Informe de incidentes de seguridad año 2004

cert@rediris.es

13 de enero de 2005

Índice

1. Introducción

Este informe de incidentes de seguridad pretende reflejar los aspectos de seguridad más relevantes detectados por el grupo de seguridad de RedIRIS, IRIS-CERT, durante el año 2004. Su objetivo, es el de informar detalladamente de estos 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 presentan en este informe algunos enlaces a los problemas más comunes, vulnerabilidades o gusanos detectados durante el año.

El presente documento, se publica en la Web de IRIS-CERT bajo http://www.rediris.es/cert/doc y junto a los informes de años posteriores. Además, se presenta en la lista de coordinación de seguridad

Durante el pasado año 2004, IRIS-CERT cambió la herramienta de gestión de incidencias que venía utilizando. En estos momentos, se hace uso del RTIR (*RT for Incident Response*), siguiendo la experiencia de otros equipos de seguridad europeos. En este contexto, IRIS-CERT, esta trabajando en un subgrupo de trabajo dentro del TF-CSIRT (*CSIRT Coordination For Europe*), para la incorporación de nuevos módulos y funcionalidades en la misma.

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 Toledo en Octubre de 2004, 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

Se presentan aquí un conjunto de datos aproximados, e información de los principales problemas de seguridad que hemos detectado a lo largo del año. En estas estadísticas solamente aparecen aquellos problemas de seguridad de los que hemos tenido noticia directa. En algunas ocasiones, no nos llega información del problema en cuestión, realizándose una gestión interna del mismo por parte de la institución.

Por otro lado, en muchas ocasiones, los responsables de las instituciones afiliadas a RedIRIS, aunque nos consta de que toman cartas en el asunto y adoptan las medidas adecuadas según el caso, no nos informan de la causa real del incidente. Esto hace, que no podamos actualizar la información relacionada con el mismo, influyendo en la exactitud y veracidad de estas estadísticas. Desde aquí instamos a todos los encargados de seguridad de las instituciones afiliadas a que, una vez analizado el problema, nos envíen un correo (manteniendo siempre el código de incidente para facilitar su gestión), con una breve descripción de los encontrado en la máquina y de la causa real del incidente (gusano, compromiso de root, virus, etc...). Ésto nos permitirá, no sólo proporcionar unas estadísticas más en consonancia con la realidad, sino tener una visión mucho más amplia de lo que está pasando en nuestra comunidad.

Dicho esto, durante el año 2004 podemos destacar los siguientes datos:

- El número de Incidentes atendidos por IRIS-CERT durante el año 2004 ha sido de 2682, teniendo en cuenta que:
  - De esos 2682, 830 corresponden a incidentes relacionados con Infracción de copyright [1], lo que supone un incremento del 177.5 %

[1] a 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, contabilizando pues estos incidentes tan sólo con fines estadísticos, por lo que debéis ser vosotros los que deis las explicaciones oportunas al origen de la denuncia.

con respecto al año anterior, confirmándose la tendencia de incremento de este tipo de incidentes en los utltimos años. En la mayoría de los casos, este tipo de ataques se debe a máquinas previamente comprometidas que están siendo usadas para estos fines ilítcitos (instalándose 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 así poder detectar posibles patrones de ataque y comportamiento.

- 44 de estos 2682 incidentes han sido dirigidos al buzón de consultas o *helpdesk* de IRIS-CERT.
- 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. En total, 72 incidentes. Ya sabéis que nuestra política ante este tipo de incidentes, como hemos comentado múltiples veces en los Grupos de Trabajo, es que nos limitamos 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. Tenemos que decir, que en la mayoría de los incidentes en los que la dirección de IRIS-CERT aparece como copia, se hacía referencia a actividad hostil originada desde máquinas de otros proveedores de Internet Españoles, y por tanto fuera de la comunidad IRIS.
- Está claro que la nueva herramienta de gestión que utilizamos nos permite realizar un análisis más fino de los incidentes tratados. Por ejemplo, nos permite determinar el número de incidentes que consideramos Informativos, esto es, que se refieren a IPs que no están dentro de nuestro ámbito de actuación (errores) o que no requieren ningún tipo de interacción por nuestra parte. De este tipo de incidentes hemos atendido 22 a lo largo del 2004.

Para realizar una comparativa con el año anterior, y quitando el número de incidentes referidos a los tipos anteriores, podríamos decir que el número de incidentes digamos reales.ªtendidos durante este año (sin

contar copyright, consultas, copia e informativos) sería de 1714, lo que supondría un incremento del 32.45 % con respecto al año pasado (se atendieron en 2003 un total de 1294 incidentes).

De estos 1714 incidentes, casi el 96 % se originaron dentro de la comunidad RedIRIS, el 3 % en máquinas de otros ISPs del dominio .es (puesto que IRIS-CERT proporciona soporte de coordinación de incidentes para el dominio .es), y el 1 % internacionalmente.

2.1. Evolución de los incidentes

heightwidthdepthdatos/evolucion.png

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 %
2004	1714	32.45 %

Nos parece interesante presentar en la figura siguiente la evolución de los incidentes relacionados con infracción de copyright en los últimos años, debido a su incremento progresivo.

heightwidthdepthdatos/evolucion-copy.png

Figura 2: Infracción de copyright

Las cifras detalladas son los siguientes:

Año	**Incidentes**	**Incremento**
2002	50	-
2003	299	177.5 %
2004	830	498 %

A continuación presentamos una gráfica en la que podemos ver la distribución de los incidentes atendidos por IRIS-CERT durante el año 2004 a lo largo de los diferentes meses.

heightwidthdepthdatos/evolucion-2004.png

Figura 3: Evolución de incidentes por meses

Los datos detallados son los siguientes:

Fecha	Total
2004/01	236
2004/02	267
2004/03	329
2004/04	320
2004/05	273
2004/06	206
2004/07	218
2004/08	149
2004/09	213
2004/10	152
2004/11	165
2004/12	154

Como podéis ver en la gráfica anterior, parece que en promedio a partir de Abril se produce un decremento de incidentes. Esto no quiere decir que los problemas de seguridad hayan disminuido (aunque efectivamente ha habido meses con una actividad más intensa que otros), sino que más bien tiene relación con el cambio de herramienta de gestión de incidentes que realizamos en Abril y la forma de contabilizar incidentes y de agrupar los mismos en la nueva herramienta.

Veamos a continuación los problemas de seguridad más significativos que hemos detectado en nuestra comunidad a lo largo de los meses del pasado año:

- **Enero** A principios del año 2004 se siguen detectando casos de escaneos al puerto 6129/tcp, utilizado por un programa de control remoto llamado Dameware, del que se publicó un fallo de seguridad ya en Diciembre de 2002. También se siguen recibiendo muchas denuncias de escaneos a los puertos de Netbios y a los del Directory Server de Microsoft, fundamentalmente debidos al Blaster (gusano aparecido en 2003) y a la vulnerabilidad en el DCOM de Microsoft, así como a puertos relacionados con vulnerabilidades ya conocidas durante el año pasado en el MS-SQL. Los escaneos a todos estos puertos, han sido generalizados durante todo el año 2004.
- **Febrero** Aparecen varios gusanos, entre ellos el MyDoom, el Bea-

gle, el DoomJuice, Netsky y el Welchia.D, así como variantes de los mismos. Por ejemplo, el caso del DoomJuice es curioso porque infecta máquinas previamente infectadas por el MyDoom, al aprovechar la puerta trasera dejada por este para expandirse. Podríamos decir, que el puerto estrella de este mes es el 3127/tcp, utilizado por diversos de estos gusanos, y por tanto, han sido los gusanos que utilizan dicho puerto los más vistos en nuestra comunidad.

- **Marzo** Tanto Marzo como Abril son meses problemáticos como se puede apreciar en la gráfica. A la actividad de los gusanos comentados anteriormente, y la aparición de nuevas variantes de los mismos, cabe destacar la aparición del troyano Phatbot que ha causado grandes problemas en bastantes instituciones de nuestra comunidad. El Phatbot es un IRC bot con características similares al Agobot, que realiza escaneos NetBios, y utiliza diversos métodos para su propagación (RPC DCOM, WebDav, puertas traseras de otros gusanos y Dameware). Las máquinas infectadas por este troyano, y controladas desde botnet, suelen ser utilizadas para ataques de DoS.
- **Abril** Sigue la línea del mes anterior, con muchas incidencias sobre todo de Phatbot. Cabe destacar la aparición de un exploit en el *Microsoft Private Communication Technology Protocol* (PCT) que se ejecuta sobre SSL (443/tcp). Este exploit abría una shell en el puerto 31337/tcp.
- **Mayo** Gran incidencia de escaneos al puerto 5000/tcp debido, por una parte, a su utilización por parte de dos gusanos (Kibuv y Bobox) para identificar Windows XP, y a la aparición de un fallo en el *Microsoft Windows Universal Plug a Play Service*. Durante el mes de Mayo aparece el gusano Sasser que aprovecha una vulnerabilidad en el *Windows Local Security Authority Service Server* (LSASS), y que genera múltiples problemas en algunas instituciones debido a un efecto colateral: el **escaneo de direcciones multicast**, produciéndose una avalancha de paquetes de registro de nuevas fuentes hacia los RPs.
- **Junio** Aparece un nuevo gusano llamado Dabber, que afecta a máquinas previamente infectadas por el Sasser, aprovechando una vulnerabilidad en el FTP dejado por dicho gusano en el puerto

5554/tcp. En Junio seguimos viendo escaneos al puerto 443/tcp (por la vulnerabilidad en el PCT), al 5000/tcp, mucho Sasser y Phatbot, y como viene siendo habitual durante todo el año escaneos netbios, microsoft-ds, Radmin (4899/tcp) y Dameware.

- **Julio** Lo más significativo de este mes, y que hace que las estadísticas aumenten ligeramente, es que empezamos a recibir muchas denuncias relacionadas con ataques de *Phishing*, tanto a través del buzón de abuse como del de cert. Estos incidentes son gestionados de forma conjunta por el CERT y el responsable de correo electrónico en nuestra comunidad
- **Agosto** A finales de Julio/Agosto aparece una herramienta que permite realizar ataques de fuerza bruta contra cuentas SSH. Los atacantes consiguen entrar en varios equipos, empleando posteriormente un exploit del núcleo de Linux en local para conseguir acceso como root, lo que les permite instalar diversos rootkit. El principal problema que nos encontramos durante los meses de verano es que en muchas instituciones, no solamente en las pequeñas, durante parte de las vacaciones la persona de contacto de seguridad no deja suplente, por lo que gran parte de los incidentes se retrasan y la respuesta (y por tanto, la resolución del problema) no es tan rápida como debiera.
- **Septiembre** No sólo en la comunidad académica, sino en la Internet Española, se detecta un incremento considerable de ataques debidos a diversos tipos de código malicioso: troyanos, gusanos y sobre todo aumento de botnets durante los meses de verano. Se trata de programas robot"que comprometen máquinas utilizando diversas vulnerabilidades y permiten crear redes de "zombie", es decir, máquinas controladas remotamente por IRC que seguramente serán utilizadas furtivamente con fines malintencionados, como por ejemplo lanzar ataques de DoS. El puerto más escaneados durante este mes siguen siendo el 22/tcp (ssh) como el mes anterior.
- **Octubre, Noviembre y Diciembre** Se sigue la tónica de meses anteriores, es decir, botnets, algunos gusanos, etc.. Cabe destacar, la aparición a finales de Diciembre de un nuevo gusano llamado Santy que utilizaba el popular buscador Google para infectar servidores Web que utilizaban una versión vulnerable de phpBB,

modificando sus páginas Web. También, a finales de Diciembre (que se mantiene todavía a principios de Enero) volvimos a detectar un incremento en las quejas relacionadas con escaneos y ataques de fuerza bruta contra cuentas SSH.

Para finalizar, y completar lo descrito con anterioridad, os mostramos la siguiente gráfica con una distribución de incidentes según nuestra taxonomía de alto nivel.

Figura 4: Incidentes por tipo según taxonomía

Como veis, existe un aplastante dominio de los ataques debidos a escaneos. Estamos convencidos que detrás de la mayoría de ellos se encuentra un problema mayor y por tanto la causa real del escaneo, por lo que os pedimos que si queréis que la información que os presentemos sea lo más veraz posible, nos contéis lo que realmente ha ocurrido o habéis encontrado, y no tan sólo contestéis con un simple *"Problema resuelto"* ;-).

2.2. Incidentes de SPAM 2004

Como sabéis, desde hace tiempo IRIS-CERT no se encarga de los incidentes relacionados con SPAM, ni con virus que utilizan exclusivamente el correo electrónico para su propagación. Este tipo de incidentes son atendidos por el responsable del correo electrónico en la comunidad.

Durante el 2004 podemos decir que el SPAM ha aumentado, sin embargo, han cambiado los mecanismos de distribución del mismo. Si hace unos años el principal canal de distribución del SPAM eran los servidores, es decir, la utilización de open-relays, lo que desde el 2003 se viene observando es que son muchos los malware que incluyen su propio motor SMTP. Por tanto, el problema del SPAM pasa de afectar de los servidores de correo (donde el problema es ya bien conocido y en general se ha hecho un gran esfuerzo para protegerlos) a los PCs de usuario. Por otro lado, durante el 2004 se han detectado varios

problemas de mail bombing producido por falsificación de cabeceras o direcciones "From:". Frente a estos nuevos problemas son varias las soluciones propuestas, que van desde promover el uso de filtros en salida en el puerto 25/tcp en las instituciones, hasta el uso de diversos enfoques e iniciativas como el SPF (*Sender Policy Framework*), AMTP (*Authenticated Mail Transfer Protocol*), RMX (*Reserve MX*), etc..

3. Links de interés

A continuación podéis encontrar algunos enlaces a documentos donde se describen algunos de los problemas más significativos detectados durante el año 2004.

1. MyDoom.A
   - http://www.symantec.com/region/mx/techsupp/avcenter/venc/data/la-w32.mydo
2. MyDoom Removal Tool (y enlaces a las diversas versiones de este gusano)
   - http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom@mm.rem
3. Doomjuice
   - http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.doomjuice.htm
4. Welchia
   - http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html
5. Welchia Removal Tool (y enlaces a las diversas versiones de este gusano)
   - http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.remo
6. Dabber
   - http://www.f-secure.com/v-decs/dabber.shtml
7. Sasser
   - http://www.kb.cert.org/vuls/id/586540
8. Santy
   - http://securityresponse.symantec.com/avcenter/venc/data/perl.santy.html
9. Beagle

- http://virusall.com/w32beagle$_a ll.html$

10. McAfee AVERT Stinger (Herramienta de eliminación de gusanos)
    - http://vil.nai.com/vil/stinger/
11. Phatbot
    - http://www.f-secure.com/v-descs/agobot$_f o.shtml$
12. Presentación sobre BotNets. Jornadas Técnicas 2004. Toledo
    - http://www.rediris.es/cert/doc/reuniones/cord/jt2004/botnets.pdf
13. Microsoft Private Communication Technology (PCT) Vulnerability Note
    - http://www.kb.cert.org/vuls/id/586540
14. Microsoft Windows Universal Plug and Play service (UpnP) Vulnerability
    - http://www.microsoft.com/technet/security/bulletin/MS01-059.mspx
15. Anti-Phishing Working Group
    - http://www.antiphishing.org/
16. SANS Top 20
    - http://www.sans.org/top20/
17. Informe de IRIS-CERT presentado en la Jornadas Técnicas de RedIRIS 2004. Toledo
    - http://www.rediris.es/cert/doc/reuniones/cord/jt2004/jt2004.pdf