Informe de incidentes de seguridad año 2003

cert@rediris.es

26 de enero de 2004

Índice

1. Introducción

Este informe de incidentes de seguridad pretende reflejar los aspectos más relevantes detectados en la gestión de incidentes atendidos por el grupo de seguridad de RedIRIS, IRIS-CERT, durante el año 2003.

Este tipo de informes se presentará al menos una vez al año en la lista de coordinación de seguridad de RedIRIS, de forma que se pueda informar detalladamente de los problemas de seguridad a los responsables de las instituciones afiliadas y además tener un registro de lo acontecido a lo largo de los años.

Además de las estadísticas, se presenta en este informe algunos enlaces de interés a los problemas más comunes, vulnerabilidades o gusanos detectados durante el año.

Para finalizar esta introducción, recomendamos echar un vistazo al informe de operación presentado por IRIS-CERT en las pasadas Jornadas Técnicas de RedIRIS, celebradas en Palma de Mallorca en Noviembre de

2003, disponible aquí. En él, se incluye además información sobre otras actividades en las que participa el equipo de seguridad, así como información sobre los distintos foros, tanto nacionales como internacionales, en los que tenemos representación.

Con toda seguridad este informe presenta bastantes lagunas que esperamos ir solucionando a lo largo del tiempo.

2. Estadísticas

Todas estas cifras son orientativas puesto que los sistemas de gestión que actualmente utilizamos hacen que no podamos presentar unas estadísticas completas, sino un conjunto de datos aproximados de los principales problemas de seguridad que hemos detectado a o largo del año. Esperemos que esto cambie cuando comencemos a usar el RT/RTIR como herramienta de gestión de incidentes y realicemos paralelamente unas estadísticas más en consonancia con las necesidades reales de nuestra audiencia.

En estas estadísticas solamente aparecen aquellos problemas de seguridad de los que hemos tenido noticia directa. Algunos de los datos más significativos son:

- El número de incidentes atendidos por IRIS-CERT durante el año 2003 ha sido de 1294, lo que implica, por primera vez en los últimos 4 años, un *decremento* del 13.44 % con respecto al año anterior, en el que se atendieron 1495 incidentes. Esta cifra no nos debe llevar a engaños, y ni mucho menos significa ni que los problemas de seguridad hayan disminuido, ni que nuestras redes sean más seguras (aunque bien es cierto que existe cada vez una mayor concienciación por parte de las instituciones frente a los problemas de seguridad). Podemos explicar este decremento si tenemos en cuenta los siguientes puntos:

  - En estas estadísticas solamente aparecen aquellos problemas de seguridad de los que tenemos directamente noticia. En algunas ocasiones, no nos llega información del problema en cuestión, realizándose una gestión interna del mismo por parte de la institución.
  - En esta cifra no están contabilizados ni los incidentes de SPAM, ni los relacionados con virus de correo electrónico, ni los casos

relacionados con infracción de copyright. En este último caso, nos limitamos a redirigir el mensaje de denuncia a la institución involucrada para que ésta aplique sus políticas internas. Como veremos más adelante, el número de denuncias de este último tipo se han sextuplicado en el año 2003.

- Ha habido una serie de gusanos tan virulentos y tan activos en la red académica (por ejemplo el Blaster que comenzó a propagarse en Agosto cuando la mayoría del personal responsable de seguridad de las instituciones estaba de vacaciones) que las instituciones, en algunos casos, en lugar de pasar las incidencias a IRIS-CERT para ocuparnos de su gestión, las han gestionado directamente de forma interna.

- De los 1294 incidentes totales atendidos durante el 2003, 1211 incidentes han involucrado de una forma u otra a instituciones afiliadas (un total del 93.58 % del total). Esto es, sólo 83 de los incidentes atendidos por el equipo de seguridad de RedIRIS no han tenido nada que ver con la red académica y de investigación española, afectando a máquinas del dominio .es del que por el momento también somos responsables, dando soporte de coordinación de incidentes.

- El 62 % de estos 1211 incidentes que han involucrado a instituciones afiliadas han sido denuncias (la mayoría de los casos desde fuera de España) de equipos atacantes o comprometidos dentro de nuestra comunidad (un total de 802 incidentes). En el 28 % de los casos la denuncias hacían referencia a máquinas de la red académica atacadas en lugar de atacantes, mientras que el 3 % (unos 41 incidentes) involucran a máquinas de nuestro ámbito de actuación tanto como origen como destino.

- En cuanto a incidentes de ámbito internacional (tanto origen como destino) hemos atendido 1200 (un 92.73 %). Como hemos comentado anteriormente, sobre todo han sido situaciones en las que se ha recibido una denuncia desde el exterior relativa a un equipo atacante en la red académica.

- También hemos recibido correos en los que aparecía la dirección de IRIS-CERT como Copia (Cc:), bien desde dentro de nuestra comunidad o desde grupos de seguridad internacionales. Nuestra política ante este

tipo de incidentes, como hemos comentado múltiples veces en los Grupos de Trabajo, es que el equipo no se encarga de su gestión directa, limitándonos a tomar nota de las máquinas involucradas para hacer un seguimiento de la actividad de esa IP o red, no involucrándonos en su resolución a no ser que se nos lo pida expresamente. Por tanto, la proporción de incidentes de este tipo no queda reflejada en estas estadísticas.

- En cuanto a los incidentes de SPAM, desde hace más de un año son atendidos por el responsable de correo electrónico en la comunidad RedIRIS, Jesús Sanz de las Heras, no involucrándose el equipo de seguridad en su resolución.[1]

- Aunque en nuestra taxonomía de alto nivel se encuentran contemplados los incidentes relacionados con virus, la realidad es que el equipo de seguridad no se encarga de atender este tipo de incidentes, siendo de nuevo el responsable del correo electrónico en nuestra comunidad, Jesús Sanz de las Heras, el encargado de gestionarlos[2]. Sobre este tema, sólo mencionar que a existido una excelente coordinación de las epidemias víricas del verano gracias al proyecto RESACA (Red de Sensores AntiVirus de la Comunidad Académica), detectándose un alto impacto en el tráfico SMTP en los servidores institucionales por ejemplo en las epidemias provocadas por virus como el Sobig y Mimail.

- Durante el 2003, se ha producido un espectacular incremento de las denuncias relacionadas con infracción de copyright (para las cuales ya sabéis que la política de IRIS-CERT es la de actuar como puro intermediario, redirigiendo la denuncia original a la institución afectada para que ésta aplique sus políticas internas, no contabilizando pues estos incidentes con fines estadísticos). De 50 denuncias recibidas en 2002, durante el 2003 se han recibido 299, lo que supone un incremento del 498 %. Al menos 30 instituciones se han visto afectadas por este tipo de denuncias, debiendose, en la mayoría de los casos, a máquinas previamente comprometidas que están siendo usadas para estos fines

[1] Para más información sobre este tipo de incidentes, consultar la sección "Incidentes de SPAM 2003"más adelante en este documento.

[2] Esta forma de actuar se refiere a aquellos virus que se propagan exclusivamente vía correo electrónico.

ilítcitos (instalandose un servidor ftp ilegal desde el cual distribuir fundamentalmente películas, pero también música, videojuegos, software, etc.). Desde IRIS-CERT os pedimos que si detectáis que se trata de una máquina previamente atacada, os pongáis en contacto con nosotros tras su análisis para indicarnos qué ficheros encontráis en la misma y asíi poder detectar posibles patrones de ataque y comportamiento.

2.1. Evolución de los incidentes

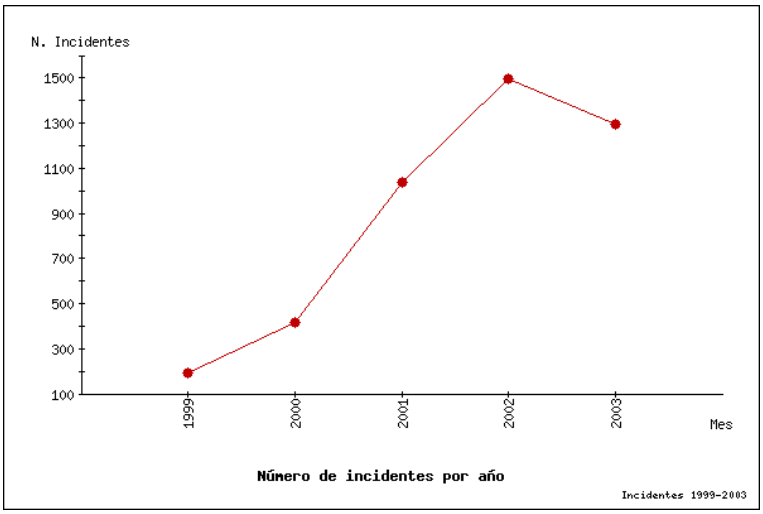

Figura 1: Evolución de incidentes por años

En la figura anterior, se observa la evolución de los incidentes de seguridad

desde el año 1999. Las cifras detalladas son los siguientes:

Año	**Incidentes totales**	**Incremento**
1999	195	-
2000	416	113.333 %
2001	1038	149.51 %
2002	1495	44.02 %
2003	1294	-13.44 %

A continuación presentamos una gráfica en la que podemos ver la distribución de los incidentes atendidos por IRIS-CERT durante el año 2003 y distribuidos por meses.

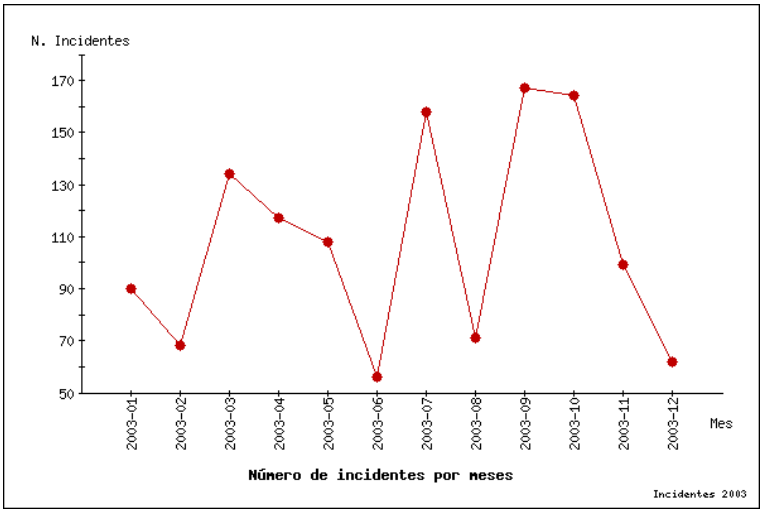

Figura 2: Evolución de incidentes por meses

Los datos detallados son los siguientes:

Fecha	**Total**	%	**P. Baja**	**P. Normal**	**P. Alta**	**P. Emergencia**
2003/01	90	6 %	17	22	51	0
2003/02	68	5 %	17	27	24	0
2003/03	134	10 %	51	30	53	0
2003/04	117	9 %	21	28	68	0
2003/05	108	8 %	13	55	40	0
2003/06	56	4 %	16	28	12	0
2003/07	158	12 %	24	110	24	0
2003/08	71	5 %	11	49	11	0
2003/09	167	12 %	50	104	13	0
2003/10	164	12 %	19	100	45	0
2003/11	99	7 %	22	56	21	0
2003/12	62	4 %	4	44	14	0

La gráfica presenta multitud de subidas y bajadas cuya explicación sería la siguiente:

- El mayor incremento de incidentes lo detectamos en Septiembre con un total de 167 atendidos durante dicho mes. Este incremento se debe a la actividad del gusano Blaster, que aunque empezó a propagarse en Agosto, el día 11 concretamente, no fue hasta la vuelta de vacaciones de verano cuando nos empezaron a llegar más denuncias e informes por parte de las instituciones afiliadas. El impacto del Blaster en la Red Académica, como en Internet en general, fue muy acusado.

- El Slammer (que afectaba a Servidores MSQ de Microsoft), a principios de año, tuvo una amplia repercusión en la red académica, obligando al NOC de RedIRIS a aplicar filtros en los troncales y en los enlaces externos para paliar sus efectos.

- En Marzo comenzamos a detectar un incremento de las denuncias por escaneo a los puertos netbios (139/tcp, 137/tcp-udp, 138/udp y 445/tcp) debido a la aparición de una vulnerabilidad que afectaba al protocolo SMB (Server Message Block), utilizado para la compartición de ficheros y recursos de impresión en máquinas Microsoft Windows

2000 y XP. Aparecieron, así mismo, una serie de herramientas (gusanos) que aprovechaban la mencionada vulnerabilidad. Ejemplo de algunas de estas herramientas son: el W32/Deloder, GT-Bot, sdbot, W32/Slackdor, que a su vez dieron lugar a diversos ataques de DoS y DDoS.

- En general, Marzo fue un mes cargado de problemas de seguridad con la aparición de múltiples vulnerabilidades en diversos servicios y productos ampliamente utilizados (sendmail, BIND, WebDAV, núcleo del S.O Linux, etc..).

- En Mayo detectamos un incremento de ataques a servidores Web que tenían instalados tablones de anuncios y/o portales dinámicos (casi todos albergados en máquinas Linux). Estos problemas seguramente se debieron al aprovechamiento de diversas vulnerabilidades de inyección de código en varias versiones del php-nuke.

- El descenso de incidentes en el mes de Junio (que también se viene observando en años anteriores) se podría deber a la coincidencia de la época de exámenes en las universidades, si bien es verdad que los ataques normalmente se deben a modas o a la aparición de gusanos/exploits específicos en una determinada fecha.

- El mismo razonamiento aplicado al mes de Junio se podría utilizar para explicar el descenso en los meses de Enero-Febrero.

- A finales de Julio aparecen diversas vulnerabilidades que afectan a los mensajes RPC utilizados para la activación de DCOM en el interface RPC de Microsoft (el primer exploit aparecido utilizaba el puerto 4444/tcp para establecer una puerta trasera). Poco después de la aparición de este exploit comienza a propagarse el gusano Blaster. El Blaster utiliza el puerto 135/tcp para lanzar el ataque, aunque también se detectó actividad relacionada con este gusano en los puertos 139/tcp y 445/tcp. Este gusano en su payload contenía una ataque de DoS contra el servidor windowsupdate.com de Microsoft.

- Tras la aparición del Blaster, aparece otro gusano, el Welchia o Nachi que aprovechaba la misma vulnerabilidad del Blaster, aunque en este caso los ataques de DoS asociados no tenían un destino especifico y utilizaban el protocolo ICMP.

- Durante Junio-Julio aparece una variante del Bugbear, el Bugbear.B. El Bugbear.B tenía funcionalidades de gusano, virus y puerta trasera (en el 1080/tcp) y se propagaba mediante mail y por recursos compartidos en redes locales de Windows.

- Durante Diciembre hemos detectado un incremento de escaneos al puerto 6129/tcp. Este puerto es empleado por un programa de control remoto llamado Dameware, del que se publicó un fallo de seguridad principios de dicho mes. Este programa de control remoto se emplea para controlar equipos Windows previamente comprometidos. Las denuncias sobre escaneos a este puerto se han hecho más intensas durante principios del año 2004.

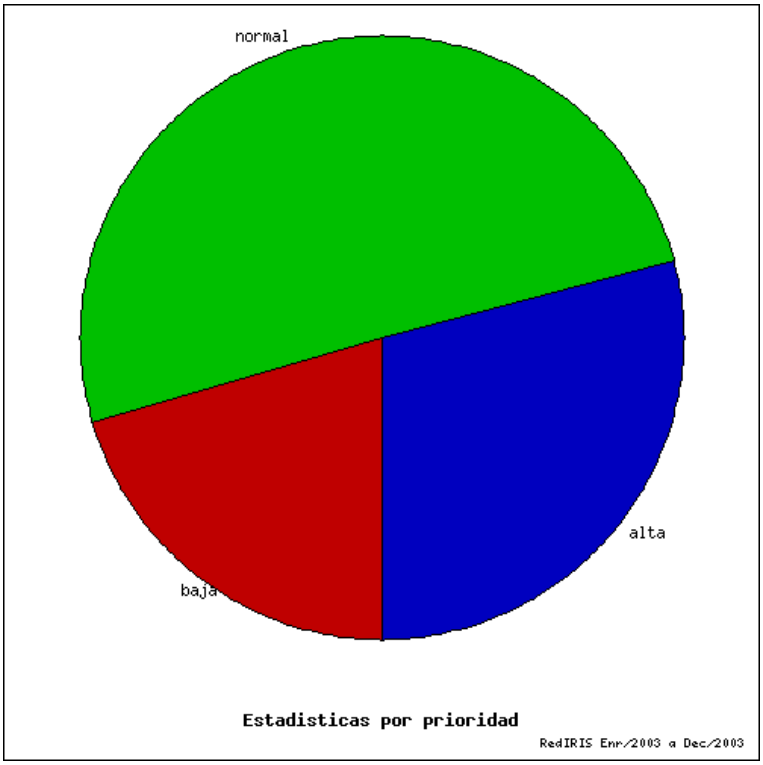

Figura 3: Porcentaje de incidentes por prioridad alcanzada

La figura anterior muestra la distribución de los incidentes atendidos por IRIS-CERT durante el año 2003 clasificados según la prioridad asignada (se puede consultar el criterio de prioridad que sigue el equipo aquí).

Esta gráfica no es realmente significativa puesto que la mayoría de los incidentes de seguridad se producen tras la recepción de un correo de queja o denuncia que en la mayoría de los casos se refiere a escaneos de puertos o pruebas. Estos escaneos, en los últimos tiempos, en muchos casos estaban relacionados con máquinas comprometidas por alguno de los gusanos comentados anteriormente (por el tipo de puerto indicado en la denuncia). En definitiva, muchos de los incidentes que se han clasificado como escaneos (prioridad de baja a normal) al final han resultado ser debidos a gusanos, troyanos, compromisos de root, etc.. (con prioridad alta), y algunos de los incidentes que se han catalogado como gusanos al final se debían a escaneos simples y por tanto falsos positivos. Para evitar esta confusión, en los últimos tiempos hemos intentado catalogar de primeras como gusanos aquellos incidentes que mostraban escaneos a puertos relacionados con puertos de propagación de los gusanos activos en ese momento. Otra opción ha sido la de catalogarlos como escaneos de prioridad normal (en lugar de baja) cuando el puerto escaneado tenía que ver con la actividad de una herramienta/gusano de moda en ese momento.

En cifras, la distribución de los incidentes atendidos por IRIS-CERT durante el 2003 en función a la prioridad alcanzada es la siguiente:

Prioridad	**Cantidad**	%
Baja	265	21 %
Normal	653	50 %
Alta	376	29 %
Emergencia	0	0 %

En la siguiente tabla aparece reflejado el porcentaje de cada uno de los incidentes clasificados a partir del primer mensaje que se recibe, y siguiendo nuestra taxonomía de alto nivel[3]. Es decir, si inicialmente se recibe un men-

[3] Nuestra taxonomía de alto nivel contempla los siguientes tipos de incidentes:

1. *Denegación de Servicio (DoS).* Con o sin éxito. Acciones que interrumpan la op-

saje indicando un escaneo de puertos, el incidente se clasifica como "sondeo", aunque posteriormente al investigar se observe que se trata de un acceso a

---

eración normal de un recurso cualquiera que sea este. Cualquier incidente que conlleve que un servicio no esté disponible a la persona o proceso cuando es necesario Dentro de esta categoría se incluyen los DDoS (Distributed Denial of Service).

2. *Sondeo.* Tráfico de red usado para descubrir información sobre máquinas y servicios conectados a la red, así como topología. Dentro de esta categoría estarían incluidos los escaneos de redes y de puertos tanto de forma repetida como aislada.

3. *Acceso a cuentas privilegiadas del sistema.* Cualquier ataque que constituya el acceso a root o a una cuenta privilegiada, teniendo el atacante acceso total a un sistema ajeno.

4. *Troyanos.* Cualquier incidente que involucre el uso de un programa que oculta su función real. Dentro de categoría estarán incluidos los controles remotos en Windows.

5. *Gusanos.* Cualquier incidente que involucre el uso de programas que tienen la característica de auto-replicación y por tanto de expandirse de máquina en máquina.

6. *Uso no autorizado.* Cualquier uso de un recurso sin autorización (cache abiertos y mal configurados, uso ilegal de cuentas de usuario, robo de password).

7. *Uso de sniffers.* Cualquier observación de paquetes en la red para obtener información privilegiada (password, información confidencial, comercial o personal).

8. *Virus.* Cualquier incidente que involucre virus (se distribuyan estos por el medio que sea).

9. *Otros.* Cualquier incidente que no encaje en los tipos descritos anteriormente.

un equipo y se proceda a investigar el incidente.

Tipo de Incidente	**Cantidad**	%
Denegación de Servicio	76	5.87 %
Sondeo	837	64.68 %
Acceso a cuentas privilegiadas	133	10.27 %
Troyanos	6	0.46 %
Gusano	213	16.49 %
Uso no autorizado	15	1.15 %
Otros	14	1.08 %

Como vemos en la tabla anterior, la suma de los incidentes debidos a escaneos de puertos y redes y los debidos a gusanos suman más de un 80 % del total de incidentes atendidos por IRIS-CERT a lo largo del año.

Las denuncias de uso no autorizado se han debido fundamentalmente a equipos Proxies mal configurados que permiten conexiones a equipos externos a la organización, y a problemas con socks proxies.

En cuanto a los incidentes catalogados como .ºtros", se han debido fundamentalmente a problemas de suplantación de personalidad, insultos o amenazas utilizando medios telemáticos, aunque en este caso nosotros lo que recomendamos es que los afectados se pongan en contacto directamente con la Policía y Guardia Civil.

En cuanto a los referente a Troyanos sobre todo se han atendido incidentes relacionados con el Subseven, RedShad y kuang2.

Este año ha sido, como el año anterior, bastante prolífico en gusanos (Blaster, Nachi, Slammer, Bugbear, etc.). Pero además de estos gusanos de nueva aparición, durante el 2003 se ha detectado actividad de algunos gusanos que ya aparecieron el el 2002 e incluso en el 2001, sobre todo Nimda (que aprovechaba una vulnerabilidad en el Internet Information Server de Microsoft), pero también Code Red, Slapper (Apache/mod_ssl), Opaserv (Netbios) y SQLSnake (Servidores SQL de Microsoft).

En cuanto a los escaneos de puertos, y si aplicamos la lógica, los puertos más escaneados han sido los relacionados con la actividad de algunos de los

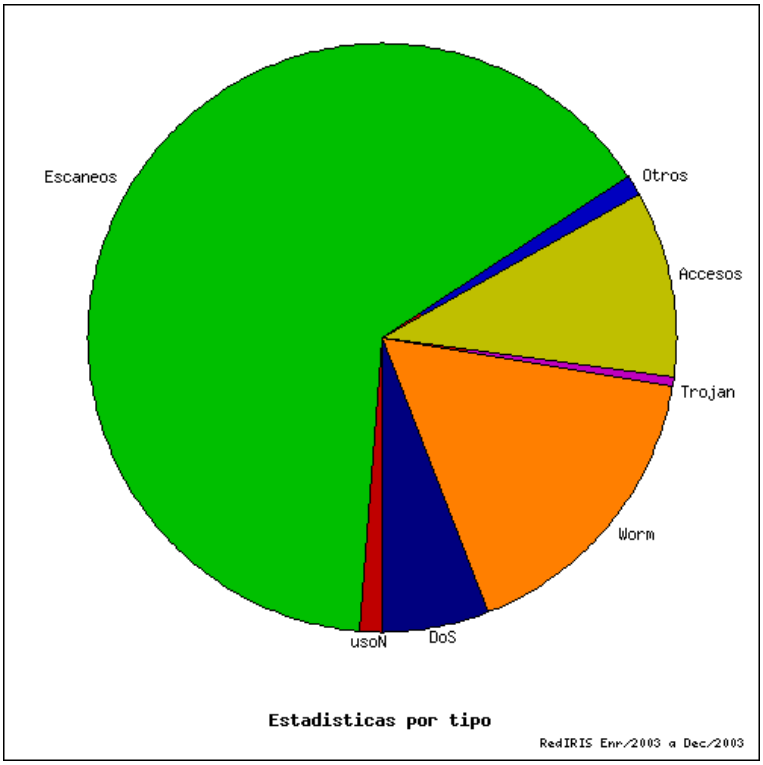

Figura 4: Porcentajes de incidentes

gusanos mencionados anteriormente y por lo tanto podemos destacar, como los puertos de los que hemos recibido más denuncias, los siguientes:

- netbios
  1. 135/tcp-udp, location service
  2. 137/tcp-udp, netbios name sarver
  3. 138/tcp-udp, netbios datagram service
  4. 139/tcp-udp, netbios session service
  5. 445/tcp-udp microsoft-ds
- http (80/tcp) (gusanos IIS, WebDAV[4])

[4]Vulnerabilidad aparecida en Marzo en una DLL (ntdll.dll). Esta DLL permite interactuar con el kernel del Windows. Esta vulnerabilidad afectaba a Windows 2000, NT 4.0 y al IIS 5.0 con WebDAV activo.

- 1434/tcp, 1433/udp (MS-SQL)
- 1080/tcp (socks proxy, puerta trasera Bugbear)
- 554/tcp (RTSP, Real Time Streaming Protocol[5])
- 6129/tcp (Dameware)

2.2. Incidentes de SPAM 2003

El incremento del spam en el año 2003 ha sido notable, y se desconocen los límites futuros de este incremento porque para el año 2004 se espera mucho más SPAM. Por tanto, podemos decir que durante el año 2003, se ha producido un aumento considerable de las denuncias de SPAM recibidas en RedIRIS (normalmente en el buzón abuse@rediris.es) respecto a sus instituciones afiliadas.

El SPAM se está aprovechando, con fines ilícitos, de un protocolo diseñado inicialmente para un entorno científico donde ha primado la confianza.

El principal canal de distribución del SPAM ya no suele ser el uso de open-relays, ya que es un aspecto de los servidores de correo bien conocido y protegido. Durante el año 2003 se han abierto nuevos agujeros para la distribución masiva de correo basura que están afectando a los equipos de usuarios finales. Ha sido frecuente que los virus, troyanos y demás maldades (malware) distribuidos en mensajes de correo electrónico infecten a los PCs incorporando, además del típico puerto de control remoto, algunas funcionalidades que permite que las máquinas infectadas puedan ser usadas como proxy.

Los proxies que se han detectado durante el pasado año son de dos tipos:

- proxy http, empleado para conexiones de tipo TCP.
- proxy socks, que han sido los mas peligrosos.

Socks es un protocolo (RFC1928) que permite establecer conexiones genéricas empleando un determinado equipo. Los spammers, a través de estos gusanos, dejan preparado el PC infectado para emplear su programas de envío de SPAM ocultando la dirección IP que hay detrás de los proxies, lo que ha creado un gran confusión en las denuncias. Por lo que se cuenta en los foros,

[5]Relacionada con una vulnerabilidad aparecida en el Real Network Media Player.

estas listas de de máquinas infectadas y preparadas para ser utilizadas son distribuidas y vendidas a potenciales spammers.

3. Links de interés

A continuación podéis encontrar algunos enlaces a documentos donde se describen algunos de los gusanos (así como las vulnerabilidades que aprovechan) que han estado activos durante el año 2003. También se presentan enlaces a los informes trimestrales del CERT/CC donde podreis obtener más información sobre algunos problemas puntuales:

1. Code Red
   - http://www.cert.org/advisories/CA-2001-19.html
   - http://www.cert.org/advisories/CA-2001-23.html
2. Nimda
   - http://www.cert.org/advisories/CA-2001-26.html
3. Slapper
   - http://www.cert.org/advisories/CA-2002-27.html
4. Bugbear
   - http://www.f-secure.com/bugbear/
5. Opaserv
   - http://www.f-secure.com/v-descs/opasoft.shtml
6. SQLsnake
   - http://www.cert.org/incident_notes/IN-2002-04.html
7. Blaster
   - http://www.cert.org/advisories/CA-2003-20.html
   - http://www.cert.org/tech_tips/w32_blaster.html

8. Nachi o Welchia
   - http://www.f-secure.com/v-descs/welchi.shtml
9. Slammer
   - http://www.f-secure.com/v-descs/mssqlm.shtml
10. CERT Summari CS-2003-01 - Marzo 2003
    - http://www.cert.org/summaries/CS-2003-01.html
11. CERT Summari CS-2003-02 - Junio 2003
    - http://www.cert.org/summaries/CS-2003-02.html
12. CERT Summari CS-2003-03 - Septiembre 2003
    - http://www.cert.org/summaries/CS-2003-03.html
13. CERT Summari CS-2003-04 - Noviembre 2003
    - http://www.cert.org/summaries/CS-2003-04.html
14. Informe de IRIS-CERT presentado en la Jornadas Técnicas de RedIRIS 2003. Palma de Mallorca
    - http://www.rediris.es/cert/doc/reuniones/cord/jt2003/iris-cert-jt2003.pdf