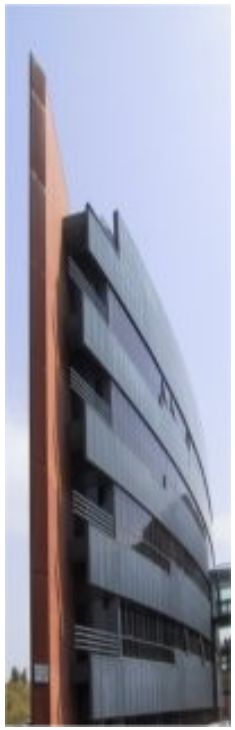
Problemas de seguridad con el servicio de DNS
GT2008

Víctor Barahona <victor.barahona@uam.es>

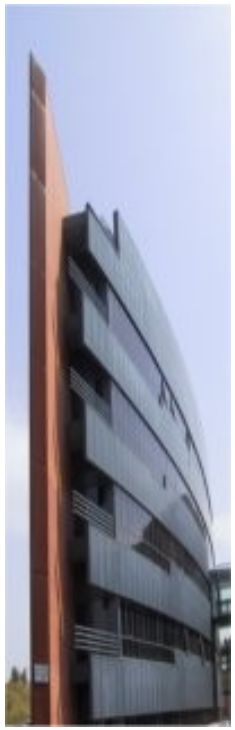
Tecnologías de la Información

Universidad Autónoma de Madrid



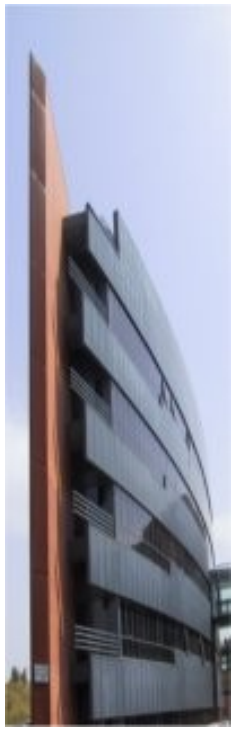
El fallo del DNS

- Es el mismo bug en todas las plataformas (diseño del protocolo)
- Enorme esfuerzo por mantener el secreto hasta tener los parches.
- Nunca había pasado antes.
- Todo planificado y bajo control…



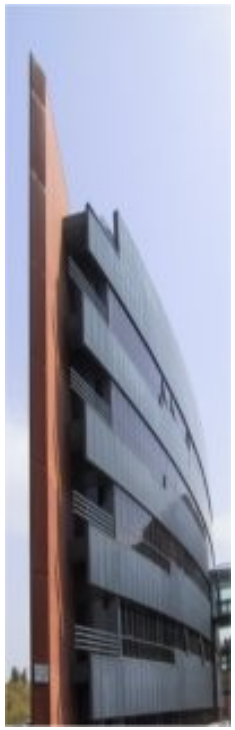
BUENO, CASI TODO…

El culebrón del fallo del DNS



- Dan Kaminsky descubre el fallo y contacta con los principales fabricantes.
- El 8-9 de Jul. los fabricantes actualizan.
- Kaminsky guardará secreto hasta el 6 de Agosto (Black Hat).
- El 21 de Jul. Halvar Flake adivina el fallo.
- El mismo día se publican por error, los detalles en el blog de Thomas Ptacek (ecopeland)

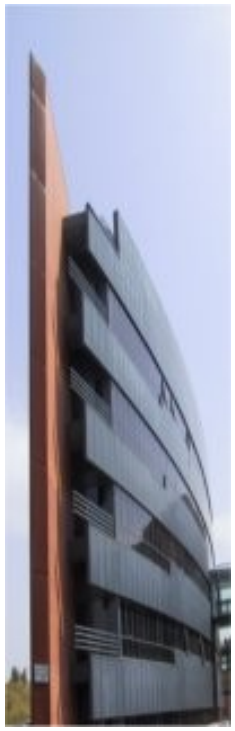
Debilidades del DNS



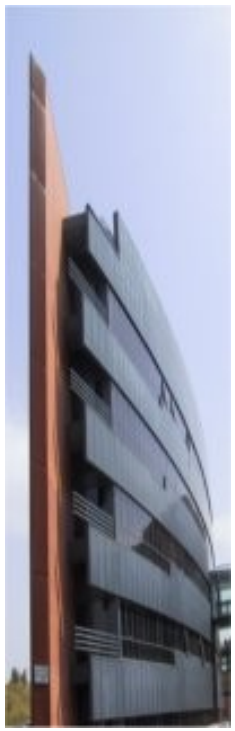
- DNS usa UDP
- Debería basar su seguridad en dos pilares:
  - La aleatoriedad del puerto origen.
  - La aleatoriedad del QID de 16 bits (0-65535)

NO ES SUFICIENTE

Paso 1: Birthday attack

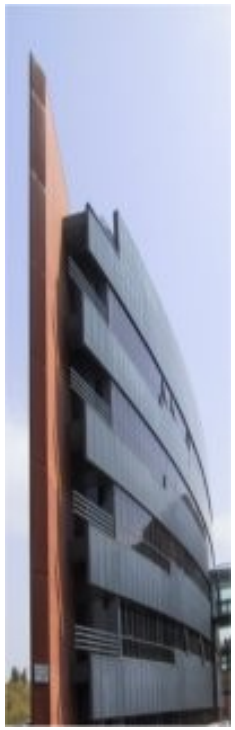


- Malote solicita registros inexistentes del dominio a atacar al DNS de victima. p.e. aaaaa.banco.es
- Malote compite con el DNS de banco enviando paquetes falsos con QID aleatorios.
- Si falla, vuelve a intentarlo con otro registro. p.e. aaaab.banco.es
- Si Malote acierta con el QID y llega antes que la respuesta de banco, conseguirá insertar un registro falso en la cache de victima.es



Paso 2: RR set poisoing (bailiwick)

- Incluido en el paquete falso malote ha incluido un registro adicionale falso. (p.e www.banco.es)
- Al venir **supuestamente** del DNS de banco, el DNS de victima almacena en su cache el registro falso.
- El secreto esta en el bailiwick check.
- Permite envenenar la cache de los DNS vulnerables en 10 segs.

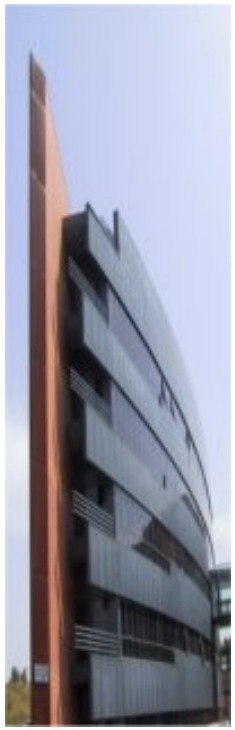


¿Es grave?

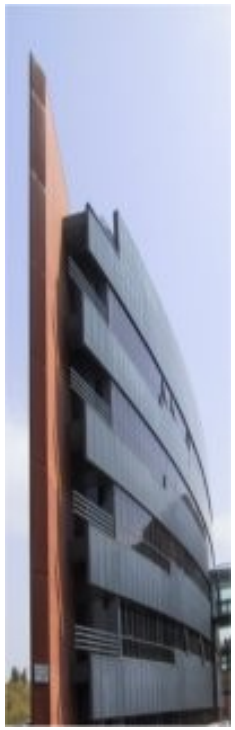
- Redirección de webs.
- Secuestro de dominios.
- Redirección de correo.
- SSL inutil
- Salto de sistemas antispam

HAY CODIGO PUBLICO

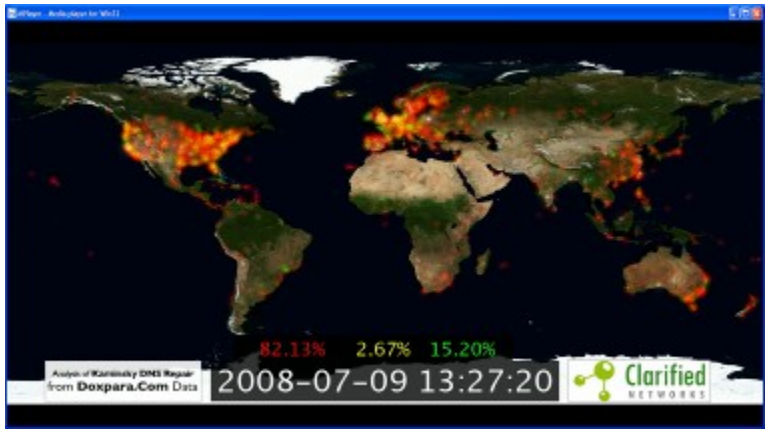
Reacción de los fabricantes

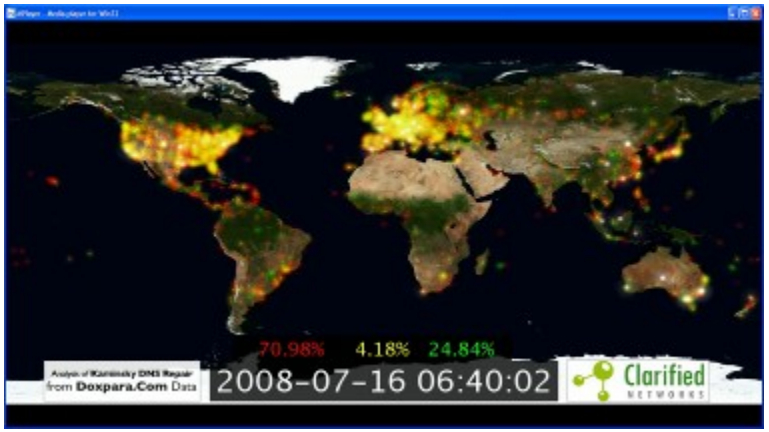


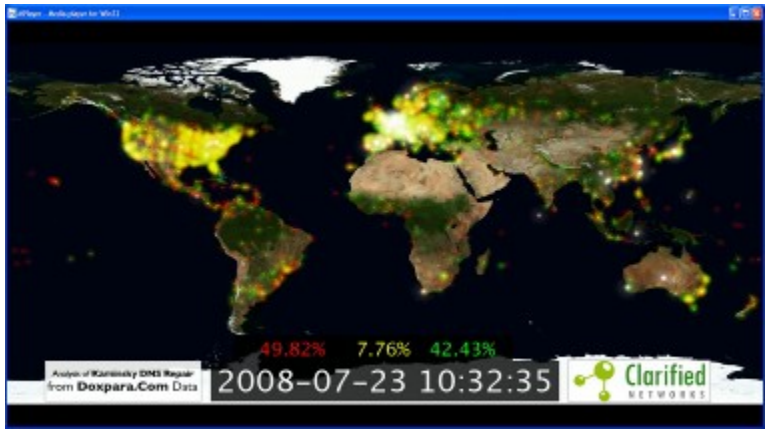
- La respuesta de la industria ha sido buena y coordinada.
- Tanto ISC como Microsoft el día 8 publicaron actualizaciones.
- La actualización consiste en aleatorizar los puertos origen de las consultas.

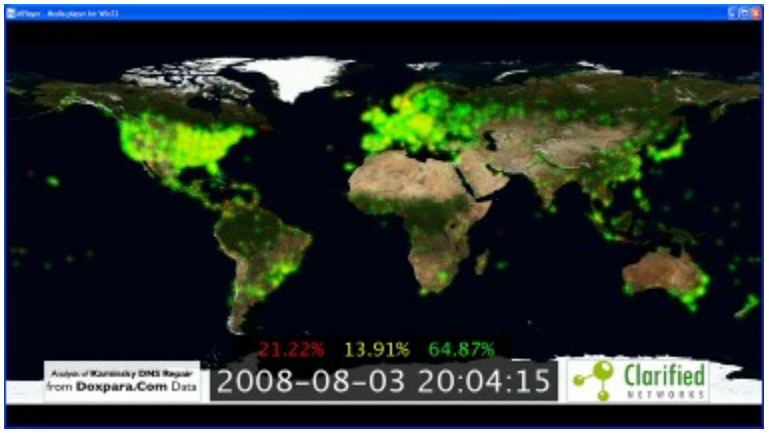


Actualizacion

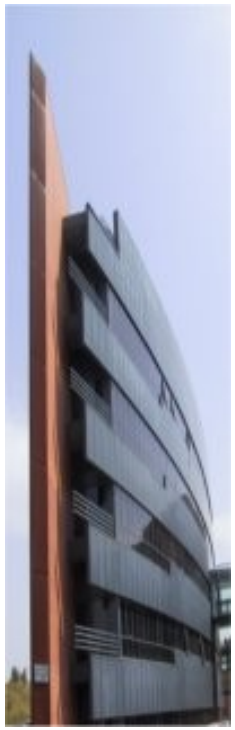






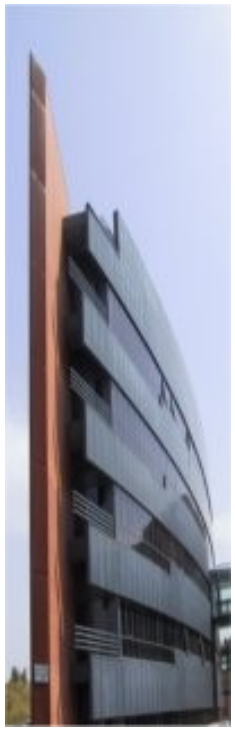


Bind: baile de versiones

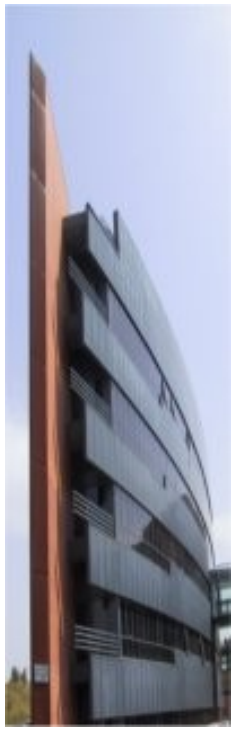


- **EOL 9.3.x:** 9.3.5-P1
- **Estables 9.4.2:** 9.4.2-P1, 9.4.2-P2
- **Estables 9.5.0:** 9.5.0-P1, 9.5.0-P2
- **Beta 9.5.1:** 9.5.1b1, 9.5.1b2, 9.5.1b3

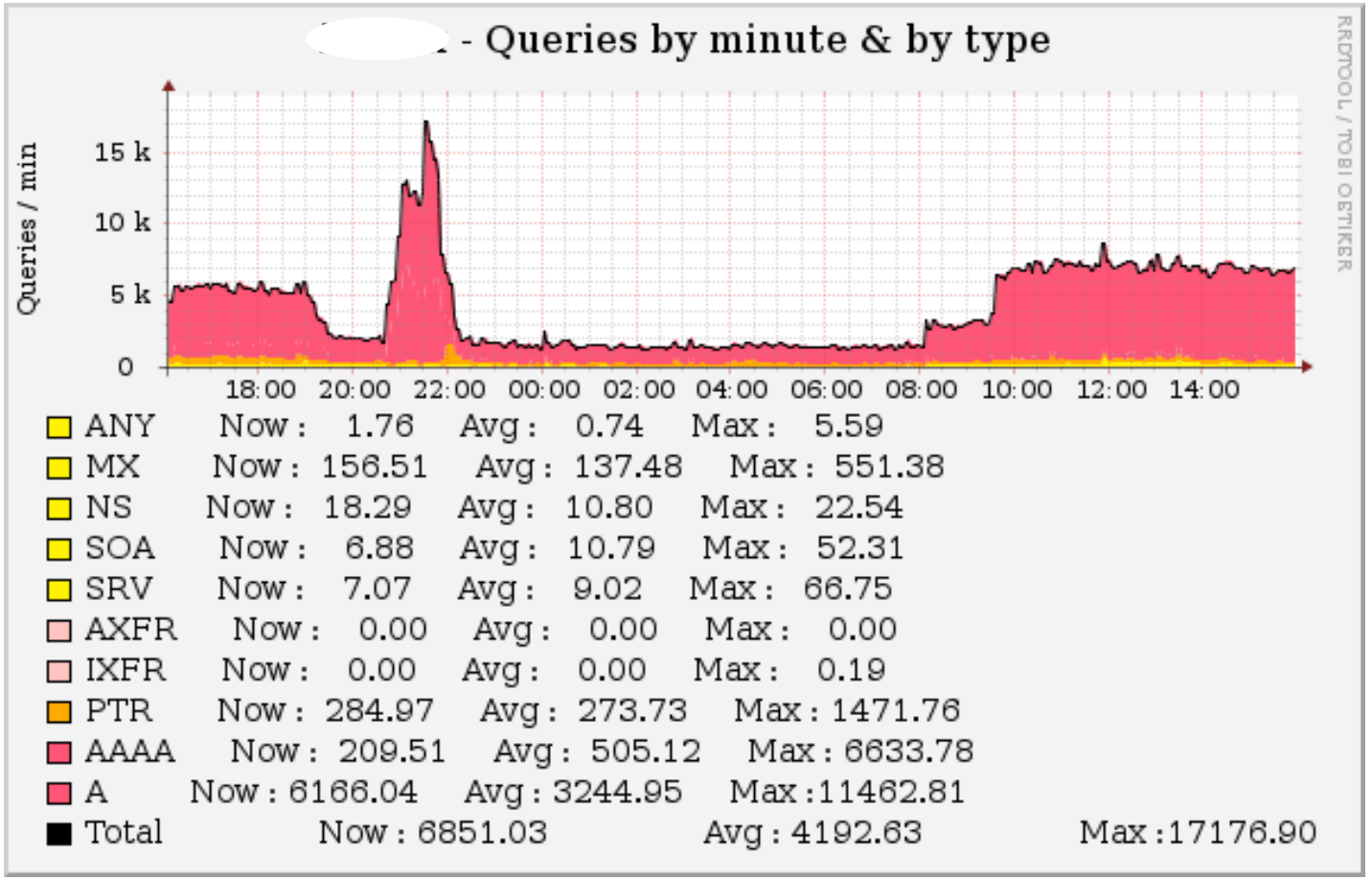
Nuestra (mala) experiencia



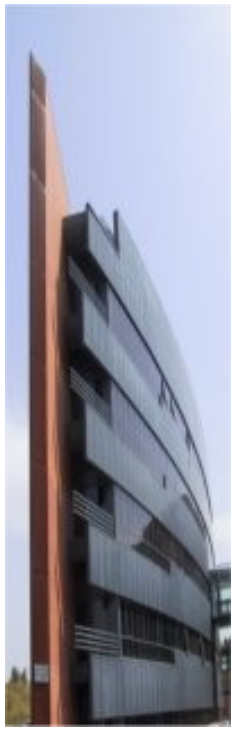
- 4 servidores solaris balanceados
- 9.5.0-P1: Bien hasta 1/Sept
- Sobre las 12am dejan de responder
- 9.5.0-P2: mejor hasta el 15/Sept
- 1 petición = 1 socket = file descriptor
- Cuando se alcanzan el número máximo de file descriptors (FD) ¡kaput!
- Solaris por defecto tiene 256 FD.
- Ahora tenemos 65535 ☺



Ojo con los picos...

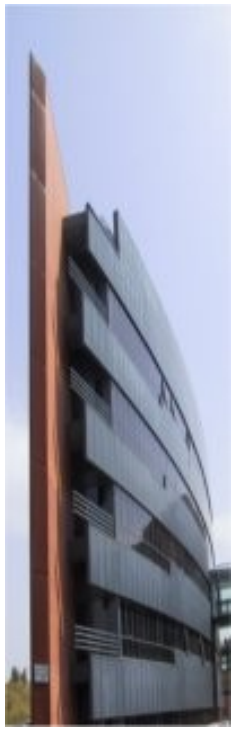


Guía del superviviente

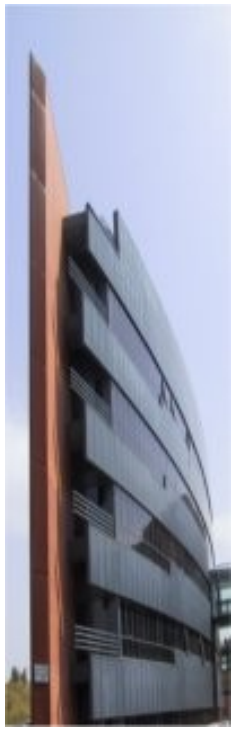


- Actualizar a la ultima versión.
- Aumentar los FD hasta donde sea posible.
- Deshabilitar las consultas recursivas.
- ¿Aislar las consultas del correo?

Soluciones a largo plazo



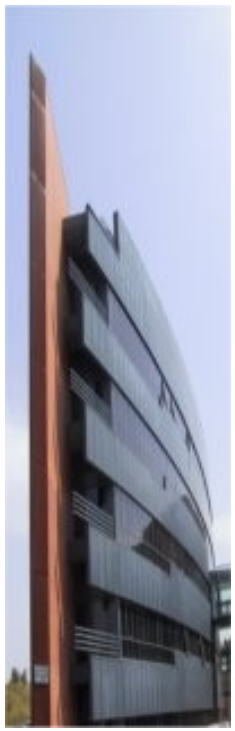
DNSSEC



Estado de los DNS academicos

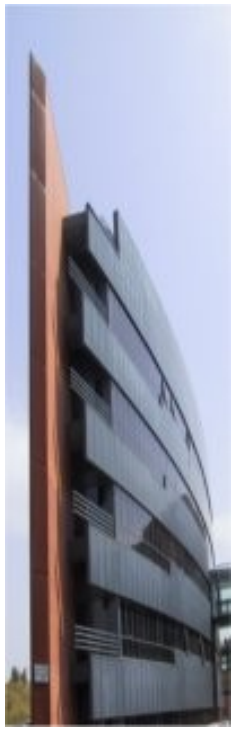
Hoja1

N serv	Dedicados	OS	Actualiz.	Version	N clientes	File Descript	Problemas
3	Mixto	RHEL 5	SI	9.3.4-6.0.2.P1.el5_2	4000		NO
3	Mixto	Ubuntu 7.10	SI	9.4.1-P1.1	1800		NO
1	SI	Centos 5	NO	9.3.4	200		NO
3	SI	Debian Etch	SI	9.3.4-2etch3	8000		NO
?	?	Debian Etch	SI	9.3.4-2etch3	?		SI
5	Mixto	RedHat 4	SI	bind-9.2.4-30.el4	27000		NO
2	SI	Solaris 9	SI	bind-9.5.0p1	5500		NO
2	SI	RedHat 4	NO	9.2.4	4000		NO
2	SI	CentOS 5.2	SI	9.3.4.6.0.2.P1.el5_2	11000		NO
3	Mixto	Solaris 8 / Centos	SI	9.3.5-P2(2), 9.2.4 (1)	15000		SI (solo logs)
2	?	Linux	SI	9.5.0.P2	?	6144	SI
?	?	Debian Etch	SI	9.3.4-2etch3			NO
?	?	Linux	SI	?	?		NO
4	NO	Solaris 9 y 10	SI	9.5.0.P2	15000	256/4096/65k	SI



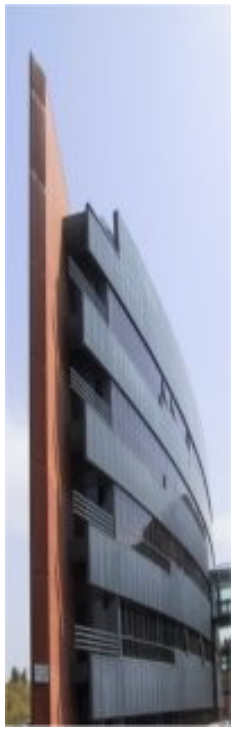
Conclusiones de la encuesta

- Solo 3/11 organizaciones que han actualizado han tenido problemas.
- 11/13 usan linux. ☺
- Todos los encuestados tienen o servidores dedicados o un entorno mixto.
- Solo 2/13 siguen en la antigua versión.



Enlaces

- ISC http://www.isc.org
- Test de recursividad http://recursive.iana.org/
- Aviso CERT http://www.kb.cert.org/vuls/id/800113
- Test paradoja del cumpleaños http://jeff.aaron.ca/cgi-bin/birthday
- Detalles de la vulnerabilidad http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
- Check my DNS http://www.doxpara.com/
- Actualización global del DNS http://www.youtube.com/watch?v=cRVMrV_ZE6A
- Código público para explotar la vulnerabilidad: http://www.caughq.org/exploits/CAU-EX-2008-0002.txt



Muchas Gracias