Virus informáticos al descubierto

Virus

Email

Internet

Sistemas móviles

Seguridad

Referencia

Virus informáticos al descubierto

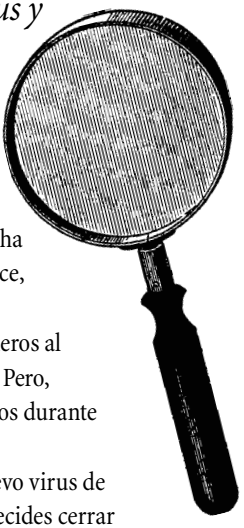
Editado y diseñado por Paul Oldfield.
Traducido por Javier Acebes.

Suegerencias: enquiries@sophos.com
Sitio Web: www.sophos.com

Contenido

Virus, ¿y qué?

Virus, hackers, crackers, delitos informáticos. Son noticia cada día y, como reclaman los medios, suponen millones. Pero ¿cuál es la verdadera importancia de los virus y otras amenazas del ciberespacio? ¿Cuál es el daño real?



Para hacerte una idea, intenta imaginar lo que podría pasar en tu oficina o en tu casa.

Imagina que tu programa antivirus no se ha actualizado desde hace meses. Y, cuando se hace, descubres que todas tus hojas de cálculo de contabilidad tienen un virus que cambia números al azar. Por supuesto, tienes copias de seguridad. Pero, claro, has estado guardando archivos infectados durante meses. ¿Con qué cuentas te quedarás?

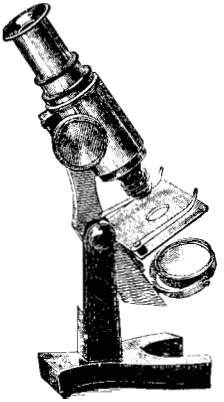
Ahora imagínate que ha aparecido un nuevo virus de email. Tu compañía recibe tantos email que decides cerrar por completo su entrada … y pierdes un pedido urgente de tu mejor cliente.

Suponte que estás en casa preparando la recta final ese Master tan importante. Ya casi has terminado tu tesis cuando

alguien instala un nuevo juego e infecta tu ordenador. El virus borra por completo el contenido del disco duro … incluyendo todo tu trabajo.

Imagina que un amigo te envía unos archivos que encontró en Internet. Cuando los abres, se ejecuta un virus que envía ciertos documentos confidenciales de tu empresa a todas las personas de tu libro de direcciones … incluyendo la competencia.

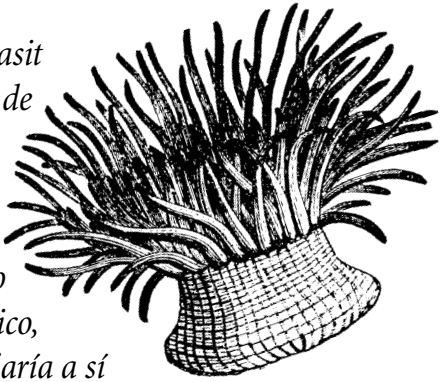
Finalmente, imagina que envías un informe con un virus a algunos de tus clientes. ¿Seguirán confiando en tu forma de hacer negocios?



Todos estos ejemplos son verídicos. Todos se podrían haber evitado tomando unas medidas muy elementales y, en su mayoría, gratuitas.

En esta guía se enumeran los riesgos y se ofrecen soluciones.

Virus, troyanos y gusanos



A mediados de los '80, Basit y Amjad Alvi de Lahore, de Pakistán, descubrieron que la gente pirateaba sus programas. Ellos respondieron escribiendo el primer virus informático, un programa que se copiaría a sí mismo y un mensaje de copyright en cada copia de un disquete que sus clientes hicieran. A partir de esta simple idea surgió una nueva contracultura. Hoy nuevos virus se extienden por todo el planeta en horas y las amenazas víricas son noticia. Pese a la fascinación que generan, la gente no está bien informada. Siga leyendo para ver cómo se transmiten los virus y cómo protegerse.

¿Qué es un virus?

Un virus informático es un programa con la capacidad de transmitirse entre ordenadores y redes, generalmente sin el conocimiento de los usuarios.

Los virus pueden tener indeseables efectos secundarios. Desde molestar con absurdos mensajes hasta borrar todo el contenido del disco duro.

¿Cómo se infecta un ordenador?

El virus tiene que ser ejecutado para conseguir infectar un ordenador.

Con este propósito, los virus pueden adosarse a otros programas u ocultar su código de manera que se ejecutan al intentar abrir ciertos tipos de archivo.

Un archivo infectado te puede llegar en un disco, adjunto en un email o al descargarlo de Internet. En cuando ejecutes el archivo, se ejecutará el código del virus. El virus intentará entonces infectar otros archivos o discos y realizar cambios en tu ordenador.

Cada tipo de virus lo hace de una manera diferente, como se explica en este capítulo en las secciones 'Virus de sector de arranque', 'Parásitos' y 'Virus de macro'.

Troyanos

Un caballo de Troya es un programa que en su ejecución realiza tareas no previstas de antemano.

El usuario ejecuta lo que cree un programa normal, permitiendo al troyano realizar tareas ocultas y, a menudo, malignas.

Por ejemplo, *Troj/Zulu* se presenta como un programa que evita el 'millennium bug' y que, sin embargo, te sobrescribe el disco duro entero.

Los troyanos se emplean a veces con la intención de extender la infección de un virus.

Los troyanos de puerta trasera son programas que permiten a otros tomar el control de tu ordenador a través de Internet.

Gusanos

Los gusanos son similares a los virus pero no necesitan portador (como una macro o un sector de arranque).

Los gusanos crean copias exactas de ellos mismos y utilizan enlaces entre ordenadores para enviarse.

Muchos virus, como *Kakworm* (*VBS/Kakworm*) o *Love Bug* (*VBS/LoveLet-A*), se comportan como gusanos y utilizan el correo electrónico para propagarse.

¿Qué hacen los virus?

El efecto de un virus, también llamado carga explosiva, es lo que más interesa a los usuarios. Estos son sólo algunos ejemplos.

Mensajes *Telefónica* muestra el mensaje 'Campaña Anti-TELEFONICA (Barcelona)'

Bromas *Yankee* toca la canción 'Yankee Doodle' a las 5.

Bloquear acceso *WM97/NightShade* bloquea el acceso a los documentos abiertos en viernes 13.

Robar datos *Troj/LoveLet-A* envía información por correo electrónico sobre el usuario y el equipo a una dirección en Filipinas.

Corromper *XM/Compatable* cambia cifras de forma aleatoria en hojas de cálculo de Excel.

Borrar datos *Michelangelo* sobrescribe parte del disco duro el 6 de marzo.

Dañar el equipo *CIH* o *Chernobyl* (*W95/CIH-10xx*) intenta sobrescribir la BIOS el 26 de abril, lo que deja inutilizable el equipo.

¿Dónde hay riesgo de virus?

Estos son los puntos donde tu oficina es vulnerable.

Internet

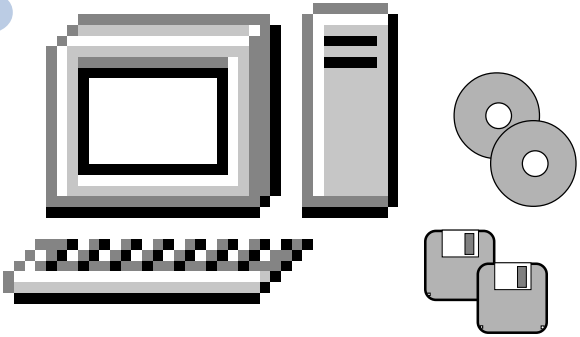
Programas o documentos descargados pueden estar infectados.

Documentos y hojas de cálculo

Pueden contener virus de macro, que pueden infectar y realizar cambios en otros documentos u hojas de cálculo.

Programas

Un programa con un virus puede infectar tu equipo tan pronto como lo ejecutes.



Email

Un email puede adjuntar un archivo infectado. Al hacer doble clic sobre él lo estás ejecutando, con el consiguiente riesgo. Algunos mensajes incluso vienen con código que se ejecuta mientras los estas leyendo.

Disquetes y CD-ROM

Un disquete puede contener virus en el sector de arranque. Además, igual que el CD-ROM, puede contener programas o documentos infectados.

Prevenir virus

Existen ciertas medidas elementales con las que puedes evitar infecciones o recuperarte si ya has sido infectado.

Informa sobre los riesgos

Conciencia a todos en la empresa de los riesgos que conlleva intercambiar discos, descargar archivos de Internet o abrir adjuntos de correo electrónico.

Instala algún programa antivirus y tenlo al día

Los programas antivirus pueden detectar y, a menudo, desinfectar virus. Si el programa ofrece escaneado en acceso, utilízalo. Así, el programa bloqueará el acceso a archivos infectados. Lee la sección 'Programas antivirus' en este capítulo.

Mantén copias de seguridad

Asegúrate de contar con copias de seguridad de todos tus documentos y programas, incluyendo el sistema operativo. Siempre podrás reemplazar los archivos infectados con los de la copia de seguridad.

Encontrarás más consejos en el capítulo 'Decálogo de seguridad antivirus'.

Virus de sector de arranque

Fueron los primeros virus en aparecer. Se propagan modificando el sector de arranque, que contiene la información de inicio del ordenador.

Al encender el ordenador, se ejecuta el programa del sector de arranque (que normalmente estará en el disco duro, aunque también en disquetes y CD-ROM) que cargará el resto del sistema operativo.

Un virus de sector de arranque sustituye este programa (normalmente oculta el original en otra parte del disco duro). La próxima vez, el ordenador se iniciará con el sector de arranque infectado y el virus se activará.

Tu equipo sólo se puede infectar si lo inicias desde un disco infectado, como un disquete que ya contiene un virus en el sector de arranque.

La mayoría de estos virus son ya bastante antiguos. Los virus que se crearon para el sistema operativo DOS no suelen infectar equipos con Windows 95, 98, Me, NT o 2000, aunque pueden dañar el programa del sector de arranque.

Form

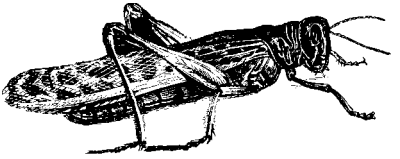
Este virus apareció hace diez años y aún se encuentra bastante activo. La versión original se activa el 18 de cada mes y produce un pitido cada vez que se pulsa una tecla.

Parity Boot

Este virus muestra de forma aleatoria el mensaje 'PARITY CHECK' y bloquea el sistema. El mensaje imita el formato de los mensajes que aparecen cuando se produce un error real de la memoria.

Parásitos (virus de archivo)

Los parásitos, también conocidos como virus de archivo, se alojan en archivos ejecutables.



Cuando se ejecuta un archivo infectado, el virus se ejecutará primero y, para permanecer oculto, iniciará el programa original.

El sistema operativo verá el virus como parte del programa que estás ejecutando y le asignará los mismos privilegios. Esto le permitirá infectar otros archivos, cargarse en memoria o realizar cualquier otra fechoría.

Los parásitos aparecieron hace ya bastante tiempo pero aún suponen una seria amenaza. Internet ha facilitado el intercambio de programas y, así mismo, la posibilidad extender estos virus.

Jerusalem

En viernes 13, borrará cada programa que se ejecute.

CIH (Chernobyl)

El 26 de algunos meses, sobrescribirá parte de la BIOS, inutilizando el ordenador. El virus también sobrescribirá el contenido del disco duro.

Remote Explorer

WNT/RemExp (*Remote Explorer*) infecta archivos ejecutables de Windows NT. Fue el primero en ejecutarse como servicio, es decir, no depende de la sesión del usuario.

Virus de macro

Estos virus aprovechan las propiedades de las macros, comandos de ciertos documentos que se ejecutan con él.

Algunos programas, como procesadores de texto o de hojas de cálculo, utilizan macros.

Un virus de macro es una macro que puede copiarse a sí misma y transmitirse de un documento a otro. Al abrir un documento infectado, el virus se introducirá en los archivos de inicio del programa, con lo tu equipo quedará infectado.

Cada documento que abras con en ese programa quedará infectado. Si tu equipo está en red, la infección se puede extender rápidamente: cualquiera con el que compartas tus documentos también podrá quedar infectado.

Macros malintencionadas podrán alterar tus documentos o la configuración.

Los virus de macro suelen atacar a alguno o varios de los tipos de archivo más comunes, como archivos de Word o Excel. Además, estos virus no dependen del sistema operativo. Pero, por encima de todo, se extienden con facilidad por el constante intercambio de este tipo de archivos.

WM/Wazzu

Infecta documentos de Word. Cambia de lugar entre una y tres palabras e inserta al azar la palabra 'wazzu'.

OF97/Crown-B

Puede infectar archivos de Word, Excel y PowerPoint. Al infectar un documento de Word, inhabilita la protección de macro en las demás aplicaciones de Office 97 para poder infectarlas también.

Programas antivirus

Los programas antivirus pueden detectar virus, evitar el acceso a archivos infectados y, a menudo, acabar con la infección. Hay diferentes tipos de programas antivirus.

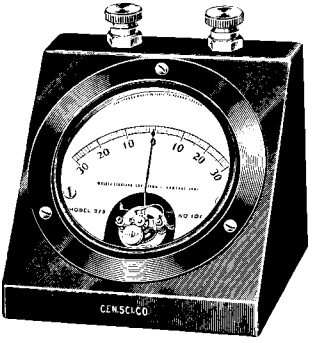
Escáner

Programas de escaneado de virus pueden detectar, y a menudo desinfectar, los virus conocidos hasta la fecha del programa. Es el tipo de antivirus más popular pero hay que actualizarlo a menudo para que reconozca virus nuevos.

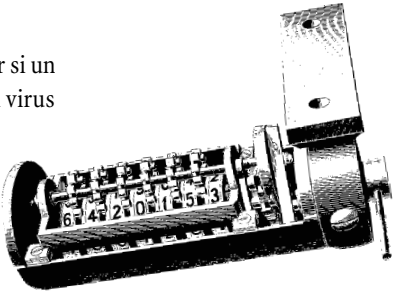
Pueden disponer de escaneado *en demanda* o *en acceso*. Muchos antivirus ofrecen ambos.

El escaneado *en demanda* lo controla el usuario y permite programar el escaneado de carpetas o unidades determinadas.

El escaneado *en acceso* se encuentra activo permanentemente y comprueba cada archivo antes de que puedas utilizarlo



Verificador



Estos programas pueden detectar si un archivo ha sido modificado. Si un virus infecta un programa o un documento, ya que lo modifica, el programa de verificación lo detectará.

Lo mejor de estos programas es que no necesitan saber nada del virus para poder detectarlo, por lo que no es necesaria una actualización constante.

El problema es que no pueden identificar si se trata de un cambio deseado o producido por un virus, por lo que pueden generar falsas alarmas. Son especialmente problemáticos los documentos, ya que cambian cada vez que trabajamos con ellos.

Además, los programas verificadores sólo pueden detectar un virus cuando ya se ha producido la infección, no pueden identificar el virus y, por lo tanto, no pueden eliminarlo.

Heurísticos

Los programas heurísticos basan su sistema para la detección de virus, conocidos o desconocidos, en reglas sobre la apariencia de los virus. A diferencia de los escáner, estos programas no necesitan actualizaciones tan frecuentes.

De cualquier manera, si aparece algún nuevo tipo de virus, el programa no lo podrá detectar y habrá que actualizarlo o sustituirlo.

Estos programas tienden a producir falsas alarmas.

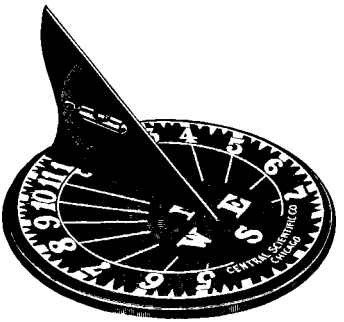
La historia de los virus

1949 El matemático John von Neumann sugiere la posibilidad de programas que se autoduplican.

1950s En los laboratorios de Bell se realiza un juego experimental en el que se utilizan programas malignos para atacar los ordenadores enemigos.

1975 El escritor John Brunner imagina un 'gusano' informático que crece por las redes.

1984 Fred Cohen acuña el término 'virus informático' en una tesis sobre estos programas.



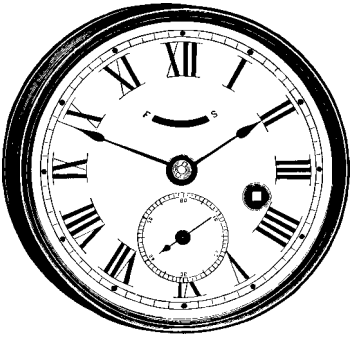
1986 El primer virus informático, *Brain*, se atribuye a dos hermanos pakistaníes.

1987 El gusano *Christmas tree (árbol de Navidad)* paraliza la red de IBM a nivel mundial.

1988 El gusano *Internet worm* se extiende por la red de la agencia de defensa americana, DARPA, de cuyo proyecto nacería Internet.

1990 Mark Washburn crea *1260*, el primer virus 'polimórfico', que muta en cada infección.

1992 Alarma general ante la llegada del virus *Michelangelo*. Finalmente muy pocos ordenadores se infectaron.



1994 Aparece *Good Times*, el primer gran virus broma.

1995 Con *Concept* comienzan los virus de macro. En el mismo año, en Australia, se crea el primer virus especialmente escrito para Windows 95.

1998 *CIH* o *Chernobyl* se convierte en el primer virus que puede dañar el ordenador físicamente.

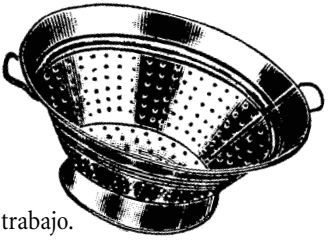
1999 *Melissa*, un virus que se envía a sí mismo por email, se extiende mundialmente. *Bubbleboy*, primer virus que se activa con sólo ver el mensaje de correo electrónico.

2000 *Love Bug* se convierte en el virus de email más extendido. Aparece el primer virus para sistemas Palm, aunque ningún usuario resulta infectado.

El coste oculto de los virus

Los virus no sólo borran o modifican datos. Las amenazas no resultan siempre tan obvias.

Ya sabemos todos que un virus puede destruir toda la información del disco duro o modificar documentos. Son problemas serios que, con un sistema de copias de seguridad, se pueden minimizar. Más graves pueden resultar otros efectos secundarios.



Por ejemplo, los virus pueden bloquear los ordenadores o forzar el cierre de la red. Esto supone la pérdida de costosas horas de trabajo.

Algunos virus pueden interferir en las comunicaciones de las que depende tu empresa. *Melissa* o *ExploreZip*, que se propagan vía email, pueden generar tal volumen de correo que bloquean el servidor. Otras veces, ante el riesgo, las empresas deciden desconectar sus servidores.

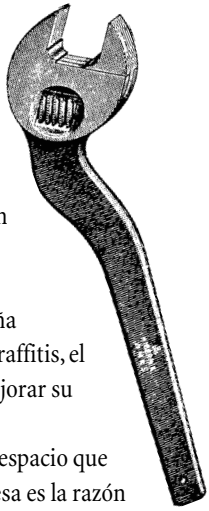
La confidencialidad también está amenazada. *Melissa* puede enviar documentos, que podrían contener datos importantes, a cualquiera en tu libro de direcciones.

Los virus pueden dañar gravemente tu credibilidad. Si tus clientes reciben documentos infectados, podrían cortar las relaciones o reclamar una compensación. Puedes quedar en entredicho y ganar mala reputación. *WM/Polypost*, por ejemplo, copia documentos con tu nombre en el grupo de noticias alt.sex.

¿Quién crea los virus?

Cuando tu ordenador o toda la red queda infectada, probablemente lo primero que dirás, improperios a parte, es '¿Por qué alguien escribe un virus?'

A primera vista no parece que crear virus reporte ningún tipo de beneficio (ni económico, ni profesional) o fama. A diferencia de los hackers, los que crean virus no tienen un objetivo concreto, el ataque es indiscriminado.



Se entiende mejor si se compara con otros tipos de delincuencia, como hacer pintadas, o el vandalismo en general.

El prototipo del programador de virus es un varón, con menos de 25 años y soltero. Su satisfacción está estrechamente ligada al reconocimiento de su pandilla o de su pequeña comunidad virtual. Igual que los que hacen graffitis, el que crea un virus busca impresionar para mejorar su estatus.

También consiguen cierto poder en el ciberespacio que no conseguirían en el mundo real. Sin duda, esa es la razón por la que escogen nombres inspirados en canciones de heavy metal o en la literatura fantástica que, al fin y al cabo, persiguen la ilusión del control y la potencia sin límites.

Otros puntos de vista

La mayoría de nosotros daría por supuesto que crear virus es simplemente malo, pero ¿lo es siempre?

Muchos de los virus son 'inofensivos' o consisten en una broma. Otros ponen de manifiesto agujeros de seguridad en ciertos programas. Hay quien afirma que son hasta útiles, en el sentido de que fuerzan a buscar soluciones. Por desgracia, lo de 'inofensivo' no vale si hablamos de seguridad.

Primero, los virus realizan cambios en los equipos sin la aprobación o conocimiento por parte del usuario. Cualquiera que sea la intención, eso no es ético (incluso ilegal en muchos paises). No se debe actuar en el ordenador de otro, igual que no se debe coger un coche sin permiso del dueño (ni aunque le cambies el aceite).

Segundo, los virus no siempre hacen lo que el autor pretende. Si el virus tiene errores, su comportamiento puede ser impredecible. Incluso puede ser inofensivo en un sistema operativo y totalmente dañino en otros.

De concepto

En ocasiones se crea un virus sólo para demostrar que es posible. Se les conoce como virus de concepto. Normalmente no tienen efectos secundarios (carga explosiva) y no suelen distribuirse de forma indiscriminada.

¿Investigación?

Algunos creadores de virus dicen que así investigan. La realidad es que el código suele ser de baja calidad y, normalmente, no es posible recoger los resultados para su estudio. No creo que eso sea investigación.

Bromas de virus

Si has recibido algún mensaje de alerta sobre los virus 'Good Times', 'Ranas de Budweiser' o 'Tarjeta virtual', has sido víctima de una broma. Este tipo de bromas sobre virus, casi siempre vía email, son bastante comunes y al final pueden ser tan costosas, en tiempo y dinero, como un virus real.

¿Qué son estas bromas?

Son alertas sobre virus inexistentes. Suelen ser mensajes de correo electrónico con ciertas características:

- Alertan sobre la existencia de un nuevo virus indetectable y muy dañino.
- Te recomiendan no leer ningún email con asuntos como Ranas de Budweiser o Tienes una tarjeta virtual.
- Aseguran que el aviso proviene de una gran compañía informática, como IBM o Microsoft, o directamente de algún organismo gubernamental.
- Advierten de cualidades bastante increíbles para un virus. Por ejemplo, *Un momento de silencio* afirmaba que 'el virus puede infectar ordenadores sin intercambio de ningún archivo'.
- Usan verborrea técnica para describir los efectos. *Good Times* decía que el virus podría 'sumir al procesador en un bucle binario infinito de complejidad n'.
- Te incitan a que mandes el mensaje de aviso a todos los usuarios que puedas.

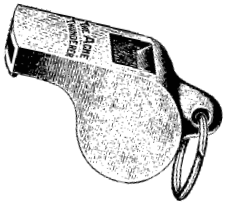
La broma que no fue tal

El 1 de abril de 2000, un email de alerta sobre el virus *Rush-Killer* comenzó a circular. Alertaba sobre un virus que utilizaba el modem para llamar al 911 (número de emergencias en EE.UU.) y pedía que difundieras la noticia. Todo hacía pensar que se trataba de una broma. Sin embargo, el virus era real. Se conoció como *BAT/911*, se extendía en Windows y hacía llamadas al 911. A veces es difícil distinguir las bromas de alertas reales; en la sección '¿Qué hacer con las bromas?' encontrarás algunos consejos.

¿Por qué son un problema?

Las bromas pueden ser tan perjudiciales y costosas como un virus real.

Si cada uno envía estas alertas a todas las personas que puede, el resultado sería un torrente de mensajes que sobrecargaría los servidores y los podría bloquear. El efecto sería el mismo que con el virus real *Love Bug*, y no se habría necesitado ni una sola línea de código.



No es sólo un problema de usuarios. A veces son las compañías las que reaccionan forma drástica, como cerrando su servidor de correo o bloqueando sus redes internas. Esto cortaría las comunicaciones, de gran importancia para muchas empresas, sin necesidad de un virus real.

Estas falsas alarmas también desvían la atención de las amenazas reales.

Pueden llegar a ser muy persistentes; ya que no son virus, los programas anti virus no las podrán eliminar.

¿Qué fue primero?

Una broma puede inspirar un virus real y viceversa. Después de que la broma *Good Times* fuera noticia, y tras ser desmentido, alguien se entretuvo en crear el virus **real** con el mismo nombre (fue conocido como *GT-Spoof)*.

¿Qué hacer con las bromas?

El daño que causan las bromas, como los virus o los mensajes en cadena, depende de su grado de difusión. Si rompes la cadena, limitarás su efecto.

Crea una directiva para la empresa

Una buena solución puede ser establecer unas reglas de comportamiento. Esto es un ejemplo:

'No se debe enviar ninguna alerta sobre ningún tipo de virus a NADIE que no sea -*nombre de la persona responsable*. TODAS las alertas sobre virus, incluyendo las confirmadas por compañías antivirus o de cualquier otra procedencia, se enviarán solamente a -*nombre de la persona responsable*. El responsable se encargará de notificar al resto cualquier alerta seria sobre virus. Cualquier otra alerta deberá ser ignorada.'

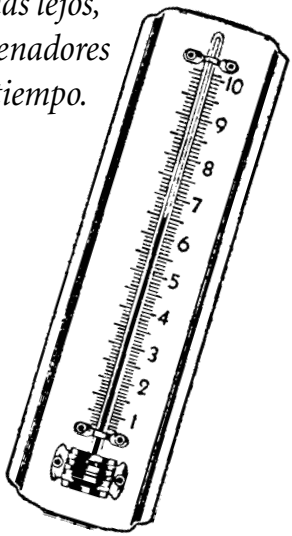
Esto ayudaría a contener el envío masivo de alertas y sólo el experto de la compañía decidirá cuando existe un riesgo real que deba ser considerado.

Infórmate sobre las bromas

Podrás obtener información sobre alertas falsas de virus en nuestra página Web: www.sophos.com/virusinfo/hoaxes.

Virus “Top 10”

¿Cuáles han sido los virus con más éxito de todos los tiempos? Esta es nuestra lista de los virus que han llegado más lejos, infectado más ordenadores ... o resistido más tiempo.



Love Bug

(VBS/LoveLet-A)

Love Bug es probablemente el virus más conocido. Atraía la curiosidad del usuario con las palabras 'Carta de amor' y en cuestión de horas había dado la vuelta al mundo.

Debut: Mayo 2000

Origen: Filipinas

Alias: Carta de amor

Tipo: Gusano en Visual Basic Script

Se activa: En la infección inicial

Efectos: La versión original enviaba un email con el asunto 'I LOVE YOU' y el texto 'lee con cariño la carta de amor que te envío'. Al abrir el archivo adjunto se ejecuta el virus. Si encontraba Microsoft Outlook en el sistema, se enviaba a todas las personas del libro de direcciones. También podía autodistribuiese entre grupos de noticias, robar información de usuarios y sobrescribir ciertos archivos.

Form

Form se mantuvo en el Top 10 durante ocho años y todavía está muy extendido. En DOS y las primeras versiones de Windows pasaba inadvertido, lo que permitió su expansión.

Debut: 1991

Origen: Suiza

Tipo: Sector de arranque

Se activa: El 18 de cada mes

Efectos: Produce un pitido cada vez que se pulsa una tecla. Puede bloquear equipos con Windows NT.

Kakworm

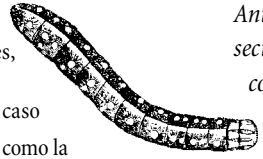
(VBS/Kakworm)

Sólo tienes que leer tu correo para que Kakworm pueda infectar tu equipo.

Debut: 1999

Tipo: Gusano en Visual Basic Script

Se activa: En la infección inicial y el día uno de cada mes, con diferentes efectos en cada caso



Efectos: El gusano llega como la firma en un mensaje de correo electrónico. Si tienes Outlook o Outlook Express con Internet Explorer 5, tu equipo puede quedar infectado al abrir o visualizar el mensaje.
El virus cambia la configuración de Outlook Express de manera que el virus se introduce en cada email que envíes. Además, el día uno de cada mes después de las 5 de la tarde, muestra el mensaje 'Kagou-Anti_Kro$oft says not today' y cierra Windows.

Anticmos

Anticmos es un típico virus de sector de arranque, se extendió con gran rapidez a mediados de los '90 y a menudo aparece en el Top 10.

Debut: Enero 1994

Origen: Apareció primero en Hong Kong, pero parece que se creó en China.

Tipo: Sector de arranque

Se activa: Aleatoriamente

Efectos: Trata de borrar los datos del tipo de unidad de disquete y de disco duro del ordenador.

Melissa

(WM97/Melissa)

Melissa es un virus de email que utiliza un poco de psicología; aparenta llegar desde alguien que conoces y que contiene un documento que te interesa especialmente. Como resultado, Melissa se propagó por todo el mundo en un sólo día.

Debut: Marzo 1999

Origen: David L Smith, programador estadounidense de 31 años, colocó un documento infectado en el grupo de noticias alt.sex

Tipo: Virus de macro para Word 97; también funciona en Word 2000

Se activa: En la infección inicial

Efectos: Envía un mensaje a las primeras 50 personas del libro (o libros) de direcciones de Microsoft Outlook, escribiendo el nombre del usuario en el asunto. Incluirá un archivo adjunto con el virus. Si cuando se abre el archivo coinciden el minuto y el día (10.05 el día 5, por ejemplo), el virus añadirá texto sobre el juego Scrabble en el documento.

New Zealand

New Zealand fue seguramente el virus más común a principios de los '90.

Debut: Final de los '80

Origen: Nueva Zelanda

Alias: Stoned

Tipo: Sector de arranque

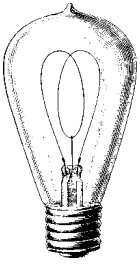
Se activa: Una de 8, si se inicia desde el disquete

Efectos: Muestra el mensaje 'Your PC is now Stoned!'. Copia el sector original de arranque en el último sector de un disco de 360K. Los discos más grandes pueden estropearse.

Concept

(WM/Concept)

Concept consiguió un éxito inmediato al incluirse, accidentalmente, en programas oficiales de Microsoft. Fue el primer virus de macro en activo y uno de los más comunes entre 1996 y 1998. El virus toma el control con una macro de inicio que Word ejecuta de forma automática e infecta con la macro GuardarComo, que se ejecuta cada vez que Word guarda un documento. Existen numerosas variantes.



Debut: Agosto 1995

Tipo: Virus de macro

Efectos: Al abrir un documento infectado, aparece el cuadro de diálogo 'Microsoft Word' en el que sólo aparece el número '1'. El código del virus contiene la frase 'Esto es suficiente para probarlo'. En realidad, esta frase nunca se muestra.

CIH (Chernobyl)

(W95/CIH-10xx)

CIH fue el primer virus en dañar el equipo. Una vez que sobrescribe la BIOS, no podrá utilizar el ordenador hasta que no sustituya el chip de la BIOS.

Debut: Junio 1998

Origen: Creado por Chen Ing-Hau, de Taiwan

Tipo: Virus parásito escrito para Windows 95

Se activa: El 26 de abril. Otras variantes lo hacen el 26 de junio o el 26 de cualquier mes

Efectos: Sobrescribe la BIOS y después el disco duro.

Parity Boot

Parity Boot se transmite en el sector de arranque de los disquetes. Su éxito demuestra que los virus de sector de arranque, los más comunes en los '80 y principios de los '90, aún tienen algo que decir. Este virus todavía se encontraba entre los más activos en 1998. Tuvo un gran impacto en Alemania, donde fue distribuido en el CD-ROM de una revista en 1994.

Debut:	Marzo 1993
Origen:	Posiblemente en Alemania
Tipo:	Sector de arranque
Se activa:	Aleatoriamente
Efectos:	Muestra el mensaje 'PARITY CHECK' y bloquea el sistema. El mensaje imita el formato de los mensajes que aparecen cuando se produce un error real de la memoria. Esto puede hacer pensar al usuario que se trata de un problema con la memoria RAM del equipo.

Happy99

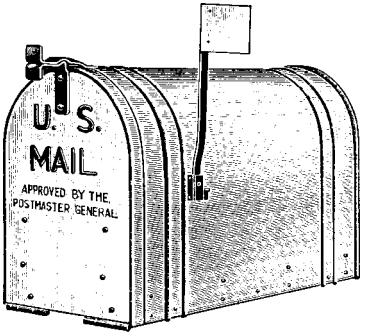
W32/Ska-Happy99

Happy99 fue el primer virus de renombre en extenderse vía email.

Debut:	Enero 1999
Origen:	El francés 'Spanska' lo envió a un grupo de noticias
Tipo:	Virus de archivo para Windows 95/98/Me/NT/2000
Efectos:	Muestra unos fuegos artificiales y el mensaje 'Feliz año 1999'. También modifica el archivo wsock32.dll del sistema de Windows de manera que cada vez que envíes un email, se enviará un segundo mensaje incluyendo el virus.

Email

Si preguntas a la gente el nombre de algún virus, probablemente la respuesta sea Love Bug o Melissa. Lo que estos virus tienen en común, a parte de haber estado en los titulares, es que se extendieron por el mundo vía email.



El email se ha convertido en la mayor fuente de virus, pero ¿por qué?

En los virus que se transmitían en disquetes la propagación era bastante lenta; es posible controlar y escanear disquetes. Mediante email puedes compartir programas rápidamente e infectar tu equipo con un simple clic. Así, los virus genéricos tienen una rápida vía de expansión y los nuevos virus se aprovechan de ciertas funcionalidades de los programas de email.

¿Coger un virus con tan sólo leer el correo?

En general se piensa que es seguro abrir cualquier mensaje siempre y cuando no se abran los archivos adjuntos. Esto ya no es cierto.

Virus como *Kakworm* y *Bubbleboy* pueden activarse con tan sólo leer un mensaje. Su aspecto no es diferente de cualquier otro mensaje pero contiene código oculto que se ejecuta al abrirlo o incluso al previsualizarlo (sólo si usas Outlook con cierta versión de Internet Explorer). Este código puede cambiar la configuración del sistema y enviar el virus a otras personas por email.

Microsoft ha corregido el problema con un 'parche' que podrás conseguir en www.microsoft.com/technet/security/bulletin/ms99-032.asp

Bromas de email

El email también se ha convertido en un popular medio para las bromas, mensajes de alarma sobre falsos virus.

Estas bromas se pueden expandir como auténticos virus y sobrecargar servidores. La diferencia es que una broma no necesita código; se aprovechan de la credulidad de la gente. Lee el capítulo 'Bromas de virus'.

Virus que se autoenvían por email

Los virus con más éxito hoy día son los que se pueden enviar a sí mismo de forma automática.

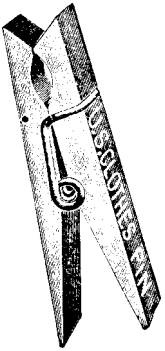
En general, estos virus vienen en forma de archivo adjunto que tiene que ser ejecutado por el usuario. En ese momento, el virus utilizará el programa de correo para enviarse a otras personas. *Melissa*, por ejemplo, se envía a las primeras 50 personas de todos los libros de direcciones a los que Microsoft Outlook tiene acceso. Otros virus se envían a todas las direcciones que tenga el usuario.

¿Qué es spam?

Se conoce como spam al correo no solicitado, normalmente propaganda basura. Es dificil acabar con este tipo de mensajes ya que normalmente no se puede identificar al autor. Lo mejor que puedes hacer es borrarlos.

El riesgo de los adjuntos

El mayor peligro no proviene del email en sí, sino de los archivos adjuntos.



Cualquier programa o documento que recibas por email puede contener un virus y al abrirlo podrías infectar tu ordenador.

Por desgracia, enviar archivos por email se ha convertido en una forma común de intercambiar información. En general se piensa que es 'inofensivo y divertido' enviar a los amigos protectores de pantalla, animaciones u otras bromas. La verdad es que esos archivos pueden contener virus.

Incluso archivos considerados seguros, como archivos con la extensión .txt, pueden suponer un riesgo. Ese 'archivo de texto' puede en realidad ser un virus en Visual Basic Script con su extensión (.vbs) oculta.

El gusano *VBS/Monopoly* es un ejemplo de virus oculto en una broma. Se supone que es 'una gracia sobre Bill Gates'. Y lo es (aparece un tablero de Monopoly con imágenes de Microsoft) pero, al mismo tiempo, se envía a sí mismo a otras personas y remite información sobre tu equipo a ciertas direcciones de email, amenazando tus posibles datos confidenciales.

Email falsificado o interceptado

Un email puede ser interceptado y leido mientras se encuentra en tránsito. La forma de protegerse es utilizar encriptación.

Además, en un email se puede falsificar el nombre del autor así como plagiar el contenido. La protección pasa por utilizar una 'firma digital' que te identifique.

Cómo detener virus de email

Plantea una política estricta sobre adjuntos

Modificar tu comportamiento (y el de otros usuarios) es la forma más sencilla de combatir este tipo de virus. No abras directamente ningún archivo adjunto, ni siquiera si viene de tu mejor amigo. No caigas en la tentación cualquiera que sea el mensaje. Si no estás seguro sobre un archivo, deberás tratarlo como si estuviera infectado. En una empresa, TODOS los archivos adjuntos tendrían que pasar, antes de usarlos, el filtro de un programa antivirus.

Desactiva Windows Scripting Host

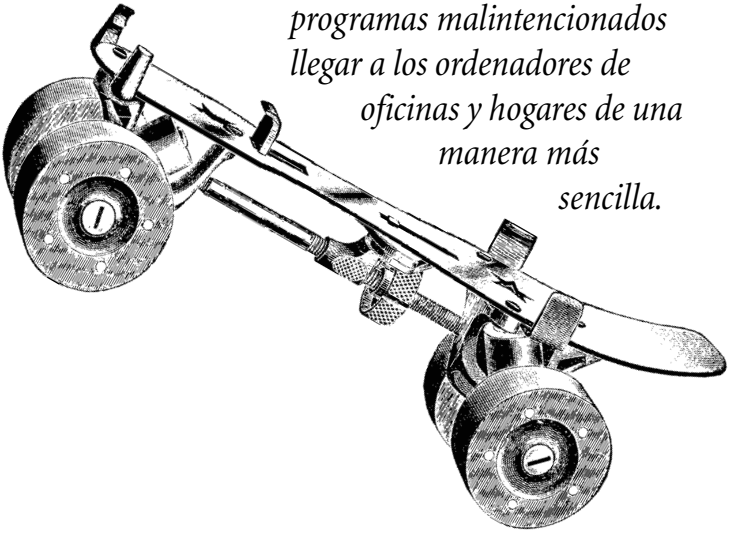
La herramienta Windows Scripting Host (WSH) sirve para automatizar ciertas tareas, como la ejecución de Visual Basic Script o Java. De igual manera, WSH permite que virus como *Love Bug* se extiendan. Es probable que no necesites WSH en tu equipo (consulta al administrador de la red). Encontrarás información sobre cómo desactivarlo en www.sophos.com/support/faqs/wsh.html. Ojo, cada vez que actualices Windows o Internet Explorer, WSH se reactivará.

Utiliza un programa antivirus

El uso de antivirus con escaneado en acceso en cada equipo y en la puerta de acceso del email previenen la infección y propagación de virus de email.

Internet

Internet ofrece a más gente más información y más rápido que nunca antes. El lado negativo es que también permite a programas malintencionados llegar a los ordenadores de oficinas y hogares de una manera más sencilla.



¿Con un clic infectado?

Internet ha incrementado el riesgo de infección.

Hace 10 años la mayoría de los virus venían en disquetes. Así, su propagación era lenta y dependía en gran medida del interés del usuario en programas nuevos. Además, los virus solían tener unos efectos bastante obvios, por lo que no iban muy lejos. Ahora que Internet está tan extendido, todo ha cambiado.

Compartir programas por Internet resulta muy sencillo. Con un simple clic tendremos un programa adjunto en un mensaje y con otro clic podremos ejecutar el que nos llegue. Cualquiera puede ofrecer programas en una página Web. De esta manera, virus de archivo (o 'parásitos'), asociados a programas circulan libres por la Red.

Los virus que más se benefician son los de macro, insertados en documentos. Es común descargar documentos o intercambiarlos vía email. Todo lo que necesitas para infectar tu ordenador es hacer clic en un archivo que hayas descargado o en un adjunto de email.

Es de sentido común pues, utilizar visualizadores de documentos que ignoran las macros y no ejecutar programas de dudosa procedencia.

¿Se puede infectar uno al visitar una página Web?

Navegar por páginas Web no es tan peligroso como ejecutar programas o documentos desconocidos. Pero el riesgo existe. El peligro depende del tipo de código utilizado y de las medidas de seguridad de tu proveedor de acceso a Internet. Estos son algunos tipos de código que hay en páginas Web.

HTML

El lenguaje base utilizado para crear páginas Web es HTML (Hypertext Markup Language), que permite dar formato al texto e insertar imágenes y enlaces a otras páginas. El código HTML en sí mismo no puede contener virus. De cualquier manera, sí puede abrir aplicaciones o documentos de forma automática, con el posible riesgo de abrir algún archivo infectado.

ActiveX

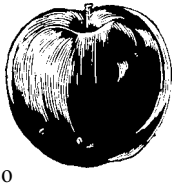
ActiveX ha sido creado por Microsoft para implementar la funcionalidad de páginas Web y sólo funciona en Windows.

Los applets de ActiveX, utilizados para crear efectos, permiten el acceso total a los recursos del sistema, lo que constituye una amenaza. De cualquier manera, una la firma digital que permite probar que el código es auténtico y que no ha sido modificado ofrece cierta seguridad.

Más código

Java

Existe una alarma generalizada sobre virus en Java en Internet. A menudo se confunden los applets de Java, utilizados para crear efectos en las páginas Web, con programas en Java o Java Script.



Los **applets** no resultan peligrosos ya que son ejecutados por el navegador en un entorno aislado. Incluso si un fallo de seguridad permitiera a uno de estos applets escapar, no se podría extender fácilmente. Los applets sólo se transmiten de servidor a usuario, no de un usuario a otro (es decir, puedes decir a otros que visiten cierta página Web, pero no enviarles un applet). Además, los applets no se guardan en el disco duro, aparte de la caché del navegador.

Si hay algún applet dañino, se trataría de un troyano, es decir, un programa que pretende servir para una cosa y hace otra diferente.

Un **programa en Java** es una aplicación escrita en lenguaje Java. Como cualquier otro programa, puede contener virus. Deberías tomar las mismas precauciones que con otros programas.

Java Script es un lenguaje de comandos que se utiliza dentro de páginas HTML y con el que se pueden realizar acciones, en potencia, de cierto riesgo. Es posible desactivar la ejecución de scripts (lea el apartado 'Seguridad en la Red' al final del capítulo).

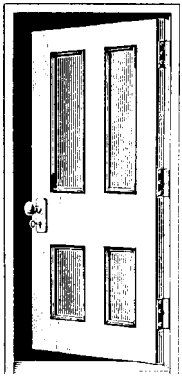
VBS script

Un guión en VBS (Visual Basic Script) se ejecuta al ver una página Web, dependiendo del navegador. No requiere ninguna acción por tu parte.

Virus de email como *Kakworm* y *Bubbleboy* utilizan este lenguaje, que también puede ejecutarse desde una página Web.

Troyanos de puerta trasera

Se conoce así a programas que, una vez instalados en un equipo, permiten su control remoto por Internet.



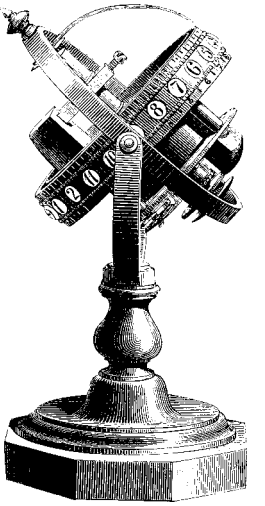
Como otros troyanos, los de puerta trasera se presentan como un programa con un determinado propósito. Al ejecutarlo (normalmente en Windows 95/98), se inserta en la rutina de inicio del sistema. El troyano vigilará hasta que el equipo se conecte a Internet. En ese momento, la persona que envió el troyano podrá tomar el control del ordenador infectado y abrir y modificar archivos, ejecutar programas o utilizar la impresora. *Subseven* y *BackOrifice* son dos conocidos ejemplos de troyanos de puerta trasera.

¿Son las cookies un peligro?

Las cookies no suponen una amenaza directa para tu equipo o la información en él. De cualquier manera, pueden suponer un riesgo para tu confidencialidad: una cookie permite a un sitio Web reconocer tu equipo y seguir el rastro de las visitas a sus páginas. Si prefieres el anonimato, siempre puedes desactivar las cookies en tu navegador.

Ataques a servidores Web

En Internet no sólo está en peligro el usuario final. Algunos hackers tienen como objetivo los servidores en los que se alojan los sitios Web.



Una forma de ataque consiste en el envío masivo de peticiones a un servidor Web para ralentizarlo o bloquearlo. Cuando esto sucede, ningún otro usuario podrá acceder a las páginas que hay en ese servidor.

Programas en CGI (Common Gateway Interface) son otro punto débil. Estos programas se ejecutan en el servidor y se utilizan, entre otros, en buscadores o para el manejo de formularios. Los hackers pueden utilizar una CGI que no esté adecuadamente implementada para tomar el control del servidor.

Seguridad en la Red

Si quieres eliminar riesgos al navegar por Internet, sigue estos consejos:

En la empresa, ten una red separada para Internet

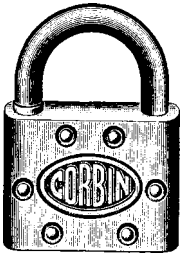
Mantén una red separada para los equipos conectados a Internet que sea independiente de la red principal. Así reducirás el riesgo que para la red principal puede supone la descarga incontrolada de archivos.

Usa cortafuegos y/o routers

Un cortafuegos (firewall) evitará la entrada de tráfico no autorizado en tu red. Un router controlará el flujo de paquetes de información desde Internet.

Configura tu navegador para que sea seguro

Desactiva las funciones de Java, ActiveX, cookies, etc., o al menos haz que se te pida confirmación antes de admitir este tipo de código. Lo podrás hacer, dependiendo del navegador, siguiendo la secuencia **Herramientas|Opciones de Internet|Seguridad|Personalizar**, donde finalmente podrás configurar el nivel de seguridad de tu navegador.



Móviles y ordenadores de mano

La última década ha llevado el mundo (de Internet) a los ordenadores; en la siguiente llegará a los teléfonos móviles. De hecho, ya es posible acceder a ciertos contenidos y servicios de la Web con los nuevos teléfonos móviles, y la tecnología no para de avanzar. Pero al mismo tiempo que se mejora la transmisión de datos (incluso en movimiento), también se abre la posibilidad para nuevas amenazas.

¿Existe algún virus para móviles?

Hasta la fecha, no se conoce ningún virus para teléfonos móviles, pese a ciertos rumores e historias que se han difundido.

Existe, sin embargo, virus que envían mensajes a móviles. Por ejemplo, *VBS/Timo-A*, un gusano que se extiende vía email, también utiliza el modem para enviar mensajes SMS a ciertos números de teléfono móvil. El conocido virus *Love Bug* es capaz de enviar texto a faxes y móviles. De cualquier manera, estos virus no pueden infectar o dañar un teléfono móvil.

Puede que la cosa cambie dado que los móviles son cada vez más sofisticados.

¿Es seguro un dispositivo móvil?

No tanto como un ordenador a la hora de almacenar datos:

- Su pérdida resulta bastante frecuente.
- En un corte de corriente se pueden perder datos.
- No hay copias de seguridad.

Al aumentar la complejidad de estos dispositivos, pueden también ser más vulnerables frente a virus y hackers.

Teléfonos WAP y virus

Es Internet en movimiento, es la tecnología WAP (Wireless Application Protocol).

La tecnología WAP permite acceder a información y servicios basados en Internet desde el teléfono móvil y ordenadores de mano. El modelo es el mismo que en la Web, esto es, un servidor central suministra los datos que son interpretados y mostrados por el navegador del sistema. Así, de momento, no hay mucha cabida para virus.

Un virus podría infectar el servidor, pero la posibilidad de extenderse o afectar a los usuarios conectados sería mínima.

Primero, en un sistema WAP no es posible que un virus se pueda replicar ya que no se almacenan aplicaciones, al contrario que en un ordenador. El teléfono muestra la información al recibirla pero no la guarda, excepto en la caché temporal del navegador.

Segundo, un virus no puede pasar de un usuario a otro.

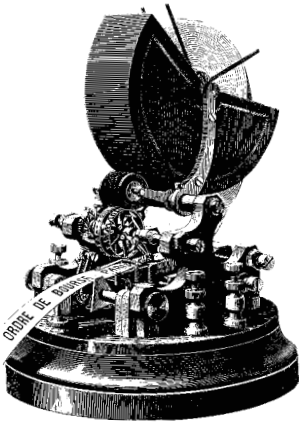
En teoría, un 'virus' podría distribuir *enlaces* a ciertos sitios WAP, incitando el uso de aplicaciones dañinas, aunque siempre desde el servidor.

Para estar al día

WAP	Protocolo para aplicaciones inalámbricas
WML	Lenguaje para aplicaciones inalámbricas
WML Script	Lenguaje de programación basado en Java Script
Cartas	Páginas en WML para dispositivos WAP
Baraja	Conjunto de cartas interrelacionadas disponibles para WAP directamente

Amenazas sobre WAP

La tecnología WAP usa una versión del protocolo para páginas Web, HTTP, que permite transmitir contenidos más complejos del que en la actualidad pueden procesar los navegadores WAP. Las futuras versiones de navegadores permitirán la descarga de archivos que, por supuesto, podrían contener virus .



En el sistema WAP, pronto será posible que el servidor distribuya la información a los móviles. Se podrían recibir las últimas noticias o nuevos email sin intervención del usuario, pero esta forma de distribución podría facilitar la propagación de virus.

Existen otras amenazas potenciales. Por ejemplo, sitios WAP con malas intenciones podrían, ofreciendo servicios aparentemente legítimos, bloquear el navegador de los usuarios o llenar la memoria del dispositivo utilizado.

Para estar al día

XML	eXtensible Markup Language, unificará el intercambio de información en la Web
WTLS	Wireless Transport Layer Security. Método de encriptación utilizado en la telefonía móvil

Sistemas operativos móviles

Ordenadores de mano y organizadores personales (PDA) es probable que ofrezcan ciertas oportunidades para virus en un futuro cercano.

Los ordenadores de mano y los PDA utilizan sistemas operativos a pequeña escala, como EPOC, PalmOS o PocketPC (antes llamado Windows CE). Estos sistemas pronto podrán utilizar versiones de aplicaciones creadas para equipos de sobremesa, con las ventajas e inconvenientes que esto conlleva. A principios de 2001, ya existían virus que podían afectar a sistemas Palm.

Los ordenadores de mano se conectan a menudo al ordenador de la oficina o de casa para sincronizar, por ejemplo, el libro de direcciones o la agenda. Esta sincronización de datos podría permitir la expansión de virus entre diferentes sistemas.

Nadie se atreve a aventurar cuál será el dispositivo del futuro: ordenadores de mano o teléfonos móviles inteligentes. En cualquier caso, los problemas de seguridad crecen al aumentar la conectividad de estos sistemas.

Para estar al día

EPOC	Sistema operativo de ordenadores de mano
PDA	Personal Digital Assistant
PalmOS	Sistema operativo de dispositivos Palm
PocketPC	Sistema operativo de Microsoft para ordenadores de mano, antes Windows CE
UPNP	Sistema Plug and Play universal de Microsoft para facilitar la conexión entre móviles y otros dispositivos

¿Virus para el frigo?

Cada vez son más los dispositivos que pueden 'hablar' con otros mediante puertos infrarrojos o radio de banda corta, lo que trae nuevos riesgos de seguridad.

Bluetooth es el estándar para comunicaciones inalámbricas en banda corta para pequeñas distancias, unos 10 m. Dispositivos como ordenadores, teléfonos móviles, faxes o incluso electrodomésticos como el video o el frigo, pueden utilizar esta tecnología, lo que les permitiría detectar otros dispositivos y comunicarse con ellos.

Cada día aparecen nuevos programas que utilizan Bluetooth. La tecnología Jini de Sun permite la conexión entre dispositivos, el intercambio de código en Java y el control remoto. El riesgo puede estar en la entrada de usuarios no autorizados o en la incursión de programas malintencionados.

Bluetooth y Jini están diseñados para que sólo programas de procedencia conocida pueden realizar ciertas tareas. Esto hace poco probable que un virus pueda penetrar, pero si lo hace, muy poco podrá hacerse para detener su expansión.

Para estar al día

3G	'Tercera generación' de telefonía móvil
Bluetooth	Tecnología inalámbrica de comunicaciones
Jini	Tecnología para el intercambio de código Java entre dispositivos
MExE	Entorno para la ejecución de programas en estaciones móviles, posible sucesor de WAP que permitiría la descarga y ejecución de código Java desde teléfonos móviles

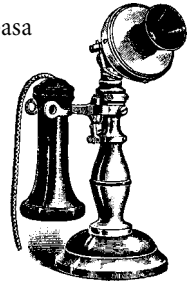
Cómo proteger sistemas móviles

En cuanto a móviles y PDA, habrá que seguir en guardia con la entrada de nuevas tecnologías. El tema principal es dónde aplicar las medidas antivirus.

Puertas de acceso y transferencia de datos

En un futuro cercano, la mejor manera de proteger sistemas móviles será comprobando los datos hacia y desde estos dispositivos. Para teléfonos móviles, por ejemplo, la puerta de acceso WAP sería un buen lugar donde establecer un sistema de protección antivirus. Toda la información pasa por esta vía de acceso sin encriptar, así que sería una oportunidad ideal para realizar el escaneado.

Para ordenadores de mano, se pueden utilizar soluciones antivirus que comprueben los datos intercambiados de manera que sea el ordenador de sobremesa el que realice el trabajo.

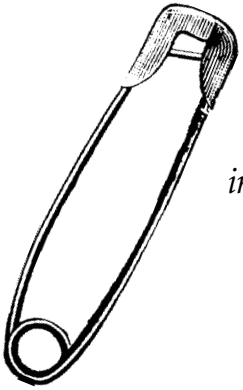


Escaneado en dispositivos móviles

Al aumentar la conectividad de estos dispositivos, cada vez será más difícil controlar la procedencia de los datos. La solución sería instalar un programa antivirus en cada sistema, una vez que la velocidad de estos dispositivos y la capacidad de memoria no sean un problema.

Decálogo de seguridad antivirus

Además de utilizar un programa antivirus, hay otras medidas muy elementales que deberías seguir para proteger tu equipo de virus. Estas diez creemos que son las más importantes.



Medidas antivirus

No uses documentos en formato .doc o .xls

Guarda documentos de Word como RTF (formato de texto enriquecido) y los de Excel como CSV (valores separados por comas). Estos formatos no admiten macros, por lo que no tendrán virus de macro, el tipo de virus más común. Pide que los documentos que te envíen estén en formato RTF o CSV. Aunque, atención, algunos virus de macro interceptan la orden GuardarComo RTF y mantienen el formato DOC con extensión RTF. Los archivos TXT son realmente seguros.

No ejecutes archivos que no has solicitado

Si no estás seguro de que un archivo está libre de virus, trátalo como infectado. Conciencia al personal de tu empresa del riesgo de descargar programas y documentos de Internet, incluyendo salva pantallas o programas de broma. Haz que cada programa tenga que ser aprobado y comprobado por el departamento técnico.

Envía alertas sólo a una persona autorizada

Bromas de virus pueden ser un problema como los virus reales. Aconseja no enviar alertas de virus a amigos, colegas o a todos en el libro de direcciones. Haz que sean enviados a sólo una persona responsable en la empresa.

Medidas antivirus

Virus

Email

Internet

Sistemas móviles


Seguridad

Referencia

Si no necesitas WSH, desactívalo

Windows Scripting Host (WSH) realiza algunas tareas automáticas en Windows pero también permite la expansión de virus como *Love Bug* o *Kakworm*. A menos que lo necesites, desactívalo. Encontrarás más información en www.sophos.com/support/faqs/wsh.html

Lee boletines sobre la seguridad de programas

Las compañías publican noticias y parches para la seguridad de sus programas. Lee el capítulo 'Enlaces de interés'.

Bloquea la entrada de ciertos tipos de archivo

Muchos virus utilizan archivos en VBS (Visual Basic Script) o SHS (objeto OLE de Windows) para extenderse. No se trata de archivos de intercambio común, por lo que puedes bloquear su entrada en el servidor.

Cambia la secuencia de inicio de tu ordenador

La mayoría de los ordenadores intentan arrancar desde la disquetera (unidad A:) en primer lugar. En la CMOS se puede cambiar la secuencia para que se arranque siempre desde el disco duro. Así ningún disquete podrá infectar el sector de arranque de su equipo. Si necesita arrancar desde un disquete, puede cambiar la configuración en ese momento.

Medidas antivirus

Protege los disquetes contra escritura

Un disquete protegido contra escritura no puede infectarse.

Suscríbete a un servicio de alerta

Así estarás al día sobre nuevos virus e identidades de virus que permitirán a tu programa antivirus detectarlos. Sophos dispone de un servicio gratuito. Encontrará información en www.sophos.com/virusinfo/notifications

Mantén copias de seguridad

Podrás recuperar documentos y programas eliminados o dañados por un virus.

Enlaces de interés

Sitios Web con información relevante:

Información sobre virus
www.sophos.com/virusinfo/analyses

Alertas y bromas de virus
www.sophos.com/virusinfo/hoaxes
www.vmyths.com

Notificación automática sobre nuevos virus
www.sophos.com/virusinfo/notifications

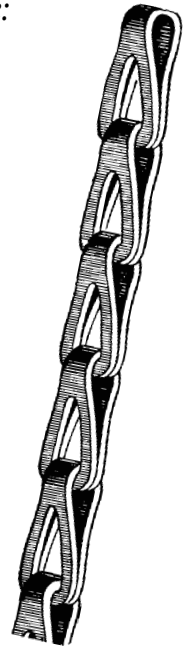
Boletines de seguridad de Microsoft
www.microsoft.com/spain/security

Centro de seguridad de Netscape
www.netscape.com/security

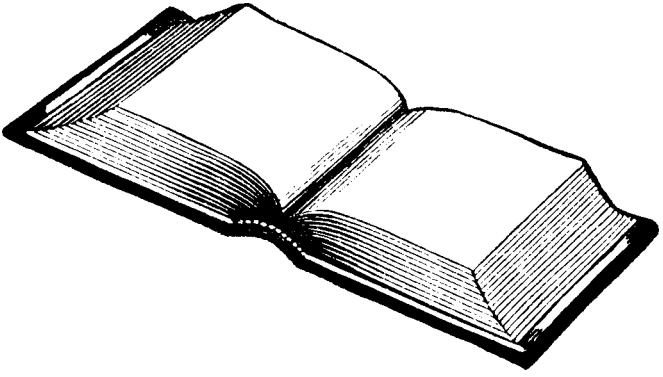
Seguridad en Java
www.java.sun.com/security

Organización mundial antivirus
www.wildlist.org

Boletín antivirus
www.virusbtn.com



Glosario



Virus

Email

Internet

Sistemas móviles

Seguridad


Referencia

ActiveX: Tecnología de Microsoft para ampliar las posibilidades de los navegadores.

Adjunto: Documento, programa o cualquier tipo de archivo incluido en un mensaje de correo electrónico.

Aplicación en Java: Programa escrito en Java con completa funcionalidad y acceso a recursos.

Applet: Pequeña aplicación, generalmente en Java.

ASCII: American Standard Code for Information Interchange. Estándar para la representación de letras y símbolos.

BIOS: The Basic Input/Output System. Programa encargado del arranque del ordenador y que hace de intermediario entre el sistema operativo y los diferentes componentes del equipo.

Broma de virus: Alerta sobre virus no existentes.

Caballo de Troya: Programa con efectos (indeseables) diferentes de los especificados.

CGI: Common Gateway Interface. Sistema que permite a un servidor Web ejecutar programas para interactuar con el usuario.

Contraseña: Secuencia de caracteres que permite a un usuario el acceso.

Cookie: Pequeño archivo que contiene cierta información acerca del equipo de un usuario. Las cookies son utilizadas por sitios Web para crear un historial de visitas y almacenar preferencias de los usuarios.

Copia de seguridad: Copia de documentos y archivos que se utilizan en el caso de pérdida o daño de los originales.

Cortafuegos: Sistema de seguridad en puntos claves de una red para permitir sólo tráfico autorizado. A menudo utilizado para restringir el acceso a una red interna desde Internet.

CSV: Comma Separated Values. Formato de archivo en el que los valores (como pueden ser los de una hoja de cálculo de Excel) se almacenan separados por comas. Este tipo de archivo no permite macros, por lo que no puede contener virus de macro.

Descarga: Transferencia de datos desde un ordenador, en general un servidor, a otro.

Disco duro: Disco magnético al vacío, generalmente dentro del ordenador, utilizado para almacenar datos.

Disquete: Soporte magnético intercambiable para almacenar datos.

Escáner de virus: Programa detector de virus. La mayoría detectan virus específicos, es decir, los virus conocidos. Ver también escáner heurístico.

Escáner heurístico: Programa de detección de virus que se basa en reglas generales de apariencia o comportamiento de virus.

Estación de trabajo: Equipo conectado a una red.

Firma digital: Identificador único del que se puede valer un usuario para asegurar la autenticidad de sus mensajes.

FTP: File Transfer Protocol. Protocolo para el intercambio de archivos en Internet.

Gateway: Ver puerta de acceso.

Gusano: Programa que auto distribuye copias de sí mismo. Al contrario que un virus, un gusano no necesita un programa anfitrión.

Virus

Email

Internet

Sistemas móviles

Seguridad


Referencia

Hacker: Persona que intenta acceder a otros ordenadores o sistemas sin permiso.

Hipertexto: Tipo de texto que permite incluir enlaces a otros archivos.

HTML: Hypertext Markup Language. Lenguaje básico para la creación de páginas Web.

HTTP: Hypertext Transport Protocol. Protocolo utilizado en Internet entre servidores y navegadores.

Identidad de virus: Descripción de un virus utilizada para su detección.

Internet: Red de redes a nivel mundial.

Java: Lenguaje de programación desarrollado por Sun Microsystems que permite crear programas o applets que no dependen de la plataforma en la que se ejecutan.

Java applet: Pequeña aplicación que a menudo se utiliza para crear efectos en páginas Web. El navegador ejecuta los applets en un entorno seguro (ver sandbox) que no permite realizar cambios en el sistema anfitrión.

Laptop: Ordenador portátil.

Macro: Conjunto de instrucciones en documentos que ejecutan comandos de forma automática, como abrir o cerrar ficheros.

Memoria RAM: Random Access Memory. Es un tipo de memoria temporal del ordenador, los datos almacenados se pierden al apagar el sistema.

Memoria ROM: Read Only Memory. Es un tipo de memoria del ordenador de sólo lectura. Normalmente se utiliza para almacenar el programa de arranque del ordenador.

Modem: MOdula y DEModula la señal generada o recibida por el ordenador para transmitir datos mediante la línea telefónica, radio o vía satélite.

Navegador Web: Programa utilizado para acceder a la información de Internet.

Notebook: Ordenador portátil de pequeñas dimensiones.

Palmtop: Ordenador de mano.

Parásito: Ver virus parásito.

PC: Personal Computer. Ordenador de sobremesa o portátil independiente.

PDA: Personal Digital Assistant. Organizador electrónico de reducido tamaño generalmente utilizado como agenda y libro de direcciones.

Puerta de acceso: Ordenador que controla el intercambio de datos (por ejemplo, una puerta de acceso de email controla todo el correo que llega a una empresa) o que sirve de intermediario entre diferentes protocolos.

Proceso de arranque: Secuencia de carga del sistema operativo.

Programa: Conjunto de instrucciones que especifican las acciones a realizar por el ordenador.

Puerta trasera: Forma no documentada de traspasar un sistema de control de acceso. Ver troyano de puerta trasera.

RAM: Ver memoria RAM.

ROM: Ver memoria ROM.

RTF: Rich Text Format. Formato de texto enriquecido que no permite macros, por lo que no puede contener virus de macros.

Sandbox: Se conoce así al entorno seguro en el que se ejecutan programas de forma controlada, como applets de Java.

Sector de arranque: Parte del sistema operativo que primero se carga en memoria al iniciar el ordenador. El programa del sector de arranque cargará por partes el resto del sistema operativo.

Sector de arranque DOS: Sector de arranque que carga el sistema operativo DOS en la memoria del ordenador. Objetivo común de virus de sector de arranque.

Sector de arranque maestro: También conocido como sector de particiones, es el primer sector físico del disco duro, que se carga y ejecuta al arrancar el ordenador. Es un elemento crítico en la secuencia de inicio del ordenador.

Servidor de archivos: Ordenador para la centralización de archivos y, generalmente, otros servicios en una red.

Servidor proxy: Tipo de servidor que actúa en Internet en nombre de otro equipo. Sirve de intermediario entre el usuario e Internet y puede utilizarse como medio de seguridad.

Servidor Web: Ordenador conectado a Internet que ofrece páginas Web y otros servicios, en general mediante HTTP.

SHS: Formato de archivo OLE de Windows creado a partir de una fracción de un archivo. Este tipo de archivo puede contener casi cualquier clase de código que se ejecutará al hacer clic sobre él. La extensión puede estar oculta.

Sistema operativo: Programa que controla el uso de los diferentes recursos de un equipo y que permite manejar archivos y ejecutar otros programas.

SMTP: Simple Mail Transport Protocol. Protocolo utilizado para el envío de correo electrónico.

Spam: Correo no solicitado, normalmente propaganda basura.

Spoofing: Literalmente parodiar, es hacerse pasar por otro, por ejemplo, falsificando la dirección de email del supuesto remitente.

Suma de verificación: Valor calculado a partir de un conjunto de datos que se puede utilizar para comprobar posteriormente la integridad de dichos datos.

TCP/IP: Transmission Control Protocol/Internet Protocol. Conjunto de protocolos estándar de Internet.

Troyano de puerta trasera: Troyano que permite el acceso no autorizado y control sobre otro ordenador.

URL: Uniform Resource Locator. Dirección Web.

VBS: Visual Basic Script. Código incrustado en un programa, documento o página Web de ejecución automática.

Virus: Programa capaz de autoduplicarse y extenderse, oculto en otros programas, por ordenadores y redes.

Virus con camuflaje: Tipo de virus que consigue ocultar su presencia ante el usuario e incluso ante programas antivirus, normalmente neutralizando funciones del sistema.

Virus de archivo: Ver virus parásito.

Virus de complemento: Virus que aprovecha el hecho de que cuando existen dos archivos ejecutables con el mismo nombre, el sistema operativo decide cuál ejecutar en función de la extensión. Por ejemplo, en DOS se ejecutará un archivo .com en vez de uno .exe en el caso de tener el mismo nombre. Así, el virus creará un archivo .com con el mismo nombre que otros archivos .exe existentes.

Virus

Email

Internet

Sistemas móviles

Seguridad


Referencia

Virus de sector de arranque: Tipo de virus que altera el proceso de arranque.

Virus de macro: Tipo de virus que utiliza macros en documentos para activarse e infectar otros documentos.

Virus de vínculo: Tipo de virus que altera las entradas de directorio para ejecutar su propio código.

Virus multiparte: Tipo de virus que combina la infección del sector de arranque y de archivos de programa.

Virus parásito: Tipo de virus que se aloja en un archivo de programa y que se activa con la ejecución de éste.

Virus polimórfico: Tipo de virus que cambia su código en cada infección, haciendo más dificil su detección.

WAP: Wireless Application Protocol. Protocolo del tipo Internet de teléfonos móviles y otros dispositivos portátiles.

Web: Ver World Wide Web.

World Wide Web: Sistema de archivos de hipertexto para la distribución de documentos por Internet.

WSH: Windows Scripting Host. Herramienta que automatiza ciertos acciones en Windows, como ejecutar código VBS o Java Script.

WWW: Ver World Wide Web.

Índice

T

U

V

W

X

Índice de virus