

# SOPHOS

Informe anual de seguridad

2005





# Sophos: Informe anual de seguridad 2005

## Resumen del año

En los últimos doce meses se han visto nuevas e imaginativas formas de ataque contra redes corporativas.

La creciente complejidad de los sistemas informáticos, de los que se demanda más movilidad, flexibilidad y conectividad, ha llevado al crecimiento exponencial de las vías por las que las amenazas se extienden.

El número y los tipos de programas maliciosos se ha incrementado y el uso de ordenadores zombis para realizar ataques coordinados ya es habitual; las nuevas amenazas han aparecido tan rápido que los términos para describirlas se acumulan (phishing, pharming, spear phishing) y la distinción entre diferentes tipos de amenazas es cada vez más tenue. Los programas espía, con la tendencia general de ocultarse y extenderse de forma desapercibida, se han convertido en una de las mayores amenazas a las que se enfrentan las empresas.

## Nuevas amenazas y tendencias

Un informe publicado en noviembre de 2005 por Financial Insights, del grupo IDC, estima que instituciones financieras

en todo el mundo perdieron más de 400 millones de euros en el año 2004 debido a ataques de pesca de información (phishing)<sup>1</sup>. La motivación económica ha provocado la alianza entre autores de virus, creadores de spam y piratas informáticos, como se ha podido comprobar durante todo el año. En un entorno en continua evolución, los criminales aúnan fuerzas para generar oleadas de ataques organizados de virus, spam, pesca de información y programas espías.

El vandalismo desorganizado de anteriores generaciones ha dado paso a una actividad criminal con objetivos específicos, en la que se generan continuas variantes de amenazas para intentar burlar la protección antivirus y los controles de spam.

En lugar de los ataques masivos incontrolados del pasado, los ataques se están volviendo más específicos, con víctimas más concretas, para no llamar demasiado la atención.

Igualmente, el número de ordenadores bajo el ataque de campañas de spam se ha reducido para evitar el control de programas anti-spam que miden el volumen de mensajes.

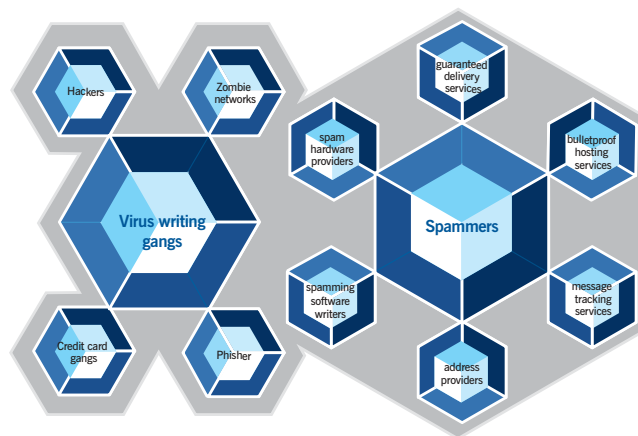


Figura 1: Ecosistema de amenazas

## Evolución en 2005

- Incremento del 48% en el número de amenazas
- 1 de cada 44 mensajes estaba infectado
- El número de troyanos casi duplica el de gusanos para Windows
- El spam médico sigue siendo el más abundante, aunque se ha disparado el pornográfico y los timos
- Los cibercriminales aúnan fuerzas y realizan ataques combinados

### Ritmo de crecimiento

El número de amenazas sigue creciendo a un ritmo que muchos creían insostenible. A principios de diciembre de 2005, Sophos Anti-Virus ya detectaba más de 114.000 virus, gusanos, troyanos y otros programas maliciosos.

Entre enero y noviembre de 2005, el número de virus, gusanos, troyanos y programas espía creció un 48% respecto al año anterior:

- 2004: 10.724 nuevas amenazas
- 2005: 15.907 nuevas amenazas

Más significativo si cabe es el incremento mensual en el número de amenazas descubiertas cada mes. En noviembre de 2005 se analizaron 1.940 nuevas amenazas, lo que supone un nuevo récord para los productos de Sophos. La figura 2 representa el ritmo de crecimiento mensual comparado con el del año pasado.

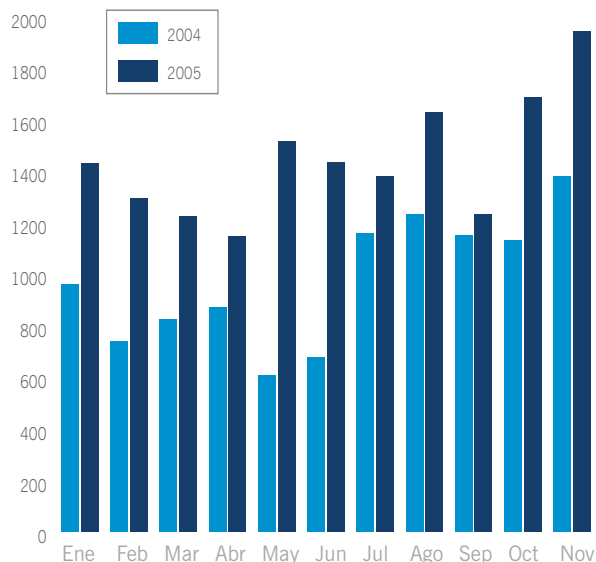


Figura 2: Nuevas amenazas - 2004 y 2005

Este incremento se atribuye al interés de bandas criminales en crear un sin fin de variantes. El incentivo económico parece estar detrás de cada vez más virus, gusanos y troyanos creados para robar dinero de usuarios y empresas inocentes.

No sólo aumenta la cantidad y variedad de amenazas, sino también la velocidad de aparición de nuevas variantes y la velocidad a la que se extienden.

De media, a lo largo del año, 1 de cada 44 mensajes en circulación estaba infectado. Esta cifra, sin embargo, ha llegado a niveles alarmantes: 1 de cada 12 mensajes durante el brote de Sober-Z a finales de noviembre de 2005<sup>2</sup>. Con este comportamiento tan agresivo, los gusanos de email pueden saturar las comunicaciones a través de Internet afectando tanto a usuarios como a empresas.

Además, los creadores de programas malintencionados intentan dificultar la tarea de los técnicos antivirus lanzando en avalancha numerosas variantes de virus y troyanos de forma casi simultánea<sup>3</sup>. Mediante variaciones en el "envoltorio" intentan burlar el filtrado de programas antivirus, al tiempo que sustituyen virus existentes cuando han perdido su efectividad.

Como resultado, son cada vez más las empresas que adoptan métodos de defensa proactivos para intentar bloquear la entrada a su organización de contenido potencialmente peligroso. Sophos complementa estas iniciativas con técnicas de detección genérica, como la potente tecnología Genotype™ que permite detectar nuevas variantes de programas maliciosos.

### Las amenazas más extendidas

Sophos cuenta con una red global de miles de estaciones de sondeo para recabar datos de virus en libertad, lo que permite evaluar el estado de los sistemas de email y detectar de forma inmediata cualquier brote vírico.

Aunque los piratas informáticos utilizan cada vez más a menudo técnicas de spam para distribuir sus troyanos, el efecto no es comparable al de gusanos y virus que se extienden por email.

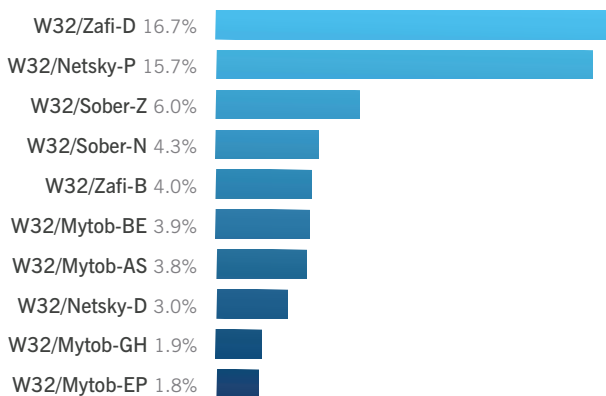


Figura 3: Virus Top 10 de Sophos en 2005

Para la mayoría de usuarios y empresas, los nombres que aparecen en la figura 3 son los más aparentes ya que es probable que alguno les haya llegado por correo o haya sido detectado en el servidor de email de la empresa.

Es curioso que los virus dominantes en la lista (figura 3) aparecieron hace ya bastante tiempo, indicativo de cómo los ataques más recientes van dirigidos a grupos más pequeños para pasar desapercibidos.

El veterano Zafi-D es un gusano responsable del 16,7% de las infecciones en el último año. De origen húngaro, el gusano se hace pasar por una felicitación navideña para atraer la atención del usuario<sup>4</sup>.

Otro viejo conocido, Netsky-P, el virus más extendido de 2004<sup>5</sup>, extendió su hegemonía durante este año. El quinceañero alemán Sven Jaschan, que admitió haber creado los gusanos Netsky y Sasser, salió en libertad condicional del juicio con una sentencia de 30 horas de servicios sociales<sup>6</sup>. Se sospecha que el autor del gusano Sober también es de origen alemán, y hay quien opina que la sentencia a Jaschan no ha servido como medida disuasoria.

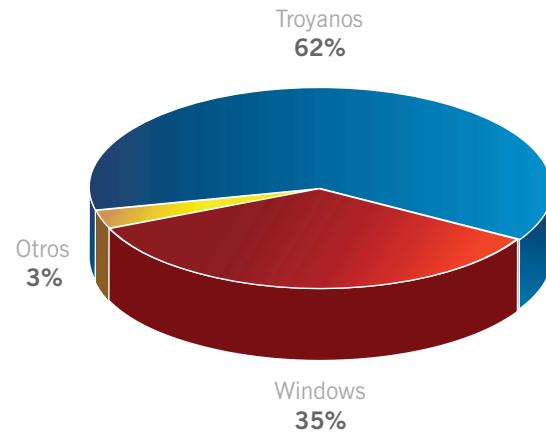
Con un poco más de tiempo, Sober-Z habría llegado a lo más alto de la lista. El gusano, que apareció en noviembre de 2005, se hace pasar por un mensaje del FBI o la CIA en relación con una investigación en el uso de sitios Web ilegales.

Sober-N, un gusano bilingüe, apareció en mayo y ofrecía entradas para la Copa del Mundo 2006 en Alemania; en menos de dos días ya había infectado ordenadores en más de 40 países<sup>7</sup>.

Sober-N permaneció oculto en los ordenadores infectados hasta que llegó el momento de pasar a la acción: miles de mensajes nacionalistas alemanes durante el período electoral tuvieron su origen en ordenadores zombi controlados por Sober-N.

### **Troyanos**

Durante el 2005, el número de troyanos ha superado al de gusanos para Windows. De hecho, los troyanos han acaparado casi dos tercios de todos los incidentes víricos durante el año (figura 4).



*Figura 4: Nuevas amenazas en 2005*

Esto es un indicativo de cómo los autores de programas malintencionados buscan ataques más específicos y controlados, en vez de ataques en masa indiscriminados.

Los cibercriminales prefieren no llamar tanto la atención para poder realizar sus actividades clandestinas sin obstáculos. Además, estos ataques más limitados les permiten hacer un uso más efectivo de los datos obtenidos.

Es mucho más sencillo robar dinero de 200 cuentas bancarias que de 200.000. Así, el uso de troyanos permite llevar a cabo ataques más manejables que con el uso aleatorio de gusanos incontrolables.

Los troyanos, al contrario que los gusanos, no se extienden de forma automática. Para infectar ordenadores, el atacante debe enviar el troyano, a menudo utilizando técnicas de spam, para lo que se utilizan ordenadores zombi.

### **Las características más peligrosas**

Durante el último año se han visto nuevas técnicas cada cual más sofisticada para infectar ordenadores y obtener lo que el atacante desea.

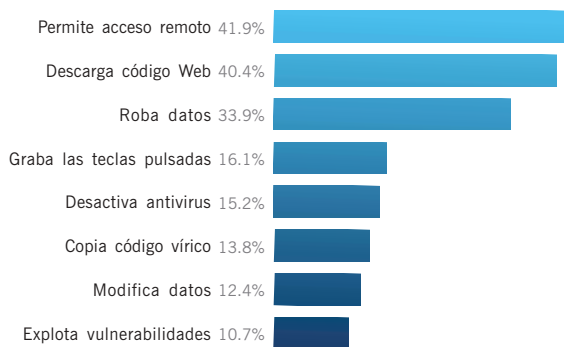


Figura 5: Características más peligrosas

Como se muestra en la figura 5, estas técnicas incluyen el robo de información, inhabilitar programas antivirus y el uso de programas maliciosos para realizar diferentes tareas. Tan peligrosos como los zombis son los programas que descargan otros componentes, haciendo necesaria la protección mediante cortafuegos en estaciones y portátiles. La seguridad de cada componente de la red es de especial importancia dada la rapidez con que aparecen programas maliciosos que se aprovechan de nuevas vulnerabilidades en los sistemas.

### Zombis

Un ordenador se convierte en zombi cuando un bot, o programa automatizado, se instala en el sistema, dando al atacante el control del mismo y entrando a formar parte de una red de zombis, o botnet. Una de las redes de zombis más destacadas del año fue la creada por el gusano Zotob, que en agosto lanzó un ataque coordinado contra importantes organizaciones mediáticas<sup>8</sup>, incluyendo la ABC, Financial Times y New York Times. La cadena de televisión CNN, otra víctima de Zotob, fue infectada "en directo", lo que afectó a su programación de forma notable.

La mayoría de los virus más extendidos este año disponen de puertas traseras que permiten el acceso no autorizado al sistema infectado, que podría transformarse en zombi.

Un estudio de Sophos ha revelado que más del 60% del spam se genera desde ordenadores manipulados sin el conocimiento del usuario, que pueden ser utilizados además para realizar ataques DDoS. El creciente riesgo para la reputación de las empresas llevó a Sophos a lanzar el servicio ZombieAlert™ en julio de 2005, que permite notificar rápidamente a cualquier empresa cuyos sistemas estén siendo utilizados para enviar spam<sup>9</sup>.

Muchos programas maliciosos también descargan archivos desde Internet, lo que requiere el uso de cortafuegos no sólo en la periferia de la red de la empresa, sino también en estaciones y portátiles.

### Programas espía

La amenaza más patente proviene, sin duda, de los programas espía. La explosión de programas espía ha disparado las alertas entorno a la seguridad informática. Estos programas se ocultan en ordenadores y pueden grabar las teclas pulsadas por el usuario, robar información confidencial y abrir las defensas de la red para la entrada de ataques sucesivos.

La figura 6 representa el porcentaje de programas espía entre los programas malintencionados analizados por Sophos a lo largo del año. En enero, sólo el 54,2% de las amenazas incluían programas espía, mientras que en noviembre ya era del 66,4%.

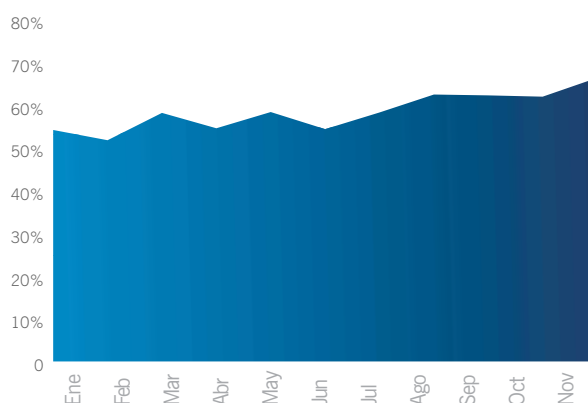
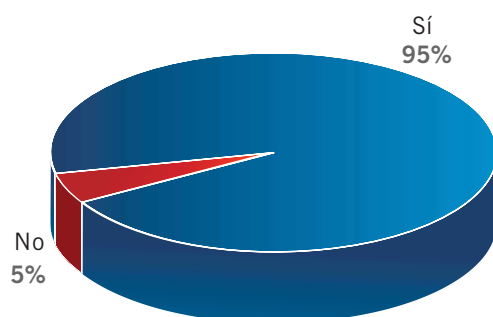


Figura 6: Proporción de programas espía

Las empresas ven en los programas espía una clara amenaza para sus intereses. En una encuesta<sup>10</sup> realizada por Sophos, una abrumadora mayoría reclama a sus soluciones antivirus protección simultánea contra programas espía (figura 7).



Fuente: Encuesta de Sophos

Figura 7: ¿Debe el software antivirus proteger contra programas espía?

Durante 2006, Sophos vaticina un mercado muy competitivo para empresas dedicadas exclusivamente a la protección contra programas espía, a menos que busquen alianzas con empresas de protección antivirus. El mercado tiende a consolidarse y empresas con productos específicos para programas espía tendrán muy difícil mantener su competitividad.

## Métodos de propagación

Los programas maliciosos utilizan diferentes técnicas para extenderse. Hoy en día, es habitual que virus y gusanos utilicen una combinación de técnicas para incrementar sus posibilidades de expansión.

La figura 8 muestra los métodos de expansión más utilizados. El gráfico no representa necesariamente la eficacia de cada método, simplemente la frecuencia con que se utiliza. Tampoco se incluyen troyanos ya que no se pueden extender por sí mismos.

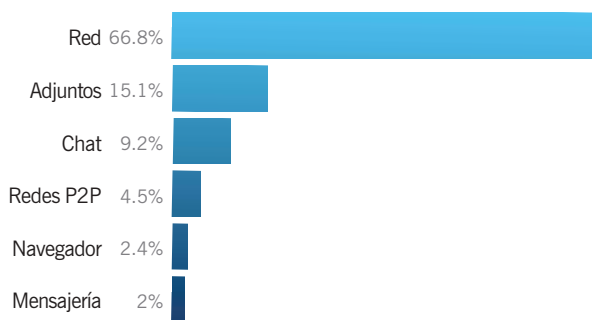


Figura 8: Modo de expansión

Aunque la protección se sigue centrando principalmente en el servidor de correo, clave en cualquier estrategia de defensa, existen otros métodos de comunicación que se subestiman.

Las empresas son, a menudo, blanco de ataques que evitan el gateway. Los gusanos de red representan un peligro en el seno de cualquier organización. El código malicioso es capaz de penetrar en la red interna a través de navegadores Web, canales de chat y programas de mensajería instantánea (MI) como AIM o MSN Messenger.

Además, controlar cada CD-ROM, unidad de almacenamiento USB, tarjeta de memoria, teléfono de última generación o reproductor MP3 que entra en contacto con ordenadores de la empresa es casi imposible, y sin embargo todos ellos suponen un posible punto de entrada de código malicioso, lo que destaca la necesidad de proteger las estaciones de trabajo y portátiles del mismo modo que otros niveles en la infraestructura informática de una organización.

En noviembre de 2005, saltaron todas las alarmas cuando se descubrió que ciertos CD de música de Sony instalaban, como parte de su protección anticopia, un programa que varios troyanos aprovechaban para penetrar en el sistema<sup>11</sup>.

La creciente variedad en técnicas de expansión hace más importante que nunca la concienciación del usuario y prácticas seguras, así como el uso de políticas internas, actualización sistemática de los sistemas y un enfoque de defensa multinivel.

## Motivación

En el pasado, los autores de virus tenían una motivación diferente, similar al que hace pintadas en las paredes para hacerse notar. Tradicionalmente, eran quinceañeros con escasa vida social los que creaban virus para incrementar su autoestima e impresionar a otros. En muchos casos dejaban mensajes y pistas en sus creaciones.

No se puede decir que esos virus fueran inofensivos (causaban numerosos problemas tanto a empresas como a usuarios domésticos), aunque su ambición era escasa.

En la actualidad, la mayoría de los programas malintencionados tienen como propósito el obtener un beneficio económico. Bandas organizadas se han dado cuenta de cómo se puede aprovechar Internet para robar dinero fácil.

Se puede hacer dinero de forma fraudulenta mediante ataques de pesca de información (phishing), spam, amenazas de denegación de servicio mediante diferentes ataques, timos o el uso de programas espía.

Además, se ha creado un mercado en torno a este ecosistema sumergido, por ejemplo, en el desarrollo de programas que se venden a distribuidores de spam para sus actividades ilícitas.

También se da el caso de empresas legítimas de publicidad que abusan de la inocencia del usuario para, tras aceptarse los términos de uso, instalar otros programas publicitarios.

Este año también se ha visto un incremento incesante de gusanos y troyanos que roban credenciales de populares juegos on-line que después se venden por Internet. Estas credenciales virtuales se cotizan en el ciberespacio, donde el intercambio de elementos virtuales mueve muchísimo dinero, y su comercialización ilegal ha llevado a varias detenciones<sup>12</sup>.

Recientemente una persona en Miami pagó 100.000 euros para adquirir una estación espacial virtual<sup>13</sup>.

De cualquier modo, la actividad criminal se sigue centrando en programas espía, pesca de información y fraude por Internet. Los criminales de Internet están aunando sus fuerzas para hacerse con el dinero de usuarios inocentes.

## Distribuidores de spam

El correo comercial no solicitado más abundante es de tipo médico (incluyendo productos que prometen mejorar su rendimiento sexual, pérdida inmediata de peso u hormonas de crecimiento). Incluso se han visto campañas de spam que se intentaban aprovechar del miedo a una posible epidemia de gripe aviar<sup>14</sup>.

El spam con contenido pornográfico se incrementó notablemente a partir de agosto, aunque en parte se debe a un cambio en la clasificación de este tipo de spam en las estaciones de monitorización de Sophos en el último cuatrimestre del año. Los mensajes con contenido sexual se han consolidado en segundo puesto.

Uno de los tipos de spam que más ha crecido es el relacionado con el mercado bursátil, pasando del 0,8% de principio de año al 13,5% en el mes de noviembre.

Un ejemplo de fraude mediante la distorsión del mercado de valores es el que se produjo cuando una campaña de spam afirmaba el desarrollado una vacuna contra la gripe aviar<sup>15</sup>.

Al mismo tiempo, la cantidad de mensajes en los que se ofrece software a precios reducidos ha disminuido de forma significativa. Cada vez se ofrecen menos productos ilegítimos por Internet. Sin embargo, sí se ha visto un incremento en los mensajes que anuncian relojes Rolex, ya sean falsos o no.

## Phishing

La pesca de información, o phishing, se ha convertido en una de las formas de spam más lucrativas y en alza. Los ataques de pesca de información van dirigidos principalmente a usuarios de PayPal, seguido de eBay y Amazon, aunque otras numerosas instituciones financieras también se ven afectadas con frecuencia.

Sólo es necesario que alguien pique el anzuelo para hacer rentable los esfuerzos del atacante.

Algunos intentos de pesca de información son especialmente retorcidos, como el que tuvo lugar en agosto en el que el atacante se hacía pasar por una ancianita en silla de ruedas en busca de un producto a la venta en eBay<sup>16</sup>.

La evolución de los ataques de pesca de información ha llevado a la "pesca con arpón" (spear phishing). En esta nueva modalidad, el ataque se centra en un pequeño número de usuarios, por ejemplo dentro de una empresa, con la intención de obtener información confidencial. Mediante sutiles técnicas de ingeniería social y falsificando la procedencia del mensaje, las posibilidades de éxito del atacante se incrementan.

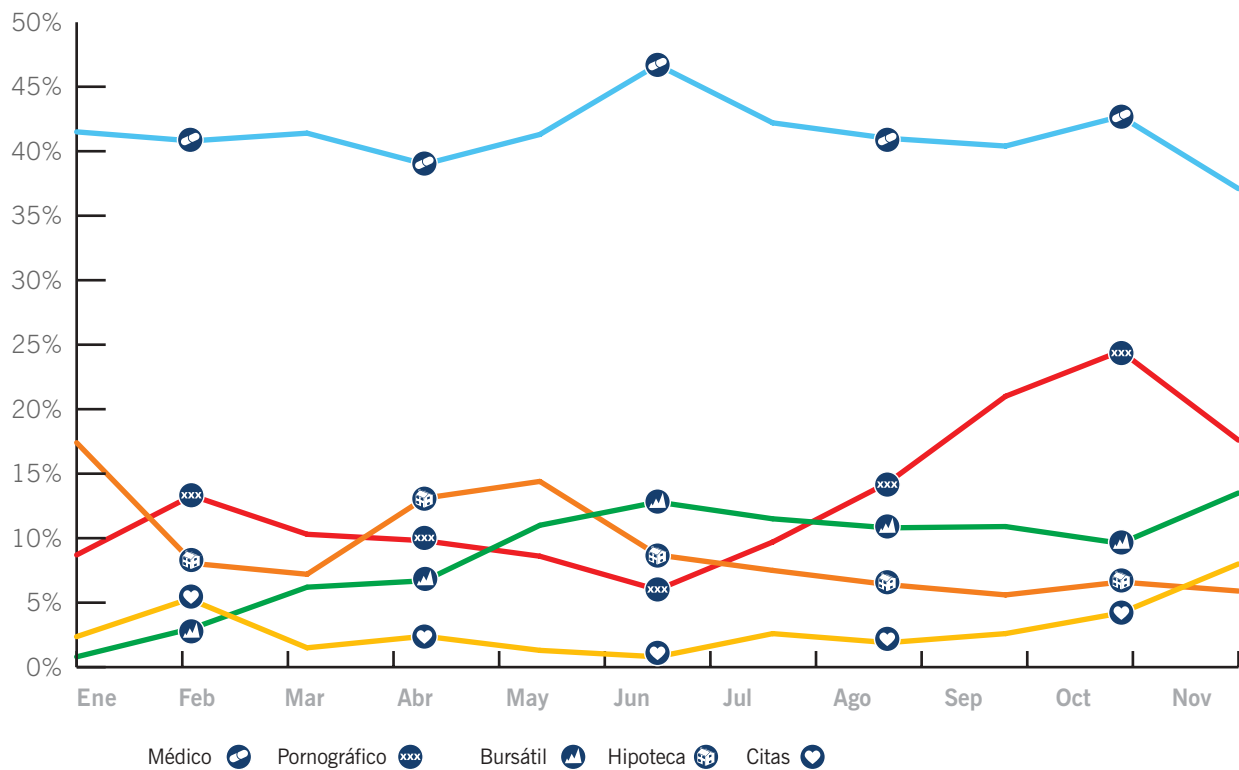


Figura 9: Categorías de spam

## Timos

Timos tan conocidos como el de "Carta desde Nigeria" (en los que se pide una pequeña suma de dinero a cambio de un beneficio espectacular) siguen circulando entre el spam habitual. Durante el último año, Sophos ha interceptado una amplia variedad de timos distribuidos en forma de spam. Se han visto timos con diferentes temas, referentes al devastador tsunami en las costas de la India<sup>17</sup>, a las acciones terroristas en julio en Londres<sup>18</sup> e incluso acerca de una lotería en el club de fútbol Liverpool<sup>19</sup>.

## Los principales países generadores de spam

La figura 10 revela los países desde los que se envía más spam. Estados Unidos se mantiene como el principal emisor de spam, aunque la proporción ha disminuido de forma espectacular respecto al año anterior<sup>20</sup>. Sophos estima que más del 60% del spam se genera desde ordenadores zombi.

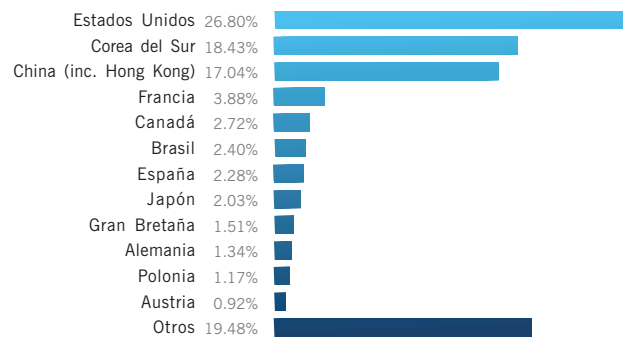


Figura 10: Países generadores de spam

El secuestro de ordenadores de usuarios inocentes a través de Internet permite a los creadores de spam ocultarse en cualquier país del mundo. Estados Unidos, Corea del Sur y China generan más del 50% del spam en todo el mundo. Sophos ha podido comprobar el acusado descenso en el spam enviado desde EE.UU. debido a varios factores, como penas de cárcel para responsables de enviar spam, una legislación más severa y sistemas de seguridad más eficaces.

La cooperación entre empresas que ofrecen acceso a Internet y la entrada en vigor de la ley CAN-SPAM también han contribuido a reducir el spam generado en Norteamérica. Como resultado, numerosos creadores de spam han decidido cambiar de negocio o de país.

## Un vistazo a 2006

### Programas espía y publicitarios

Los programas espía seguirán en aumento en 2006 y ya se está viendo cómo los atacantes utilizan zombis para instalar programas publicitarios y aplicaciones no deseadas. Mientras que los programas publicitarios no son siempre ilegales, su uso se está tergiversando y llevando demasiado lejos por motivos económicos<sup>21</sup>. Con la proliferación de programas espía y publicitarios, en 2006 más y más empresas buscarán protección en soluciones integradas de administración centralizada, en vez de productos para usuarios domésticos.

### No se ve el final del spam

En enero de 2004, Bill Gates auguró que el spam sería "algo del pasado en un par de años"<sup>22</sup>. Sin embargo, Sophos puede constatar que estos rumores sobre la desaparición del spam han sido exagerados: la amenaza está más presente que nunca pese a los esfuerzos de gobiernos en todo el mundo y a las mejoras en productos anti-spam.

### Sistemas de prevención de intrusión (HIPS)

Estos sistemas de seguridad incluyen control de comportamiento e inspección de aplicaciones además de los tradicionales antivirus y cortafuegos. Sophos sugiere a las empresas la selección cuidadosa de un tipo de protección que se ajuste a sus necesidades, en vez de un producto que asegure curar todos los males.

### Virus en móviles

Aunque se ha producido un incremento en el número de virus para teléfonos móviles, su cantidad sigue siendo insignificante<sup>23</sup> comparada con el número de virus para Windows. Los autores de virus están más interesados en robar dinero a través de Internet que en anecdóticos ataques a teléfonos móviles.

En un sondeo de Sophos, el 70% de empresas opinaba que ciertas organizaciones antivirus estaban exagerando los peligros de virus para móviles.

## Microsoft

La entrada de Microsoft en la protección antivirus puede suponer una espina para las empresas antivirus dedicadas a usuarios domésticos. Sin embargo, en el entorno empresarial Microsoft deberá demostrar antes que es capaz de crear una protección fiable. En una encuesta de Sophos tras la epidemia causada por el gusano Zotob, el 35% de los participantes acusaban a Microsoft como último responsable del problema por la vulnerabilidad en el código de Windows<sup>24</sup>.

Es muy probable además que los nuevos virus estén diseñados para inhabilitar la protección antivirus de Microsoft, igual que sucede en la actualidad con su producto contra programas espía y su cortafuegos<sup>25</sup>.

## Creadores de virus

Motivos económicos parecen alentar la creación de programas maliciosos, ya sea para robar información confidencial, enviar spam<sup>26</sup>, realizar ataques DDoS<sup>27</sup> o instalar programas publicitarios en ordenadores afectados. Los gusanos de email tradicionales tienden a disminuir, mientras que los ataques controlados mediante troyanos<sup>28</sup> seguirán aumentando.

## Agujeros de seguridad

Aunque los ataques seguirán centrándose en vulnerabilidades de Microsoft, se verán cada vez más infecciones a través de agujeros en otros productos cuyo uso se ha generalizado (por ejemplo, navegadores Web alternativos o programas de email para el gateway).

## Zombis

Con las mejoras de seguridad en Windows XP incluidas en la actualización Service Pack 2 (como cortafuegos y actualización de seguridad automática), a los atacantes se les cierran numerosas vías de entrada a los ordenadores conectados a Internet. Ahora deberán hacer uso de otros trucos para engañar al usuario e inhabilitar la seguridad desde el interior del sistema para poder instalar el resto de componentes.

El lanzamiento de la actualización para Windows XP SP2, con nuevas funciones de seguridad, ha contribuido a la defensa de usuarios domésticos contra ataques clandestinos.

Ya no se puede hablar de Boca Ratón, en Florida, como la capital mundial del spam, y parece que Rusia ha tomado el relevo. Desafortunadamente, los creadores de spam se aprovechan de la falta de protección en ordenadores domésticos con conexión de alta velocidad en todo el mundo para enviar sus mensajes.

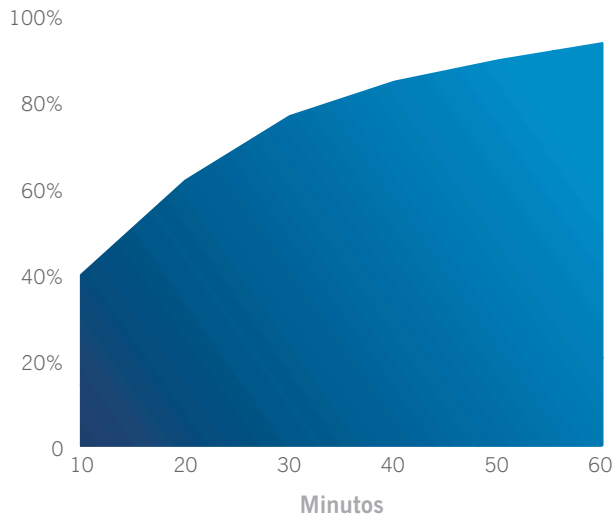
## Protección necesaria

Los ataques sobre ordenadores no protegidos se producen con mayor rapidez que nunca. Vulnerabilidades en los sistemas permiten la expansión de amenazas por Internet sin la intervención del usuario, como en el caso del gusano Zotob. En estos ataques pueden caer infectados cientos de miles de ordenadores en tan sólo una hora. Los programas que aprovechan vulnerabilidades aparecen antes de que el usuario pueda protegerse, a veces incluso antes de que exista un parche de seguridad.

Microsoft creó 29 parches de seguridad críticos entre enero y noviembre de 2005 (una media de 2,4 al mes), así como numerosos parches de menor importancia.

Un estudio de Sophos demuestra cómo al conectar a Internet un ordenador con Windows XP sin parches de seguridad existe una probabilidad del 40% de caer infectado en tan sólo 10 minutos, pasando al 94% en 60 minutos (figura 11). Los ataques son tan rápidos que probablemente no habría tiempo suficiente para descargar los parches de seguridad.

Por el contrario, un ordenador con Windows XP SP2 y los parches correspondientes estará en una posición mucho mejor para repeler estos ataques. El problema es que muchos de los programas maliciosos inhabilitan la seguridad del sistema permitiendo la entrada del resto de amenazas.



*Figura 11: Riesgo de infección de un ordenador no protegido en Internet*

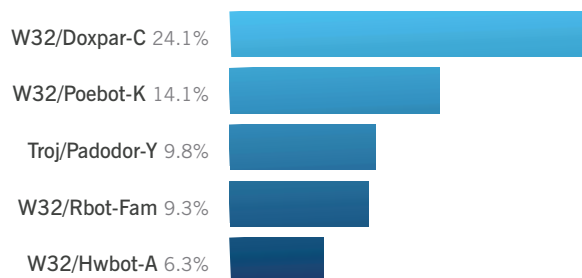
El peligro de los gusanos de Internet es que no requieren intervención del usuario; para caer infectado no es necesario visitar ninguna página Web, ni recibir un email o ejecutar un programa. Sólo es necesario conectarse a Internet sin la protección adecuada del sistema.

La infección se produce de forma invisible para el usuario que, sin sospecharlo, podría estar contagiando a otros usuarios, suministrando información confidencial al atacante o enviando spam por todo el mundo.

## Resumen

La creciente variedad de nuevas amenazas, la velocidad con la que se extienden y la complejidad de las redes modernas tendrán un gran impacto para las empresas en 2006. La combinación de métodos de infección a diferentes niveles consolidará la tendencia en empresas de adquirir soluciones de protección completas suministradas por un solo fabricante.

En la figura 12 se muestran los gusanos de Internet más extendidos.



*Figura 12: Gusanos de Internet más extendidos*

Sophos es el líder mundial en soluciones integradas de control de amenazas para empresas, educación y gobiernos. Nuestros productos, caracterizados por su gran precisión y facilidad de uso, protegen a más de 35 millones de usuarios en más de 150 países. Con más de 20 años de experiencia, Sophos cuenta con dedicados técnicos antivirus y anti-spam, y con una red global de análisis de amenazas, para responder con rapidez ante cualquier nueva amenaza – por compleja que resulte – y garantizar así el más alto nivel de satisfacción del cliente.

## Referencias

- 1 IDC - Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc, Nov 2005
  - 2 Sober-Z se hace pasar por el FBI y la CIA  
[www.esp.sophos.com/pressoffice/news/articles/2005/11/soberfbi.html](http://www.esp.sophos.com/pressoffice/news/articles/2005/11/soberfbi.html)
  - 3 La tecnología Genotype protege contra el ataque masivo de Mytob  
[www.sophos.com/pressoffice/news/articles/2005/04/va\\_mytobmultitude.html](http://www.sophos.com/pressoffice/news/articles/2005/04/va_mytobmultitude.html)
  - 4 El gusano Zafi se extiende con forma de felicitación navideña  
[www.esp.sophos.com/pressoffice/news/articles/2004/12/pr\\_zafid2.html](http://www.esp.sophos.com/pressoffice/news/articles/2004/12/pr_zafid2.html)
  - 5 La guerra de los gusanos: Netsky-P encabeza la lista  
[www.sophos.com/pressoffice/news/articles/2004/12/pr\\_uk\\_20041208yeartopten.html](http://www.sophos.com/pressoffice/news/articles/2004/12/pr_uk_20041208yeartopten.html)
  - 6 El autor del gusano Sasser sale libre tras el juicio  
[www.esp.sophos.com/pressoffice/news/articles/2005/07/pr\\_20050708sasserfree.html](http://www.esp.sophos.com/pressoffice/news/articles/2005/07/pr_20050708sasserfree.html)
  - 7 El gusano Sober-N se extiende a más de 40 países  
[www.sophos.com/pressoffice/news/articles/2005/05/va\\_sobern2.html](http://www.sophos.com/pressoffice/news/articles/2005/05/va_sobern2.html)
  - 8 Gusano ataca CNN, ABC, The Financial Times y The New York Times  
[www.sophos.com/pressoffice/news/articles/2005/08/va\\_breakingnews.html](http://www.sophos.com/pressoffice/news/articles/2005/08/va_breakingnews.html)
  - 9 Sophos lanza su nuevo servicio ZombieAlert que identifica el envío de spam  
[www.esp.sophos.com/pressoffice/news/articles/2005/07/pr\\_20050713zombiealert.html](http://www.esp.sophos.com/pressoffice/news/articles/2005/07/pr_20050713zombiealert.html)
  - 10 El 95% de los usuarios solicita a los fabricantes de antivirus la detección de programas espía  
[www.esp.sophos.com/pressoffice/news/articles/2005/07/pr\\_20050726pollspyav.html](http://www.esp.sophos.com/pressoffice/news/articles/2005/07/pr_20050726pollspyav.html)
  - 11 Un troyano explota la vulnerabilidad del software anticopia de Sony  
[www.esp.sophos.com/pressoffice/news/articles/2005/11/stinx.html](http://www.esp.sophos.com/pressoffice/news/articles/2005/11/stinx.html)
  - 12 Detenida una banda en Corea por el robo a usuarios de juegos on-line  
[www.sophos.com/pressoffice/news/articles/2005/07/va\\_krarrests.html](http://www.sophos.com/pressoffice/news/articles/2005/07/va_krarrests.html)  
  
Troyano roba nombres de usuario y contraseñas de usuarios de juego de rol on-line  
[www.sophos.com/pressoffice/news/articles/2005/01/va\\_legmiry.html](http://www.sophos.com/pressoffice/news/articles/2005/01/va_legmiry.html)
  - 13 Compra una estación espacial virtual por 100.000 euros  
[www.informationweek.com/story/showArticle.jhtml?articleID=173601281](http://www.informationweek.com/story/showArticle.jhtml?articleID=173601281)
  - 14 Sophos advierte sobre mensajes de spam que pretenden vender medicamentos contra la gripe aviar  
[www.esp.sophos.com/pressoffice/news/articles/2005/10/sa\\_tamifluspam.html](http://www.esp.sophos.com/pressoffice/news/articles/2005/10/sa_tamifluspam.html)
  - 15 Creadores de spam se aprovechan del miedo a la gripe aviar  
[www.sophos.com/pressoffice/news/articles/2005/10/sa\\_tamifluspam.html](http://www.sophos.com/pressoffice/news/articles/2005/10/sa_tamifluspam.html)
  - 16 Se hacen pasar por una abuelita en silla de ruedas para timar a usuarios de eBay  
[www.sophos.com/pressoffice/news/articles/2005/08/sa\\_samaritan.html](http://www.sophos.com/pressoffice/news/articles/2005/08/sa_samaritan.html)
  - 17 Timo: Carta de víctima del tsunami  
[www.esp.sophos.com/virusinfo/hoaxes/tsunami.html](http://www.esp.sophos.com/virusinfo/hoaxes/tsunami.html)
  - 18 Timo en torno a los atentados terroristas de Londres  
[www.sophos.com/pressoffice/news/articles/2005/08/sa\\_419bombscam.html](http://www.sophos.com/pressoffice/news/articles/2005/08/sa_419bombscam.html)
  - 19 Timo mediante un falso mensaje del Liverpool FC  
[www.sophos.com/pressoffice/news/articles/2005/11/liverpoolfc.html](http://www.sophos.com/pressoffice/news/articles/2005/11/liverpoolfc.html)
  - 20 Sophos revela los países generadores de spam  
[www.sophos.com/pressoffice/news/articles/2004/12/sa\\_dirtydozenyear.html](http://www.sophos.com/pressoffice/news/articles/2004/12/sa_dirtydozenyear.html)
-

- 
- 21 El FBI arresta a un sospechoso de crear zombis  
[www.sophos.com/pressoffice/news/articles/2005/11/ancheta.html](http://www.sophos.com/pressoffice/news/articles/2005/11/ancheta.html)
  - 22 Gates vaticina la desaparición del spam  
[news.bbc.co.uk/1/hi/business/3426367.stm](http://news.bbc.co.uk/1/hi/business/3426367.stm)
  - 23 Gusano para teléfonos móviles Mabir no tan extendido  
[www.sophos.com/pressoffice/news/articles/2005/04/va\\_mabir.html](http://www.sophos.com/pressoffice/news/articles/2005/04/va_mabir.html)
  - 24 Usuarios culpan a Microsoft de las últimas epidemias  
[www.sophos.com/pressoffice/news/articles/2005/08/va\\_zotobpoll.html](http://www.sophos.com/pressoffice/news/articles/2005/08/va_zotobpoll.html)
  - 25 Aparece el primer troyano que ataca la protección contra programas espía de Microsoft  
[www.sophos.com/pressoffice/news/articles/2005/02/va\\_bankash.html](http://www.sophos.com/pressoffice/news/articles/2005/02/va_bankash.html)
  - 26 Troyano de spam Sober-Q no burla la tecnología Genotype de Sophos  
[www.esp.sophos.com/pressoffice/news/articles/2005/05/va\\_soberq.html](http://www.esp.sophos.com/pressoffice/news/articles/2005/05/va_soberq.html)
  - 27 Arrestado un presunto creador de 100.000 zombis  
[www.sophos.com/pressoffice/news/articles/2005/10/va\\_dutchbotarrests.html](http://www.sophos.com/pressoffice/news/articles/2005/10/va_dutchbotarrests.html)
  - 28 Los piratas informáticos atacan organizaciones con infraestructuras críticas  
[www.esp.sophos.com/pressoffice/news/articles/2005/06/va\\_niscc.html](http://www.esp.sophos.com/pressoffice/news/articles/2005/06/va_niscc.html)
-