Informe de incidentes de seguridad año 2006

cert@rediris.es

5 de febrero de 2007

Índice

1. Introducción

Como viene siendo habitual, mostramos en el siguiente documento lo acontecido, a nivel de seguridad, durante el año 2006 en la Red Académica y de Investigación Española (RedIRIS). Se muestran pues no sólo algunos números y estadísticas, sino también una descripción de los problemas más comunes, así como enlaces a sitios que aporten más información y mecanismos para paliar o solucionar dichos problemas. Además, presentamos las tendencias, que desde nuestro punto de vista protagonizarán el 2007.

La intención de este documento además, es la de recopilar las tendencias y problemas más significativos sufridos durante el pasado año en toda la comunidad Internet, con el fin de poder comparar estos resultados con lo detectado en nuestra comunidad, denotando sus peculiaridades, cosa que nos ayudará a enfrentarnos de forma más efectiva a los problemas que nos depara el futuro.

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

Recomendamos la lectura del informe de operación presentado por IRIS-CERT en las pasadas Jornadas Técnicas de RedIRIS, celebradas en Granada en Noviembre de 2006, disponible aquí. En él, se incluye además información sobre otras actividades y foros en los que participa el equipo de seguridad, así como enlaces a otras presentaciones de interés general.

Estamos abiertos a cualquier sugerencia que nos permita mejorar la calidad del presente informe. Para ello, pulsad aquí, y enviad vuestra sugerencias.

2. Estadísticas

Como remarcamos todos los años, el presente informe recoge tan sólo aquellos problemas de seguridad de los que hemos tenido noticia directa en el CERT de RedIRIS, bien por notificaciones externas o internas, o por los sistemas de detección que hemos implementado, y a los que hemos dedicado una especial atención durante el pasado año, intentando ser lo más proactivos posible.

La clasificación de los incidentes dentro de la taxonomía de alto nivel que tenemos definida, se realiza a partir de la información que nos hacen llegar los contactos técnicos en las instituciones afiliadas, por lo que su exactitud depende absolutamente de cuan exactos son a la hora de describir el problema sufrido y las medidas adoptadas para su resolución. Por lo tanto, para que este informe sea lo más veraz posible, necesitamos la colaboración de los encargados de seguridad de las instituciones afiliadas, instándoos qa que, cuando se recibe una notificación de un incidente de seguridad desde el CERT, una vez analizado el problema, se envíe un correo (manteniendo siempre el código de incidente para facilitar su gestión), con una descripción detallada de las causas que originaron el problema, cualquier evidencia encontrada en la máquina comprometida, las medidas adoptadas para la resolución del problema, así como cualquier otra información que se considere de interés.

A pesar de reiterar este punto año tras año, en los informe y en las reuniones de coordinación que organizamos, son muchos los incidentes de los que no se recibe respuesta alguna. Para mejorar el servicio y la calidad de la información que proporcionamos, una nueva funcionalidad que incorporará la próxima versión del RTIR (*Request Tracker for Incident Response*) [1] nos permitirá clasificar los incidentes en función de las causas que han conducido al cierre de los mismos.

Antes de comenzar arrojando cifras sobre las estadísticas obtenidas durante el año 2006, nos gustaría aclarar la forma en la que el RTIR, nues-

[1] El RTIR es la herramienta que desde mediados de 2004 viene utilizando el CERT parea la gestión de los incidentes de seguridad.

tra herramienta de gestión, organiza la información. Esta aclaración, permitirá entender mejor los datos mostrados a continuación.

Para lo que nos interesa en este documento, el RTIR trabaja con 3 tipos de entidades:

- *Incident Report*. Cualquier notificación que se recibe en los buzones del CERT (una vez eliminado el SPAM).
- *Investigation*. Investigaciones lanzadas a partir de los *Incident Report* que permiten enviar una notificación al responsable del origen del problema.
- *Incident*. Entidad superior que agrupa todos los *Incident Reports* e *Investigations* relativas a un mismo problema (normalmente una misma IP).

2.1. Cifras para el año 2006

El año 2006 arroja los siguientes números:

- El número de *Incident Reports* recibidos durante el 2006 ha sido de 3661, de los cuales, 1729 corresponden a *Incident Reports* procedentes de los sistemas de alerta implantados a lo largo del presente año por los miembros del CERT.
- El número total de Incidentes se eleva a **1974**, de los cuales:
  - 45 Incidentes corresponden el buzón abuse *AbuseDesk*. Se trata de problemas relacionados con Open Proxies [2].
  - 1117 has sido generados por nuestros sistemas de alerta:
    - De esos 1117, en 53 de los casos se han recibido además denuncias procedentes de otras fuentes, y en 28 además se han recibido denuncias para RedIRIS.
    - 134 de esos 1117, correspondían a máquinas infectadas dentro de la comunidad RedIRIS.

[2] El buzón abuse se empezó a gestionar utilizando la herramienta RTIR a partir de Noviembre 2006.

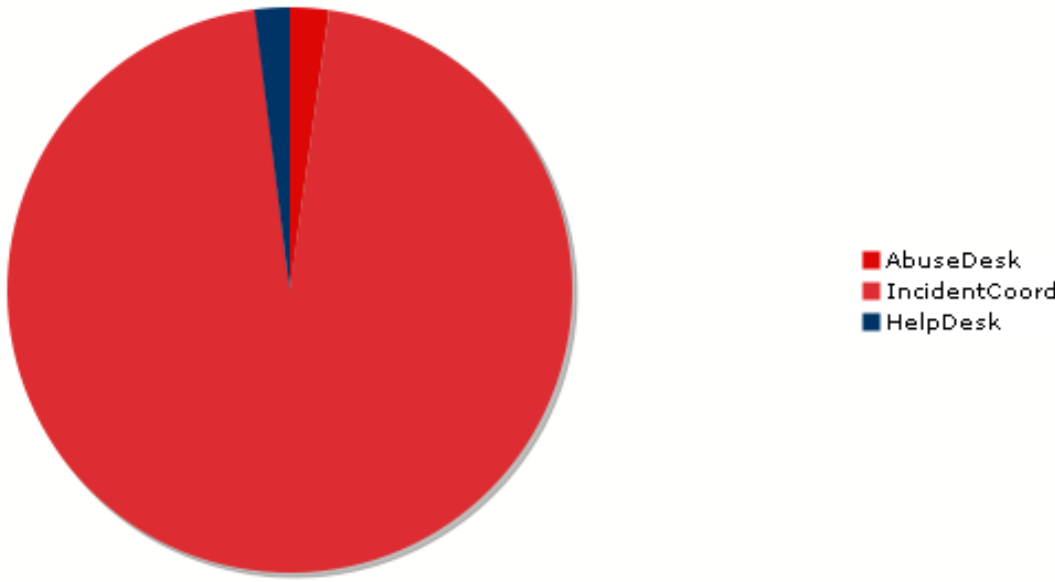

Figura 1: Clasificación en función al tipo de problema recibido en nuestros buzones

- 37 Incidentes tenían como destino el buzón de consultas o *Help-Desk* 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 71.
- 48 Incidentes has sido Informativos [3].
- Del total de Incidentes, de 686 (correspondientes tanto a la comunidad como a fuera de la comunidad) no hemos recibido ningún tipo de respuesta, lo que supone un 30.91 % más que en el año 2005 (524). Como hemos comentado antes, este punto resta calidad al servicio y a los informes aquí mostrados al no poder dar

[3]Que se refieren a IPs que no están dentro de nuestro ámbito de actuación o casos en los que no se requiere ningún tipo de interacción por nuestra parte.

información veraz al 100 %.

Como viene siendo habitual, para poder comparar con el año anterior, y quitando los incidentes correspondientes a *Helpdesk*, *AbuseDesk*, Informativos y Copia, durante el 2006 se atendieron **1773** incidentes reales, lo que supone un 42 % más que durante el año 2005 (1248).

Durante los últimos Grupos de Trabajo celebrados en Granada en el contexto de las JJTT06 comentamos que el número de denuncias recibidas (estábamos hablando de Noviembre de 2006) era menor que en el mismo periodo del año anterior. Las causas esgrimidas para explicar este decremento eran:

- Los patrones de ataque han cambiado. En los últimos años estamos asistiendo a ataques más silenciosos e inteligentes, por ende más difíciles de detectar. Atrás han quedado los ataques masivos de algunos gusanos que en muchos casos causaron verdaderos problemas en muchas de nuestras instituciones. Hay que dejar claro, que esto no significa que nuestra red sea más segura, muy al contrario, se ha incrementado el número de equipos comprometidos y que forman parte de redes de bots [4]. Además según Secunia el número de vulnerabilidades que su equipo ha descubierto a lo largo del 2006 asciende a 75, lo que supone un incremento considerable respecto a las descubiertas en el año 2005 (53) [5]

Si al final del año, hemos obtenido un incremento respecto al año anterior ha sido (42 %) es, como veremos a continuación, gracias al esfuerzo que hemos dedicado durante los últimos meses del 2006 a realizar una detección automática de posibles máquinas comprometidas dentro y fuera de nuestra comunidad, mediante el uso de Darknets, Monitorización de flujos de Red (detección de anomalías y escaneos) y LogSurfer (para la detección de intentos de inyección de código HTTP, y ataques SSH).

2.2. Evolución de los incidentes a lo largo de los años

En el siguiente gráfico se muestra la evolución de los incidentes de seguridad desde el año 1999.

[4] http://www.ciphertrust.com/resources/statistics/zombie.php

[5] Más información disponible en http://secunia.com/gfx/Secunia$_Y ear$ – $end_R eport_2 006.pdf.@, habiendo publicado además un total de 5000 advisories de seguridad durante ese año. Lo que no sque a$

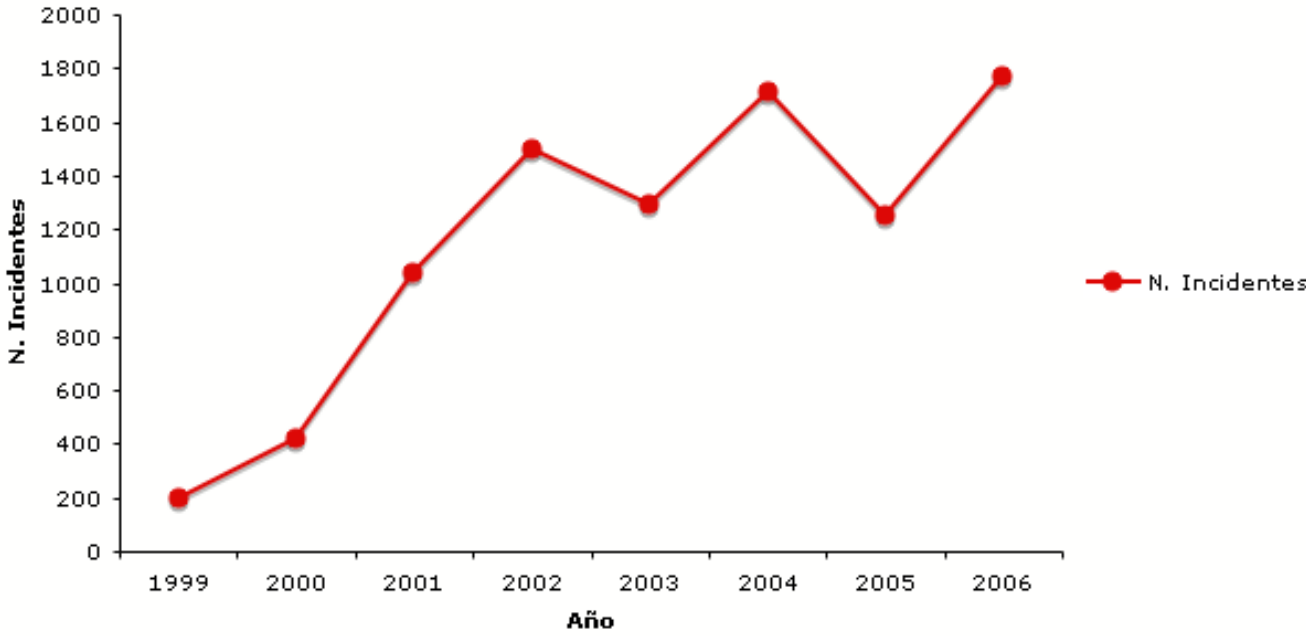

Figura 2: Evolución de incidentes por años

Las cifras detalladas son los siguientes [7]:

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 %
2005	1248	-27.48 %
2006	1773	42 %

[7]Estas cifras corresponden a los incidentes reales, una vez eliminados los correspondientes a consultas, copia, informativos y abuse.

Vamos a aprovechar para hacer un poco de historia, enumerando los cambios en tendencias que a lo largo de los años se han ido detectando [8].

Durante el año 1999, los ataques eran menos sofisticados, caracterizados por la utilización de herramientas automatizadas tipo nmap, mscan etc. En el 2000 aparecen los ataques de DDoS (Denegación de Servicio Distribuidos) y algunas herramientas basadas en este tipo de ataques (TFN, Trinoo, etc..). Son famosos los ataques de DDoS contra portales como eBuy o Amazon, así como problemas de saturación en algunas NRENs. Reaparecen los gusanos, con escasa carga dañina, así como algunos gusanos multiplataforma (popor ejemplo el sadmin). H Hasta este momento, los ataques estaban dirigidos fundamentalmente a entornos Linux, especialmente servidores, para aprovechar al máximo la capacidad de proceso y las líneas de comunicaciones dedicadas a los mismos.

En 2001 aparecen los primeros gusanos que afectan a plataformas Windows, como los ya famosos CodeRed y Nimda, manteniéndose los servidores como principal objetivo de los atacantes. Durante 2002 la tendencia sigue siendo la misma, sin embargo, comenzamos a asistir a una mayor incidencia de problemas en máquinas de usuarios finales, algo que como sabemos y sufrimos, se sigue produciendo en la actualidad. Este cambio de tendencia se explicaba en su momento por la existencia de una mayor concienciación de los administradores de los problemas de seguridad que afectan a los servidores, unida a la escasa cultura de actualización de los equipos finales. Además, durante ese año 2002, diversas vulnerabilidades en programas de correo electrónico propiciaron la aparición de gusanos que se trasmitían utilizando este medio y que utilizan las máquinas comprometidas para enviar SPAM.

El año 2003 quedará en la memoria como el año de los gusanos de propagación masiva (y rápida!) como el Blaster (los equipos se volvían a infectar mientras que se actualizaban) y Slammer. Además, el SPAM causado por Virus y Gusanos incorporan la novedad de incluir su propio motor SMTP.

El 2004 no hace más que aumentar los problemas descritos para el año 2003; se confirma la tendencia de ataques a plataformas comunes y usuarios domésticos, aparecen los primeros casos de uso ilícito de los equipos atacados mediante la instalación de repositorios warez y dlos problemas de infracción

[8]Para más información sobre lo los datos concretos de cada año, visite los informes disponibles aquí.

de copyright, surgen gusanos con código altamente cambiante, y aparecen los problemas de Phishing (que suponen un verdadero campo de batalla en la actualidad) y las primeras redes de máquinas zombies (botnets) de las que hablaremos en la próxima sección.

El 2005 constituye la antesala de lo que se ha visto confirmado durante el año 2006: Phishing, botnets, ataques de fuerza bruta ssh y problemas de inyección de código HTML debido fundamentalmente a la existencia de versiones vulnerables de PHP. También empezamos a ver que los ataques comienzan a ser menos masivos, más dirigidos y más difíciles de detectar.

En el año 2006, objetivo del presente informe, se repiten los problemas que ya se detectaron en el año anterior, destacando entre ellos:

- Intentos de acceso/ataques de fuerza bruta SSH, debidos a la utilización de frases de paso débiles por parte de los usuarios, y en los que los atacantes, en la mayoría de las ocasiones, no intentan comprometer el equipo, sino tan sólo propagar el acceso.

- Compromiso de sistemas debidos a vulnerabilidades en los sistemas PHP instalados, que han tenido tantísimos éxito debido a la proliferación de Blogs [9], Wikis y Foros que utilizan este tipo de sistemas. Una vez estos sitios Web bajo control, se utilizan para lanzar una gran variedad de ataques como Phishing, SPAM (sobre Phishing), uso de troyanos bancarios, etc...

- Red de máquinas zombies (botnets). Las máquinas zombies son el origen de gran parte de las quejas que recibimos. De hecho, según algunos artículos de prensa e informes de otras organizaciones, España está a la cabeza de máquinas zombies que pertenecen a estas redes de botnets en el mundo. Estas redes son cada vez más complejas y difíciles de detectar, siendo utilizadas para lanzar ataques muy variados. Quizá lo más destacado es que empieza a verse que aunque el protocolo de control más empleado sigue siendo el IRC, cada vez se ven más redes de bots que utilizan el HTTP como protocolo de control, para saltarse los filtros que muchos sitios implementan para controlar este tipo de redes.

- En el año 2006 se ha hecho amplio uso de un nuevo tipo de exploits (sobre todo para productos Microsoft Office) que ofrece una gran ven-

[9] El fenomeno blog se considera uno de los fenómenos más importantes en Internet en los últimos tiempos.

taja para los atacantes. Se trata de los llamados *0-day-exploits*, nombre que se le da a los exploits que no han salido a la luz y que los propios hackers se hacen con el objetivo concreto de obtener el control de una maquina.

- Durante el año pasado han aumentado los problemas relacionados con el spyware y el robo de identidad. Los ataques de Phishing que incorporar nuevos patrones de ataques han conseguido gran protagonismo durante este año.

- Por último, se ha producido una modificación en los objetivos perseguidos por los atacantes. Se detectan cada vez más ataques dirigidos, con motivaciones políticas, religiosas o con afán de lucro. Hemos pasado del ansia por aprender, al ansia por poseer y hacer valer a la fuerza nuestras ideas.

En un artículo publicado recientemente en Internet [10] se afirmaba que parece que en estos momentos estamos viviendo una situación bastante contradictoria, en la que estamos sufriendo el mayor número de amenazas e incidentes de la historia, aunque la percepción general es que estamos más seguros que en años anteriores. Las causas esgrimidas para tal afirmación eran:

- El cambio en la estrategia de los atacantes (de infecciones masivas a infecciones más silenciosas que pasan desapercibidas).

- Malware menos perceptible que oculta mejor su actividad.

- Todavía no se ha llevado a cabo un cambio de filosofía en los sistemas de detección: de detección de patrones de ataques (firmas de ataques) a detección de anomalías.

Sin duda alguna, esta percepción es completamente aplicable a la Red Académica y de Investigación Española.

2.3. Algunos datos más

A continuación se muestra la proporción de incidentes que tienen su origen en la misma.

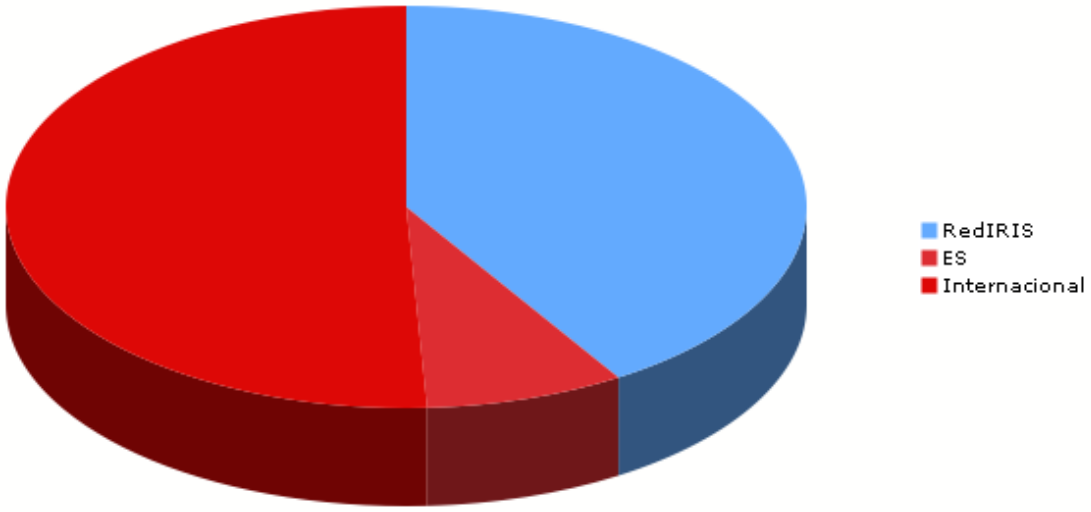

Figura 3: Clasificación según origen de la incidencia

Como puede verse en la gráfica anterior, algo ha cambiado con respecto a años anteriores. Si en los informes de años anteriores el número de incidentes, como cabe esperar, originados en nuestra comunidad eran los más frecuentes, durante el 2006 este porcentaje se ha decrementando significativamente pasando de un 93 % en el año 2005 a un 41 % en el 2006. Al mismo tiempo, durante este año se ha producido un espectacular incremento del número de incidentes originados internacionalmente (pasando de un 1 % a un 51 %). ¿Significan estos datos que nuestra comunidad es cada vez más segura y el mundo exterior cada vez más inseguro?. Nada más lejos de la realidad. Este incremento/decremento espectacular se debe al esfuerzo dedicado durante este año a implantar sistemas de alarma, que en un principio no estaban destinados a detectar tan sólo actividad maliciosa en máquinas de nuestra comunidad, sino en la Internet en general. Esto ha hecho, que sobre todo al principio de poner en marcha estos sistemas de monitorización

[10]Disculpad si no incluimos la fuente, pero no poseemos el dato concreto de la fuente en cuestión.

(fundamentalmente los destinados a detectar ataques de inyección de código), se detectaran muchos más casos originados fuera de nuestra comunidad que dentro. De todas formas, el avisar a los responsables de estas máquinas externas tiene gran valor, puesto que podemos atajar el problema en el mismo origen.

A continuación se muestra una gráfica que muestra la clasificación según el origen de la incidencia a lo largo de los años.

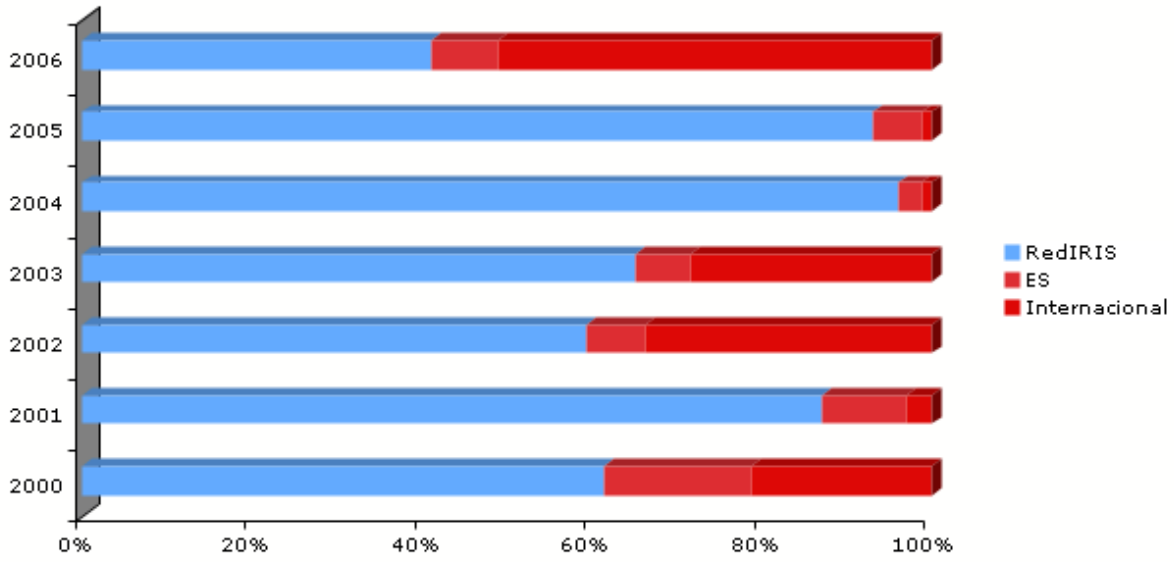

Figura 4: Clasificación según origen de la incidencia a lo largo de los años

La siguiente gráfica muestra la distribución de incidentes atendidos por el equipo en los distintos meses del 2006.

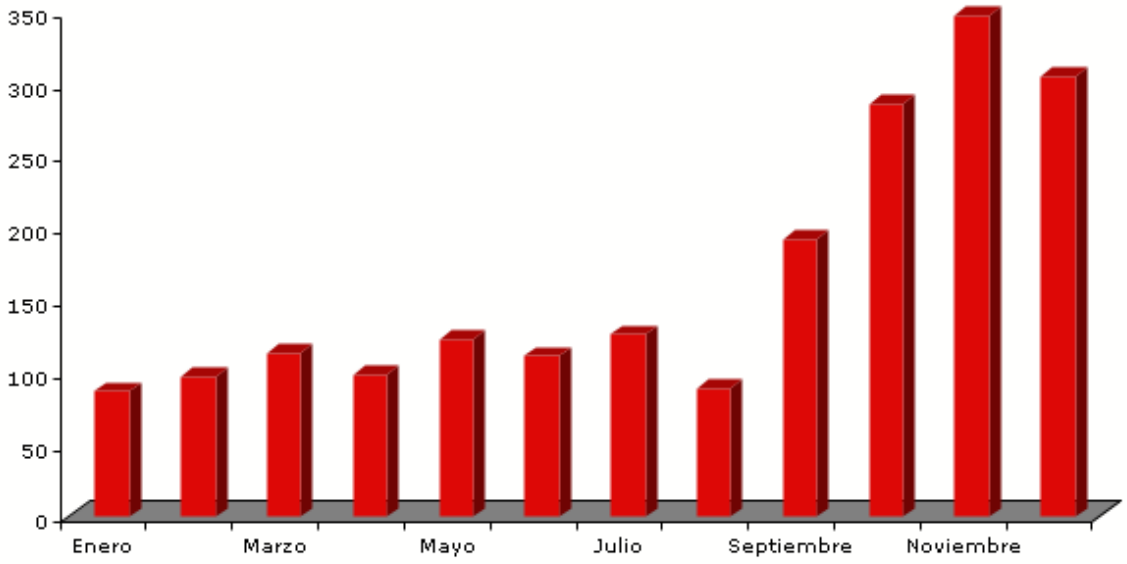

Figura 5: Evolución de incidentes por meses

Los datos detallados son los siguientes:

Fecha	**Total**
2006/01	87
2006/02	97
2006/03	113
2006/04	98
2006/05	123
2006/06	111
2006/07	126
2006/08	89
2006/09	192
2006/10	286
2006/11	347
2006/12	305

Como se puede ver en la gráfica/tabla anterior, es a partir de Septiembre de 2006 cuando se ponen en marcha diversos sistemas de detección automática, lo que tiene su efecto directo en el número de incidentes atendidos diariamente. El gran reto para el año que viene es el de automatizar el procesamiento de este tipo de incidentes para que requieran el mínimo de intervención por parte de un operador.

El pequeño descenso del último mes del año quizá tenga su explicación debido a periodo vacacional, en el que muchos ordenadores de nuestras instituciones afiliadas se mantienen infectados, pero no son detectados hasta que no son encendidos después de las vacaciones de Navidad. Ésto último se ha experimentado en muchas Universidades de nuestra comunidad (infecciones controladas durante las vacaciones de Navidad que se han convertido en verdaderas locuras tras "la vuelta al cole").

A modo ilustrativo, mostramos a continuación una gráfica que muestra la evolución de los incidentes mes a mes a lo largo de los año.

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

Como puede apreciarse, y siguiendo la norma de lo que ocurre año tras año, 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"*.

También cabe destacar el incremento en el número de incidentes correspondientes a Uso no Autorizado. Este incremento se debe a uno de nuestros sistemas de detección automática, concretamente el LogSurfer. Los incidentes clasificados como Uso no Autorizado corresponde, en su mayoría, a intentos de inyección de código Web.

Por último, aparecen de nuevo incidentes clasificados como Virus (que no aparecían en las gráficas de los años anteriores). Concretamente 7 incidentes. Se ha clasificado así porque es la respuesta que hemos tenido de vosotros *"La máquina tenía un virus y ha sido limpiada"*.

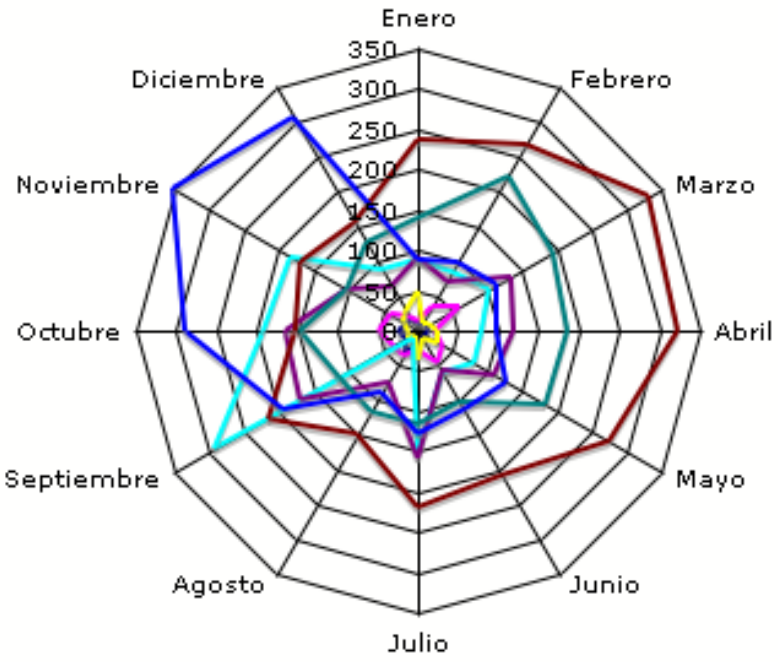

Figura 6: Evolución de incidentes por meses a lo largo de los años

2.4. El SPAM durante el 2006

En los problemas de seguridad empieza a tener más peso la componente delictiva y de Ingeniería Social que la tecnológica. Siempre que una nueva tecnología global ha aparecido, los responsables del malware han buscado la forma de aprovecharla con fines dañinos y/o criminales, y este año 2006 posiblemente haya sido donde mas se ha notado, siendo el phishing el problema socialmente más impactante. Los problemas de seguridad en el correo electrónico durante el 2006 han sido proporcionales al crecimiento exponencial de PCs comprometidos (zombies) y botnets. Esto ha facilitado la posibilidad de hacer distribuciones masivas por correo electrónico provocando un aumento de los usos ilegales bajo el nombre de spam como: troyanos, phishing, spyware, extorsiones etc.

La propia tecnología del correo electrónico y sus protocolos asociados deriva el problema de la seguridad al eslabón mas débil de la cadena: el

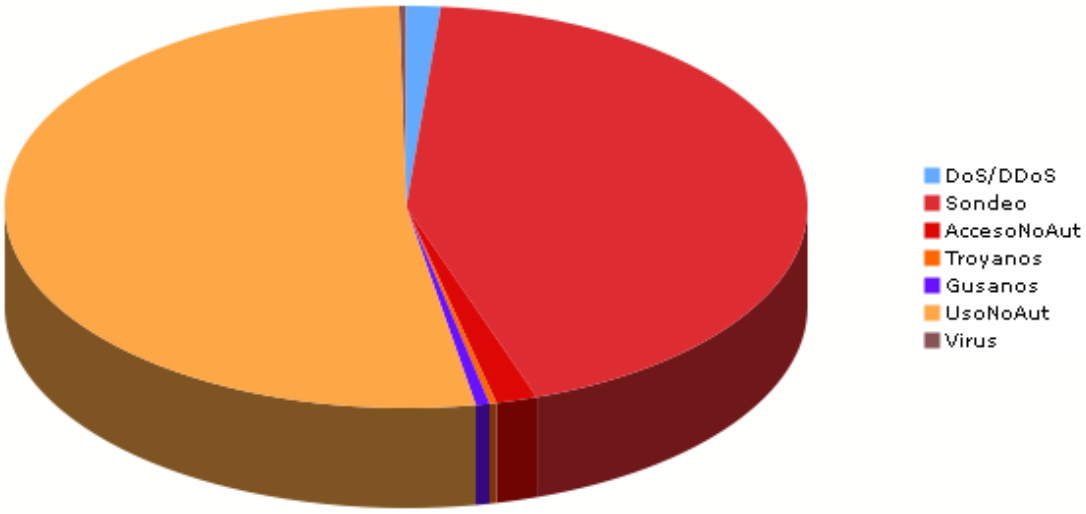

Figura 7: Incidentes por tipo según taxonomía

usuario. Los usuarios son numerosos, generalmente muy vulnerables y pocas veces parcheados, y por tanto hacia cuyo bolsillo se han dirigido muchos de los ataques. Considero que el correo electrónico (spam) está llegando al punto de inflexión para que empiece a remitir el impacto del spam. La presión de las técnicas antispam, la futura aprobación durante el año 2007 por parte del IETF de nuevos estándares de autenticación del emisor como DKIM y SPF, la distribución de un Windows más seguro o el movimiento de usuarios hacia otros sistemas operativos como Linux y Mac, provocaran que los criminales se muevan y aprovechen otras tecnologías a medida que se vayan estabilizando, convergiendo y sean de uso extendido como por ejemplo las plataformas de 64-bit, malware en vídeos, los teléfonos móviles o sobre todo la tecnología VoIP.

Según los datos recogidos en 2006 por SAnet (Red de Sensores AntiSPam) en RedIRIS, se ha considero spam al 60 % de las conexiones SMTP con destino a direcciones IP de la Comunidad RedIRIS. Este tráfico SMTP, gestionado por los servidores de correo, se ha incrementado notablemente a pesar de las medidas antispam implementadas en los últimos años. Un porcentaje muy alto de este tráfico (50-60 %) es tráfico oscuro que suele ser

procesado por los servidores. Este tráfico es ocasionado por conexiones procedentes de IPs comprometidas con algún tipo de malware que implementa capacidad de instalar su propio motor SMTP, lo cual se emplea para difundir spam, virus, ataques de diccionario (*Directory Harvest Attacks*) , denegación de Servicio (DoS) o mensajes a destinatarios no existentes. La mayor parte de las soluciones de seguridad en el correo electrónico no tienen en cuenta este tráfico indeseado a través del puerto 25 que es aceptado, analizado y rechazado con la consiguiente usurpación de los recursos necesarios para su procesamiento.

Uno de los hechos mas sintomáticos ha sido la tendencia a la baja de los virus y sus epidemias que tanto daño provocaron en el pasado, con un incremento de malware mas peligroso.

En 2006 RedIRIS, con el objetivo de mejorar el servicio de correo electrónico, comenzó dos iniciativas que se desplegarán a lo largo del 2007. Estas iniciativas son: Spanish Whitelisting y unas Recomendaciones Comunes de Tráfico SMTP entrante. Ambas iniciativas pretende ser exportadas al resto de operadores españoles para mejorar el intercambio de tráfico SMTP. La *Whitelisting* pretende evitar el bloqueo de determinadas IPs incluidas en la *whitelisting*. En este listado están todas las Estafetas de la Comunidad RedIRIS, así como las de muchos IPS españoles. Más información disponible aquí.

La otra iniciativa pretende adoptar medidas comunes por parte de la Comunidad RedIRIS para abordar el grave problema del spam. El objetivo de estas recomendaciones es definir un marco común consensuado para toda la Comunidad RedIRIS. Estas Recomendaciones fueron aprobadas en la Reunión IRIS-MAIL/25 (Noviembre 2006, Granada) y están pensadas como pautas a seguir por los Servicios de Correo Electrónico de instituciones de la comunidad académica española. Más información disponible aquí.

3. Vulnerabilidades y Tendencias

3.1. Principales problemas durante 2006

- El 2006 empezó como terminó 2005, con una grave vulnerabilidad en la forma en la que Windows maneja los archivos Windows Media File (.WMF), que afectaba a todas las versiones de Windows. La forma de explotar este fallo, tan sólo visualizando una imagen, y la contro-

vertida respuesta de Microsoft en cuanto a la distribución del parche correspondiente, generó un gran revuelo y expectación en el mundillo, obligando a Microsoft a romper su ciclo de actualizaciones mensuales. Más información aquí.

- Aumenta el parque de ordenadores Macintosh (con su MAC OS X de Apple), y con él la aparición de los primeros troyanos (teóricos) que afectan a este Sistema Operativo, lo que hace abrir el debate sobre la seguridad/inseguridad de este SO. Más información aquí.

- Aparecen vulnerabilidades importantes en sistemas ampliamente utilizados como sendmail y BIND que obligan a los administradores ha actualizar gran cantidad de servidores. http://www.sendmail.org/ y http://www.isc.org/bind/

- Gran incidencia de vulnerabilidades en diversos productos (browsers, servidores de correo, media players, etc..) que permiten el acceso (no autorizado) remoto a los sistemas, con la finalidad de acceder al contenido, programas, información confidencial, etc... Según Secunia se ha incrementado en un 25 % con respecto al año pasado las vulnerabilidades de este tipo. De todos los sistemas afectados, los productos de Microsoft aparecen como los más afectados por este tipo de vulnerabilidades.

- Múltiples vulnerabilidades críticas en productos Microsoft que afectan sobre todo a su Navegador más utilizado y la suite Office [11]. Con la proliferación de estas vulnerabilidades, aparecen también los ya comentado *0-day-exploits*[12].

- Aparecen los primeros virus que aprovechan, no sólo el correo sino también los teléfonos móviles para distribuirse (*SMiShing*).

- Las cuotas de fraude bancario online (*Phishing*) durante el 2006 siguen incrementándose, suponiendo una verdadera epidemia, tanto en su versión de sitios Web fraudulentos [13], como el envío de correos que

[11] Un total de 10 vulnerabilidades fueron descubiertas en varios productos Microsoft vía *0-day attacks*.

[12] Aunque no son exclusivos de esta plataforma.

[13] Según el Anti-Phinshing Working Group el número de sitios fraudulentos se van incrementando más de 8 veces de año en año.

parecen ser enviados desde nuestras entidades bancarias apuntando a sitios controlados por los phishers. El uso de troyanos bancarios también se dispara. Además, los phisher tienden a seguir una aproximación más dirigida al negocio, escogiendo víctimas que ellos perciben como más lucrativas.

- Aparecen los primeros troyanos bancarios diseñados para capturar la información a partir de los teclados virtuales.
- Aparece el *vishing*, que no es más que Phishing sobre voz IP.
- El cibercrimen se ha convertido en una realidad, con ataques dirigidos con fines políticos, económicos, religiosos, etc..
- Gran incidencia de vulnerabilidades en diversos productos (browsers, servidores de correo, media players, etc..) que permiten el acceso (no autorizado) remoto a los sistemas, con la finalidad de acceder al contenido, programas, información confidencial, etc.., en los mismos . Según Secunia se ha incrementado en un 25 % con respecto al año pasado las vulnerabilidades de este tipo. De todos los sistemas afectados, los productos de Microsoft aparecen como los de mayor incidencia en este tipo de vulnerabilidades.
- Los gusanos de distribución masiva dejan el paso a otras formas más sutiles de infección como por ejemplo, el uso de sitios maliciosos para aprovechar vulnerabilidades conocidas en los navegadores más populares para infectar las máquinas que los visitan. El uso de técnicas de ocultación basadas en rootkits se hace muy común.
-

3.2. Predicciones para 2007

- Una mayor concienciación por parte de los administradores de seguridad está haciendo que los servicios de correo sean cada vez más seguros, lo que fuerza a encontrar nuevas formas de infectar máquinas a los ratios acostumbrados. El mecanismo escogido parece ser el Web, debido a la proliferación de sitios Web sobre todo basados en tecnologías Cross Site Scripting y Web 2.0. Otro ratio de infección importante lo supondrán

los correos que en lugar de adjuntar Virus o similares, incluyan enlaces a sitios maliciosos, que contienen troyanos y spyware.

- Otra razón por la que los Ataques Web han tomado durante el 2006 y seguirán tomando gran protagonismo durante el 2007, es la gran proliferación de blogs, Wikis y webs participativas en general. Lo que se ha dado en llamar Web 2.0 no es una tecnología, sino una forma de concebir la Web de forma completamente diferente. El uso de la tecnología Ajax [14] *(Asynchronous Javascript and XML)*, acarrea nuevos problemas listos para ser aprovechados (El código fuente está a la vista, desde una página Web se pueden manipular las variables de otra página Web, etc..). Además, según diversos estudios, el 80 % de los servidores de Internet son vulnerables a ataque de CSS *(Cross Site Scripting)*, siendo por lo general ataques difíciles de detectar e independientes de la plataforma. En 2007 asistiremos a cada vez más ataques Web, utilizando ataques de CSS o aprovechando tecnologías emergentes como Ajax o la Web 2.0.

- Uso de técnicas de ocultación basadas en rootkits con fines lucrativos.

- Uso de robo de identidad/datos o adware con fines lucrativos.

- Desarrollo de troyanos incrustados en películas o imágenes, que permitan saltarse los filtros y antivirus, o que simplemente se utilicen para distribuir código malicioso entre usuarios de una forma rápida.

- El Phishing seguirá siendo una amenaza seria durante el 2007. Previsiblemente, a los ya conocidos vectores de ataque (junto a los nuevos aparecidos en el 2006; mensajes de phishing que incluyen un número de teléfono, *vishing*, etc..) se añadirán otros con el fin de aprovechar al máximo las ventajas lucrativas que reportan. Sin embargo, puede que el Phishing vaya perdiendo fuerza durante el próximo año para dejar paso a técnicas de ingeniería social más interesantes y novedosas.

- Muchas fuentes ven a las botnets como principal amenaza durante el 2007, y coincidimos con esta afirmación. Estas redes de máquinas zombies resultan muy atractivas a manos de cibercriminales ya que concentran mucho poder para realizar gran cantidad de ataques (muy potentes) en Internet.

[14] Que permite que se refresquen pequeñas partes de una página Web.

- Algunas fuentes predicen un incremento en el descubrimiento de vulnerabilidades en redes sociales tipo LinkedIn, My Space, You Tube, Second Life, etc... Este tipo de vulnerabilidades se han visto ya en el 2006 y han tenido un fuerte impacto mediatico. Debido a que son ampliamente utilizadas por el público, el descubrimiento y explotación de una vulnerabilidad en este tipo de redes podría ocasionar un gran impacto. Ante este tipo de vulnerabilidades, el uso de gusanos Web se hará muy generalizado.
- Y a principios del 2007 llega el esperado Windows Vista .....