

Contents

1	Introducción	1
2	Estadísticas	2
2.1	Cifras para el año 2007	2
2.2	Evolución de los incidentes a lo largo de los años	3
2.3	Algunos datos más	7
2.4	El SPAM durante el 2007	11
3	Tendencias	13
4	Links de interés	15

1 Introducción

Un año más, publicamos el resumen de seguridad de incidencias relativo a la Red Académica y de Investigación Española (RedIRIS) para el año 2007.

El siguiente documento está dividido en varias secciones que comprenden desde un análisis de las estadísticas sobre los incidentes atendidos por el Equipo de Seguridad de RedIRIS (IRIS-CERT) durante el año 2007, con comparaciones con los datos de años anteriores, hasta una descripción de los problemas más comunes detectados (incluyendo un capítulo específico sobre el SPAM y los problemas de seguridad del correo electrónico).

Incluimos así mismo, un apartado dedicado a describir cuales podrían ser los problemas más significativos para el próximo año 2008.

Para finalizar, proponemos un listado de enlaces a sitios relevantes donde poder ampliar la información sobre determinados temas que puedan ser de utilidad para el lector.

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 se anuncia en la lista de coordinación de seguridad de RedIRIS, IRIS-CERT.

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

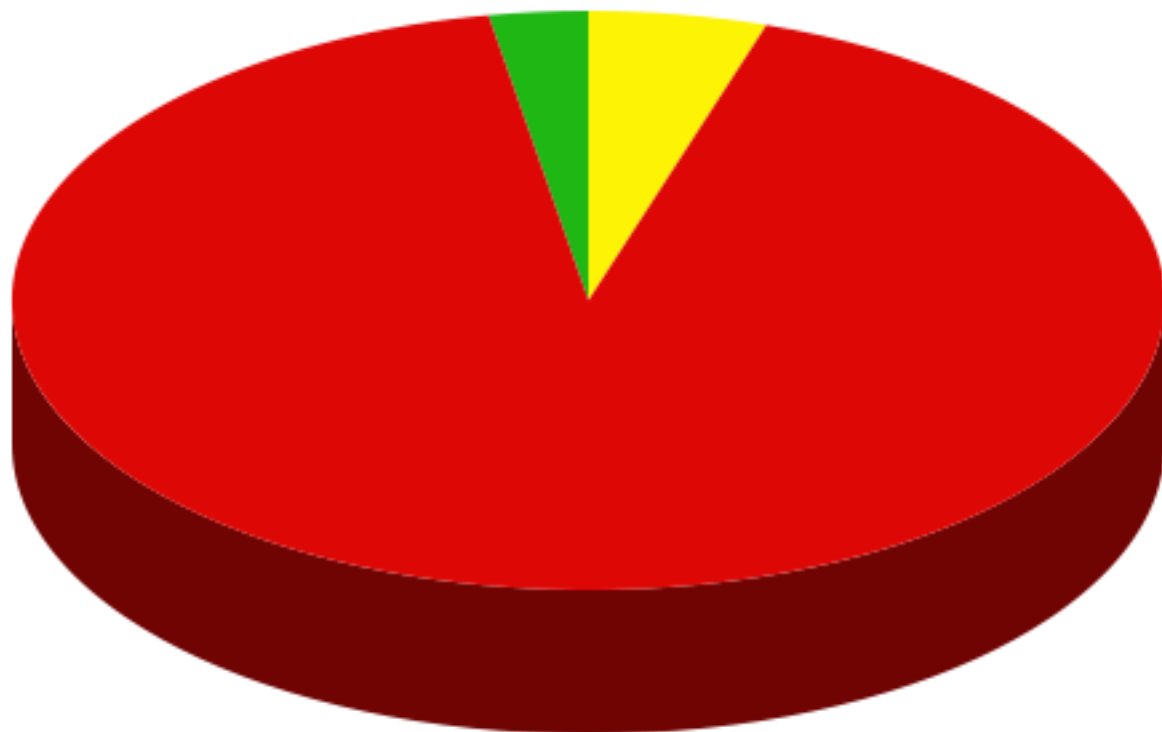
2 Estadísticas

Como remarcamos año tras año, 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 e internas, o por los sistemas de detección automática que hemos implantado.

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 sean éstos 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.

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, o el típico *“El problema ha sido solucionado”*.

2.1 Cifras para el año 2007



Durante el 2007 se han recibido un total de **6329 *Incidents Reports***¹, de los cuales 1797 corresponden a *Incident Reports* procedentes de los sis-

¹Cualquier información que se recibe en los buzones del CERT (una vez eliminado el SPAM).

temas de detección automáticos implantados por el CERT (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)). Esos 1797 *Incidents Reports* procedentes de los sistemas de alerta, han generado un total de 1067 Incidentes² en nuestro sistema³, de los cuales 612 hacían referencia exclusivamente a máquinas infectadas dentro de nuestra comunidad. De esos 612, en 96 ocasiones se han recibido además algún tipo de notificación externa que confirmaba el problema.

El número total de Incidentes atendidos por IRIS-CERT durante el 2007 se eleva a 3473, de los cuales:

- 169 Incidentes corresponden al buzón abuse *AbuseDesk*. Se trata pues de problemas relacionados con abusos en correo electrónico, fundamentalmente problemas relacionados con Open Proxies⁴.
- 36 Incidentes tenían como destino el buzón de consultas o *HelpDesk* de IRIS-CERT.
- 65 Incidentes han sido Informativos⁵.
- 254 Incidentes se han recibido en el buzón del CERT como copia (Cc:). Ante este tipo de Incidente, el equipo no actúa directamente, manteniéndose atento a la información que se recibe y contrastando ésta con nuestras propias fuentes.

Del total de incidentes (3473) , no se ha recibido respuesta alguna para 1239 casos (correspondientes tanto a máquinas comprometidas dentro de la comunidad como fuera de la misma). Esto supone aproximadamente un 80% más que en el año 2006 (686). De esos 1239 Incidentes sin respuesta, 833 eran Incidentes sin respuesta a problemas que se localizaban en nuestra comunidad. Como podréis imaginar, estas cifras de Incidentes sin resolución no hacen más que restar calidad y veracidad a los informes que aquí os presentamos. Otra vez más os pedimos vuestra colaboración para que una

²Entidad superior que agrupa a todos los *Incidents Reports* e *Investigations* relativas a un mismo problema (normalmente a una misma IP).

³RTIR <http://bestpractical.com/rtir/>

⁴El buzón abuse se empezó a gestionar utilizando la herramienta RTIR a partir de Noviembre 2006.

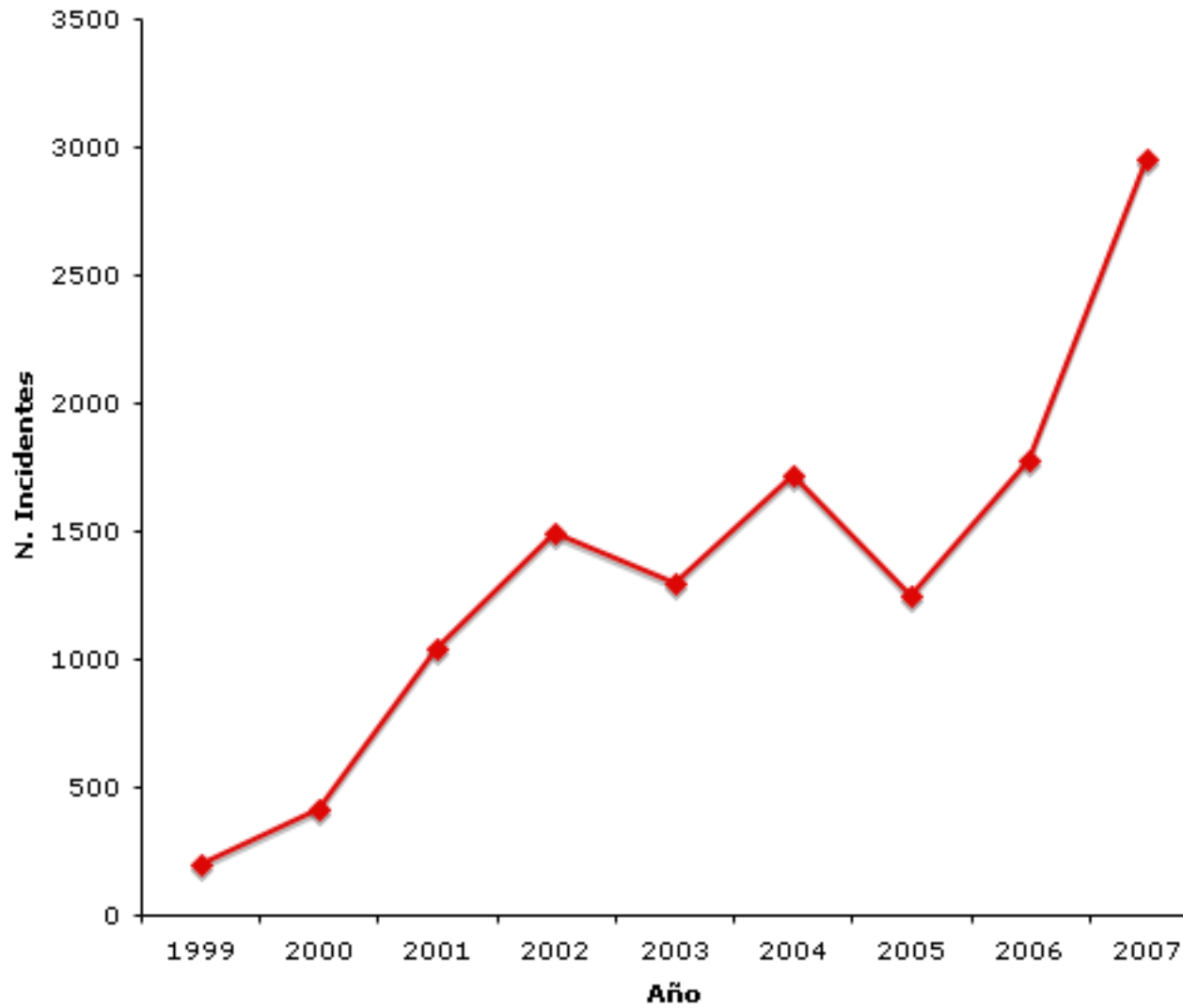
⁵Que se refieren a IPs que no están dentro de nuestro ámbito de actuación o casos en los que no se requiere ningún tipo de interacción por nuestra parte.

vez analizado el problema por vuestra parte nos paséis toda la información que arrojan vuestras investigaciones para que actualicemos nuestros registros y sistemas de estadísticas.

Como viene siendo habitual, para poder comparar con los años anteriores y quitando los incidentes correspondientes a *Helpdesk*, *AbuseDesk*, Informativos y Copia, durante el 2007 se atendieron **2949 incidentes reales**, lo que supone un **66.32% más que durante el año 2006** (1773).

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 a lo largo de los años desde el año 1999.



Las cifras detalladas son los siguientes ⁶:

⁶Estas cifras corresponden a los incidentes reales, una vez eliminados los correspondientes a consultas, copia, informativos y abuse.

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%
2007	2949	66.32%

Durante el año 2007, seguimos en la línea de lo que ya comentábamos el año pasado:

- Escaneos indiscriminados de puertos, en busca de máquinas vulnerables. De los escaneos de puertos, se sigue manteniendo como uno de los más frecuentes, como ocurría en años anteriores, los intentos de acceso/ataques de fuerza bruta SSH.
- El Web se establece definitivamente como el primer vector de ataque para intentar infectar a víctimas vulnerables (vulnerabilidades en los sistemas PHP instalados, y errores de programación y falta de concienciación de los programadores Web, vulnerabilidades conocidas en los navegadores más utilizados, inyección de código SQL, XSS, etc.). Una vez bajo el control de los atacantes, estos sitios son utilizados para lanzar otro tipo de ataques, fundamentalmente Phishing y uso de troyanos bancarios.
 - La aparición de la Web 2.0, como una segunda generación de aplicaciones web dinámicas e interactivas donde el usuario tiene mayor protagonismo y participación, frente a las webs estáticas tradicionales donde el usuario era un receptor pasivo, ha hecho que en los últimos años proliferen blogs, wikis y webs participativas que son un reclamo para los atacantes.
 - Aparecen herramientas especializadas como el MPack⁷ para controlar y automatizar ataques Web. Se trata de una aplicación basada

⁷MPack se vendía en foros underground de Rusia a precios que oscilaban entre los 500\$ y 1000\$.

en PHP que se ejecuta sobre un servidor comprometido, y que incluye diferentes exploits que se pueden utilizar para comprometer a las víctimas en función al software específico que estén ejecutando. El método más habitual para hacer que los usuarios accedan al servidor comprometido es mediante el uso de IFRAMES en el código HTML que apuntan a dicho servidor MPack, incrustados en otros servidores Web también comprometidos.

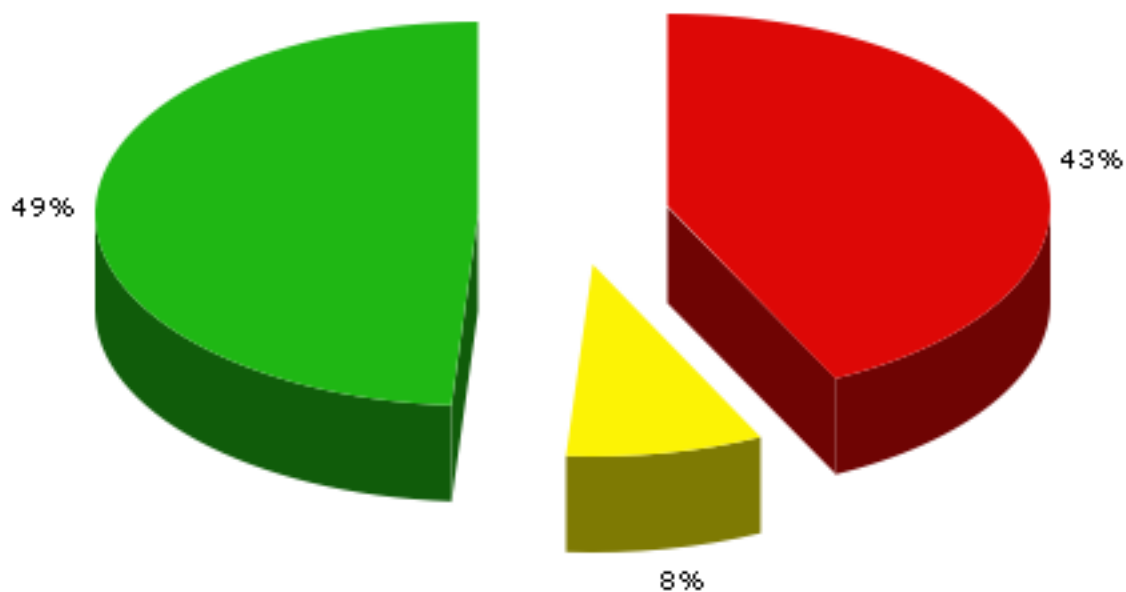
- Los ataques de Phishing y otros tipos de fraude on-line, han seguido teniendo un gran protagonismo durante el año 2007, y debido a que resulta un mecanismo relativamente sencillo y lucrativo para los atacantes. No se espera que este tipo de estafas vayan en decremento en los próximos años.
 - Durante el año 2007 se han detectado diversos casos de phishing dirigidos específicamente a entidades y bancos españoles, como fue el caso de la Agencia Tributaria a principios de año, y los ataques de Phishing contra entidades financieras españolas mediante un kit específico, en el que estaban involucrados los principales bancos y cajas de este país, y que no sólo simulaba la página Web del banco, sino que también intentaba infectar a las víctimas que visitaban la página a través de un Javascript y dependiendo del navegador del visitante.
- El número de máquinas “zombies” y de redes de bots no hace nada más que aumentar durante este último año, y con ellas los ataques que desde las redes se lanzan (SPAM, DDoS, fraude on-line etc.). Las redes de bots van evolucionando y siendo cada vez más complejas (por ejemplo las redes Fast-Flux). Se utilizan nuevos métodos de infección (se calcula que el 60% de los exploits relacionados con botnes son exploits de navegadores) y nuevos usos delictivos de las mismas. Como ya comentábamos en nuestro informe del año pasado, cada vez son más las redes de bots que utilizan el HTTP y sistemas de control no centralizados (similares a las redes P2P⁸) como protocolos de control para saltarse los filtros que muchos sitios implementan para evitar las tradicionales redes que utilizan el IRC como protocolo de control. También cada

⁸Como el caso de Storm Worm del que hablaremos más adelante.

vez más están operadas no verdaderas redes criminales perfectamente organizadas.

- Surge una nueva generación de malware (que algunos han dado por llamar Malware 2.0) , de carácter altamente cambiante y que utiliza técnicas automáticas para ofuscar las variantes y dificultar así la identificación mediante firmas del espécimen por parte de las casas antivirus.
 - El mejor exponente de este Malware 2.0 sería el Storm Worm, cuyas primeras variantes aparecieron en el mes de Enero, y que causó estragos en Internet propagándose a una velocidad de vértigo.
- Como comentábamos ya el año pasado, el patrón de ataque sigue siendo más dirigido, inteligente y silencioso, con algún tipo de trasfondo (económico, religioso, político o simplemente al ansia de poseer, etc..).
 - Por citar algunos casos a nivel mundial de ataques dirigidos y con fines políticos/económicos, destacamos el Ataques contra sitios Web del Gobierno de Estonia , o Ataque Web Europeo, a gran escala que se produjo en Junio, utilizando precisamente el MPack.

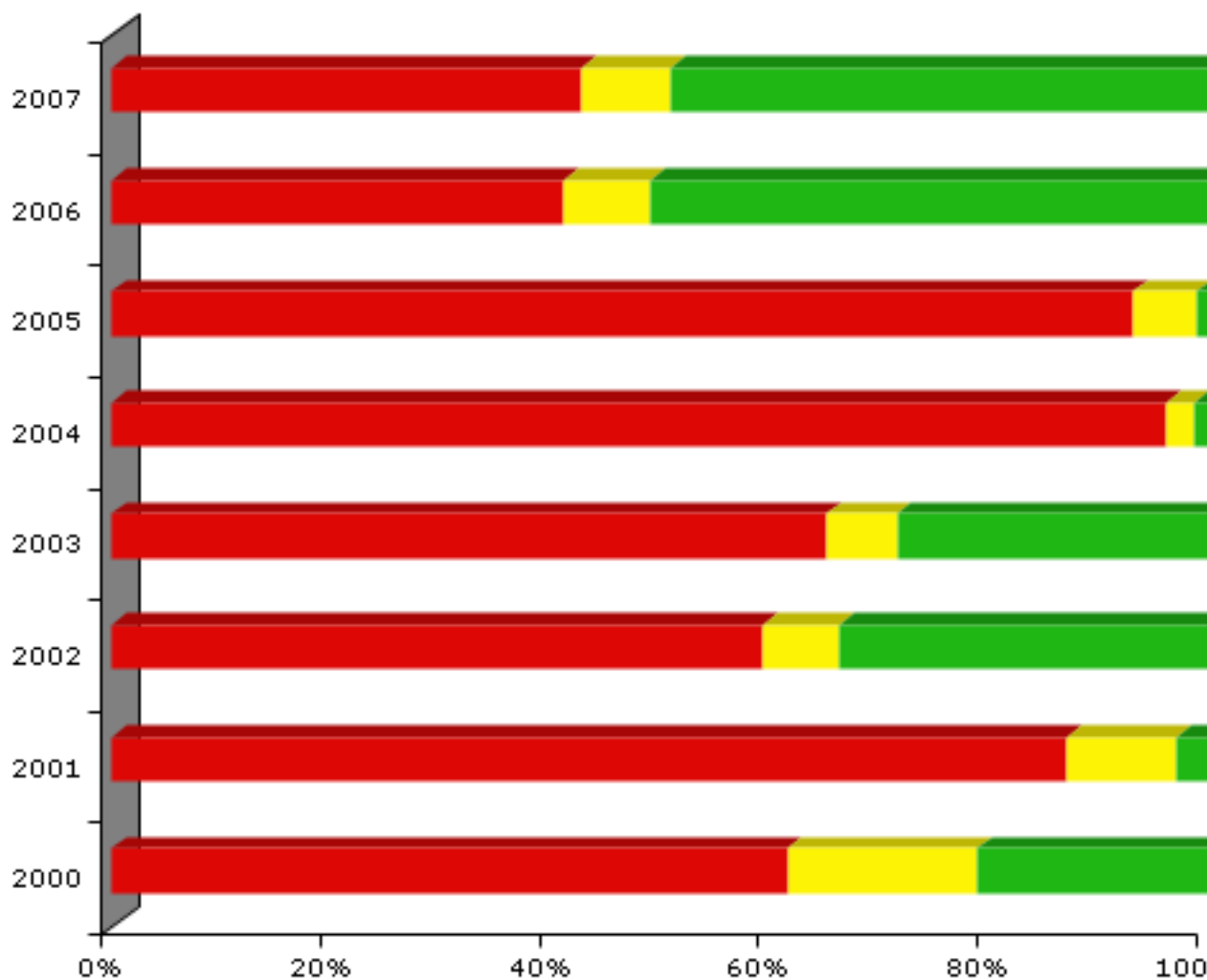
2.3 Algunos datos más



Como vemos en la gráfica anterior, y como ya comentábamos en el Informe del año 2006, el porcentaje de incidentes originados en nuestra comunidad se mantiene en el ratio del año pasado (de un 41% en 2006 a un 43% en el 2007). También se mantiene el ratio de los incidentes originados internacionalmente (49% del total), que junto al 8% de incidentes originados en máquinas de ISPs Españoles deben su incremento a los sistemas de monitorización implantados,

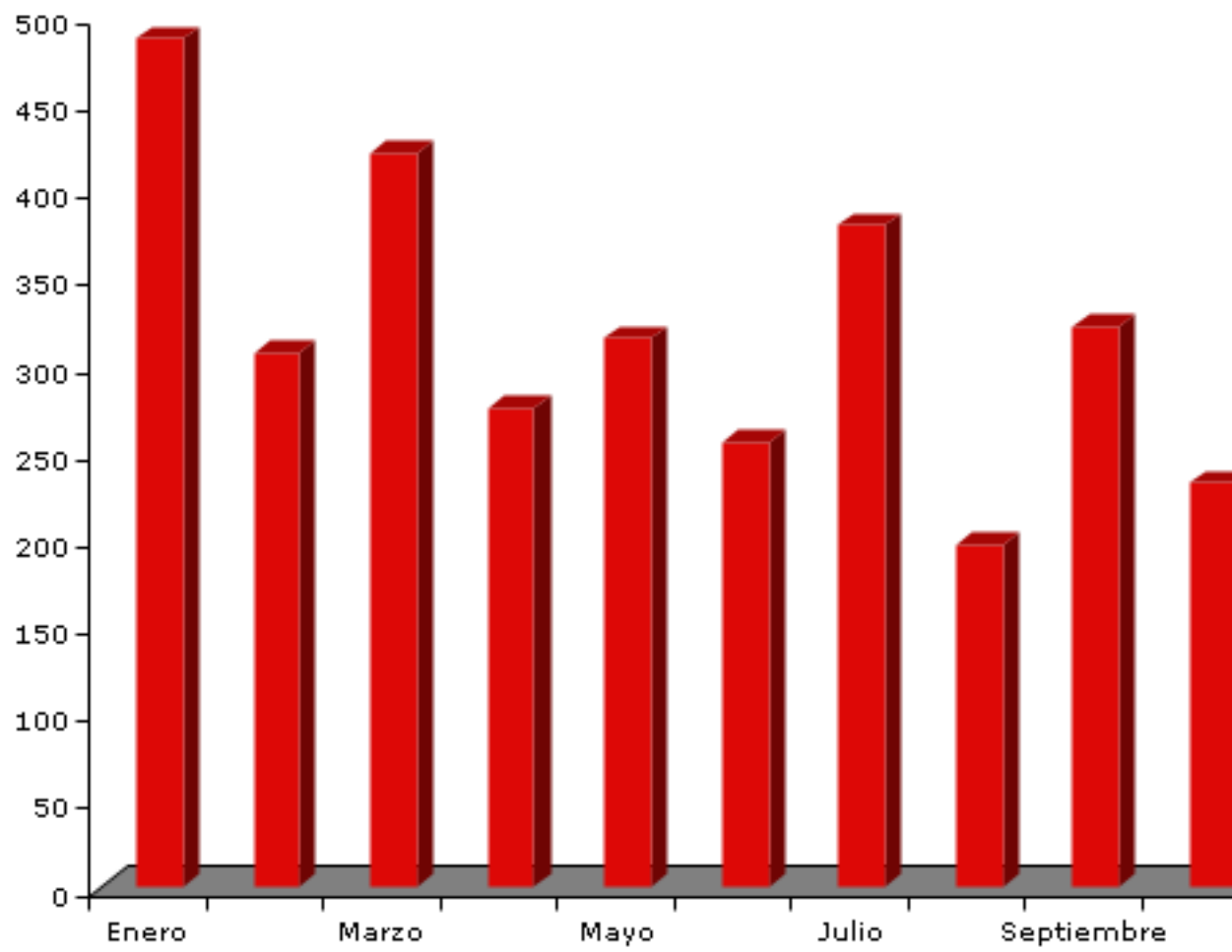
que no se limitan a detectar actividad maliciosa en nuestra comunidad sino también en Internet en general (fundamentalmente ataques de inyección de código Web).

A continuación se plasma una gráfica donde se muestra la clasificación según el origen de la incidencia a lo largo de los años, donde se ve más claramente esta variación en origen que comentamos en el párrafo anterior.



La siguiente gráfica muestra la distribución de los incidentes por meses a lo largo del año 2007.

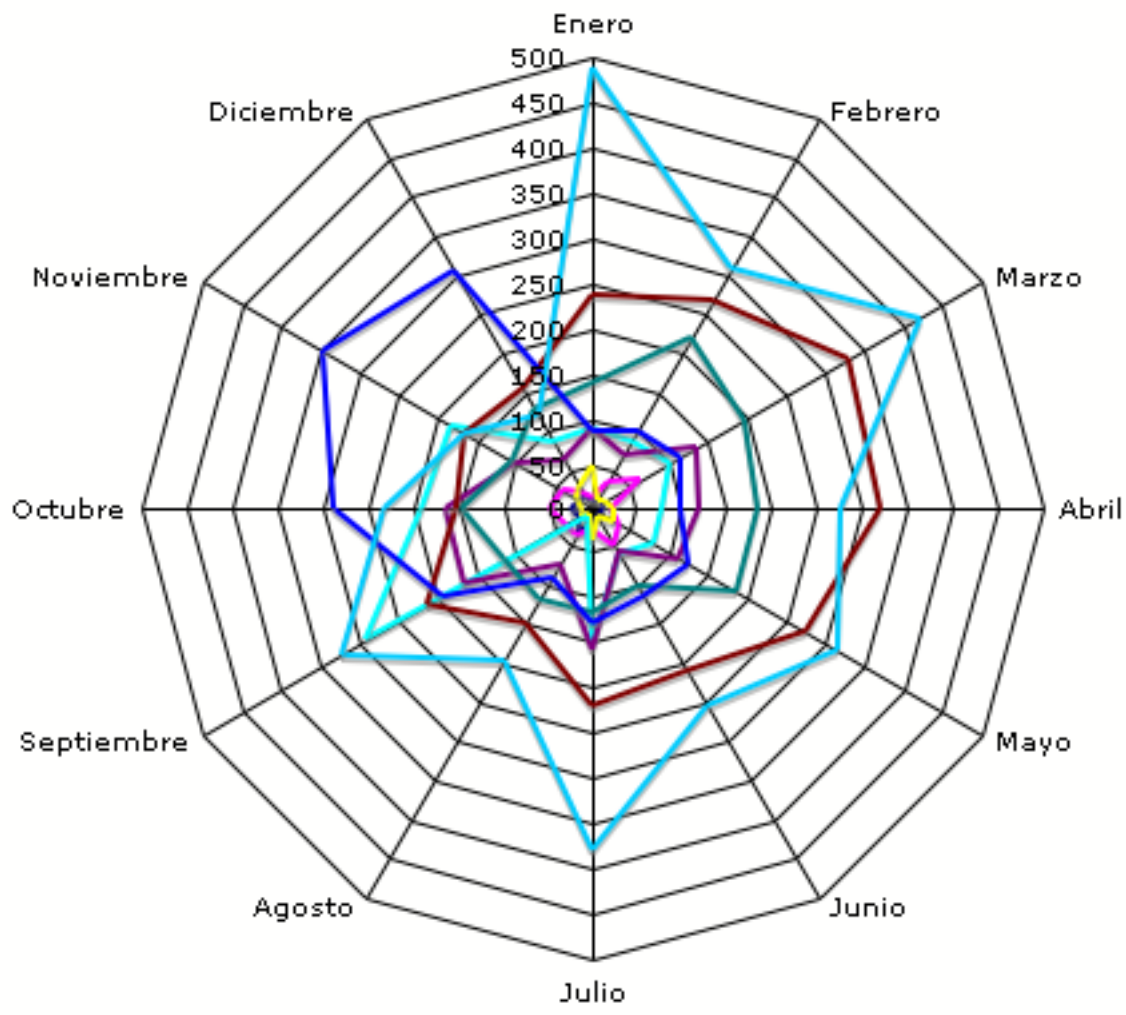
Evolucion por Meses en 2007



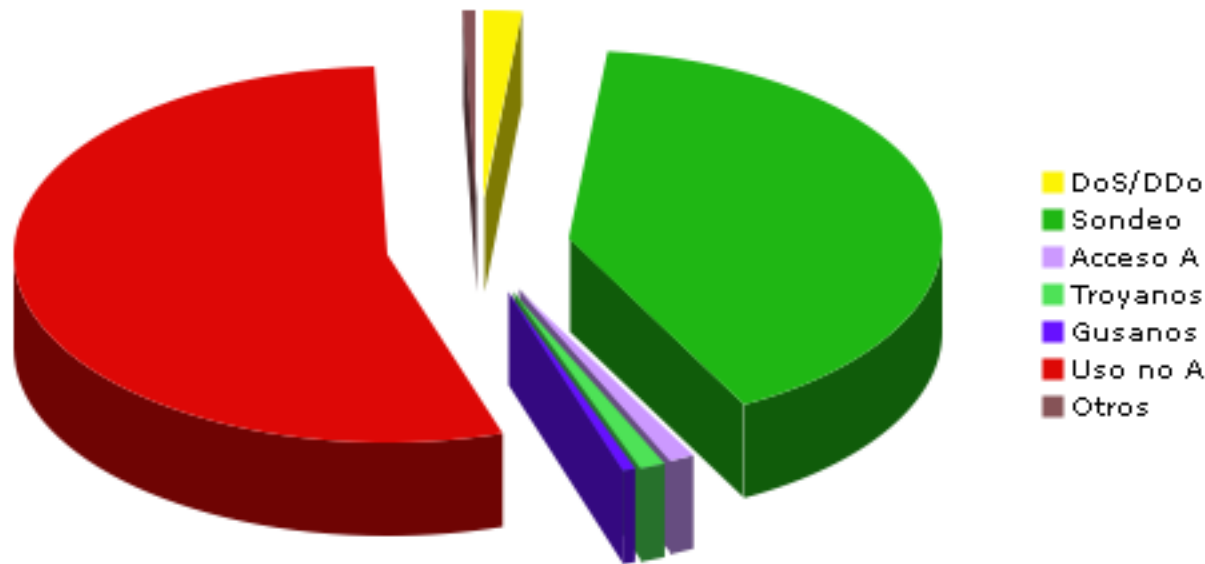
Los datos son los siguientes:

Fecha	Total
2007/01	487
2007/02	307
2007/03	421
2007/04	275
2007/05	315
2007/06	255
2007/07	380
2007/08	196
2007/09	322
2007/10	232
2007/11	165
2007/12	118

A modo ilustrativo, mostramos a continuación una gráfica que muestra la evolución de los incidentes por meses a lo largo de los años.



Para finalizar, mostramos una gráfica con la distribución de incidentes según la taxonomía de alto nivel que manejamos.



Como sigue siendo habitual, los escaneos siguen teniendo gran protagonismo (la mayoría de los casos se trata de problemas mayores de toda índole, pero la falta de información por vuestra parte nos hace englobarlos en este apartado de sondeos generales).

También es elevado el número de incidentes clasificados como “Uso no Autorizado”, que corresponden en su mayoría a casos de Phishing albergados

en máquinas de ISPs Españoles y de problemas relacionados con inyección de código Web.

2.4 El SPAM durante el 2007

Durante mucho tiempo el término spam se ha definido como “la distribución masiva de correo electrónico no deseado”, es decir, como un problema que afectaba exclusivamente a los buzones de los usuarios. Sin embargo, en la actualidad supone un serio problema para las propias infraestructuras de servidores. Durante los últimos años el spam se ha consolidado como el canal más efectivo para llevar a cabo actividades de ingeniería social maliciosa. Los objetivos vienen siendo la propagación de gusanos a través de enlaces web y adjuntos para capturar nuevas maquinas (zombies) y poder llevar a cabo las diferentes actividades delictivas en la red: ataques DoS, campañas de phishing, e-marketing, etc. Es por tanto el spam uno de los mejores detectores de maquinas comprometidas (zombies) que si bien son usadas para campañas de spam pueden ser utilizadas para cualquier otro tipo de a mas gran escala.

Durante el año 2007 se han visto incrementados los esfuerzos para mejorar las campañas de spam intentando que los mensajes fueran cada mas convincentes, con el objetivo de incitar a la descarga de adjuntos o enlaces web. También destacar los continuos esfuerzos de los spammers para actualizar las direcciones de correo insertadas en las bases de datos con oleadas de “mensajes vacíos” para comprobar si las direcciones eran o no correctas. También cabe destacar en este apartado los ataques a portales de redes sociales tipo Myspace con el objetivo de disponer de información de los usuarios de forma mas perfilada con el objetivo de lanzar campañas de spam mas segmentadas.

Se ha detectado, como método de dispersión de gusanos en el spam, una reducción del uso de adjuntos en los mensajes de spam y un aumento de la inserción de enlaces web con direcciones falsificadas. Por el contrario, y curiosamente, podríamos destacar la aparición de adjuntos comprometidos en los correos tipo Adobe Acrobat PDF para intentar evadir los filtros anti-spam de los servidores. También aparecieron otros formatos como Microsoft Excel, Word, ZIP y MP3, aunque las oleadas de spam con estos formatos fueron reducidas ya que sólo duraron los meses de verano y a finales de año prácticamente desapareció.

En 2006 los niveles de trafico SMTP basura rondaba el 85%. Durante el 2007 estos niveles han llegado a superar el 90% de todas las transacciones SMTP. Este incremento ha sido provocado por el Storm Worm, especializado

en la creación de botnes y que se estima comprometió unas 8 millones de maquinas. Estas botnets fueron usadas para enviar spam, crear sitios de phishing y lanzar ataques DOS como los producidos contra las páginas web del gobierno de Estonia.

Para finalizar comentar que los sistemas de reputación identifican si una IP está o no comprometida. Estas listas se pueden consultar a través de DNSB para bloquear gran cantidad de spam. En concreto el 85% del spam es rechazado por estos sistemas de reputación. Para protegerse de estos mecanismos, los nuevos gusanos consultan las listas publicas de reputación y eliminan de sus redes las IP dadas de alta para mejorar la efectividad de la distribución. Es por eso que las listas de reputación públicas pueden disminuir su efectividad.

3 Tendencias

Creemos que el apartado Predicciones para 2007 que escribíamos en el informe para el año 2007, coincide con la situación que hemos vivido este año.

Creemos que 2008 seguirá en la misma línea (gran número de máquinas zombies que lanzan diversidad de ataques, dirigidos y con fines lucrativos en muchas ocasiones. Ataques a aplicaciones Web, Phishing, troyanos bancarios y otros tipos de fraude on-line, vishing, etc..).

Si los ataques se han criminalizado, es de esperar que en los próximos años se deba prestar una atención especial a la protección de la infraestructura crítica. La amenaza ahora son los ataques masivos para tomar control de los principales sistemas de misión crítica de un estado como son la banca central, servicios públicos, servicios de emergencia, etc..

Los Servicios Web seguirán siendo el punto de mira de ataques. Los gusanos y otro tipo de malware altamente cambiante, más complicado en su concepción y con inteligencia para discernir el tipo de vulnerabilidad a explotar en la víctima también serán habituales durante el próximo año. También deberemos estar atentos a los ataques dirigidos a redes sociales tipo MySpace, LinkedIn, YouTube etc.

A finales del año 2007 se empezó a hablar en algunos artículos del Phishing 2.0, como una nueva forma de ataque phishing utilizando servidores DNS maliciosos. Se trataría de modificar la configuración DNS de las máquinas infectadas (normalmente utilizando malware basado en Web) para que redireccionen las peticiones DNS a ese o esos servidores maliciosos. En la mayoría

de los casos las víctimas serán redireccionadas a sitios legítimos, pero en ciertas ocasiones será redireccionadas a sitios maliciosos de Phishing. Como el ataque se realiza a nivel DNS, los software antiphishing no detectarán este tipo de ataques. El artículo al que hacemos referencia, pronostica así mismo que los ataques DNS lanzados desde sitios Web 2.0 serán más y más corrientes a lo largo del próximo año 2008.

En otro orden de cosas, el HoneyNet Project en uno de sus *Know Your Enemy Whitepapers* publicado el pasado año 2007, *Known Your Enemy: Fast-Flux Service Networks*, habla de una interesantísima técnica de ataque compuesta de redes de sistemas comprometidos con registros DNS públicos altamente cambiantes, en algunos casos cada pocos minutos. Estas arquitecturas cambiantes, hacen que la actividad sea más difícil de detectar y de parar, siendo un arma muy potente para el cibercrimen.

Con respecto al SPAM, éste seguirá creciendo en la red a corto y medio plazo pero se mantendrá el que llega a los buzones. Mejorarán las técnicas anti-spam y se impondrán las técnicas del nivel de reputación de las IPs.

Actualmente el spam es una de las formas que utilizan los hackers para alcanzar a los usuarios y realizar así sus fechorías, pero esta tendencia se está ampliando a otros canales como la mensajería instantánea o los blogs. Es decir, los ejércitos de maquinas comprometidas (botnets) usadas para distribuir spam pueden ser usadas para enviarlo a través de otro tipo de canales. Dependerá de a través de qué canales consiguen mayores beneficios económicos. En opinión del responsable del correo electrónico en la comunidad RedIRIS, este canal será el teléfono a través de aplicaciones como la VoIP para realizar actividades de phishing, timos etc. Este nuevo sistema tiene muchas más ventajas que el phishing por correo y permite a las victimas dar de alta números secretos y de tarjetas de crédito a medida que una voz le invita a hacerlo.

4 Links de interés

A continuación podéis encontrar algunos enlaces a documentos con información adicional.

- SANS Top-20 2007 Security Risks (2007 Annual Update)
- DNS attack could signal Phishing 2.0

- The HoneyNet Project Whitepapers
- Malicious Website/Malicious Code: Large scale European Web Attack
- PHP Security
- Predicciones para 2007
- Predicciones para 2007
- Ataques de DoS contra sitios Web del Gobierno de Estonia
- CastleCops
- SANS
- ShadowServer