Informe de seguridad

2007

SOPHOS

secured.

SOPHOS

Informe de seguridad **2007**

Introducción

En el 2006 se ha visto a un aumento de actividades ilícitas por parte de cibercriminales que siguen perfeccionando sus técnicas para engañar a la gente, y que son cada vez más difíciles de detectar. Sitios web maliciosos, campañas de Spam que cambian en sólo algunos segundos para no ser detectados y falsificaciones de sistemas de buzón de voz de empresas legítimas - son sólo tres ejemplos para mostrar con qué rapidez evolucionan las amenazas.

Sophos protege contra un total de 207.684 amenazas, con Mytob en primera posición de la clasificación de programas maliciosos. Los programas maliciosos siguen extendiéndose a través de spam, mensajería instantánea, sitios web falsos, correo electrónico y unidades compartidas de red. A esto se le suma que Internet se ha convertido en una fuente significativa de amenazas, llena de programas espía, adware, aplicaciones no deseadas y sitios web maliciosos. Los cibercriminales buscan el libre acceso a datos personales y confidenciales de sus víctimas, para extraer ganancias financieras o generar beneficios a través de ordenadores infectados.

Como los piratas continúan creando ataques más específicos, la cantidad de mensajes infectados sigue decreciendo. La proporción de mensajes infectados en 2005 fue de uno de cada 44, mientras en 2006 fue de sólo uno de cada 337.

Los diferentes modos cada vez más complejos para obtener información confidencial de usuarios y empresas se transforman en campañas de spam, técnicas complejas de acción y una avalancha de nuevas estafas. Y aún cuando se hayan dictado nuevas leyes y que éstas hayan sido aplicadas con vigor, el desafío para el año que viene es inmenso.

Un vistazo a 2006

- Autores de programas maliciosos renuncian a ataques generales y se vuelcan hacia ataques más específicos
- Crecimiento explosivo de troyanos de descarga para espiar a los usuarios
- Total de amenazas de programas maliciosos para los que se ofrece protección: 207.684
- 41.536 nuevos programas maliciosos detectados por Sophos
- Troyanos sobrepasan virus y gusanos de Windows 4:1
- Nuevo gusano de email, Stratio, con más de 100 variantes en noviembre
- Email con archivos infectados: bajó de 1 a 337
- La mayoría de spam sigue viniendo de ordenadores poco protegidos en EE.UU

Sólo un 34% de las empresas piensa que la seguridad en 2007 será mejor que en 2006.

Fuente: Encuesta online de Sophos, diciembre 2006

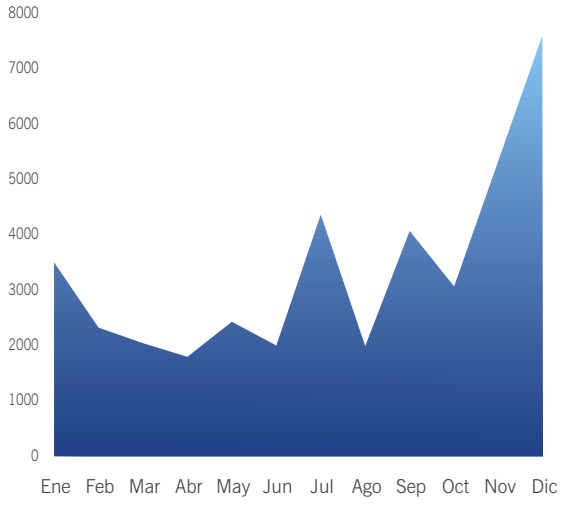
Programas maliciosos

El crecimiento de programas maliciosos

En 2006, Sophos identificó 41.536 nuevas amenazas. Los creadores de virus continúan encontrando nuevas maneras para infectar los ordenadores y engañar a los usuarios, para extraer información confidencial. Hubo un crecimiento particular en noviembre con 7.612 nuevas amenazas, casi cuatro veces más que en noviembre de 2005 con 1.940.

Sophos cuenta con que la tendencia siga al alza en el 2007. Las tentativas serán aun más evolucionadas para obtener datos y generar beneficios ilícitos.

El aumento en el gráfico se debe a la aparición de la familia de programas maliciosos llamada Stratio, también conocida como Stration o Warezov. El gusano de email enviado en masa se ha reproducido y unas miles de variantes han sido enviadas como spam en noviembre. (Stratio se describe más detalladamente abajo.)



Nuevas amenazas de programas maliciosos de cada mes en 2006

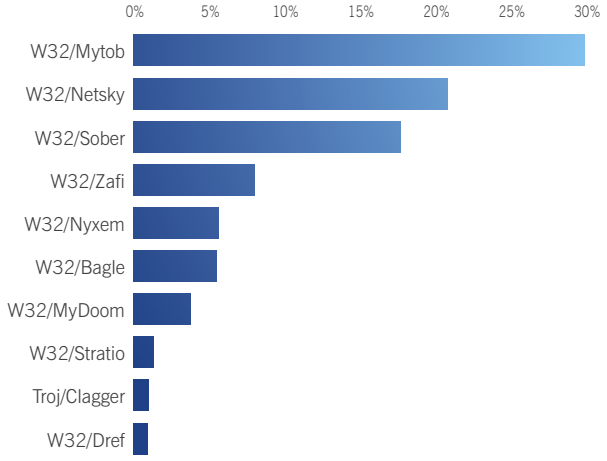
Las diez principales amenazas de email

Sophos cuenta con una red global de miles de estaciones de sondeo para recabar datos de los últimos virus que se propagan a través de mail y detectar de forma inmediata cualquier brote vírico.

Si bien la proporción de mensajes infectados bajó de 1/44 en 2005 a apenas 1/337 (es decir, un 0.3%) en 2006, hubo programas maliciosos tenaces que aparecían siempre en la bandeja de entrada. Gusanos tales como Mytob, Netsky y Sober se extendieron vía email en 2006.

1 Mytob

La clasificación del Top 10 de las familias de gusanos muestra que las variantes del gusano Mytob sigue invadiendo a usuarios poco protegidos en todo el mundo. Mytob apareció en marzo de 2005 y hasta el día de hoy sigue infectando los ordenadores. Farid Essebar de 18 años, residente marroquí de origen ruso, conocido por su firma “DiablO”, fue sentenciado a dos años de prisión por difundir el gusano Zotob.[1] Evidencias lo asocian además con la creación de otras variantes de Mytob.



Clasificación de las familias de programas maliciosos en 2006

2 Netsky

El 8 de mayo de 2004, fue arrestado el adolescente alemán Sven Jaschan por haber creado los gusanos Netsky y Sasser que dieron la vuelta al mundo. En julio de 2005 recibió la sentencia de un año y nueve meses de libertad vigilada y 30 horas de servicios sociales.[2]* Pero, a pesar de la sentencia, la familia Netsky, en particular, Nestky-P y Nestky-D continúan apareciendo en el ranking.

Una preocupación adicional es que Netsky-D es capaz de transgredir la seguridad de Windows Vista, el último sistema operativo de Microsoft.[3] Aunque Vista incluye una seguridad adicional que ayuda a proteger el ordenador de un ataque, esta amenaza nos muestra lo importante que es actualizar la protección antivirus.

3 Sober

Sober también sigue extendiéndose en el mundo entero. Hizo su primera aparición en octubre de 2003 y continúa estando presente en el Top 10 de Sophos. Su variante más divulgada es Sober-Z, que apareció a finales de 2005, se envía en forma de documento adjunto, pretendiendo ser del FBI, la CIA o autoridades alemanas y ataca los ordenadores desactivando su programa de seguridad. Dejó de extenderse el 6 de enero de 2006, pero aún cuando sólo se expandió durante algunos días a principios de año, logró colocar a la familia de gusanos Sober en tercera posición de la lista de programas maliciosos mas prolíficos del 2006.**

4 Zafi

Otro veterano, Zafi, visto por primera vez en abril de 2004, se extiende recolectando direcciones de email. La cuarta versión de este código, Zafi-D es el más expandido de la familia de gusanos.[5] Oculto bajo una felicitación de Navidad y con técnicas de ingeniería social logra que los usuarios abran el documento adjunto. Llegó a estar presente en uno de cada diez mensajes en circulación y se convirtió en líder del Top 10 en el año 2005.

* Hace dos años, Jaschan, quien fue contratado por una empresa alemana de seguridad, para darse a conocer, envió un mensaje peligroso que decía que los autores de virus podían obtener un empleo en el mundo de la informática, a pesar de su comportamiento malicioso.

**Irónicamente, un joven de 20 años, de nombre desconocido, que tenía fotos pornográficas de niños en su ordenador, se entregó a las autoridades creyendo que el mensaje provenía de ellos, siendo un mensaje del autor de Sober-Z.[4].

5 Nyxem

Este programa malicioso enviado en masa, también conocido como gusano Kama Sutra por camuflarse como fotografías y películas pornográficas, causó pánico a principios de 2006.[6] Con una carga devastadora capaz de destruir los archivos DOC, XLS, MDB, MDE, PPT, PPS, ZIP, RAR, PDF, PSD y DMP.

6 Bagle

La familia de los gusanos Bagle surgió en enero de 2004 y a pesar de su antigüedad, sigue infectando ordenadores. En febrero de 2006 aparecieron nuevas variantes, como Bagle-CM que se hace pasar por un mensaje ofreciendo entradas gratuitas a los Juegos Olímpicos de Invierno en Turín,[7] o Bagle-CO que contenía frases de amor en una tarjeta de San Valentín.

Estas amenazas tienen tanto éxito debido a que siguen existiendo ordenadores sin la protección apropiada. Variantes de Bagle continuarán expandiéndose por email hasta que los usuarios no instalen un antivirus contra estas amenazas.

Microsoft Windows Vista

Microsoft publicó Windows Vista, el sucesor de Windows XP, en noviembre de 2006. Vista se jacta de un gran número de componentes de seguridad, como el Control de cuentas de usuario, que permite al usuario escoger caso por caso qué se ejecuta y qué no, ofreciendo así una mejor protección contra programas maliciosos. El servicio de mensajería Windows Mail tiene una gran variedad de opciones predeterminadas que pueden evitar la ejecución de programas maliciosos. Ésta es una buena noticia para los usuarios: un sistema operativo que ofrezca mejor protección contra amenazas, seguramente sea un buen complemento a las políticas de seguridad.

Sin embargo, es importante que los usuarios no confíen solamente con la seguridad avanzada de Windows Vista para proteger sus sistemas contra los ataques de programas maliciosos.

Sophos probó Microsoft Vista con las opciones predeterminadas y encontró tres gusanos de email extendidos en todo el mundo que son capaces de transgredir la seguridad del sistema: Stratio-Zip, Netsky-D y MyDoom-O. Estas tres variantes representan casi un 40% del total de los virus en circulación en noviembre de 2006.

Microsoft tiene un desafío adicional que enfrentar el año que viene. Al contar con la mayor parte del mercado de sistemas operativos, los autores de programas maliciosos seguirán buscando las vulnerabilidades de los códigos en Vista. Aunque Microsoft ha hecho un enorme avance otorgando parches para los agujeros de seguridad conocidos en el código, los programas maliciosos capaces de transgredir la seguridad de los ordenadores son muy habituales.

7 MyDoom

La familia de los gusanos MyDoom se ha extendido por el mundo entero durante años. Visto por primera vez en enero de 2004, MyDoom llamó tanto la atención que la compañía de Software SCO ofreció hasta 250.000 dólares estadounidenses, por cualquier información que llevara al arresto y sanción de los autores.[8]

Otra preocupación es que la variante más extendido –MyDoom-O – es capaz, al igual que Netsky, de infectar ordenadores Vista, lo que muestra una vez más lo importante que es poner al día la protección antivirus.[9]

8 Stratio

Stratio, un gusano enviado en masa que apareció en agosto de 2006, entró en el ranking gracias a su agresiva expansión.[10] Este gusano llega en forma de email con diferentes disfraces, incluyendo uno en que se presenta irónicamente como un parche para evitar la infección de un virus. El programa malicioso se oculta dentro de un archivo comprimido Zip y es uno de los tres gusanos capaces de infectar ordenadores Vista.

Se llegaron a enviar miles de versiones diferentes de Stratio llegando algunos días a más del 50% del total de los programas maliciosos detectados. La intención del gusano Stratio es divulgar imágenes spam, incorporando píxeles aleatorios que actúan como interferencias evitando así los filtros anti-spam. Lo que causó un notable crecimiento del spam a través de Internet a finales de 2006. Los mensajes anunciaban mayoritariamente tiendas farmacéuticas en línea.

9 Clagger

Clagger es el único troyano que aparece en los puestos más altos. Dado que los troyanos no pueden autoduplicarse, Clagger debe haber sido enviado a millones de direcciones de email para aparecer en el ranking, lo que demuestra la rapidez y el éxito con la cual pueden desarrollarse las campañas de spam. Intentando explotar una lista de vulnerabilidades conocidas, el troyano se instala en el ordenador. Su propósito es bajar programas espía para obtener información confidencial. Llegaban en mensajes con archivos ejecutables que pretendían provenir de empresas conocidas, como Amazon o PayPal.[11] En el informe de Sophos a mediados de 2006, Clagger se posicionaba en el octavo lugar del ranking, lo que demuestra el éxito de este troyano.

10 Dref

Identificado por primera vez a mediados de 2005. Versiones anteriores de Dref se extendían a través de canales de IRC y por email. Este gusano de Windows enviado en masa desactiva la protección antivirus y se envía a todas las direcciones de email que encuentra en el ordenador infectado, esparciendo así más programas maliciosos. Versiones más recientes, como el gusano Dref-N, hacía que los usuarios abrieran el archivo infectado haciéndose pasar por una gran noticia como una declaración de guerra nuclear o el anuncio de la muerte de George Bush.[12] Aún cuando los usuarios están informados de los riesgos que conlleva abrir archivos no solicitados, la curiosidad los convierte en víctimas de estos ataques.

La última versión, Dref-V, fue responsable de un 93,7% de los virus detectados en las últimas 48 horas del 2006, oculto detrás de una tarjeta de felicitación navideña.[13]

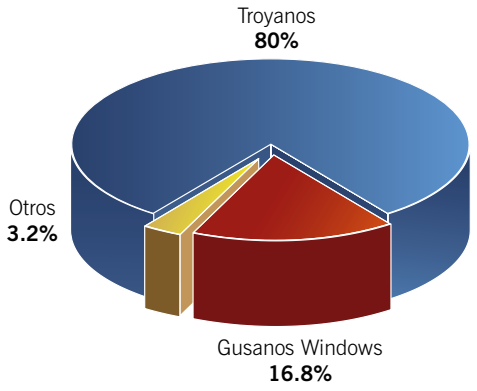
Las amenazas de email en 2007

El email seguirá siendo un factor importante para los creadores de programas maliciosos, pero Sophos prevé que el numero de mensajes con gusanos disminuirá. Será reemplazado, en cambio, por mensajes con técnicas de spam mediante imágenes y enlaces hacia sitios Web infectados. Existen dos razones para este cambio. Primero, un mensaje sin archivo ejecutable como documento adjunto es más probable que llegue al destinatario; y segundo, los gusanos son difíciles de controlar. Los virus y gusanos que más se expanden llaman demasiado la atención. Al infectar los sitios Web con troyanos de descarga y programas espía, los autores de códigos maliciosos pueden escoger mejor a sus víctimas.

Troyanos

Aún cuando los gusanos, como Dref y Stratio, se divulgaron por todo el mundo, el número de troyanos es ampliamente superior, aunque aparezcen en forma de pequeñas campañas enfocadas hacia grupos específicos de usuarios.

La proporción de troyanos se mantuvo constante durante el año 2006, con un promedio de alrededor un 80% de los programas maliciosos detectados durante todo el año. La tendencia de 2005 en el cual los troyanos sobrepasan a los gusanos sigue prevaleciendo.



Troyanos contra virus y gusanos de Windows 2006

Programas espía y de descarga

Los programas espía siguen causando dolores de cabeza y han provocado un significativo incremento del nivel de seguridad. Son la segunda preocupación más importante de seguridad para las empresas.[14] Se ocultan discretamente en los ordenadores, graban las teclas pulsadas y envían datos confidenciales a terceros sin que nadie se dé cuenta. También pueden preparar la red para futuros ataques.

Los creadores de programas espía en su afán de obtener información confidencial son cada vez más despiadados. Persisten en enviar programas espía "tradicionales" pero, eso no quita que también se estén orientando hacia nuevos métodos como ofrecer, mediante spam, programas gratuitos que atraen la atención del usuario. Cuando se accede a la web de descarga, los programas maliciosos infectan el ordenador.

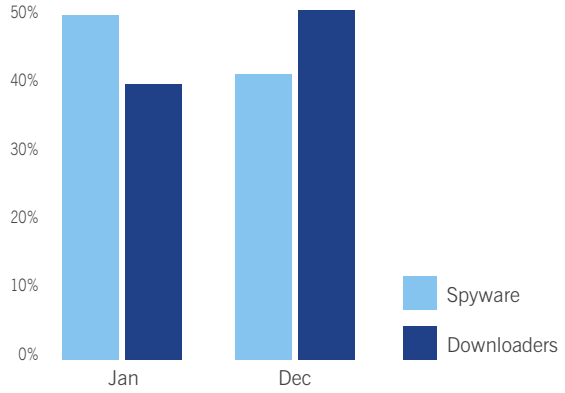
En realidad, este tipo de troyano no es nuevo, pero los programas de descarga están jugando un rol importante en la creación de programas maliciosos y vemos que las maneras de infectar son cada vez más complejas, en el cual el sitio infectado intentará evaluar la seguridad del ordenador, buscando vulnerabilidades o una manera de evitar el cortafuegos, con el objetivo de encontrar la manera de introducir el código malicioso en el ordenador de la víctima. Con el fin de disimular esta tentativa, algunos programas de descarga usarán otro que conduce a otro programa de descarga en otro sitio, el cual nos transfiere a otro sitio y así sucesivamente. El último programa de descarga tiene la función de bajar el programa espía que extrae información confidencial o da acceso a terceros no autorizados.

Familias muy extendidas han usado troyanos de descarga (por ejemplo, el gusano Bagle[15]) y muchas de las amenazas divulgadas a través de IRC cuentan con troyanos de descarga. Otro ejemplo es Zlob, también conocido como Popupper or Puper. [16] Esta familia de troyanos incluye una amplia variedad de componentes. Zlob emplea generalmente sitios pornográficos para incitar a los usuarios a descargar archivos que pretenden ser un códec de vídeo requerido para visualizar películas para adultos o una herramienta para obtener contraseñas de acceso a sitios de pago.

La versatilidad de los troyanos de descarga hace que sean más atractivos y el uso de programas maliciosos aumenta dramáticamente ; Sophos cree que prevalecerán junto a los programas espía. Las víctimas, en particular las que visitaron sitios pornográficos, desafortunadamente no irán a declarar. Además, el complicado camino entre el programa de descarga inicial y la instalación del programa malicioso eventual, hace la protección más difícil para los vendedores más pequeños de seguridad. En consecuencia, muchas empresas podrían desear sustituir sus medidas de seguridad por una solución única para poder bloquear programas maliciosos, spam, programas espía, adware y piratas de manera centralizada.

El gráfico siguiente muestra el porcentaje de email con programas espía y el porcentaje de mensajes asociados a sitios desde los cuales se descargan programas espía. Se puede ver claramente la tendencia hacia los programas de descarga.

El código malicioso situado en páginas web está preparado para enviar el troyano de descarga, que cambia con frecuencia para evitar su detección. Algunas veces, Sophos pudo observar modificaciones de códigos maliciosos siete veces al día en algunos sitios. Algunos de los programas publicitarios más conocidos también son modificados y presentados de maneras diferentes por sus creadores con el objetivo de evitar los dispositivos de seguridad.



Programas espía y de descarga en 2006

Programas maliciosos, sus orígenes

Además de elaborar protección contra programas maliciosos, los expertos de SophosLabs investigan la procedencia del código y los sitios web que los albergan.

Creación de programas maliciosos

El análisis forense de SophosLabs para determinar dónde se crean programas maliciosos, reveló algunas diferencias interesantes en la motivación y técnicas utilizadas por diferentes grupos de piratas en el mundo entero.

Por ejemplo, un 30% de programas maliciosos son creados en China. La mayoría toman la apariencia de puertas traseras, pero un porcentaje significativo (el 17%) de programas maliciosos de este país están destinados a robar contraseñas de jugadores online.[17]

Brasil es responsable del 14,2% de los programas maliciosos analizados por SophosLabs, la mayoría son troyanos con el fin de robar información confidencial de usuarios de banca por Internet.

Piratas rusos y suecos (responsable de un 4,1% y un 3,8% de programas maliciosos, respectivamente) crean por lo general puertas traseras que permiten el acceso no autorizado a ordenadores comprometidos. Por ejemplo, la familia Bifrose de troyanos representa un 15% de los programas maliciosos en Suecia y está diseñado para abrir puertas traseras.

Ucrania también parece ser cuna de creaciones de puertas traseras y “bots”, con un 3,4% de todos los programas maliciosos analizados por SophosLabs.

Saber que los autores de programas maliciosos chinos están interesados en robar información a jugadores en línea y que los autores brasileños prefieren extraer información de banca, ayuda a los expertos de seguridad y a las autoridades a mejorar la seguridad. Sophos cree que los piratas en China, Rusia y Brasil seguirán por una ruta similar en 2007, y será interesante ver qué países suben en la lista y hacia qué tipo de programa malicioso se inclinarán.

Países cuyos sitios web albergan programas maliciosos

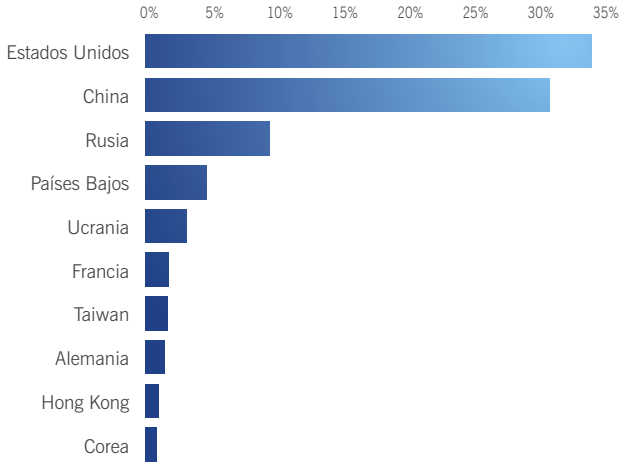
El gráfico de abajo indica la proporción de direcciones de páginas web que contienen programas maliciosos observados por SophosLabs durante 2006. Están clasificados según el país que alberga el sitio Web.

Dada la inmensa cantidad de ordenadores existentes en Norteamérica, no es sorprendente que Estados Unidos encabece la lista, hospedando a más de un tercio de los sitios que contienen códigos maliciosos.

Un país que llama la atención, sin embargo, es Holanda. Su presencia en el cuarto lugar con un 4,7%, se puede explicar debido a que tradicionalmente las compañías que albergan sitios web en este país son muy permisivas con sus usuarios, hasta los protege con el pretexto de la libertad de expresión. De hecho, el país alberga varios sitios que incluyen información y código dedicado a hackers y crackers.

Sophos opina que las compañías que albergan sitios web, como miembros de la comunidad global de Internet, deben actuar de manera responsable, supervisando más de cerca los contenidos que publican sus clientes, y colaborar con las autoridades para que un código malicioso detectado en un sitio público sea rápidamente retirado.

Será interesante ver cómo estas tendencias se desarrollan este año. Es difícil hacer un pronóstico en este aspecto debido a que depende mucho de los esfuerzos de los gobiernos por erradicar los sitios que albergan programas maliciosos. Muchas veces, los sitios atacados carecen de las medidas necesarias para impedir el acceso a piratas informáticos. Con programas maliciosos tan bien camuflados, los administradores que no cuenten con la protección adecuada ni siquiera se darán cuenta del peligro que albergan.



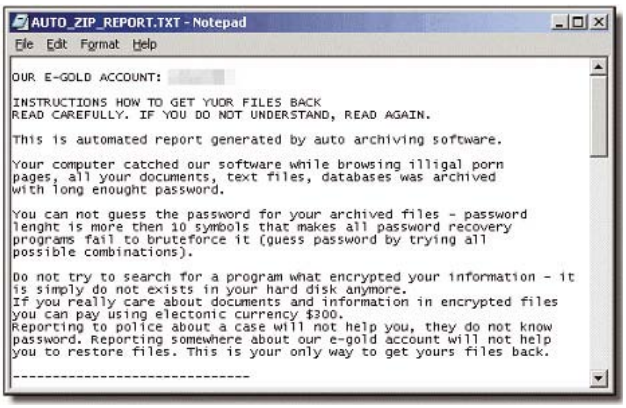
Principales 10 países cuyos sitios web albergan programas maliciosos en 2006

Software de secuestro

Este tipo de programa malicioso se utiliza para “secuestrar” datos de un ordenador encriptándolos y pidiendo un rescate a cambio de la contraseña. En casos más agresivos, se amenazaba incluso con borrar un archivo cada 30 minutos hasta que se pagase el rescate. Normalmente, los rescates se pagan a través de e-Gold o Western Union para ocultar la verdadera identidad del hacker. Esta técnica, que tiene su origen en Rusia, ahora se puede observar en todo el mundo.[18]

Ejemplos de software de secuestro durante el año 2006 son el gusano Arhiveus[19] y el troyano Zippo.[20]

Sin embargo, a pesar de estos ejemplos más conocidos, los programas de secuestro no aparecen en el ranking Top 10 de programas maliciosos y continuará siendo así en el 2007. Este tipo de extorsión no es muy habitual, dado que requiere cierta implicación y un gran esfuerzo por parte de los piratas informáticos. Además, es poco probable que las compañías estén dispuestas a pagar por el rescate, dado que la mayoría dispone de copias de seguridad.


AUTO_ZIP_REPORT.TXT - Notepad

File Edit Format Help

OUR E-GOLD ACCOUNT:

INSTRUCTIONS HOW TO GET YUOR FILES BACK
READ CAREFULLY. IF YOU DO NOT UNDERSTAND, READ AGAIN.

This is automated report generated by auto archiving software.

Your computer catched our software while browsing illigal porn pages, all your documents, text files, databases was archived with long enought password.

You can not guess the password for your archived files - password lenght is more then 10 symbols that makes all password recovery programs fail to bruteforce it (guess password by trying all possible combinations).

Do not try to search for a program what encrypted your information - it is simply do not exists in your hard disk anymore.
If you really care about documents and information in encrypted files you can pay using electonic currency $300.
Reporting to police about a case will not help you, they do not know password. Reporting somewhere about our e-gold account will not help you to restore files. This is your only way to get yours files back.

Ejemplos de software de secuestro

Software engañoso

Sophos ha constatado que, cada vez más, los autores de programas maliciosos y las compañías de adware se aprovechan de la inseguridad de los usuarios para ganar dinero.

En el año 2006 se ha visto un aumento de software engañoso, programas que hacen creer al usuario que su ordenador está infectado, y después incitan a comprar un programa que desinfectará el ordenador.

En un ejemplo, mensajes enviados con técnicas de spam informaban al usuario de la presencia en su ordenador de ciertos programas maliciosos, y ofrecían un producto llamado “Spyware Cleaner” como solución. El autor, Zhijian Chen de Portland, Oregón, ganó miles de dólares con este engaño, pero tuvo que pagar luego una multa de 84.000 dólares estadounidenses en abril de 2006.[21]

Las compañías de software deben tomar medidas estrictas cuando empresas afiliadas de publicidad quebrantan las leyes instalando programas maliciosos a ordenadores de usuarios inocentes para generar beneficios.

Programas maliciosos para móviles

Los programas maliciosos en dispositivos móviles siguen siendo un problema relativamente pequeño, si se compara con programas maliciosos destinados a ordenadores Windows. Sin embargo, poco a poco, la amenaza comienza a concretarse.

Algunas empresas de seguridad son en parte responsables por haber insistido demasiado en estas amenazas. En una encuesta web realizada por Sophos en junio de 2005, el 70% de los participantes pensaba que ciertas empresas de seguridad sobrestimaban las amenazas de virus para móviles.[22]

Sin embargo, en otra encuesta de Sophos en noviembre de 2006, un 81% mostró su preocupación por futuros ataques de programas maliciosos a teléfonos móviles[23], aunque el 64% de las empresas reconoce no disponer de protección para móviles ni ordenadores de mano.[24]

Es evidente que la protección para dispositivos móviles será importante en el 2007. Muchas empresas estarán poco dispuestas a comprar dispositivos para los cuales las medidas de seguridad todavía no existen. Los fabricantes deberán trabajar cada vez más con los expertos en materia de seguridad para elaborar una protección contra el robo de datos, amenazas y otras infracciones en seguridad.

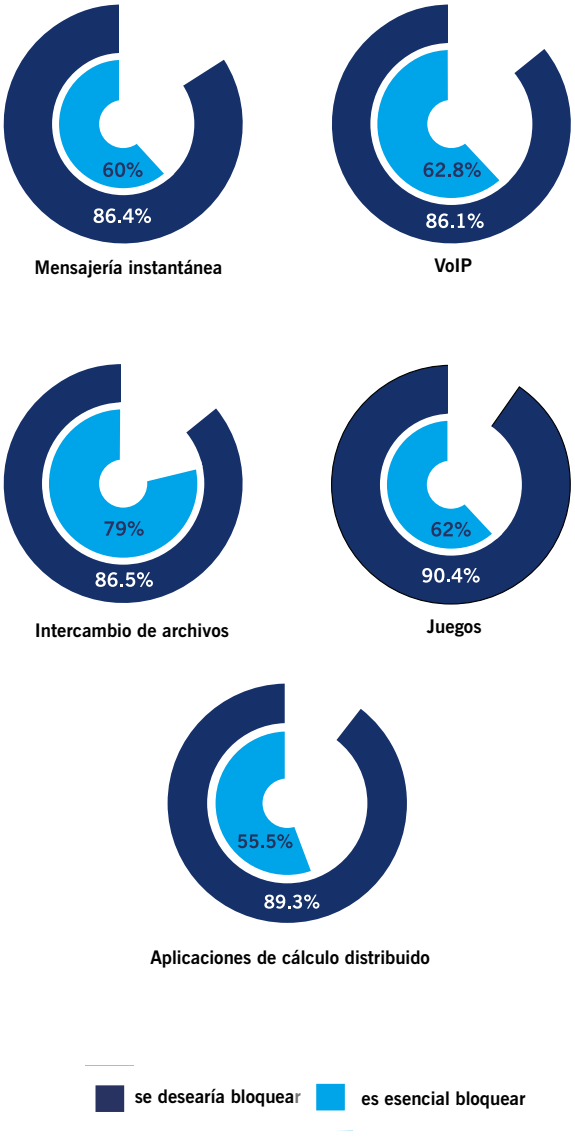
Amenazas internas

Aparte de las amenazas directas en materia de seguridad, los departamentos informáticos cada vez tienen más responsabilidad en la productividad de las empresas y en proteger el ancho de banda de la red, restringiendo el uso de aplicaciones no deseadas o no autorizadas y garantizando el uso eficiente y legal de la Web.

Restricción de aplicaciones

Un estudio realizado por Sophos en septiembre de 2006 revela que la preocupación principal de los administradores es no poder restringir el uso de aplicaciones.[25] Un 86,1% de los encuestados quisieran poder bloquear las aplicaciones de voz sobre IP (VoIP) y un 62,8% lo considera esencial.

Las empresas seguirán queriendo controlar las redes de sus entornos empresariales pero, a medida que la seguridad se hace más compleja, más difícil resulta educar a los usuarios. En lugar de confiar solamente en ellos y poner en peligro la integridad de la red, es preferible fortalecer las barreras contra esas posibles amenazas. La idea puede resultar muy atractiva para los dueños de las empresas, ya que esto significará también una reducción en el número de distracciones para los empleados. Impidiendo el uso de ciertas aplicaciones no esenciales, los departamentos informáticos podrán incrementar la producción de las empresas.



Navegar por Internet

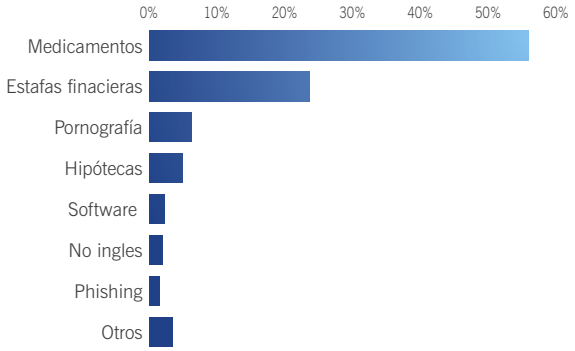
Durante el año 2006, los sitios web maliciosos se convirtieron en una amenaza creciente para las empresas, al igual que la libertad de los empleados para navegar por Internet de manera descontrolada, lo que puede afectar a la productividad y al ancho de banda de la red. Según una encuesta, los trabajadores pasan un 20% de su tiempo en Internet, por asuntos personales o entretenimiento.[26]

Los autores de programas maliciosos buscan constantemente puntos de acceso a las redes. Hoy en día, el punto más débil es la Web. La aparición de Web 2.0 amplía el nivel de vulnerabilidad de los usuarios y redefine los intercambios entre los usuarios de Internet. Además del acceso a sitios no regulados, descargar aplicaciones, escuchar música o ver vídeos es cada vez más habitual. Las defensas actuales de las empresas no protegen de manera adecuada contra el conjunto de nuevas amenazas provocado por el comportamiento de los usuarios, y la necesidad de disponer de dispositivos de seguridad para Internet se hace cada vez mayor.

Tipos de spam

El spam de tipo médico, principalmente relacionado con medicación para la mejora del rendimiento sexual, con la pérdida de peso o con hormonas de crecimiento, continúa siendo el tipo de spam más importante y ha aumentado durante este año. Este tipo de spam siempre ha sido popular entre los mensajes publicitarios, quizás porque los consumidores prefieren comprar estos productos de manera anónima a través de Internet o simplemente porque son difíciles de encontrar de manera legal. A finales de 2006, los mensajes de spam de contenido médico representaban la mitad de la totalidad de spam.

Podemos constatar otra alza (alrededor de un 10%): el spam relacionado con timos bursátiles, que representa un cuarto de la totalidad de mensajes de spam. En estas campañas bursátiles, conocidas como "pump-and-dump", se utiliza sobre todo spam en imágenes (detallado a continuación), con la intención de aumentar artificialmente el valor de ciertas acciones para permitir a los timadores hacer fortuna de manera rápida.



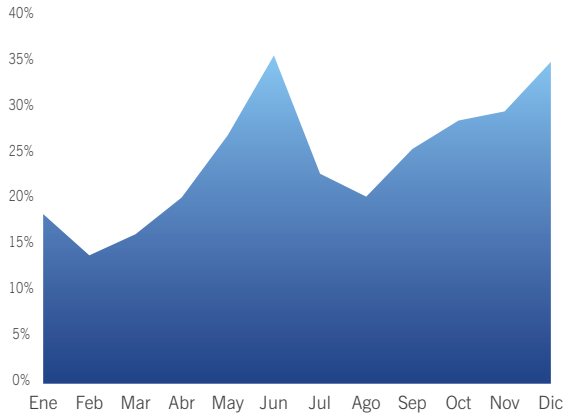
Categorías de spam dominante en 2006

Por otro lado, los mensajes de spam de contenido pornográfico han disminuido considerablemente: en 2005, representaban un 17% y, a finales de 2006, sólo un 6%. Puede que la legislación más severa dirigida especialmente hacia este tipo de comunicación ofensiva desalentase a los autores y que optaran por utilizar los mensajes basura para otro tipo de mercancías y servicios.

El spam de hipotecas también bajó en la clasificación a un 5%, mientras que en 2005 era de un 12%.

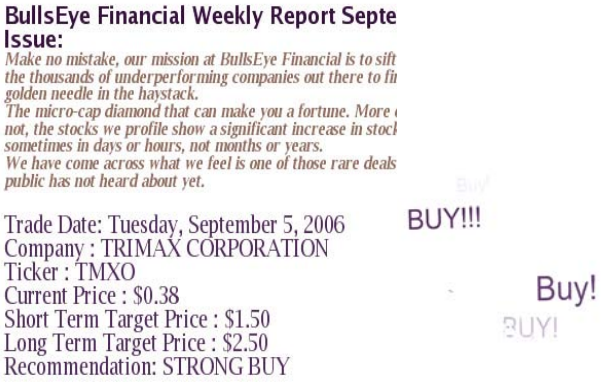
Spam en imágenes

Uno de los crecimientos clave en 2006 fue el aumento del spam con imágenes, que subió de un 18,5% en enero a un 35,1% a finales de diciembre. La posibilidad de que los usuarios lean este tipo de mensajes es mayor, ya que el uso de imágenes evita su detección por parte de los filtros anti-spam basados en el análisis del texto. La imagen en formato GIF suele contener múltiples capas, que añaden interferencias y complican aún más el análisis.



Porcentaje de spam en imágenes del total de spam

La gran mayoría de los mensajes de spam en imágenes se utilizan en campañas bursátiles pump-and-dump como la citada anteriormente, cuya intención es aumentar artificialmente el valor de ciertas acciones para permitir a los timadores obtener beneficios de manera rápida.

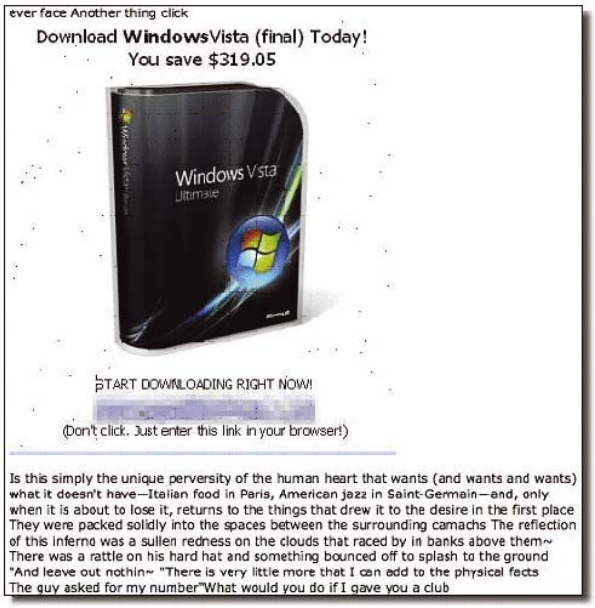


Mensajes de spam Pump-and-dump que cambia cada 15 segundos para mostrar el mensaje subliminal "COMPRA"

Otro tipo de spam en imágenes

A finales de año, los autores de spam intentaron ganar dinero con la edición de Microsoft Windows Vista, ofreciendo una edición en oferta del nuevo sistema operativo. No está muy claro si la intención del spam era vender ediciones pirateadas de Windows Vista o simplemente robar los datos de las tarjetas de crédito.[27]

Otro spam en imágenes utilizaba la nueva técnica con una antigua estratagema: la pornografía como anzuelo. Durante la campaña de spam, destinada a usuarios australianos, se enviaban mensajes que fingían provenir de una joven que estaba de visita en el país.[28] El mensaje no contenía texto, pero sí una imagen que invitaba a los usuarios a visitar un sitio web que contenía una imagen de pornografía suave y un enlace al troyano Troj/Dloadr-AMA.



Spam en imágenes que ofrece Vista a precio excepcional

Pesca de información

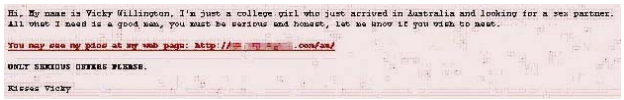
Una encuesta realizada por SophosLabs en 2006 reveló que un 75% de los mensajes de pesca de información va dirigido a usuarios de PayPal o eBay[29], pero éstas no son las únicas instituciones objetivo de los ladrones de identidades por Internet.

Los primeros casos organizados de pesca de información por teléfono (también conocida como “vishing”) se vieron en 2006, en los que los timadores pedían a los destinatarios de los mensajes que llamaran por teléfono a un número específico, en lugar de contestar por email o ir al sitio web. Los hackers son cada vez más astutos y ya no se conforman con crear sitios web falsos, si no que pueden llegar a recolectar mensajes de las centrales telefónicas de las empresas para hacerse pasar por la compañía legítima.[30]

Es muy probable que, en 2007, los piratas informáticos intenten aprovechar las vulnerabilidades de las aplicaciones de voz sobre IP (VoIP) para la pesca de información por teléfono.

Mientras tanto, las técnicas tradicionales de pesca de información continúan afectando a muchos usuarios de email.

Uno de los ejemplos de peor gusto a la hora de abusar de la generosidad de la gente se produjo con motivo de las víctimas del huracán Katrina[31], momento que un joven de 20 años de Miami aprovechó para recolectar dinero desde un sitio web falso.



Spam en imágenes con pornografía como anzuelo

Probablemente veamos cómo la pesca de información toma nuevas direcciones en 2007. Aunque los usuarios son cada vez más cautelosos con los mensajes que parecen provenir de organizaciones conocidas, los timadores utilizan trucos muy astutos para engañar a los usuarios y hacerles creer que el mensaje es verdadero. Puesto que las autoridades han mejorado sus técnicas para identificar estafas internacionales de pesca de información, es probable que los delincuentes se vuelquen en un público más indirecto mediante estafas financieras.

Los doce principales países emisores de spam

Sophos examina todos los mensajes de spam recibidos en su red mundial de captación de spam. Mediante este análisis, los expertos de SophosLabs concluyeron que, si bien Estados Unidos ha seguido avanzando notablemente en sus esfuerzos para reducir las cifras de emisión de spam, sus ordenadores siguen enviando más spam que los de cualquier otro país.

De forma general, el análisis sigue más o menos la misma línea que en 2005, aunque hay algunas excepciones.

China y Corea del Sur intercambiaron sus posiciones. La disminución significativa de spam de Corea del Sur puede atribuirse a la próspera inversión en su infraestructura de Internet y a la adquisición continuada de sistemas operativos más resistentes. Los usuarios son más conscientes de las amenazas para la seguridad y protegen sus ordenadores de forma adecuada, disminuyendo el riesgo de que se infecten y se utilicen para emitir spam.

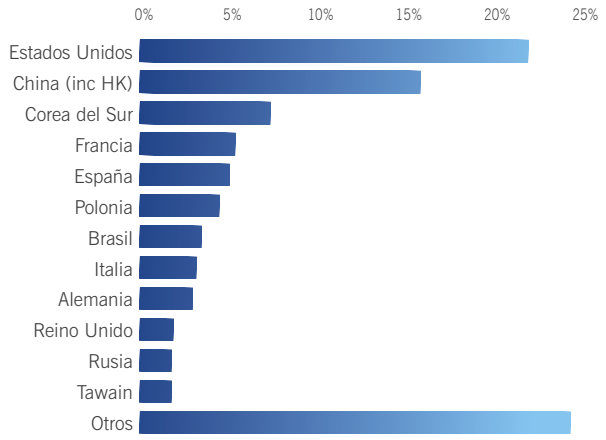
Canadá bajó de la quinta posición en 2005 a la decimoséptima en 2006, gracias a los esfuerzos de las autoridades para garantizar la ejecución adecuada por parte de los proveedores de servicios de Internet (ISP).

Mientras que Estados Unidos, Corea del Sur y China representan más de un 45% de la totalidad de spam, la clasificación por continentes revela que Europa supera a Estados Unidos y es responsable de la tercera parte del spam mundial. Esto puede atribuirse a varios factores, como las condenas para los creadores de spam, legislaciones más estrictas o mejores sistemas de seguridad.

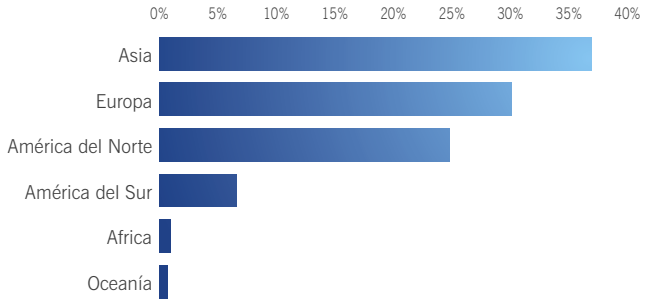
Hasta un 90% del spam se envía desde ordenadores "zombi", también conocidos como ordenadores "botnet", secuestrados por troyanos, gusanos y virus bajo el control de hackers. Estos ordenadores pueden encontrarse en cualquier lugar, lo que significa que los piratas no necesitan estar en el mismo país que el ordenador secuestrado para enviar el spam.

Las redes de ordenadores zombi pueden enviar cientos de millones de spam en unas pocas horas, por lo que suponen un serio reto para los encargados de la seguridad de Internet.

Sea cual sea su ubicación, los creadores de spam pueden aprovechar las conexiones de banda ancha inseguras de cualquier lugar del mundo para enviar mensajes de publicidad no deseados.



Los doce principales países emisores de spam en 2006



Clasificación de los continentes emisores de spam en 2006

Timos

Los delincuentes siguieron utilizando Internet con la intención de estafar a usuarios inocentes y hacerse con dinero o información confidencial.

La estafa conocida como timo 419, que debe su nombre al número del artículo que se infringió en el código penal de Nigeria, donde se originaron muchos de estos timos, suele ofrecer grandes cantidades de dinero. Una vez que la víctima entra en la trampa, el estafador pide información confidencial para luego poder apoderase de su identidad y obtener su dinero.

Los timadores han adoptado muchos disfraces diferentes en los últimos 12 meses:

- Un agente moribundo del KGB que afirma conocer secretos sobre el asesinato de John F. Kennedy[32]
- Un joven de 19 años que asegura haber encontrado la cura contra el SIDA[33]
- Una falsa negociación de un sargento militar americano desde Baghdad[34]
- Abogados que pretenden representar los bienes de las víctimas del desastre del Concorde[35]
- Supuestos remedios para curar a personas heridas en el desastre minero de Virginia del Oeste[36]
- La secretaria de un magnate del petróleo en prisión[37]
- Una agencia de modelos australiana que busca personas interesadas en la televisión y el cine[38]
- El Ministro escocés de la Cultura, Turismo y Deporte[39]

Los timos de email no desaparecerán en 2007, por lo que los usuarios de ordenadores seguirán corriendo el riesgo de que los timadores de Internet les estafen.

Crimen y castigo

El dinero es, sin duda, la primera motivación para los autores de virus y spam hoy en día. En el pasado, la motivación de los creadores de programas maliciosos era demostrar lo que eran capaces de hacer pero, hoy en día, esa motivación es generar beneficios, robar identidades e información confidencial, lanzar ataques de denegación de servicio y, a veces, distribuir software de secuestro.

Dada esta finalidad lucrativa de los programas maliciosos, las legislaciones para juzgar y condenar a los culpables se están volviendo cada vez más severas.

Dada esta finalidad lucrativa de los programas maliciosos, las legislaciones para juzgar y condenar a los culpables se están volviendo cada vez más severas.

En 2006 vimos ciertas acciones importantes contra creadores de spam, estafadores, pescadores de información y autores de programas maliciosos. Pero, puesto que el crimen en Internet es un fenómeno global, sigue siendo indispensable tomar las medidas necesarias contra los cibercriminales a nivel mundial. Las leyes se siguen adaptando en todo el mundo, teniendo en cuenta los últimos crímenes cometidos en Internet.[40] El Reino Unido, por ejemplo, ha comenzado a ocuparse de los ataques de denegación de servicio, una iniciativa muy aplaudida, ya que las redes "zombi" y el chantaje por Internet se han convertido en elementos clave de la avalancha de crímenes.

Estados Unidos ha dado el ejemplo imponiendo sanciones y multas severas a los creadores de spam más prolíficos, ayudado por legislaciones como CAN-SPAM y la información que compartían los proveedores de servicios de Internet. Durante el primer trimestre de 2006, varios miembros de bandas responsables de la distribución masiva de pornografía reconocieron pertenecer a un círculo criminal de spam. Jennifer Clason, de New Hampshire, Andrew Ellifson, de Arizona, y Kirk Rogers, de California, formaban parte de una banda que enviaba por email miles de mensajes anunciando sitios web para adultos.[41]

Jeanson James Ancheta, un hacker de 21 años de California que se hizo con el control de 400.000 ordenadores para crear una red "zombi", fue condenado a 57 meses de prisión en mayo de 2006.[42] Ancheta, que admitió comercializar las redes de bots por Internet, vendía el acceso al software que permitía tomar el control de los ordenadores para propagar spam y lanzar ataques de denegación de servicio contra sitios web. Los sitios web afectados por estos ataques podían convertirse más tarde en víctimas de chantaje y pagar grandes cantidades de dinero para recuperar el acceso del público a su sitio. Ancheta hizo aun más dinero instalando programas publicitarios en los ordenadores "zombi". De esta forma, pudo comprar servidores de ordenadores y realizar ataques adicionales, comprarse ropa nueva y un lujoso BMW. Además de ir a la cárcel, Ancheta fue condenado a pagar 15.000 dólares a organizaciones militares cuyos ordenadores se vieron afectados por los ataques.

Las autoridades marroquíes condenaron a Farid Essebar y Achraf Bahloul a prisión en septiembre de 2006 por su participación en la creación y difusión del gusano Zotob, que aprovechaba la vulnerabilidad de seguridad MS05-039 de programas de Microsoft en agosto de 2005 y bloqueó los ordenadores de la CNN, la ABC, The Financial Times y The New York Times.[43] La corte condenó a Essebar, estudiante de ciencias de 19 años, a dos años de prisión y a Bahloul, de 22 años de edad, a un año de prisión por crear y divulgar este gusano.

Es habitual que los autores de programas maliciosos dejen su firma en los códigos maliciosos, a veces, junto a otros mensajes y Essebar, residente marroquí de origen ruso, utilizaba la firma "Diabl0" presente en el código del gusano W32/Zotob-A. Los analistas de Sophos han asociado también al "Diabl0" a otros veinte gusanos más, como por ejemplo, a la amenaza más prolífica en el 2006, el gusano Mytob.

En agosto de 2006, otro hacker californiano de 21 años, Christopher Maxwell, fue condenado a 3 años de prisión después de reconocerse culpable de haber infectado 50.000 ordenadores pertenecientes a bases militares de EEUU, escuelas y un hospital en Seattle.[44] Sus ataques alteraron las operaciones del hospital y reportaron a Maxwell y a su banda más de 100.000 dólares mediante la introducción de programas publicitarios en ordenadores infectados.

En septiembre, la Autoridad de Comunicaciones Australiana (ACMA) comenzó una investigación sobre las actividades de un hombres sospechoso de difundir más de dos mil millones de mensajes de spam de Viagra",[45] mientras que en Estados Unidos se emprendió una acción contra dos empresas acusadas de haber enviado mensajes de apuestas y bebidas alcohólicas a menores.[46]

También en EE.UU., William Bailey Junior, de Carolina del Norte, se enfrentó a una pena máxima de 55 años de cárcel y 2.750.000 de dólares de multa de ser condenado culpable por obtener información de manera ilegal sobre 80.000 miembros del Colegio de Física de América.

Las autoridades rusas arrestaron a una banda que realizaba chantajes a empresas por Internet mediante ataques de denegación de servicio.[47] La banda se hizo con más de 4 millones de dólares de empresas británicas después de haberlas amenazados con atacar sus sitios web y hacerlas inaccesibles al mundo exterior. El grupo, que se servía de ordenadores "zombi" para lanzar ataques de denegación de servicio, tenía como objetivo casinos y sitios de apuestas por Internet. Ivan Maksakov, Alexander Petrov y Denis Stepanov fueron condenados a una multa de 3.700 dólares cada uno y a 8 años de prisión.

En diciembre, el tribunal alemán condenó a un hombre a cuatro años de prisión y, a otro, a una sentencia de 39 meses por haber participado en una acción criminal que consistía en introducir troyanos en ordenadores de usuarios inocentes que marcaban números de teléfonos de tarifas especiales para entrar en contacto con sitios web pornográficos.[48] Infectando más de 100.000 ordenadores con este troyano, la banda consiguió más de 12 millones de euros.

Resumen

Aunque la encuesta de Sophos revela que muchas empresas piensan que la seguridad en el año 2007 será peor que el año anterior, el problema, si se trata de manera correcta, no es irremediable. Los criminales continuarán buscando nuevas formas de infectar ordenadores y robar información confidencial pero las prácticas de seguridad eficaces y las actualizaciones de la protección deberían ayudar en la protección de las redes empresariales. Las empresas deben tomar ahora las medidas para asegurarse de que están completamente protegidas, introducir una política y procedimientos severos y proteger todas las vías que conducen hacia sus redes y ordenadores para reducir al máximo las posibilidades de ataques.

Para saber más sobre los productos de Sophos, visite **esp.sophos.com**

Fuentes

1 www.sophos.com/pressoffice/news/articles/2005/08/va_diablo.html
2 www.sophos.com/pressoffice/news/articles/2005/07/va_sasserfree.html
3 www.es.sophos.com/pressoffice/news/articles/2006/11/toptennov.html
4 www.sophos.com/pressoffice/news/articles/2005/12/soberzcrim.html
5 www.es.sophos.com/pressoffice/news/articles/2005/12/toptensummary05.html
6 www.es.sophos.com/pressoffice/news/articles/2006/02/nyxempanic.html
7 www.sophos.com/pressoffice/news/articles/2006/02/baglecm.html
8 www.sophos.com/pressoffice/news/articles/2004/01/va_mydoombounty.html
9 www.es.sophos.com/pressoffice/news/articles/2006/11/toptennov.html
10 www.es.sophos.com/pressoffice/news/articles/2006/09/stration-worm.html
11 www.sophos.com/pressoffice/news/articles/2006/02/claggerh.html
12 www.sophos.com/pressoffice/news/articles/2006/11/drefn.html
13 www.sophos.com/pressoffice/news/articles/2007/01/drefv.html
14 Worldwide Secure Content Management 2005-2009 forecast update and 2004 vendor shares: spyware, spam, and malicious code continue to wreak havoc. IDC. September 2005
15 www.sophos.com/pressoffice/news/articles/2004/03/va_baglegraphic.html
16 www.sophos.com/virusinfo/analyses/trojzloba.html
17 www.es.sophos.com/pressoffice/news/articles/2006/11/chinamalware.html
18 www.sophos.com/pressoffice/news/articles/2006/04/ransom.html
19 www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html
20 www.es.sophos.com/pressoffice/news/articles/2006/03/zippo.html
21 www.sophos.com/pressoffice/news/articles/2006/04/spywarechen.html
22 Sondeo web Sophos, Junio 2005
23 Sondeo web Sophos, Noviembre 2006
24 Sondeo web Sophos, Enero 2007
25 Sondeo web Sophos, Septiembre 2006
26 Burstek releases 2005 internet usage study. www.findarticles.com/p/articles/mi_m0EIN/is_2006_March_20/ai_n16109780
27 www.sophos.com/pressoffice/news/articles/2006/12/vistaspam.html
28 www.sophos.com/pressoffice/news/articles/2006/08/vicky-image-trojan.html
29 www.sophos.com/pressoffice/news/articles/2006/07/top-phishing-targets.html
30 www.sophos.com/pressoffice/news/articles/2006/07/paypalvox.html
31 www.sophos.com/pressoffice/news/articles/2006/08/hurricane-phisher.html
32 www.sophos.com/pressoffice/news/articles/2006/08/kennedy-scam.html
33 www.es.sophos.com/pressoffice/news/articles/2006/07/aidscure.html
34 www.sophos.com/pressoffice/news/articles/2006/01/iraq419.html
35 www.sophos.com/pressoffice/news/articles/2006/04/concorde419.html
36 www.sophos.com/pressoffice/news/articles/2006/01/sago.html
37 www.sophos.com/pressoffice/news/articles/2006/01/yukos.html
38 www.sophos.com/pressoffice/news/articles/2006/09/model-scam.html
39 www.sophos.com/pressoffice/news/articles/2006/06/scottishmp419.html
40 www.cybercrimelaw.net
41 www.sophos.com/pressoffice/news/articles/2006/03/clason.html
42 www.sophos.com/pressoffice/news/articles/2006/05/anchetasentence.html
43 www.es.sophos.com/pressoffice/news/articles/2006/09/zotob-jail.html
44 www.sophos.com/pressoffice/news/articles/2006/08/maxwell-sentence.html
45 www.sophos.com/pressoffice/news/articles/2006/09/viagra-spammer.html
46 www.sophos.com/pressoffice/news/articles/2006/08/kid-spam-lawsuit.html
47 www.sophos.com/pressoffice/news/articles/2006/10/extort-ddos-blackmail.html
48 www.sophos.com/pressoffice/news/articles/2006/12/dialgang.html

Acerca de Sophos

Sophos es un líder mundial en soluciones integradas de control de amenazas para empresas, educación y gobiernos. Con más de 20 años de experiencia en la lucha contra virus, programas espía y spam, SophosLabs ofrece protección, incluso en los entornos más complejos, contra amenazas conocidas y desconocidas. Nuestros aclamados productos protegen ya a más de 35 millones de usuarios en más de 150 países contra virus, programas espía, intrusión, aplicaciones no deseadas, ataques de pesca de información, spam y abusos en políticas de email. Respuesta inmediata y dedicación a clientes corporativos, así como soporte técnico 24 horas, definen los servicios que nos han llevado a los más altos niveles en la satisfacción del cliente.

Boston, EE.UU. • Mainz, Alemania • Milán, Italia • Oxford, GB • París, Francia
Singapur • Sydney, Australia • Vancouver, Canadá • Yokohama, Japón

© Copyright 2007. Sophos Plc.

Marcas registradas y copyrights reconocidos por Sophos. Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sin la previa autorización escrita por parte del propietario.

SOPHOS
secured.