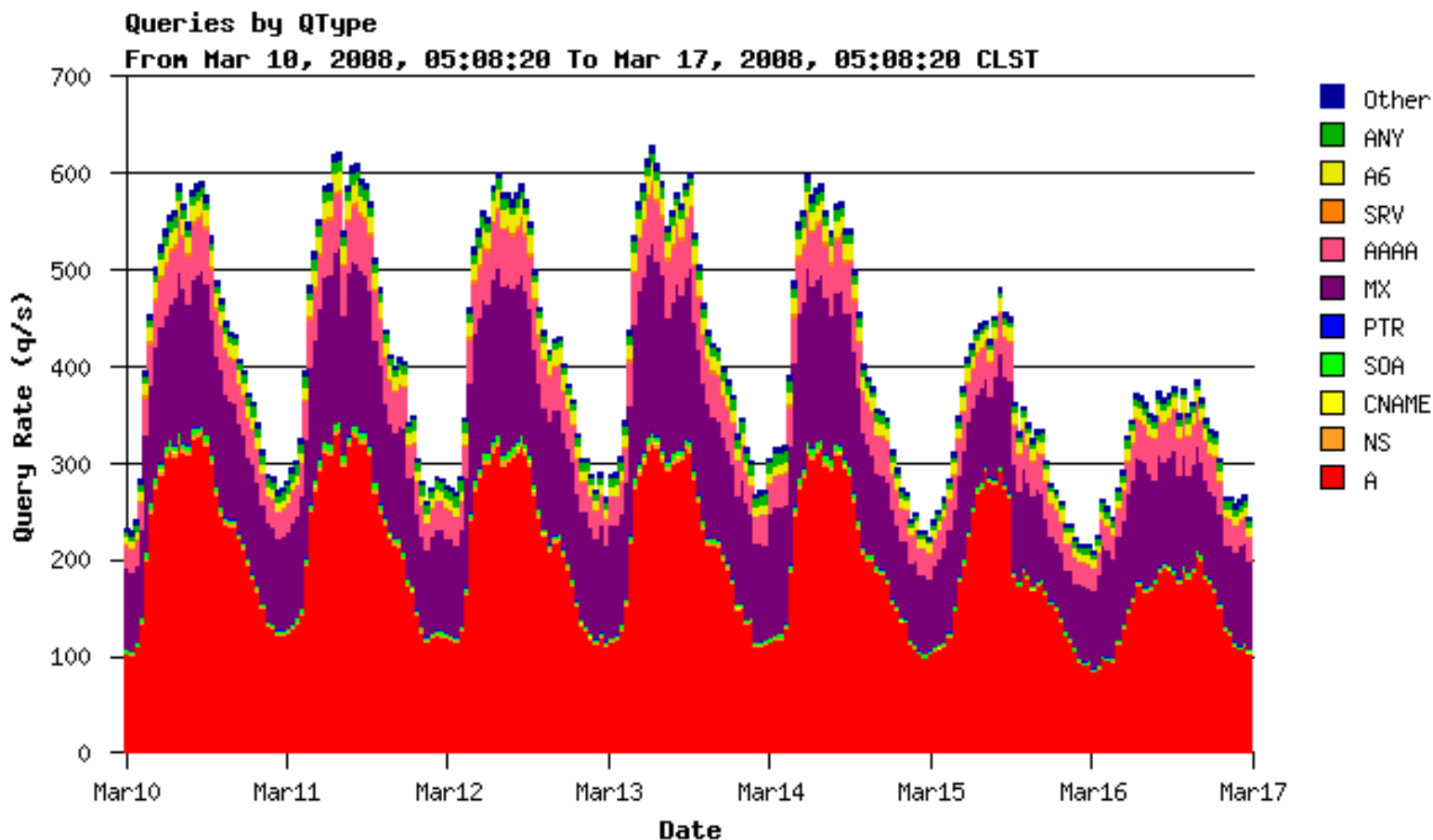
## DNS - Kaminsky

- solución (parche)
  - aletoreidad en el puerto
  - $2^{11}$  2048 puertos posibles
  - $2^{16} * 2^{11} = 2^{27} = 134.271.728$



# NIC Chile - marzo 2008

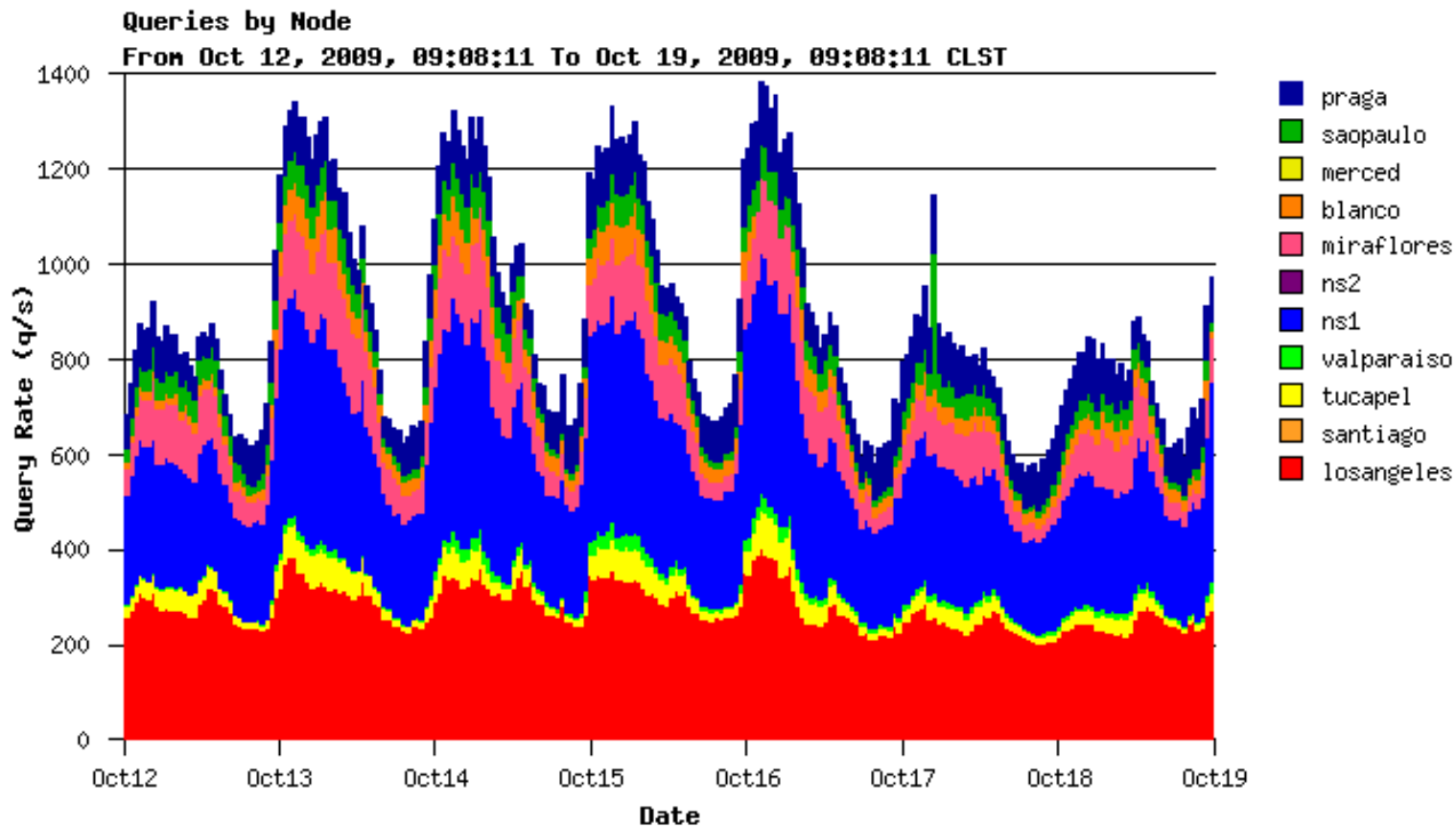
Seguridad en .cl





# NIC Chile - octubre 2009

Seguridad en .cl





# NIC Chile

;; QUESTION SECTION:

;cl. IN SOA

;; ANSWER SECTION:

cl. 3600 IN SOA ns.nic.cl. info.nic.cl. 2009102014 1200  
300 2592000 900

;; AUTHORITY SECTION:

cl. 3600 IN NS slave.sth.netnod.se.  
cl. 3600 IN NS ns-ext.isc.org.  
cl. 3600 IN NS ns3.nic.fr.  
cl. 3600 IN NS a.nic.cl.  
cl. 3600 IN NS ns.nic.cl.  
cl. 3600 IN NS cl1.dnsnode.net.



# NIC Chile - DNS

Seguridad en .cl





## NIC Chile - DNS

- anycast
  - tiempo de respuesta
  - load balancing
  - 800 a 1300 queries/segundo en 2 de los 6 nodos
- diversidad
  - enlaces
  - Hardware: Dell, Hewlett Packard, SUN
  - Software: BIND9, NSD3
  - OS: CentOS, Solaris

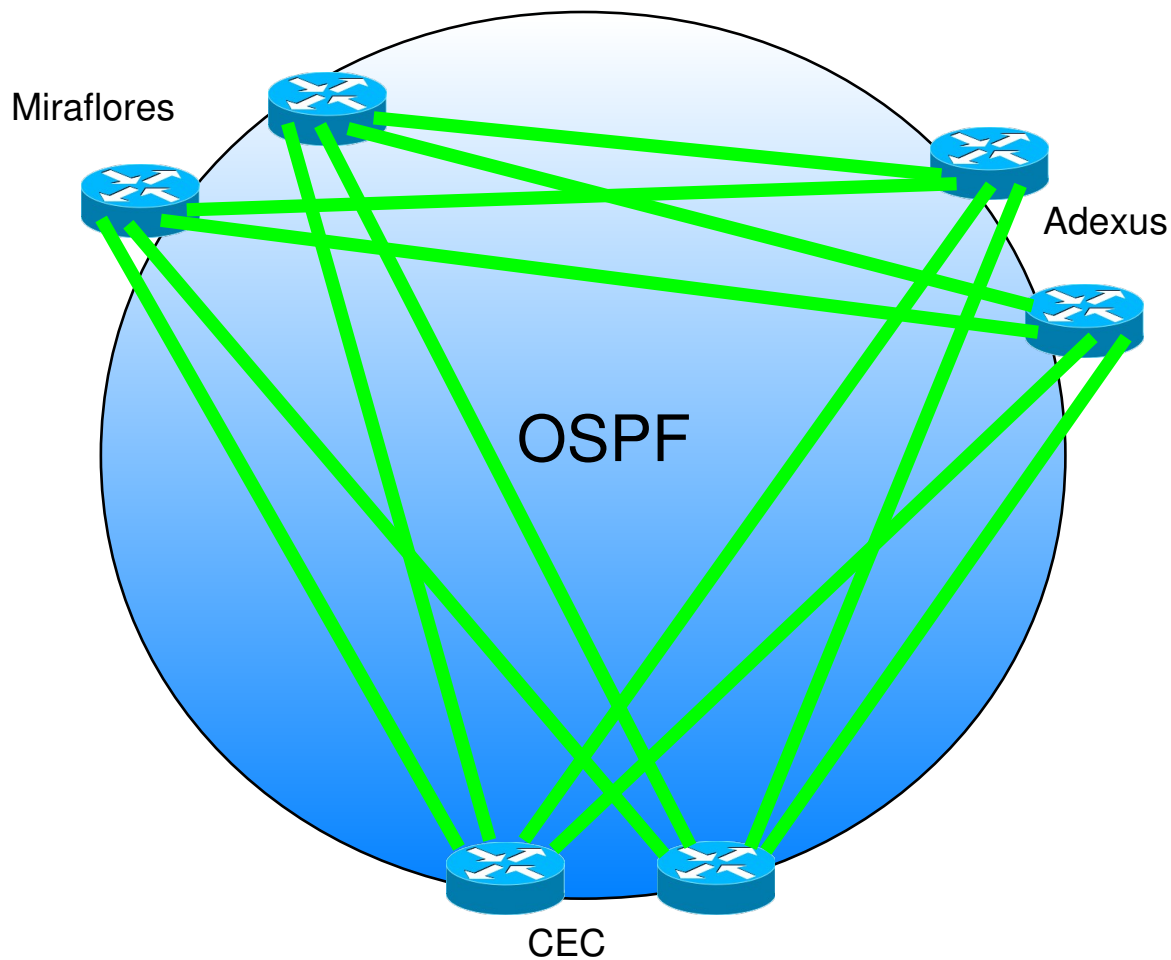


## NIC Chile

- [secundario.nic.cl](http://secundario.nic.cl)
  - 33.768 dominios
  - 300 a 800 queries/segundo
  - 9.541 dominios fallan su transferencia de zona más de 10 veces por semana



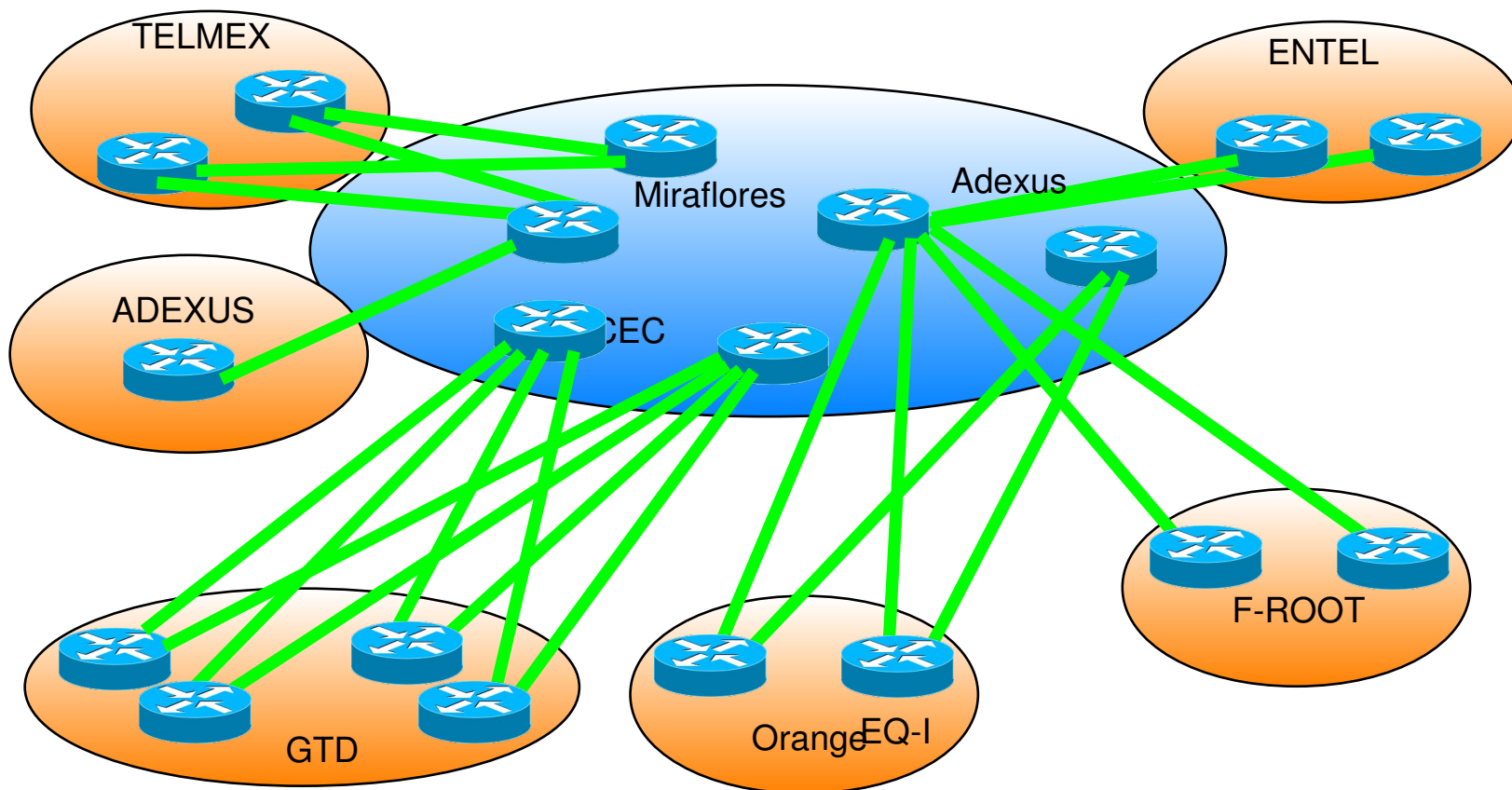
# NIC Chile - Enlaces Internos





# NIC Chile - Enlaces Externos

Seguridad en .cl





## Relator

Fermin Uribe-Echevarria Marbach  
Ingeniero de Proyectos  
NIC Chile  
furibe@nic.cl