Diccionario de amenazas

Amenazas informáticas y para la seguridad de los datos de la A a la Z

SOPHOS

En colaboración con el Centro para la seguridad en Internet

Amenazas informáticas y para la seguridad de los datos de la A a la Z

Este libro está dirigido tanto a profesionales de la informática como a todas aquellas personas que utilicen ordenadores en su trabajo o, simplemente, naveguen por Internet. En él, le explicamos de forma sencilla y fácil de entender toda la realidad sobre las amenazas a las que se exponen los ordenadores y los datos.

Gracias a las soluciones de seguridad para estaciones de trabajo, correo electrónico, Internet, cifrado y redes fáciles de desplegar, administrar y utilizar, Sophos ayuda a los jefes informáticos a centrarse en el negocio. Más de 100 millones de usuarios confían en nosotros para protegerse de la mejor forma posible contra las complejas amenazas actuales y los analistas nos ratifican como uno de los líderes.

Sophos cuenta con más de 20 años de experiencia y una red internacional de centros de análisis de amenazas que nos permiten actuar de forma inmediata ante la aparición de nuevas amenazas. Contamos con sedes centrales en Boston, Massachusetts y Oxford (Reino Unido).

Suscríbase al blog de la empresa blogs.sophos.com, y síganos en Twitter @Sophos_News y Facebook facebook.com/securitybysophos.

El Centro para la seguridad en Internet (o CIS, por sus siglas en inglés) es una organización sin ánimo de lucro (501c3) dedicada a mejorar la preparación para la seguridad informática y la capacidad de respuesta de entidades de los sectores público y privado. El CIS produce contenido para automatizar la seguridad y cotas de referencia de configuración consensuadas y recomendadas; además, sirve como principal recurso de ciberseguridad para los gobiernos estatales, locales, territoriales y étnicos, y proporciona recursos que ayudan a los socios a conseguir sus objetivos de protección mediante soluciones rentables y asesoramiento especializado. Consiga más información en cisecurity.org o @CISecurity.

Contenido

Introducción 3

Amenazas de la A a la Z 5

Hardware y software de seguridad 53

Consejos de seguridad 73

Cronología de los programas maliciosos 91

Introducción

Todos sabemos qué son los virus informáticos o, al menos, eso pensamos.

El primer virus informático, Elk Cloner, apareció hace treinta años y mostraba un breve poema cuando los ordenadores infectados se arrancaban por quincuagésima vez. Desde entonces, los ciberdelincuentes han creado millones de virus y programas maliciosos (virus de correo electrónico, troyanos, gusanos de Internet, programas espía, registradores de pulsaciones en el teclado), y algunos de ellos han llegado a propagarse por todo el mundo e incluso salir en las noticias.

Los virus que llenan las pantallas de los ordenadores de porquería o eliminan archivos son muy conocidos. Mucha gente sigue creyendo que los programas maliciosos no son más que bromas o sabotajes. A principios de los años 90, el virus Michelangelo sembró el pánico en todo el mundo. En los años 2000, mientras millones de ordenadores se infectaban con el virus SoBig-F y se preparaban para descargar programas desconocidos de Internet a una hora concreta, las empresas de antivirus se peleaban con los proveedores de Internet para que cerrasen los servidores y evitar una catástrofe. Algunas películas de Hollywood (por ejemplo, *Independence Day*) contribuyeron a esta idea, mostrando ataques de virus que hacían parpadear las pantallas y sonar alarmas.

Sin embargo, hoy en día, la realidad es muy distinta. Las amenazas siguen siendo existiendo pero son discretas y selectivas, y están más pensadas para ganar dinero que para provocar el caos.

En la actualidad, pocos programas maliciosos eliminan la información almacenada en discos duros, dañan hojas de cálculo o muestran mensajes. Ese tipo de vandalismo ha dado paso a ataques mucho más lucrativos. Los virus actuales pueden cifrar todos los archivos y pedir un rescate por ellos. Los *hackers* pueden hacer chantaje a las empresas amenazándolas con lanzar ataques de denegación de servicio para impedir que los clientes accedan a sus sitios web.

Sin embargo, lo más habitual es que los virus no causen daños aparentes ni se hagan notar lo más mínimo. En lugar de eso, pueden instalar de forma silenciosa registradores de pulsaciones del teclado que esperan a que las víctimas visiten un sitio web de banca electrónica para grabar los datos de la cuenta y la contraseña, y enviarlos al ciberdelincuente por Internet. Los *hackers* son ladrones de identidades y utilizan dichos datos para clonar tarjetas de crédito o saquear cuentas bancarias.

Las víctimas ni siquiera son conscientes de que los ordenadores se han infectado. Una vez cumplida su labor, los virus pueden eliminarse por sí solos para evitar ser detectados.

Muchos otros programas maliciosos se hacen con el control de los equipos para convertirlos en zombis a control remoto y utilizarlos sin el conocimiento de los usuarios en la divulgación de millones de mensajes de correo no deseado con los que obtienen ganancias o para atacar a otros usuarios desprevenidos con más programas maliciosos.

En vista del auge de redes sociales como Facebook o Twitter, los ciberdelincuentes están utilizando estos sistemas para encontrar nuevos métodos con los que infectar equipos y robar identidades.

Los ataques ya ni siquiera están dirigidos a grandes cantidades de víctimas para evitar llamar la atención y que las empresas de antivirus los neutralicen rápidamente. Además, los ataques a gran escala pueden proporcionar a los ciberdelincuentes más datos robados de los que pueden hacerse cargo. Por eso, las amenazas están empezando a elegir sus víctimas con más cuidado.

Los ataques de *spearphishing* son un ejemplo de este tipo. Al principio, los ataques de suplantación de identidades (o *phishing*) se basaban en el envío de campañas masivas de mensajes que parecían provenir de bancos y pedían a los clientes que volviesen a introducir sus datos confidenciales para robarlos. Sin embargo, los ataques de *spearphishing* (literalmente, "pesca con arpón") se restringen a un número limitado de gente, normalmente, de una misma empresa. El mensaje parece provenir de compañeros de departamentos de confianza que solicitan información sobre contraseñas. El principio básico es el mismo, pero los ataques suelen tener más éxito, ya que las víctimas creen que el mensaje es interno y bajan la guardia.

Sigilosas, a pequeña escala y selectivas: por ahora, estas parecen ser las cualidades que están adoptando las amenazas para la seguridad.

Pero, ¿y más adelante? Predecir cómo se transformarán es casi imposible. Algunos analistas opinaban que los virus no pasarían de unos cuantos cientos y, según el propio Bill Gates, el correo no deseado ya no sería un problema en 2006. Por ahora, no está claro de dónde provendrán las amenazas ni lo peligrosas que serán. Pero lo que sí sabemos es que, mientras existan oportunidades de obtener ganancias económicas, los *hackers* y los delincuentes seguirán intentando acceder a los datos para utilizarlos de forma ilegal.

Amenazas de la A a la Z

Amenazas avanzadas persistentes (APT por sus siglas en inglés)

Las amenazas avanzadas persistentes son un tipo de ataque selectivo y suelen provenir de ciberdelincuentes que disponen del tiempo y los recursos necesarios para planificar infiltraciones en redes.

Los agresores gestionan los ataques de forma activa una vez que se introducen en una red y suelen buscar información, confidencial o comercial, en lugar de simples datos financieros. Se dice que estas amenazas son persistentes porque los delincuentes pueden permanecer en la red durante algún tiempo. Las amenazas avanzadas persistentes no deben confundirse con las redes de *bots*, que suelen lanzar ataques oportunistas e indiscriminados contra cualquier víctima disponible en lugar de buscar información específica.

Programas publicitarios

Los programas publicitarios muestran anuncios en los ordenadores.

Los programas publicitarios, también conocidos como *adware*, muestran barras o ventanas con anuncios en los equipos al utilizar determinadas aplicaciones, pero no siempre son peligrosos. En algunos casos, la publicidad sirve para financiar el desarrollo de software útil y distribuirlo de forma gratuita (por ejemplo, muchas aplicaciones de Android y barras de herramientas de navegadores obtienen financiación de esta manera).

Pueden convertirse en un problema cuando:

- se instalan en los ordenadores sin consentimiento de los usuarios
- se instalan en otras aplicaciones y muestran publicidad al utilizarlas
- secuestran el navegador para mostrar más anuncios (véase **Secuestrador de navegadores**)
- recopilan datos sobre la navegación web del usuario sin su consentimiento y los envían a otros por Internet (véase **Programas espía**)
- están diseñados para que resulte difícil desinstalarlos

Los programas publicitarios pueden ralentizar el funcionamiento de los equipos. Las descargas de anuncios también pueden afectar a la velocidad de las conexiones a Internet. A veces, los programas publicitarios pueden contener defectos de programación y afectar a la estabilidad de los ordenadores.

Algunos programas antivirus detectan este tipo de programas como aplicaciones no deseadas para que el usuario los autorice o los elimine del equipo. También existen programas especialmente diseñados para detectar *adware*.

Servidor proxy anónimo

Los servidores proxy anónimos permiten a los usuarios ocultar las actividades de navegación por Internet. Normalmente, se utilizan para burlar los filtros de seguridad web, por ejemplo, para acceder a sitios no permitidos en un ordenador de trabajo.

Los servidores proxy anónimos generan riesgos de seguridad y responsabilidades legales para las empresas:

- Seguridad: los servidores proxy anónimos eluden las medidas de seguridad web y permiten que los usuarios accedan a páginas web no autorizadas.
- Responsabilidades: las empresas pueden enfrentarse a responsabilidades legales si sus equipos se utilizan para visualizar pornografía o material violento, o para incitar comportamientos ilegales. Las infracciones de licencias de terceros por las descargas ilegales de software, películas y MP3 también pueden tener repercusiones.

Gusano de ejecución automática

Los gusanos de ejecución automática son programas maliciosos que abusan de la función de autoejecución de Windows para ejecutarse de forma automática al conectar el dispositivo en el que están almacenados a un ordenador.

Los gusanos de ejecución automática suelen distribuirse en unidades USB e infectan los equipos al conectarlas. La función de reproducción automática utiliza una tecnología similar. Se inicia en un medio extraíble e insta a los usuarios a elegir entre escuchar música con el reproductor de medios predeterminado o abrir el disco en el Explorador de Windows. Los delincuentes han abusado igualmente de la función de reproducción automática, por ejemplo, con el gusano Conficker, uno de los casos más conocidos.

En los sistemas operativos más recientes que disponen de todos los parches, Microsoft ha desactivado de forma predeterminada la opción de ejecución automática, lo que debería contribuir a que estos gusanos representasen una amenaza mucho menor en el futuro.

Troyano de puerta trasera

Los troyanos de puerta trasera permiten hacerse con el control de ordenadores ajenos sin el permiso de los usuarios.

Los troyanos de puerta trasera pueden hacerse pasar por programas legítimos para engañar a los usuarios y que los ejecuten. En otros casos (cada vez más habituales), los usuarios permiten la entrada del troyano en el ordenador sin saberlo al hacer clic en un enlace recibido en un mensaje de correo no deseado o al visitar una página web maliciosa.

Al ejecutarse, el troyano se autoincluye en la rutina de inicio del ordenador y, a partir de ese momento, puede vigilar el equipo hasta que el usuario se conecta a Internet. Una vez que el ordenador está conectado a internet, la persona que envió el troyano puede realizar muchas acciones como, por ejemplo, ejecutar programas en el equipo infectado, acceder a archivos personales, modificar y cargar archivos, registrar las pulsaciones en el teclado o enviar mensajes de correo no deseado.

Entre los troyanos de puerta trasera más conocidos se incluyen Netbus, OptixPro, Subseven, BackOrifice y, más recientemente, Zbot o ZeuS.

Para evitar la entrada de este tipo de troyanos, es aconsejable mantener los equipos actualizados, instalar los parches más recientes (para corregir vulnerabilidades del sistema operativo), y utilizar programas antivirus y anti-*spam*. Además, el uso de cortafuegos puede evitar que los troyanos accedan a Internet para ponerse en contacto con los *hackers*.

Programas maliciosos de sector de arranque

Los programas maliciosos de sector de arranque modifican el programa destinado a iniciar el equipo para propagarse.

Al encender un ordenador, el hardware busca el programa del sector de arranque, que suele encontrarse en el disco duro (aunque también puede estar en un CD-ROM/DVD o unidades flash), y lo ejecuta. A continuación, el programa carga el resto del sistema operativo en la memoria.

Los programas maliciosos de sector de arranque sustituyen el sector de arranque por una versión propia modificada y, normalmente, ocultan el original en algún otro lugar del disco duro. Al volver a iniciar el ordenador, se utiliza el sector de arranque infectado y se activa el programa malicioso.

Hoy en día, algunos programas maliciosos utilizan el sector de arranque para cargarse antes que el sistema operativo con el fin de ocultar su presencia (por ejemplo, el *rootkit* TDL).

Red de *bots*

Las redes de *bots* son grupos de ordenadores infectados controlados de forma remota por un *hacker*.

Una vez que el software malicioso (*bot*) infecta un equipo, el agresor puede controlarlo de forma remota por Internet. A partir de ese momento, el equipo se convierte en un zombi a las órdenes del *hacker* sin que el usuario llegue a percatarse. Los grupos de equipos infectados de esta manera se denominan redes de *bots*.

Los delincuentes pueden compartir el control de la red de *bots* o vender acceso a la misma para que otros puedan utilizarla con fines maliciosos.

Por ejemplo, un creador de correo no deseado puede utilizar una red de este tipo para enviar *spam*. La mayor parte del correo no deseado se distribuye de esta forma, ya que permite a los remitentes evitar ser detectados y sortear las listas negras en las que se hayan podido incluir sus servidores. Además, puesto que los dueños de los ordenadores pagan por el acceso a Internet, reduce los costes.

Los delincuentes también utilizan redes de *bots* para lanzar ataques distribuidos de denegación de servicio (DDoS, por sus siglas en inglés), para los que organizan miles de ordenadores que intentan acceder de forma simultánea al mismo sitio web, haciendo que el servidor sea incapaz de ocuparse de todas las solicitudes que recibe y bloqueando el acceso al sitio web. Consulte **Zombi**, **Ataque de denegación de servicio**, **Correo no deseado**, **Troyano de puerta trasera**, **Centro de comando y control**.

Secuestrador de navegadores

Los secuestradores de navegadores cambian la página de inicio y el motor de búsqueda predeterminados de los navegadores web sin el permiso de los usuarios.

Una vez secuestrado el navegador, puede ser difícil volver a cambiar la página de inicio. Algunos secuestradores modifican el registro de Windows para que la configuración del secuestro se restaure cada vez que se reinicie el ordenador. Otros eliminan opciones en el menú de herramientas de navegación para impedir que se restaure la página de inicio.

El secuestro de navegadores se utiliza para mejorar la clasificación de una página web en los resultados de las búsquedas (al igual que las técnicas de optimización de motores de búsqueda SEO BlackHat) y fomentar así los ingresos generados por la publicidad.

Los secuestradores de navegadores pueden ser muy perseverantes y astutos. Los delincuentes secuestran clics (técnica conocida como *clickjacking* o ataques de redireccionamiento de la interfaz) mediante la inserción de varias capas transparentes u opacas en una página web. Esta técnica puede conseguir que los usuarios hagan clic en botones o enlaces diferentes a los que pretendían pulsar. En realidad, los agresores secuestran los enlaces a una página y los redirigen a otra, normalmente, propiedad de otro dominio, aplicación o ambos.

A pesar de no alojarse en los ordenadores, esta amenaza afecta igualmente a la navegación por Internet de los usuarios.

Ataque por fuerza bruta

En los ataques por fuerza bruta, los ciberdelincuentes prueban una gran cantidad de combinaciones posibles del teclado o contraseñas para acceder de forma ilegal a un sistema o archivo.

Los ataques por fuerza bruta suelen utilizarse para superar sistemas criptográficos como los protegidos con contraseñas. Los ciberdelincuentes utilizan programas informáticos para probar una gran cantidad de contraseñas y descifrar el mensaje o acceder al sistema.

Para evitar ataques por fuerza bruta, es importante utilizar contraseñas lo más seguras posible. Consulte **Cómo elegir contraseñas seguras**.

Desbordamiento del búfer

Los desbordamientos del búfer se producen cuando un programa sobrescribe otras partes de la memoria del equipo para almacenar más datos de los permitidos, provocando errores o bloqueos.

Los ataques de desbordamientos del búfer envían más datos de los previstos a un programa para aprovechar este punto débil. El programa puede leer demasiados datos para los que no ha reservado espacio y sobrescribir partes de la memoria que el sistema operativo está utilizando para otras tareas, lo que puede permitir la ejecución de código no autorizado o bloquear el sistema.

Al contrario de lo que suele creerse, los desbordamientos del búfer no solo se producen en servicios (como los sistemas operativos de Windows) o programas principales, sino que pueden ocurrir en cualquier aplicación.

Centro de comando y control

Los centros de comando y control son ordenadores que controlan redes de *bots*, es decir, redes de equipos secuestrados. Algunas redes de *bots* utilizan sistemas de mando y control distribuidos que las hacen más fuertes.

Desde el centro de mando y control, los ciberdelincuentes pueden enviar órdenes a los equipos para que realicen las actividades deseadas.

Los centros de mando y control suelen utilizarse para lanzar ataques distribuidos de denegación de servicio porque pueden enviar órdenes a una gran cantidad de ordenadores para que realicen la misma acción al mismo tiempo. Consulte **Red de *bots***, **Zombi**, **Ataque de denegación de servicio**.

Cookie

Las cookies son archivos que se guardan en los equipos para que los sitios web puedan recordar determinados datos.

Al navegar por Internet, los sitios web pueden colocar archivos denominados cookies en los equipos. Estos archivos sirven a los sitios web para recordar los datos de los usuarios y hacer un seguimiento de las visitas. Las cookies pueden poner en peligro la privacidad, pero no infectan los ordenadores.

En un principio, las cookies se diseñaron para que fueran útiles. Por ejemplo, al visitar un sitio web, las cookies pueden almacenar las preferencias o los datos de inicio de sesión del usuario para que no tenga que volver a introducirlos la próxima vez. Las cookies también pueden ser beneficiosas para los administradores web, ya que muestran las páginas web más utilizadas y ofrecen información muy útil a la hora de planificar la renovación del diseño de un sitio.

A veces, sin el conocimiento ni el consentimiento de los usuarios, se almacenan en los equipos cookies en forma de pequeños archivos de texto que contienen información sobre las actividades realizadas en un sitio web. Al volver a visitar ese sitio, esos datos se devuelven al servidor web, una vez más, sin permiso.

Poco a poco, los sitios web crean perfiles sobre los comportamientos y los intereses de los usuarios que visitan sus páginas. Dicha información puede venderse o compartirse con otros sitios para que los anunciantes personalicen la publicidad, mostrar anuncios consecutivos al visitar varios sitios distintos y hacer un seguimiento del número de veces que se visualiza un determinado anuncio.

Para limitar el seguimiento del comportamiento con cookies, utilice las opciones de privacidad y seguridad del navegador de Internet.

Filtración de datos

Las filtraciones de datos son divulgaciones no autorizadas de información que pueden dar lugar a robos o fugas de datos.

Su prevención es una de las principales preocupaciones para las empresas. Las filtraciones se producen cuando la información confidencial (como identidades de trabajadores, clientes o el público en general) no se protege adecuadamente.

Los usuarios pueden publicar y compartir datos sin comprender plenamente los riesgos y las consecuencias de una posible filtración de datos.

Para evitar estas filtraciones pueden utilizarse diferentes técnicas, por ejemplo, software antivirus, cifrado, cortafuegos, control del acceso, políticas escritas y formación. Consulte **Fuga de datos**, **Robo de datos**, **Cómo proteger los datos**.

Fuga de datos

Las fugas de datos se producen como resultado de movimientos incorrectos y accidentales de la información, en lugar de robos intencionados.

Las fugas de datos suelen producirse por el extravío de dispositivos que contienen datos como portátiles, tabletas, CD/DVD, teléfonos móviles o memorias USB. Al perderse, se corre el peligro de que los datos caigan en las manos equivocadas, a menos que se haya utilizado una técnica sólida para proteger la información, como el cifrado. Consulte **Filtración de datos**, **Robo de datos**, **Cómo proteger los datos**.

Robo de datos

Los robos de datos se producen de forma deliberada, no accidental.

Los robos de datos pueden producirse tanto dentro de la empresa (por ejemplo, a manos de un trabajador descontento) como mediante ataques de delincuentes desde el exterior.

Los delincuentes suelen utilizar programas maliciosos para acceder a equipos y robar datos. Una de las prácticas más habituales es el uso de troyanos para instalar software de registro de pulsaciones en el teclado y vigilar todo lo que escribe el usuario como, por ejemplo, nombres y contraseñas para acceder a cuentas bancarias.

En 2013, por ejemplo, se produjo un robo de nombres, números de la seguridad social y otros datos delicados de personas involucradas en casos judiciales pendientes en la Oficina Administrativa de las Cortes del estado de Washington.

Entre los robos de datos ocurridos recientemente se incluyen algunos de los más destacados de la historia:

- 2011: La compañía de publicidad por correo electrónico Epsilon sufre una filtración de millones de nombres y direcciones de correo electrónico de las bases de datos de clientes como Best Buy, Marks & Spencer o Chase Bank. Los costes iniciales de retención y reparación previstos alcanzan los 225 millones de dólares pero podrían ascender a los 4 000 millones.
- 2011: Sony Corp. sufre filtraciones que ponen en peligro las cuentas de 100 millones de clientes, con unos costes para la empresa que alcanzan los 2 000 millones de dólares.
- 2011: Los servidores de Global Payments, empresa procesadora de pagos para Visa, sufren una filtración y dejan al descubierto la información de 7 millones de titulares de tarjetas.
- 2012: Se publican más de 6 millones de contraseñas de LinkedIn mal cifradas en un sitio web de delincuencia clandestino.
- 2013: El popular sitio web de ofertas diarias LivingSocial sufre el robo de 50 millones de nombres, direcciones de correo electrónico y contraseñas cifradas.

Los robos de datos también se producen como consecuencia del extravío de dispositivos que contienen datos (portátiles, unidades USB, etc.). Consulte **Filtración de datos**, **Fuga de datos**, **Cómo proteger los datos**.

Ataque de denegación de servicio

Los ataques de denegación de servicio (DoS, por sus siglas en inglés) impiden que los usuarios accedan a un equipo o un sitio web.

En este tipo de ataques, los delincuentes intentan sobrecargar o bloquear un servicio para que los usuarios legítimos no puedan utilizarlo. Normalmente, los ataques de denegación de servicio están dirigidos a servidores web y tienen como objetivo impedir la entrada a un determinado sitio web. No se roban ni se secuestran datos, pero la interrupción del servicio puede resultar costosa para las empresas.

El tipo de ataque DoS más habitual es el utilizado para enviar a un ordenador más tráfico del que puede recibir. Los ataques de denegación de servicio utilizan una gran variedad de métodos, pero la inundación de servidores web con solicitudes desde redes de *bots* es el más sencillo y habitual. Este tipo de ataques se denominan ataques distribuidos de denegación de servicio (DDoS, por sus siglas en inglés). Consulte **Red de *bots***, **Centro de mando y control**, **Zombi**.

Secuestro de DNS

El sistema de nombres de dominios o DNS es la guía telefónica de Internet y sirve para que los equipos puedan traducir nombres de sitios web como www.sophos.com a números de direcciones IP para poder comunicarse.

Los secuestros de DNS cambian la configuración de los equipos para que ignoren el DNS o utilicen un servidor de DNS controlado por los ciberdelincuentes, que redirigen la comunicación a sitios fraudulentos. Este tipo de ataques suele utilizarse para llevar a los usuarios a páginas de inicio de sesiones bancarias falsas y otros servicios por Internet con el fin de robar credenciales.

También puede utilizarse para redirigir sitios de seguridad a servidores que no existen y que los usuarios no puedan actualizar los programas de protección.

Programas maliciosos en documentos

Los programas maliciosos en documentos aprovechan vulnerabilidades de aplicaciones de lectura o edición de documentos.

Mediante la incrustación de contenido malicioso en documentos, los ciberdelincuentes pueden aprovechar las vulnerabilidades de las aplicaciones utilizadas para abrirlos. Entre los ejemplos más habituales se incluyen documentos específicamente modificados de Word, Excel y PDF.

La tristemente célebre filtración de datos sufrida por RSA Security en 2011 comenzó cuando un empleado abrió una hoja de cálculo de Excel que contenía *malware* camuflado de forma minuciosa. Consulte ***Exploit***.

Descarga automática

Las descargas automáticas infectan los equipos con *malware* cuando los usuarios visitan un sitio web malicioso.

Las descargas automáticas se producen sin que los usuarios se den cuenta. Con solo visitar un sitio web infectado, el programa malicioso puede descargarse y ejecutarse en el ordenador. El programa malicioso aprovecha las vulnerabilidades del navegador (y los complementos) para infectar el equipo.

Los ciberdelincuentes atacan sitios web legítimos continuamente para secuestrarlos e inyectar código malicioso en las páginas. Así, cuando los usuarios visitan ese sitio legítimo (aunque secuestrado), el código infectado se carga en el navegador, iniciando el ataque automático. De esta forma, los delincuentes pueden infectar los equipos de los usuarios sin tener que engañarles para que visiten un sitio web específico.

Para protegerse contra las descargas automáticas, es aconsejable utilizar navegadores actualizados y programas de protección de estaciones de trabajo que incluyan filtrado de seguridad web. Consulte ***Exploit***.

Distribución de programas maliciosos por correo electrónico

Como su propio nombre indica, los programas maliciosos de correo electrónico se distribuyen a través del correo electrónico.

Durante muchos años, algunas de las familias de virus más prolíficas (por ejemplo, Netsky o SoBig) se distribuyeron en forma de archivos adjuntos a mensajes de correo electrónico. Estas familias de virus dependían de que los usuarios hicieran doble clic en dichos archivos para ejecutar el código malicioso, infectar el equipo y enviarse a otras direcciones de correo electrónico desde el mismo ordenador.

Hoy en día, los ciberdelincuentes tienen otros objetivos y usan principalmente Internet para distribuir los programas maliciosos. Los mensajes de correo electrónico se siguen utilizando, pero más para distribuir enlaces a sitios infectados que como portadores de archivos maliciosos. Sin embargo, incluso en la actualidad, algunas familias de programas maliciosos (por ejemplo, Bredo) utilizan la distribución por correo electrónico para ejecutar código malicioso en los equipos.

Utilice tecnología sólida contra correo no deseado, software moderno de seguridad para estaciones de trabajo y sistemas operativos actualizados. Además, la formación puede fomentar la concienciación de los usuarios sobre los timos por correo electrónico, y los adjuntos o enlaces aparentemente legítimos. Consulte **Red de *bots***, ***Exploit***, **Mensajes de suplantación de identidades**, **Correo no deseado**.

Exploit

Los *exploits* aprovechan vulnerabilidades para acceder a equipos e infectarlos.

Normalmente, aprovechan vulnerabilidades especificas presentes en una aplicación y pierden toda eficacia en cuanto dicha vulnerabilidad se corrige. Los ciberdelincuentes utilizan y comparten *exploits* de día cero antes de que los proveedores del software descubran la vulnerabilidad (y creen un parche para corregirla).

Para protegerse contra los *exploits*, asegúrese de que el antivirus y el software de seguridad de las estaciones de trabajo están activados y que los equipos disponen de todos los parches necesarios, tanto del sistema operativo como de las aplicaciones. Consulte **Vulnerabilidad**, **Descarga automática**, **Desbordamiento del búfer**.

Antivirus falsos

Los antivirus falsos avisan sobre la existencia de amenazas que no existen para asustar a los usuarios y que instalen software malicioso o paguen por productos de limpieza innecesarios.

Los antivirus falsos, también conocidos como *scareware*, suelen instalarse a través de sitios web maliciosos y se hacen pasar por escaneados en línea. Los ciberdelincuentes atraen tráfico a estos sitios mediante el envío de mensajes de correo no deseado que contienen enlaces o secuestrando sitios web legítimos. A menudo, intentan contaminar los resultados de motores de búsqueda conocidos para que los usuarios accedan a los sitios de distribución maliciosos tras realizar una búsqueda.

Los antivirus falsos tienen una finalidad económica y aportan numerosas ganancias a los ciberdelincuentes. La gran cantidad de beneficios generados proporciona recursos significativos para invertir en la creación y distribución de antivirus falsos. Las bandas de *hackers* son expertas en crear rápidamente sitios web falsos de aspecto profesional que se hacen pasar por proveedores de seguridad legítimos.

El uso de antivirus legítimos actualizados y software de seguridad para estaciones de trabajo ofrece protección contra los programas antivirus falsos. Otra buena medida de protección es la formación y la concienciación de los usuarios sobre los riesgos de hacer clic en enlaces sospechosos.

Hacktivismo

Hacktivismo es el término utilizado para describir los ataques informáticos con fines políticos o sociales dirigidos normalmente a empresas, gobiernos, personalidades y organizaciones.

Los grupos hacktivistas redirigen el tráfico, lanzan ataques de denegación de servicio, desfiguran páginas web y roban información con el fin de expresar sus opiniones.

Un grupo hacktivista acaparó los titulares en 2011 por los ataques a Sony, PBS, el Senado de los Estados Unidos, la CIA y la filial del FBI InfraGard, entre otras víctimas.

Otros grupos hacktivistas han participado en actividades que consideran de desobediencia civil mediante ataques distribuidos de denegación de servicio contra sitios web de gobiernos, bancos y otras instituciones. En un ataque de otro de estos grupos a un contratista del gobierno federal norteamericano, se publicaron 90 000 direcciones de correo electrónico de personal militar de los EE. UU.

La diversidad de los objetivos parece indicar que ninguna institución está realmente a salvo, aunque solo una pequeña minoría se ve afectada por los ataques de los hacktivistas.

Bulo

Los bulos son declaraciones falsas o sin corroborar que intentan engañar o timar a los usuarios.

El objetivo de los bulos puede ser conseguir dinero, instalar programas maliciosos o consumir ancho de banda (haciendo que los usuarios reenvíen mensajes del bulo).

Los bulos por correo electrónico pueden:

- Advertir sobre programas maliciosos nuevos muy peligrosos y difíciles de detectar.
- Sugerir que no se lean mensajes con determinados asuntos porque supuestamente contienen programas maliciosos.
- Afirmar que una empresa de software importante, un proveedor de Internet o una institución gubernamental han publicado la advertencia.
- Afirmar que el programa malicioso hace cosas poco probables.
- Incitar a reenviar la advertencia.
- Afirmar que, al hacer clic en "Me gusta" en algún comentario o usuario de Facebook, se puede ganar dinero, hacer donativos o conseguir premios gratis.

Cuando muchos usuarios reenvían este tipo de bulos, pueden producirse inundaciones del correo electrónico que sobrecargan los servidores. Los bulos también pueden distraer y entorpecer los esfuerzos por solucionar amenazas reales.

La mejor defensa contra los bulos es la formación de los usuarios. También resulta útil buscar información en Internet sobre todo aquello que parezca un bulo.

Cebo

Los cebos son un tipo de seguridad trampa que los especialistas utilizan para detectar ataques informáticos o recolectar muestras de programas maliciosos.

Los especialistas en seguridad y los investigadores suelen utilizar cebos para obtener información sobre las amenazas y los ataques actuales.

Existen muchos tipos de cebos. Algunos están formados por equipos conectados a la red que se utilizan para capturar programas maliciosos. Otros ofrecen servicios de red falsos (por ejemplo, servidores web) para registrar la entrada de ataques.

Gusano de Internet

Un gusano es un tipo de programa malicioso que se duplica en Internet o redes locales.

Los gusanos se diferencian de los virus informáticos en que pueden propagarse por su cuenta, en lugar de necesitar un programa o archivo portador. Para ello, crean copias de sí mismos y utilizan las comunicaciones entre ordenadores.

Conficker, un ejemplo de este tipo de gusanos, aprovecha una vulnerabilidad del sistema para infectar los equipos presentes en la red. Estos gusanos pueden propagarse a gran velocidad e infectar grandes cantidades de equipos.

Algunos abren puertas traseras en los ordenadores que los ciberdelincuentes pueden utilizar para hacerse con el control. Después, los ordenadores pueden utilizarse para enviar correo no deseado. Consulte **Zombi**.

Registro de pulsaciones

El registro de pulsaciones es el proceso mediante el cual terceros no autorizados guardan pulsaciones en el teclado de los usuarios de forma secreta.

Los programas maliciosos suelen utilizarlo para robar nombres de usuario, contraseñas, datos de tarjetas de crédito y otros datos delicados.

Programas maliciosos

O *malware*, es el término genérico utilizado para englobar programas peligrosos como virus, gusanos, troyanos y programas espía. A menudo, los términos *malware* y virus se utilizan indistintamente.

Los programas antivirus suelen detectar una gama más amplia de amenazas (en lugar de solamente virus) y pueden ser una defensa eficaz contra los gusanos, los troyanos y los programas espía.

Programas maliciosos para teléfonos móviles

Los programas maliciosos para teléfonos móviles están diseñados para ejecutarse en dispositivos móviles como teléfonos inteligentes y ordenadores de mano.

Desde finales de 2010, año en el que se identificaron las primeras muestras para dispositivos Android e iOS, se han descubierto miles de variedades de programas maliciosos para dispositivos móviles.

En la actualidad, los investigadores tienen noticia de muchas más aplicaciones maliciosas para el sistema Android que para iOS, probablemente, porque el primero permite instalar aplicaciones desde fuentes de terceros. Los sitios de intercambios de archivos suelen alojar versiones maliciosas de aplicaciones y juegos conocidos.

Con los programas maliciosos para dispositivos móviles (al igual que los dirigidos a ordenadores personales), los ciberdelincuentes persiguen beneficios económicos. De forma similar a los que amenazan Windows, los programas maliciosos para dispositivos móviles distribuyen antivirus falsos y roban información confidencial. Otros envían mensajes SMS o realizan llamadas a líneas telefónicas de tarifas especiales (si el dispositivo infectado forma parte de una red telefónica).

Incluso las fuentes de confianza pueden alojar aplicaciones peligrosas para la privacidad de los usuarios. Ciertos marcos publicitarios pueden compartir la información de identificación personal de los usuarios, como la ubicación o el número de teléfono. Estas aplicaciones pueden clasificarse como aplicaciones no deseadas.

Para evitar la entrada de programas maliciosos en los dispositivos móviles, es aconsejable mantenerlos al día con todas las actualizaciones de seguridad, y descargar e instalar solamente aplicaciones de fuentes de confianza como Google Play o Apple iTunes.

Los programas de seguridad para móviles proporcionan una capa de protección adicional. Para informarse sobre cómo mantener protegidos los dispositivos Android o descargar una herramienta gratuita, visite:

www.sophos.com/es-es/androidsecurity.

Virus parásito

Los virus parásitos, también conocidos como virus de archivos, se adhieren a programas para propagarse.

Al iniciar un programa infectado con un virus parásito, se ejecuta el código del virus. Después, para ocultarse, estos virus devuelven el control al programa original.

Para los sistemas operativos de los equipos, los virus forman parte del programa que el usuario desea ejecutar, por lo que les otorgan los mismos derechos. Con tales derechos, el virus puede copiarse, instalarse en la memoria o realizar cambios en el ordenador.

Los virus parásitos aparecieron pronto, pero después se volvieron poco habituales. Sin embargo, están volviendo a surgir con más frecuencia, con ejemplos como Sality, Virut y Vetor.

Parches

Los parches son complementos de software diseñados para corregir defectos, incluidas vulnerabilidades de seguridad, en sistemas operativos y aplicaciones.

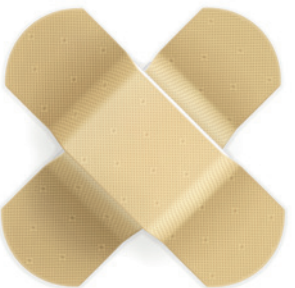
La instalación de parches contra vulnerabilidades nuevas de la seguridad es fundamental para protegerse contra los programas maliciosos. Muchas de las amenazas más destacadas aprovechan vulnerabilidades de seguridad. Si los parches no se aplican o no se actualizan de forma puntual, se corre el riesgo de permitir la entrada de ciberdelincuentes en los ordenadores.

Muchos proveedores de software publican parches nuevos de forma periódica. Por ejemplo, Microsoft publica correcciones el segundo martes de cada mes, mientras que Adobe publica actualizaciones trimestrales de Adobe Reader y Acrobat el segundo martes de cada trimestre.

Para mantenerse informado sobre las vulnerabilidades y los parches más recientes, suscríbase a listas de correo sobre vulnerabilidades como las que ofrecen los proveedores de más renombre. Por ejemplo, Microsoft ofrece información sobre seguridad en http://technet.microsoft.com/es-es/security/dd252948.aspx.

Los usuarios particulares de Microsoft Windows pueden utilizar Windows Update (Windows Vista/7) o el Centro de seguridad (Windows XP) para activar las actualizaciones automáticas. Los usuarios de Apple OS X pueden hacer clic en el logotipo de Apple que aparece en la parte superior izquierda de sus escritorios y seleccionar la opción de actualizaciones del software.

Las empresas deben asegurarse de que todos los equipos que se conectan a la red cumplen una política de seguridad definida que obligue a tener instalados los parches de seguridad más recientes, incluidos los necesarios para los sistemas operativos y las aplicaciones. Consulte ***Exploit***, **Vulnerabilidad**.



Mensajes de suplantación de identidades

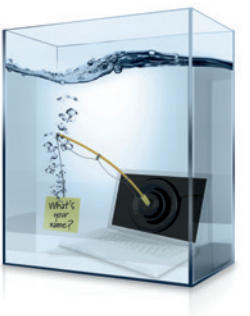
La suplantación de identidades es el proceso mediante el cual los ciberdelincuentes engañan a los usuarios para que revelen información delicada.

Normalmente, a través de los timos de mensajes de suplantación de identidades, los usuarios reciben un mensaje de correo electrónico que parece provenir de una institución de confianza, por ejemplo:

- Bancos
- Redes sociales (Facebook, Twitter)
- Juegos por Internet
- Servicios en línea con acceso a la información financiera del usuario (por ejemplo, iTunes, préstamos universitarios, servicios contables)
- Departamentos de la empresa del usuario (desde el equipo de soporte técnico hasta el administrador del sistema, el servicio de asistencia, etc.)

Para protegerse contra los ataques de suplantación de identidades, es aconsejable no hacer clic en enlaces incluidos en mensajes de correo electrónico. En su lugar, introduzca la dirección del sitio web en la barra del navegador y vaya a la página correcta, o utilice un marcador o un favorito. Los mensajes de suplantación de identidades también pueden incluir adjuntos que pueden infectar el equipo al abrirlos.

Los programas de software contra suplantaciones de identidades pueden bloquear muchos mensajes de este tipo.



Aplicación no deseada (PUA)

Las aplicaciones no deseadas son programas que, a pesar de no ser maliciosos, pueden no ser aceptables en entornos empresariales y provocar riesgos para la seguridad.

Algunas aplicaciones no maliciosas y posiblemente útiles en el contexto adecuado, pueden no ser aceptables en las redes empresariales como, por ejemplo, los programas publicitarios, las herramientas de administración remota de ordenadores personales y los escáneres que detectan vulnerabilidades en sistemas informáticos.

Ciertos antivirus y programas de seguridad para estaciones de trabajo pueden detectar aplicaciones no deseadas en los ordenadores de los usuarios y denunciar su presencia.

Ransomware

Los programas de *ransomware* impiden acceder a los archivos o a los equipos hasta que se paga un rescate.

El software malicioso puede secuestrar los datos. Por ejemplo, el troyano Archiveus copia el contenido de la carpeta Mis documentos en un archivo protegido con contraseña y elimina los archivos originales. Después, deja un mensaje para informar al usuario de que es necesaria una contraseña de 30 caracteres para acceder a la carpeta y que la recibirá al realizar compras en una farmacia virtual.

En algunos casos, la contraseña o clave está oculta en el código del troyano y los analistas de programas maliciosos pueden extraerla. Sin embargo, algunos delincuentes utilizan cifrado asimétrico o de claves públicas (con una clave para cifrar los datos y otra distinta para descifrarlos), lo que dificulta en gran medida la recuperación de la contraseña.

Rootkit

Los *rootkits* son programas de software que ocultan otros programas o procesos en ejecución en los ordenadores.

Los programas maliciosos suelen instalarlos tras las infecciones para ocultar sus actividades. Los *rootkits* pueden ocultar registradores de pulsaciones o rastreadores de contraseñas, que capturan información confidencial y la envían a los *hackers* por Internet. También pueden permitir que los ciberdelincuentes utilicen el equipo con fines ilegales (por ejemplo, para lanzar ataques de denegación de servicio contra otros equipos o enviar mensajes de correo no deseado) sin el conocimiento del usuario.

Hoy en día, los productos de seguridad para estaciones de trabajo detectan y eliminan *rootkits* como parte de las rutinas de limpieza estándar de programas maliciosos. Sin embargo, para mitigar algunos de ellos, pueden ser necesarias estrategias más complejas.

Ingeniería social

La ingeniería social está compuesta por los métodos que utilizan los ciberdelincuentes para engañar a las víctimas y que realicen determinadas acciones, como abrir páginas web maliciosas o ejecutar adjuntos no deseados.

Muchas de las técnicas de ingeniería social se centran en engañar a los usuarios para que revelen nombres de usuario y contraseñas, que los ciberdelincuentes utilizan para enviar mensajes como usuarios internos y ampliar sus intentos de robar datos.

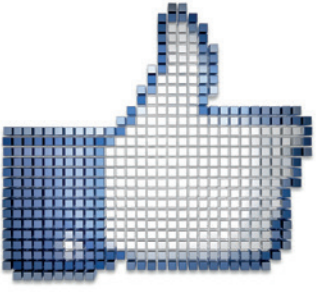
Por ejemplo, en agosto de 2013, los ciberdelincuentes distribuyeron mensajes de correo electrónico que imitaban los mensajes enviados por Facebook al etiquetar a un usuario. Los enlaces incluidos en los mensajes llevaban a sitios en los que se recomendaba instalar un complemento para ver los vídeos supuestamente publicados en Facebook. En realidad, el complemento era un programa malicioso diseñado para robar contraseñas guardadas y entrar en las cuentas de usuarios de Facebook.

Redes sociales

Los sitios de redes sociales nos permiten comunicarnos y compartir información, pero también pueden utilizarse para distribuir programas maliciosos y robar información personal.

Los sitios de redes sociales como Facebook y Twitter siguen ganando popularidad como vectores de ataque. Los delincuentes pueden utilizar la información publicada en Internet para obtener datos sobre los usuarios y aplicarlos en técnicas de ingeniería social o averiguar las respuestas a las preguntas de seguridad de otros sitios. Además, pueden secuestrar las cuentas de los amigos y utilizarlas para distribuir *malware* u otro contenido malicioso.

Tenga cuidado con los enlaces en los que hace clic. Asegúrese de que todos los equipos que utiliza para conectarse al sitio están protegidos con los parches y el software de seguridad más reciente. Utilice contraseñas seguras y diferentes en cada cuenta. Si está disponible, aproveche la autenticación de doble factor. Preste atención a lo que publica en Internet y utilice las opciones de privacidad disponibles para limitar la visibilidad de la información. Consulte **Cómo protegerse en Internet**.



Correo no deseado

Se denomina correo no deseado o *spam* a los mensajes de correo electrónico masivos no solicitados, el equivalente virtual de la publicidad que llega a los buzones tradicionales.

Los remitentes de correo no deseado suelen disfrazar los mensajes para intentar sortear los programas anti-*spam*. El correo no deseado llega cada vez más a menudo a través de direcciones de correo electrónico legítimas de usuarios de Yahoo!, Hotmail o AOL cuyas credenciales se han secuestrado.

Además, los timadores están dirigiendo programas maliciosos a proveedores importantes de servicios de correo electrónico para intentar secuestrar los agentes de transferencias y enviar correo no deseado.

El correo no deseado suele ser rentable. Los remitentes de correo no deseado pueden enviar millones de mensajes en una sola campaña por muy poco dinero. Con solo un destinatario de entre 10 000 que realice una compra, pueden obtener beneficios.

Importancia del correo no deseado

- El correo no deseado se utiliza a menudo para distribuir programas maliciosos (consulte **Distribución de programas maliciosos por correo electrónico**).
- Los remitentes de correo no deseado suelen utilizar ordenadores ajenos para enviar *spam* (consulte **Zombi**).
- El correo no deseado, al igual que los bulos y los virus por correo electrónico, utilizan ancho de banda y ocupan espacio en las bases de datos.
- Por otra parte, pueden confundir mensajes importantes con correo no deseado y pasarlos por alto o eliminarlos.
- El correo no deseado hace perder el tiempo al personal. Los usuarios sin protección anti-*spam* tienen que comprobar qué mensajes son correo no deseado y eliminarlos.

Además, en la actualidad, los creadores de *spam* están aprovechando la popularidad de la mensajería instantánea y redes sociales como Facebook y Twitter para sortear los filtros de correo no deseado y engañar a los usuarios para que revelen información delicada y financiera.

Spearphishing

El *spearphishing* (literalmente, "pesca con arpón") es un tipo de ataque selectivo de suplantación de identidad en el que se utilizan mensajes de correo electrónico falsos para convencer a las personas de una empresa para que revelen información sensible o credenciales.

A diferencia de los ataques de suplantación de identidades normales que envían mensajes en masa, el *spearphishing* se realiza a pequeña escala y de forma muy específica. Los mensajes se envían a usuarios de una única empresa y parecen proceder de otro empleado de la misma, que necesita confirmar el nombre de usuario y la contraseña del usuario objetivo. A veces, los mensajes parecen proceder de un departamento de confianza que normalmente necesita tales datos como el departamento informático o de recursos humanos. Los enlaces incluidos en los mensajes llevan a una versión falsa del sitio web o la red interna de la empresa para robar credenciales. Consulte **Distribución de programas maliciosos por correo electrónico**.

Falsificación (de correo electrónico)

La falsificación de direcciones de correo electrónico se utiliza como técnica de ingeniería social.

Las falsificaciones pueden utilizarse de diferentes formas con fines maliciosos.

Los delincuentes que se dedican a suplantar identidades para engañar a los usuarios y que revelen información confidencial utilizan direcciones falsificadas para que los mensajes parezcan provenir de fuentes de confianza como, por ejemplo, bancos. Los mensajes de correo electrónico pueden llevar a sitios web falsos (por ejemplo, imitaciones de páginas de banca electrónica) diseñados para robar datos y contraseñas de cuentas.

Los mensajes de correo electrónico también pueden parecer mensajes internos de la empresa (por ejemplo, del administrador de sistemas) en los que se pide al usuario que cambie la contraseña o confirme otros datos.

Los delincuentes que utilizan el correo electrónico para timos o fraudes pueden ocultarse y evitar ser detectados mediante direcciones falsificadas. Consulte **Distribución de programas maliciosos por correo electrónico**.

Programas espía

Los programas espía permiten a los ciberdelincuentes y a los anunciantes recolectar información delicada de los usuarios sin su permiso.

Los programas espía pueden introducirse en los equipos al visitar determinados sitios web. Algunos muestran ventanas emergentes para que el usuario descargue herramientas de software supuestamente necesarias, mientras que otros descargan programas de forma automática.

Al ejecutarse, los programas espía pueden hacer un seguimiento de las actividades (por ejemplo, los sitios web visitados) y enviar informes a terceros no autorizados como anunciantes.

Los programas espía consumen memoria y capacidad de procesamiento, lo que puede afectar a la velocidad de los equipos o hacer que se bloqueen.

Las soluciones de protección de estaciones de trabajo y los antivirus de calidad pueden detectar y eliminar programas espía, que se consideran como un tipo de troyano. Consulte **Programas publicitarios**.

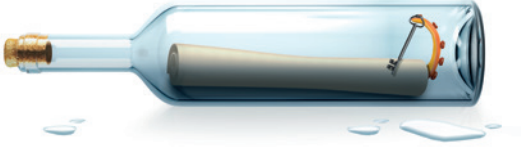
Inyección de código SQL

La inyección de SQL es una técnica utilizada para abusar de programas de consultas de bases de datos que no realizan comprobaciones exhaustivas.

Los ciberdelincuentes utilizan inyecciones de código SQL junto con secuencias de comandos entre sitios y programas maliciosos para introducirse en sitios web y extraer datos o incrustar código malicioso.

El código SQL inyectado envía órdenes a través de un servidor web vinculado a una base de datos SQL. Si el servidor no está diseñado o protegido correctamente, puede tratar los datos introducidos en campos de formularios (por ejemplo, el nombre de usuario) como si fueran órdenes que deben ejecutarse en el servidor de la base de datos. Por ejemplo, un agresor puede introducir un comando diseñado para extraer el contenido de la base de datos de registros de clientes e información de pagos en su totalidad.

Los escaneados de aplicaciones web pueden ayudar a detectar este tipo de ataques mediante un sistema avanzado de patrones diseñados para detectar comandos SQL transmitidos al servidor web. Al igual que con cualquier otro sistema basado en patrones, para conseguir la máxima protección y poder hacer frente a los nuevos métodos de incrustación de código SQL, los patrones deben estar actualizados. Los escaneados frecuentes de las aplicaciones web pueden ayudar a detectar vulnerabilidades de SQL y ofrecer recomendaciones para corregirlas.



Archivos y comportamientos sospechosos

Al escanear archivos, las soluciones de seguridad para estaciones de trabajo los etiquetan como limpios o maliciosos. Cuando un archivo presenta una serie de características o comportamientos dudosos, se etiqueta como sospechoso.

Los comportamientos sospechosos hacen referencia a actividades dudosas realizadas por los archivos al ejecutarse en los equipos como, por ejemplo, cuando se copian en una carpeta del sistema.

La protección en tiempo de ejecución analiza el comportamiento de todos los programas que se ejecutan en el equipo y bloquea cualquier actividad con apariencia maliciosa o sospechosa. Consulte **Desbordamiento del búfer**.

Troyano (caballo troyano)

Los troyanos son programas maliciosos que se hacen pasar por software legítimo pero esconden funciones dañinas.

Los troyanos fingen realizar una actividad cuando, en realidad, realizan otra distinta, normalmente, sin el conocimiento del usuario. Uno de los ejemplos más conocidos son los códecs que algunos sitios exigen para ver vídeos en Internet. Al instalar el códec, pueden instalarse también programas espía y otros programas maliciosos.

Otro buen ejemplo es el enlace malicioso "Cool Game". Al descargar e instalar el programa del juego, resulta no ser un juego, sino un troyano que secuestra el equipo o elimina los datos del disco duro.

Los troyanos suelen distribuirse con aplicaciones de software pirateadas y *keygens* que crean códigos de licencias ilegales para software descargable. Consulte **Troyano de puerta trasera**.

Virus

Los virus son programas informáticos maliciosos que pueden propagarse a otros archivos.

Los virus pueden tener efectos dañinos como, por ejemplo, mostrar mensajes molestos, robar datos o ceder el control de los equipos a los ciberdelincuentes.

Los virus pueden acoplarse a otros programas u ocultarse en código de ejecución automática al abrir ciertos tipos de archivos. A veces, aprovechan defectos en la seguridad de los sistemas operativos para ejecutarse y propagarse de forma automática.

Los archivos infectados pueden recibirse de diferentes maneras, por ejemplo, en adjuntos de correo electrónico, descargas de Internet o unidades USB. Consulte **Virus parásito**, **Distribución de programas maliciosos por correo electrónico**, **Gusano de Internet**, **Programas maliciosos**.

Vulnerabilidad

Las vulnerabilidades son defectos presentes en programas de software que los ciberdelincuentes utilizan para atacar ordenadores.

Las vulnerabilidades de seguridad son habituales en los productos de software y pueden permitir la entrada de ataques. Los proveedores de software responsables, al descubrir algún problema, crean y publican parches para solucionar la vulnerabilidad.

Algunas empresas contratan investigadores para que detecten vulnerabilidades nuevas. También existen ciberdelincuentes que venden las vulnerabilidades nuevas en el mercado negro.

Los ataques que aprovechan vulnerabilidades antes de que los proveedores las descubran o publiquen parches para corregirlas se denominan ataques de "día cero".

Para paliarlas, es aconsejable aplicar los parches más recientes o activar las funciones de actualización automática de los sistemas operativos y cualquier aplicación instalada. Consulte ***Exploit***, **Parches**.

Zombi

Los zombis son ordenadores infectados controlados de forma remota por los ciberdelincuentes. Forman parte de un amplio grupo de equipos secuestrados que se denomina red de *bots*.

Una vez que el ciberdelincuente puede controlar el ordenador de forma remota por Internet, el equipo se convierte en un zombi. Normalmente, los zombis se utilizan para enviar correo no deseado, lanzar ataques de denegación de servicio e infectar otros sistemas. Consulte **Red de *bots***.

Hardware y software de seguridad

Protección contra programas maliciosos

Los programas de protección contra programas maliciosos (también conocidos como anti-*malware*) protegen los equipos contra amenazas de virus y demás programas maliciosos, incluidos troyanos, gusanos y programas espía.

El software anti-*malware* utiliza escaneados para identificar programas que son o pueden ser maliciosos. Los escaneados pueden detectar:

- Programas maliciosos conocidos: el escáner compara los archivos presentes en el equipo con una biblioteca de identidades de programas maliciosos conocidos. Si encuentra alguna que coincida, emite una alerta e impide acceder al archivo. La detección de programas maliciosos conocidos depende de las actualizaciones frecuentes de la base de datos con las identidades de virus más recientes o de la conexión a una base de datos de programas maliciosos en la nube.
- Programas maliciosos desconocidos: el escáner analiza el comportamiento probable de un programa. Si presenta todas las características de un virus, se impide acceder a él aunque el archivo no coincida con ningún virus conocido.
- Archivos sospechosos: el escáner analiza el comportamiento probable de un programa. Si el comportamiento se considera inadecuado, el escáner advierte que podría tratarse de un programa malicioso. La mayoría de paquetes anti-*malware* ofrecen escaneados tanto en acceso como en demanda.

Las detecciones en acceso están activas siempre que el equipo esté en uso, revisan los archivos de forma automática al intentar abrirlos o ejecutarlos, y pueden evitar que se acceda a archivos infectados.

Los escáneres en demanda permiten iniciar o programar escaneados de unidades o archivos específicos.

Anti-*spam*

Los programas anti-*spam* pueden detectar mensajes de correo electrónico no deseados y evitar que lleguen a los buzones de los usuarios.

Estos programas utilizan una combinación de métodos para determinar si un mensaje de correo electrónico podría tratarse de correo no deseado. Pueden:

- Bloquear correo electrónico procedente de equipos incluidos en listas de equipos bloqueados disponibles en el mercado o en una lista local de direcciones de equipos que han enviado correo no deseado con anterioridad a la empresa.
- Bloquear mensajes de correo electrónico que incluyan determinadas direcciones web.
- Comprobar si el correo electrónico procede de direcciones web o nombres de dominios auténticos. Los creadores de correo no deseado suelen utilizar direcciones falsas para intentar sortear los programas anti-*spam*.
- Buscar palabras o frases clave que suelen aparecer en el correo no deseado (por ejemplo, "tarjeta de crédito", "adelgazar").
- Identificar patrones que indiquen que el remitente del mensaje de correo electrónico está intentando disfrazar sus palabras (por ejemplo, "p0rno dur*").
- Buscar código HTML (el código utilizado para escribir páginas web) innecesario, que los creadores de *spam* suelen utilizar para ocultar los mensajes y desorientar a los programas anti-*spam*.
- Combinar toda la información que encuentran para determinar la probabilidad de que un mensaje de correo electrónico sea correo no deseado. Si la probabilidad es lo suficientemente alta, pueden bloquearlo o eliminarlo, según la configuración elegida.

El software anti-*spam* debe actualizarse con frecuencia con reglas nuevas para que pueda reconocer las técnicas más recientes utilizadas por los creadores de correo no deseado.

Dispositivos

Los dispositivos combinan elementos de seguridad de hardware y software en una única solución, lo que permite simplemente conectarlos en lugar de tener que instalar el software por separado.

Los tipos de dispositivos más habituales son los dispositivos para correo electrónico, Internet o de gestión unificada de amenazas (UTM), y se colocan en la puerta de enlace entre los sistemas informáticos de las empresas e Internet para filtrar el tráfico y bloquear programas maliciosos, correo no deseado y fugas de datos.

Los dispositivos para el correo electrónico bloquean correo no deseado, suplantaciones de identidades, virus, programas espía y otros programas maliciosos, y dependiendo de la solución, pueden utilizar también técnicas de cifrado y filtrado del contenido para evitar fugas de información delicada o confidencial a través del correo electrónico.

Los dispositivos para Internet bloquean programas maliciosos y espía, suplantaciones de identidades, servidores proxy anónimos y otras aplicaciones no deseadas en la puerta de enlace a Internet. También pueden ofrecer herramientas para imponer políticas sobre el uso de Internet.

Los dispositivos de UTM eliminan las complicaciones de desplegar y administrar varias soluciones aisladas para proteger las empresas contra virus, correo no deseado y ataques informáticos.

Restricción de aplicaciones

La restricción de aplicaciones permite controlar el uso de aplicaciones que pueden no ser adecuadas para los equipos o las redes de una empresa.

La restricción de aplicaciones puede utilizarse para limitar las actividades de los usuarios a las aplicaciones elegidas por la empresa. Por ejemplo, puede establecer una política que solo permita utilizar Internet Explorer y bloquee todos los demás navegadores de Internet. El control de las aplicaciones que los usuarios pueden ejecutar reduce los riesgos de fugas de datos y programas maliciosos.

Entre las categorías de aplicaciones que las empresas pueden querer restringir se incluyen programas de intercambio de archivos, juegos, reproductores multimedia, herramientas de gestión remota y clientes de mensajería instantánea.

Por otra parte, los cortafuegos de última generación pueden filtrar el tráfico de red según determinadas aplicaciones para proporcionar un nivel de control adicional.

Control de dispositivos

El control de dispositivos ayuda a controlar el uso de dispositivos de almacenamiento extraíbles, unidades ópticas y protocolos de redes inalámbricas.

El control de dispositivos es un componente fundamental de las estrategias de prevención de fugas de datos. Por ejemplo, ayuda a evitar los programas maliciosos que se propagan a través de memorias USB.

Muchas empresas utilizan el control de dispositivos para imponer políticas relacionadas con el uso de dispositivos de almacenamiento extraíbles. Dependiendo de la solución utilizada, el control de dispositivos puede ayudar a determinar qué dispositivos pueden conectarse a los ordenadores mediante una política central.

Cifrado

Las soluciones de cifrado cifran ordenadores de sobremesa y portátiles, medios extraíbles, CD-ROM, archivos de red, dispositivos de almacenamiento en la nube, otros dispositivos y el correo electrónico para proteger los datos. Para acceder a la información, es necesario utilizar las claves adecuadas para descifrar los datos mediante una contraseña.

Algunas soluciones de cifrado pueden configurarse para que los usuarios autorizados puedan descifrar los datos de forma automática y no tengan que introducir la clave o contraseña de cifrado para acceder a la información.

Según el producto, las soluciones de cifrado suelen incluir funciones de gestión de claves (que facilitan el almacenamiento, el intercambio y la recuperación de las claves de cifrado), imposición de políticas de cifrado, gestión centralizada y creación de informes. El cifrado de cualquier dato almacenado por terceros es una medida de seguridad importante. Además, los empleados pueden acceder a los datos cifrados mientras se desplazan desde sus dispositivos móviles, incluidos teléfonos inteligentes y tabletas.

Las soluciones de cifrado permiten proteger la información confidencial y cumplir las leyes de protección de datos.

Protección de estaciones de trabajo

Los programas de protección de estaciones de trabajo protegen ordenadores y dispositivos contra una amplia gama de amenazas para la seguridad, la productividad y el cumplimiento de las normativas, y permiten administrar de forma centralizada la seguridad en multitud de estaciones.

Los productos de seguridad para estaciones de trabajo incluyen en una misma solución los productos independientes necesarios para protegerlas contra las amenazas actuales. Normalmente, integran la protección de multitud de funciones en un agente o en una consola centralizada para facilitar la gestión y la creación de informes. Pueden incluir:

- Software antivirus
- Cortafuegos
- Control de dispositivos
- Control del acceso a la red
- Restricción de aplicaciones
- Protección en tiempo de ejecución
- Tecnología de cifrado
- Protección web
- Administración de parches
- Prevención de fugas de datos

Es aconsejable utilizar programas de protección de estaciones de trabajo que incluyan funciones de escaneado del contenido web, ya que los programas maliciosos suelen distribuirse a través de sitios web. También puede plantearse la posibilidad de activar las funciones de filtrado de seguridad del navegador web que utilice.

Descargue una evaluación gratuita de Sophos Enduser Protection en www.sophos.com/es-es/endpoint.

Cortafuegos

Los cortafuegos evitan accesos no autorizados a ordenadores y redes.

Como su propio nombre indica, los cortafuegos funcionan como barrera entre las redes o partes de estas, bloqueando el tráfico malicioso y frenando intentos de ataques informáticos.

Los cortafuegos de red se instalan en los límites que separan dos redes, normalmente, entre Internet y la red de una empresa. Pueden ser dispositivos de hardware o programas de software instalados en un ordenador que funciona como puerta de enlace a la red de la empresa.

Los cortafuegos cliente se ejecutan en los ordenadores de los usuarios y protegen solo el equipo en el que están instalados.

En ambos casos, el cortafuegos analiza todo el tráfico, tanto entrante como saliente, para comprobar que cumple determinados criterios. Si los cumple, lo permite; si no, lo bloquea.

Los cortafuegos cliente también pueden advertir a los usuarios cada vez que un programa intenta realizar una conexión para preguntarles si deben permitirla o bloquearla.

Los cortafuegos pueden filtrar el tráfico basándose en:

- Las direcciones de origen y destino, y los números de los puertos (filtrado de direcciones).
- El tipo de tráfico de red (por ejemplo, filtrado de protocolos HTTP o FTP).
- Los atributos o el estado de los paquetes de información enviados.

Escaneado de HTTPS

Los programas maliciosos y otras amenazas pueden ocultarse en el tráfico cifrado procedente de sitios web de confianza. El escaneado de HTTPS descifra, escanea y vuelve a cifrar los datos.

El escaneado de HTTPS detecta y elimina de forma automática el contenido malicioso sin necesidad de intervención humana para conservar la privacidad del tráfico cifrado.

Sistemas de prevención de intrusiones

Los sistemas de prevención de intrusiones vigilan las redes y los sistemas para detectar actividades maliciosas.

Estos sistemas pueden registrar información sobre las actividades, así como bloquearlas y crear informes al respecto para informar a los administradores de red y evitar infecciones.

IPsec

IPsec autentica y cifra los paquetes del protocolo de Internet (IP) de las sesiones de comunicación.

IPsec incluye protocolos para establecer la autenticación entre agentes al principio de una sesión y negocia las claves criptográficas que se utilizarán durante la misma.

Protección de dispositivos móviles

La protección de dispositivos móviles está formada por las políticas, los procedimientos y las herramientas para proteger este tipo de dispositivos.

El número de ataques dirigidos a dispositivos móviles ha aumentado y lo seguirá haciendo a medida que los integramos en nuestra vida diaria.

Su protección y la de los datos que almacenan debería ser una de las máximas prioridades para cualquier empresa. Asegúrese de que las políticas y los procedimientos están actualizados para incluir los dispositivos móviles. Los consejos para la protección de ordenadores personales pueden aplicarse también a los teléfonos inteligentes y las tabletas: actualice el software de forma periódica, tenga cuidado al instalar aplicaciones nuevas, utilice software de seguridad actual e investigue cualquier actividad sospechosa. Los sistemas de administración de dispositivos móviles pueden ayudar a las empresas a centralizar muchas de estas funciones.

Control del acceso a la red (NAC)

Las soluciones de control del acceso a la red (NAC) protegen las redes y la información que almacenan contra las amenazas que representan los usuarios y los dispositivos que acceden a ellas.

Las soluciones de NAC realizan tres funciones principales:

- Autenticación de usuarios y dispositivos, o verificación de identidades.
- Evaluación de los ordenadores que intentan acceder a la red para asegurarse de que están libres de virus y cumplen los criterios de seguridad.
- Imposición de políticas según la función del usuario para que todos puedan acceder a la información correspondiente a su puesto e impedir accesos no autorizados a otros datos.

Protección en tiempo de ejecución

La protección en tiempo de ejecución bloquea los intentos de acceso a partes sensibles de un equipo.

La protección en tiempo de ejecución analiza el comportamiento de todos los programas que se ejecutan en el equipo y bloquea cualquier actividad con apariencia maliciosa o sospechosa. Por ejemplo, comprueba cualquier cambio que se esté realizando en el registro de Windows, lo que podría indicar que un programa malicioso se está instalando y configurando para iniciarse de forma automática al arrancar el ordenador.

Las soluciones de protección en tiempo de ejecución incluyen:

Sistemas de prevención de intrusiones en el host (HIPS), que vigilan el comportamiento del código para bloquear programas maliciosos antes de que se publique una actualización específica para su detección. Muchas soluciones HIPS vigilan el código cuando se ejecuta e intervienen si se considera sospechoso o malicioso.

Sistemas de prevención de desbordamientos del búfer (BOPS), que detectan ataques dirigidos a las vulnerabilidades tanto del sistema operativo como de las aplicaciones. El sistema genera alertas cuando se identifican intentos de aprovechar procesos en ejecución mediante técnicas de desbordamiento del búfer.

Gestión unificada de amenazas (UTM)

La gestión unificada de amenazas agrupa varias funciones de seguridad en un solo dispositivo de red.

Con la gestión unificada de amenazas, las empresas pueden desplegar varias capas de protección sin las complicaciones de utilizar varios dispositivos y consolas de administración independientes. Las soluciones de UTM pueden incluir funciones como cortafuegos de última generación, filtrado de contenido web, anti-*spam* y antivirus para correo electrónico, cortafuegos de aplicaciones web y administración de la protección en estaciones de trabajo.

Filtrado de direcciones o contenido web

El filtrado de direcciones o contenido web es una tecnología que permite a las empresas bloquear sitios web específicos o categorías completas.

La mayoría de los ataques de suplantación de identidad y programas maliciosos se llevan a cabo a través de Internet. Al restringir el acceso a determinados sitios web, las empresas pueden reducir los riesgos de que los usuarios se conviertan en víctimas de estos ataques.

Redes VPN y VPN SSL

Las redes privadas virtuales (o VPN, por sus siglas en inglés) sirven para conectar oficinas y ordenadores remotos a una red central.

Este método suele exigir la autenticación de los usuarios remotos mediante la introducción de contraseñas o claves. Las redes VPN permiten a los usuarios acceder a los servidores de la empresa o comunicarse con ellos de forma segura por Internet.

Control de aplicaciones web

El control de aplicaciones web bloquea aplicaciones no deseadas que podrían ocasionar problemas para la seguridad, como los programas de intercambio de archivos o mensajería instantánea.

Concede el ancho de banda adecuado a las aplicaciones vitales para la empresa para mejorar su velocidad, y bloquea o limita el uso de aplicaciones no deseadas o poco productivas.

Cortafuegos de aplicaciones web

Los cortafuegos de aplicaciones web analizan las actividades y detectan ataques y sondeos para ayudar a proteger los servidores contra delincuentes.

Los cortafuegos de aplicaciones web podrían considerarse como dispositivos cortafuegos tradicionales que además realizan tareas propias de otros sistemas, como filtrar el contenido o el correo no deseado, y detectar intrusiones y virus. Los cortafuegos de aplicaciones web suelen utilizarse para proteger servidores web a los que se puede acceder desde Internet.

Consejos de seguridad

Cómo evitar virus, troyanos, gusanos y programas espía

Utilice programas antivirus o de seguridad para estaciones de trabajo

Instale programas antivirus o de seguridad para estaciones de trabajo en todos los ordenadores de sobremesa y servidores, y no olvide mantenerlos actualizados. Los programas maliciosos nuevos pueden propagarse muy rápido, por lo que es aconsejable disponer de una infraestructura que pueda actualizar todos los ordenadores de la empresa fácilmente, con frecuencia y sin demasiada antelación.

Para proteger la empresa contra virus, correo no deseado y programas maliciosos distribuidos por correo electrónico, instale un programa de filtrado del correo en la puerta de enlace.

Y no olvide proteger los ordenadores, tanto portátiles como de sobremesa, y los dispositivos móviles de los empleados que trabajan desde casa.

Descargue una evaluación gratuita de Sophos Enduser Protection en www.sophos.com/es-es/endpoint.

Bloquee los tipos de archivos que suelen portar programas maliciosos

Bloquee la recepción por correo electrónico y la descarga en Internet de tipos de archivos ejecutables. Es poco probable que su empresa necesite recibirlos del exterior.

Suscríbase a un servicio de alertas por correo electrónico

Plantéese la posibilidad de añadir un canal de información en directo sobre programas maliciosos al sitio web o a la red interna de la empresa para que los usuarios estén informados sobre las amenazas informáticas más recientes.

Utilice un cortafuegos en todos los ordenadores

Utilice un cortafuegos para proteger los equipos conectados a una red. Muchos gusanos pueden entrar incluso en redes cerradas a través de unidades USB, CD-ROM y dispositivos móviles. Los portátiles y los teletrabajadores también necesitan la protección de un cortafuegos.

Mantenga actualizados los parches del software

Es aconsejable utilizar funciones de actualización automática (de parches), sobre todo, en los ordenadores de Windows. Los parches suelen cerrar agujeros que pueden permitir la entrada de programas maliciosos.

Realice copias de seguridad de los datos con frecuencia

Guarde con frecuencia copias de seguridad del trabajo y los datos importantes, y compruebe que se han creado correctamente. También es aconsejable buscar un lugar seguro para almacenarlas, preferiblemente en una ubicación externa para protegerlas en caso de incendio. Si algún equipo se infecta con programas maliciosos, podrá restaurar todos los programas y datos perdidos. La información delicada almacenada en copias de seguridad debe cifrarse y protegerse físicamente.

Implemente una solución de control de dispositivos

Impida la conexión de dispositivos no autorizados a los ordenadores. Las unidades USB, los reproductores de música, los teléfonos móviles y otros dispositivos no autorizados pueden portar programas maliciosos que infectan los equipos al conectarlos.

Cómo evitar bulos

Establezca una política sobre avisos de virus

Configure una política sobre avisos de virus. Por ejemplo:

> "No reenvíe advertencias sobre virus de ningún tipo a otros usuarios, a excepción de la persona responsable de los asuntos relacionados con la protección antivirus, tanto si las advertencias proceden del proveedor antivirus como si las ha confirmado una empresa informática importante o cualquier otra persona de confianza. Todas las advertencias sobre virus deben enviarse exclusivamente a [nombre de la persona responsable]. Una de sus obligaciones es notificar a todo el personal sobre este tipo de asuntos. Las advertencias de virus procedentes de cualquier otra fuente deben ignorarse."

No reenvíe cartas en cadena

No reenvíe ninguna carta en cadena incluso aunque ofrezcan recompensas o afirmen contener información útil.

Cómo proteger los datos

Cifre los ordenadores, el correo electrónico y los dispositivos

Al cifrar los datos, podrá estar seguro de que solo los usuarios autorizados con las claves y contraseñas de cifrado necesarias acceden a la información. Gracias al cifrado, los datos estarán seguros en todo momento, incluso si están almacenados en un portátil, CD-ROM o cualquier otro dispositivo que se pierda o sea objeto de un robo, o si están incluidos en un mensaje de correo electrónico interceptado.

Utilice funciones de control de dispositivos y restricción de aplicaciones

Evite que los usuarios accedan a sitios de intercambio de archivos P2P y unidades USB, causas habituales de las fugas de datos.

Permita el acceso exclusivo a la red de los ordenadores que cumplan las políticas de seguridad, que pueden incluir requisitos de cifrado o tecnologías de control de dispositivos y restricción de aplicaciones.

Impida el acceso de los empleados a servicios de correo en la nube

Establezca controles para vigilar o bloquear el uso de servicios de almacenamiento en la nube como Dropbox por parte de los usuarios. Los controles deben incluir funciones de filtrado de direcciones web, restricción de aplicaciones y cifrado de datos. Si lo desea, puede prohibir el acceso y las transferencias de información confidencial a servicios de almacenamiento en la nube poco seguros.

Implemente controles del contenido saliente

Determine qué datos delicados desea controlar (por ejemplo, cualquier archivo que contenga el término "confidencial" o números de tarjetas de crédito) y decida cómo pueden utilizarse. Por ejemplo, puede configurar avisos que informen a los usuarios sobre posibles fugas de datos o impedir la distribución de los datos por correo electrónico, en blogs o en foros.

Con una solución de cifrado, los usuarios pueden elegir los servicios de almacenamiento en la nube que prefieran porque los archivos se cifran siempre y las claves son siempre propias. Y puesto que el cifrado se lleva a cabo en la estación de trabajo antes de sincronizar los datos, el control sobre la seguridad de los datos es total.

Cifrado de redes inalámbricas

Configure las redes inalámbricas de la empresa para que utilicen funciones potentes de cifrado como las que ofrece WPA2. Anime a los empleados a utilizar cifrado también en las redes inalámbricas de sus hogares.

Cómo evitar el correo no deseado

Utilice programas de filtrado del correo en la puerta de enlace del correo electrónico

Es aconsejable utilizar software de filtrado del correo electrónico en la puerta de enlace para proteger la empresa contra correo no deseado y programas espía, virus y gusanos distribuidos por correo electrónico.

No realice compras a partir de mensajes de correo no solicitados

Al realizar compras, puede estar financiando la distribución de más correo no deseado. Los creadores de *spam* pueden añadir su dirección de correo electrónico a listas que venden a terceros y recibirá aún más correo basura. O, lo que es peor, podría ser víctima de fraudes.

Si no conoce al remitente de un mensaje no solicitado, elimínelo

El correo no deseado puede contener programas maliciosos que dañan o ponen en peligro los equipos al abrir los mensajes.

No utilice el modo de "vista previa" del visualizador de correo electrónico

Muchos creadores de correo no deseado pueden hacer un seguimiento de los mensajes visualizados aunque no se haga clic en ellos.

La opción de vista previa abre el mensaje de correo electrónico e informa a los creadores de *spam* sobre su entrega. Al abrir el correo electrónico, intente decidir qué mensajes son correo no deseado basándose exclusivamente en el asunto.

No exponga en exceso su dirección de correo electrónico

El grado de exposición en Internet de las direcciones de correo electrónico es el factor más decisivo en la cantidad de correo no deseado que reciben. Estas son algunas de las malas costumbres que revelan las direcciones de correo electrónico a los creadores de *spam*:

- Publicarlas en listas de correo archivadas en Internet
- Enviarlas a servicios en línea con políticas de privacidad dudosas
- Revelarlas de forma pública en redes sociales (Facebook, LinkedIn, etc.)
- Utilizar direcciones fáciles de averiguar formadas por el nombre, los apellidos y la empresa
- No separar el correo electrónico de trabajo y personal

Utilice el campo CCO al enviar un mensaje de correo electrónico a varias personas a la vez

El campo CCO (o copia carbón oculta) impide que los destinatarios vean quién más ha recibido el mensaje. Al incluir todas las direcciones en el campo Para, los creadores de correo no deseado pueden recolectarlas e incluirlas en listas de distribución.

Utilice una o dos direcciones de correo electrónico secundarias

Si rellena formularios de registro o encuestas en sitios de los que no quiere recibir más información, utilice una dirección de correo electrónico secundaria para no recibir correo no deseado en la dirección principal.

Desactive la opción para recibir más ofertas o información

Al rellenar formularios en sitios web, busque la opción que permite especificar si acepta recibir más ofertas o información. Active o desactive las casillas según corresponda.

Cómo evitar ataques de suplantación de identidad

No responda a mensajes de correo electrónico que soliciten información financiera personal

Sospeche de cualquier mensaje que solicite contraseñas o información de cuentas, o que incluya enlaces para proporcionar dichos datos. Ni los bancos ni las empresas de comercio electrónico suelen enviar mensajes así.

Preste atención a los mensajes sospechosos

Los mensajes de correo electrónico que intentan suplantar identidades suelen utilizar saludos generales como "Estimado cliente". También pueden incluir afirmaciones preocupantes (por ejemplo, acerca de números de cuentas robados), estar mal escritos y pedirle que realice acciones como hacer clic en un enlace o enviar información personal a una dirección desconocida.

Pero también pueden ser más específicos y muy creíbles. Preste atención a los comportamientos poco habituales, adjuntos vacíos o irrelevantes (que pueden ocultar programas maliciosos) o solicitudes de visitas a enlaces que no se corresponden con el asunto del mensaje o el remitente.

Escriba la dirección de los sitios web de banca electrónica en la barra de direcciones para visitarlos

No haga clic en enlaces incluidos en mensajes de correo electrónico no solicitados. Los ladrones de identidades los utilizan para llevar a los usuarios a sitios falsos. En su lugar, es aconsejable escribir la dirección completa en la barra de direcciones del navegador.

Vigile con frecuencia las cuentas

Inicie sesión con frecuencia en las cuentas en línea y revise los extractos. Si detecta transacciones sospechosas, informe al banco o al proveedor de la tarjeta de crédito.

Asegúrese de que los sitios web que visita son seguros

Revise la dirección web de la barra de direcciones. Si el sitio web se encuentra en un servidor seguro, la dirección debe empezar por https:// (la "s" significa seguro) en lugar del componente http:// habitual. Compruebe que la barra de estado del navegador muestra un pequeño icono con un candado. Estos símbolos indican que el sitio web utiliza tecnologías de cifrado.

Sin embargo, es imposible garantizar que ningún sitio sea totalmente seguro, ya que los ciberdelincuentes pueden crear sitios web con cifrado para robar información personal.

Tenga cuidado con los mensajes de correo electrónico y los datos personales

Realice todas las transacciones de forma segura. No comparta los códigos PIN ni las contraseñas con nadie, no los anote y no utilice la misma contraseña en todas las cuentas de Internet. No abra ni responda a mensajes de correo no deseado para que los remitentes no sepan que la dirección es válida y la sigan utilizando en otros timos.

Mantenga protegidos los ordenadores

Los programas anti-*spam* ayudan a recibir menos mensajes de correo electrónico de suplantación de identidades. Los cortafuegos también ayudan a proteger la información personal y a bloquear comunicaciones no autorizadas. Es aconsejable utilizar siempre software antivirus para detectar y desactivar programas maliciosos como programas espía y troyanos de puerta trasera incluidos en mensajes de suplantación de identidades. Mantenga el navegador de Internet actualizado con los parches de seguridad más recientes.

Notifique siempre cualquier actividad sospechosa

Si recibe un mensaje de correo electrónico que no sea auténtico, reenvíelo a la empresa falsificada. Muchas compañías cuentan con direcciones de correo electrónico especiales para notificaciones de este tipo.

Cómo protegerse en Internet

Esta sección ofrece consejos generales sobre cómo utilizar de forma segura Internet y el correo electrónico. Consulte también nuestros consejos sobre **Cómo evitar ataques de suplantación de identidad** y **Cómo evitar virus, troyanos, gusanos y programas espía**.

Instale todos los parches de seguridad

Los ciberdelincuentes aprovechan a menudo las vulnerabilidades de los sistemas operativos y programas para intentar infectar ordenadores. Esté al tanto de los parches de seguridad del sistema operativo, el navegador, los complementos y cualquier otra parte del código del ordenador que pueda servir de objetivo a los *hackers*. Si puede, configure el equipo para que descargue los parches de seguridad de forma automática.

Utilice cortafuegos

Los cortafuegos de red se instalan en los límites de la empresa y permiten el paso exclusivo de los tipos de tráfico autorizados. Los cortafuegos cliente se instalan en los ordenadores de la red para permitir solamente el tráfico autorizado, y bloquear ataques informáticos y gusanos de Internet. Además, evitan que los ordenadores se comuniquen con Internet a través de programas no autorizados.

No haga clic en enlaces incluidos en mensajes no solicitados

Los enlaces incluidos en mensajes de correo electrónico no solicitados pueden llevar a sitios web falsos que roban toda la información introducida (por ejemplo, números de cuentas y contraseñas) para utilizarla con fines ilegales.

Además, muy a menudo, los ciberdelincuentes envían enlaces en mensajes de correo no deseado para llevar a los usuarios a páginas web maliciosas.

Utilice contraseñas distintas en todos los sitios

Es aconsejable utilizar contraseñas distintas en todos los sitios en los que disponga de cuentas de usuario. De esta forma, si alguna contraseña corre peligro, solo se verá afectada una cuenta. Además, asegúrese de elegir contraseñas difíciles de averiguar y no utilice palabras que aparezcan en el diccionario.

Plantéese la posibilidad de bloquear el acceso a determinados sitios web o tipos de contenido

En los entornos empresariales, puede resultar útil impedir que los usuarios accedan a sitios inadecuados que puedan suponer una amenaza para la seguridad (por ejemplo, mediante la instalación de protección contra programas espía en los equipos). Para ello, puede utilizar programas de filtrado web o dispositivos de hardware. Incluso si los usuarios tienen permiso para visitar sitios web, es aconsejable escanear todas las páginas que visitan para detectar amenazas para la seguridad.

Escanee el correo electrónico para detectar programas maliciosos y correo no deseado

Los programas anti-*spam* pueden detectar mensajes no deseados (además de programas maliciosos ocultos) e impedir que lleguen a los buzones de los usuarios.

No haga clic en mensajes emergentes

Si aparecen ventanas emergentes, por ejemplo, con advertencias sobre infecciones en el ordenador y ofertas de herramientas de eliminación de virus, no haga clic en los enlaces ni acepte descargas. De lo contrario, podría descargar código malicioso como programas antivirus falsos.

Utilice routers

Los routers pueden servir para limitar las conexiones entre Internet y determinados ordenadores. Además, muchos de ellos incluyen cortafuegos de red.

Cómo elegir contraseñas seguras

Las contraseñas protegen contra fraudes y fugas de información confidencial, pero poca gente elige contraseñas realmente seguras.

Elija contraseñas lo más largas posible

Cuanto más larga es una contraseña, más difícil es que los delincuentes la averigüen o la encuentren probando todas las combinaciones posibles (por ejemplo, con ataques por fuerza bruta). Las contraseñas de 14 o más caracteres son mucho más difíciles de averiguar.

Utilice diferentes tipos de caracteres

Incluya números, signos de puntuación, símbolos y letras mayúsculas y minúsculas. En los dispositivos móviles que no estén diseñados para introducir caracteres especiales fácilmente, intente utilizar contraseñas más largas con caracteres distintos.

No utilice palabras que aparezcan en el diccionario

No utilice palabras ni nombres propios que puedan encontrarse en diccionarios. Los ciberdelincuentes pueden probar de forma automática todas las palabras del diccionario para averiguar contraseñas.

No utilice información personal

Es probable que otras personas conozcan la fecha de su cumpleaños, el nombre de su cónyuge o sus hijos, o su número de teléfono, y pueden sospechar que haya utilizado cualquiera de esos datos como contraseña.

No utilice su nombre de usuario

No utilice como contraseña el nombre de usuario o el número de la cuenta.

Utilice contraseñas difíciles de identificar mientras las escribe

No utilice caracteres repetidos ni teclas cercanas entre sí en el teclado.

Plantéese la posibilidad de utilizar una frase como contraseña

Utilice una cadena de palabras en lugar de una sola palabra. Las combinaciones poco probables de palabras pueden ser difíciles de averiguar.

Intente memorizar las contraseñas

Memorice las contraseñas en lugar de anotarlas. Utilice una cadena de caracteres que signifiquen algo para usted o utilice técnicas de memorización que le ayuden a recordar la contraseña. Existen programas gratuitos muy buenos para gestionar las contraseñas.

Los programas de gestión de contraseñas de calidad pueden ayudar a elegir contraseñas únicas, cifrarlas y almacenarlas de forma segura en el ordenador, por ejemplo, KeePass, RoboForm y 1Password.

Use contraseñas distintas para cada cuenta

Si un ciberdelincuente averigua alguna de sus contraseñas, al menos solo podrá poner en peligro una cuenta.

No revele las contraseñas a nadie

Si recibe una solicitud para que confirme una contraseña, aunque parezca que procede de un organismo de confianza o alguien de su empresa, nunca es aconsejable revelar las contraseñas (consulte **Mensajes de suplantación de identidad**).

No utilice contraseñas en ordenadores públicos

No introduzca contraseñas en ordenadores de uso público (por ejemplo, en hoteles o cibercafés) que pueden no estar protegidos correctamente o tener registradores de pulsaciones instalados.

Cambie las contraseñas con regularidad

Cuanto más cortas y sencillas sean las contraseñas utilizadas, más a menudo deben actualizarse.

Cómo utilizar medios extraíbles de forma segura

Forme a los usuarios

Muchos usuarios no son conscientes de los posibles peligros de utilizar medios extraíbles como memorias USB o CD/DVD, que pueden propagar programas maliciosos y provocar fugas de datos. La formación de los usuarios ayuda a reducir los riesgos de forma considerable.

Identifique los tipos de dispositivos

Los ordenadores interactúan con una variedad cada vez mayor de medios extraíbles como, por ejemplo, unidades USB, reproductores de MP3 y teléfonos inteligentes. Al poder ver los medios extraíbles que intentan conectarse a la red, resulta más fácil configurar las restricciones y los permisos adecuados.

Implemente una solución de control de dispositivos

El control de los tipos de medios extraíbles permitidos y los datos que se pueden intercambiar es un componente fundamental de cualquier estrategia de seguridad. Elija soluciones que puedan establecer permisos (o restricciones) tanto para dispositivos individuales como clases enteras.

Cifre los datos

El cifrado de datos evita que se produzcan fugas, algo especialmente útil cuando se utilizan medios extraíbles que se extravían fácilmente, ya que impide que terceros sin autorización visualicen o copien los datos que almacenan.

Cómo realizar compras por Internet de forma segura

¿Podemos fiarnos del sentido común y la intuición?

Por desgracia, resulta poco práctico que los usuarios decidan si un sitio web es seguro o no a simple vista.

Aunque los clientes no se den cuenta, los ciberdelincuentes suelen atacar sitios web legítimos mal protegidos. El hecho de que una empresa sea grande y conocida no garantiza que su sitio web sea seguro.

Al realizar cualquier compra desde ordenadores o dispositivos protegidos con los programas antivirus más recientes, cortafuegos y parches de seguridad, se reducen de forma considerable las posibilidades de ser víctima de un fraude.

No haga clic en ningún enlace proporcionado por Internet sin solicitarlo, por ejemplo, incluido en mensajes de correo electrónico, redes sociales o instantáneos. Los creadores de correo no deseado y los ciberdelincuentes utilizan técnicas de ingeniería social como cebos para llevar a los usuarios a sitios web infectados o fraudulentos.

No revele información delicada como sus datos personales o financieros a menos que esté totalmente seguro de la legitimidad de la empresa.

Familiarícese con las condiciones de uso y la política de protección de datos

Lea la letra pequeña. Las condiciones pueden esconder obligaciones o costes inesperados.

Realice compras solamente en sitios web que utilicen cifrado

Las direcciones web que empiezan por https:// en lugar de http:// (la "s" significa seguro) cifran la información durante las transferencias.
Los iconos con candados que aparecen en los navegadores de Internet son otro indicativo de que el sitio web utiliza técnicas de cifrado.

Sin embargo, es imposible garantizar que estos sitios sean seguros, ya que los ciberdelincuentes pueden crear sitios web con cifrado para robar información personal.

Proporcione la menor cantidad de información personal posible

Deje en blanco campos optativos como la fecha de nacimiento, el número de teléfono móvil, las aficiones, etc. Muchos operadores de sitios web solicitan información optativa además de la información obligatoria para procesar transacciones. Los campos obligatorios suelen estar señalados con un asterisco.

No revele nunca su contraseña

Aunque otra persona vaya a realizar una compra en su nombre, es aconsejable que introduzca la contraseña personalmente y no la comparta con nadie.

Para impedir que usuarios posteriores accedan a su cuenta sin permiso, no seleccione nunca la opción "recordar contraseña" en ordenadores compartidos.

Utilice proveedores locales siempre que sea posible

Cuando los vendedores están ubicados en otros países, puede resultar mucho más difícil y caro solucionar cualquier problema e imponer las leyes de derechos del consumidor.

Revise los extractos bancarios

Revise con frecuencia las transacciones de las cuentas bancarias, sobre todo, después de realizar compras por Internet para asegurarse de que todos los pagos son legítimos. Si descubre algún pago que no reconoce, informe inmediatamente a su banco.

Conserve las confirmaciones de los pedidos y los recibos

Conserve siempre la información importante relacionada con cualquier compra, bien de forma impresa o electrónica. Dicha información puede resultar muy útil si necesita resolver cualquier problema más adelante.

Cómo protegerse durante desplazamientos

Forme a los usuarios

No subestime los riesgos de fugas de datos que generan los portátiles y los medios extraíbles mal protegidos. Las empresas deben crear políticas claras sobre el uso de dispositivos móviles.

Utilice contraseñas seguras

Las contraseñas son la primera línea de defensa y deben ser siempre lo más seguras posible. Consulte **Cómo elegir contraseñas seguras**.

Ponga en práctica comprobaciones adicionales de la seguridad

Las tarjetas inteligentes y los tokens exigen introducir información adicional (por ejemplo, un código y una contraseña) para acceder al ordenador. Con los lectores de huellas digitales, los usuarios deben confirmar su identidad mediante una huella digital para arrancar el sistema o iniciar sesión.

Cifre todos los datos importantes

Si los datos están cifrados, seguirán estando seguros aunque el portátil o el medio extraíble se pierda o sea objeto de un robo. Si no quiere cifrar el disco duro al completo, puede crear un disco virtual para almacenar la información confidencial de forma segura.

Restrinja el uso de la función *Plug and Play*

La función *Plug and Play* permite que las unidades USB, los reproductores de MP3 y los discos duros externos se conecten a los portátiles de forma automática para facilitar las copias de datos. En lugar de esta función, bloquee el ordenador para que solo se puedan conectar los dispositivos autorizados.

Conexiones remotas seguras

Las redes inalámbricas de aeropuertos, cafeterías, hoteles y otros lugares públicos ofrecen grandes oportunidades para el espionaje. Configure una red privada virtual en todos los portátiles y dispositivos móviles para proteger las comunicaciones con los servidores de la empresa. Ciertas aplicaciones y sitios web pueden protegerse también mediante la utilización de SSL para cifrar las comunicaciones.

Cómo proteger al personal que se desplaza

Los teléfonos inteligentes son herramientas de trabajo estándar que almacenan información empresarial delicada y permiten acceder al correo electrónico durante desplazamientos. Por eso, son vulnerables a los ataques de los creadores de programas maliciosos que buscan nuevos métodos para engañar a los usuarios y robar datos confidenciales.

Aunque los virus y los programas espía para dispositivos móviles siguen siendo un problema relativamente pequeño en comparación con la cantidad mucho mayor de programas maliciosos dirigidos a ordenadores Windows, los riesgos para la reputación, las comunicaciones y la continuidad de las empresas están ganando mayor seriedad. Entre dichos riesgos se incluyen los robos de datos, la interrupción de las redes de telefonía móvil y el secuestro de teléfonos para enviar mensajes SMS no autorizados que generen beneficios.

Los dispositivos móviles pueden infectarse de muchas formas, por ejemplo, a través de mensajes de correo electrónico y multimedia, tarjetas de memoria externa, sincronizaciones con ordenadores e incluso Bluetooth.

Asegúrese de que la política de seguridad incluye medidas para proteger los dispositivos móviles como, por ejemplo:

- Gestión de amenazas: identificación y eliminación de virus, programas espía y correo no deseado.
- Control y gestión del acceso de dispositivos mediante la imposición de políticas de contraseñas y gestión de las aplicaciones.
- Protección de datos: cifrado de datos confidenciales en dispositivos y eliminación remota de datos.
- Control del acceso a la red: control de las conexiones VPN en redes públicas y validación de los dispositivos que se conectan a la red corporativa.

Descargue una evaluación gratuita de Sophos Mobile Control en www.sophos.com/es-es/mobilecontrol.

Cronología de los programas maliciosos

¿Cuándo empezaron a representar una amenaza los virus, los troyanos y los gusanos?

El virus Brain, escrito en 1986, suele considerarse el primer virus de la historia, a pesar de ser solamente el primer virus para ordenadores de Microsoft. Los programas con todas las características de los virus datan de mucho antes. La cronología siguiente destaca los momentos clave de la historia de los virus.

1949: "Autómatas celulares" autorreplicables

John von Neumann, el padre de la cibernética, publicó un artículo en el que sugería que un programa informático podía autorreproducirse.

1959: Core Wars

H. Douglas McIlroy, Victor Vysottsky y Robert P. Morris, de la empresa Bell Labs, crearon un programa informático denominado Core Wars en el que los programas (u "organismos") competían para conseguir tiempo de procesamiento en el equipo.

1960: Programas "conejo"

Los programadores empezaron a escribir marcadores de posición para ordenadores de grandes sistemas. Cuando no había tareas en espera, estos programas añadían una copia de sí mismos al final de la cola. Se les dio el sobrenombre de programas "conejo" porque se multiplicaban utilizando los recursos del sistema.

1971: El primer gusano

Bob Thomas, un desarrollador que trabajaba en ARPANET, la red precursora de Internet, escribió un programa denominado Creeper (literalmente, "trepador") que pasaba de ordenador a ordenador mostrando un mensaje.

1975: Código autoduplicable

A. K. Dewdney escribió Pervade como subrutina para un juego que se instalaba en ordenadores que utilizaban el sistema UNIVAC 1100. Al jugar, el procedimiento copiaba en silencio la versión más reciente de sí mismo en todos los directorios accesibles, incluidos los directorios compartidos, para después propagarse por la red.

1978: El gusano Vampiro

John Shoch y Jon Hupp, de Xerox PARC, empezaron a experimentar con gusanos diseñados para realizar tareas útiles. El gusano Vampiro estaba parado durante el día pero, por la noche, asignaba tareas a los ordenadores infrautilizados.

1981: Virus de Apple

Joe Dellinger, un alumno de la Universidad A&M de Texas (EE. UU.), modificó el sistema operativo de disquetes de Apple II para que actuase como un virus.

El virus no llegó a publicarse por tener efectos secundarios imprevistos, pero dio lugar a versiones posteriores cuya propagación sí se permitió.

1982: Virus de Apple con efectos secundarios

Rich Skrenta, de 15 años, escribió Elk Cloner para el sistema operativo Apple II. Elk Cloner se ejecutaba al iniciar un equipo con un disquete infectado, infectaba cualquier otro disquete que se introducía en la unidad y mostraba un mensaje cada vez que el ordenador se arrancaba por quincuagésima vez.

1985: Troyano de correo

El troyano EGABTR se distribuía a través de buzones de correo y se hacía pasar por un programa diseñado para mejorar la visualización de imágenes. Sin embargo, una vez ejecutado, eliminaba todos los archivos del disco duro y mostraba un mensaje.

1986: El primer virus para ordenadores personales

Supuestamente, el primer virus para ordenadores personales IBM, Brain ("cerebro"), lo escribieron dos hermanos en Pakistán al descubrir que la gente copiaba su software. El virus colocaba una copia de sí mismo y un mensaje sobre los derechos de autor en cualquier disquete en el que los usuarios guardaban una copia.

1987: El gusano del árbol de Navidad

Se trataba de una tarjeta navideña por correo electrónico que incluía código de programación. Al ejecutarse, dibujaba un árbol de Navidad según lo prometido pero, además, se reenviaba a todos los contactos de la agenda de direcciones del usuario. El tráfico paralizó la red internacional de IBM.

1988: El gusano de Internet

Robert Morris, un estudiante de 23 años, publicó un gusano en la red DARPA de los EE. UU. El gusano se propagó a miles de ordenadores y, a causa de un error, volvía a infectarlos muchas veces haciendo que se bloqueasen.

1989: El troyano que pide un rescate

El troyano AIDS (SIDA, en inglés) se alojaba en un disquete que ofrecía información sobre el SIDA y el virus VIH. El troyano cifraba el disco duro del equipo y solicitaba un pago a cambio de la contraseña.

1991: Primer virus polimórfico

Tequila fue el primer virus polimórfico de difusión generalizada. Los virus polimórficos cambian de aspecto en cada infección para dificultar su detección.

1992: Michelangelo siembra el pánico

El virus Michelangelo se diseñó para borrar discos duros de ordenadores el 6 de marzo de cada año (fecha del cumpleaños de Michelangelo). Dos empresas distribuyeron por error discos y ordenadores infectados, lo que sembró el pánico en todo el mundo, pero pocos equipos llegaron a infectarse.

1994: Primer bulo por correo electrónico

El primer bulo por correo electrónico advertía a los usuarios acerca de un virus malicioso que podía borrar el disco duro al completo con solo abrir un mensaje de correo electrónico titulado "Good Times" (literalmente, "buenos tiempos").

1995: Primer virus de documentos

Aparece el primer virus de documento o "macro", Concept, que se propagaba a través de las macros de Microsoft Word.

1998: Primer virus para hardware

CIH o Chernobyl se convirtió en el primer virus capaz de paralizar hardware. El virus atacaba la BIOS, necesaria para arrancar el ordenador.

1999: Virus por correo electrónico

Melissa, un virus que se reenviaba por correo electrónico, se extendió por todo el mundo.

También apareció Bubbleboy, el primer virus en infectar ordenadores al visualizar un mensaje de correo electrónico.

2000: Ataques de denegación de servicio

Los ataques de denegación de servicio lanzados por los ciberdelincuentes dejaron Yahoo!, eBay, Amazon y otros sitios muy conocidos sin conexión durante varias horas.

Love Bug se convirtió en el virus por correo electrónico de mayor éxito hasta la fecha.

2000: Virus para Palm

Apareció el primer virus para el sistema operativo Palm, aunque no infectó ningún dispositivo.

2001: Virus propagados a través de sitios web o recursos compartidos de red

Los programas maliciosos empezaron a aprovechar vulnerabilidades de software para propagarse sin la intervención de los usuarios. Nimda infectaba equipos con solo visitar un sitio web. Sircam utilizaba su propio programa de correo electrónico para propagarse, aunque también se propagaba a través de recursos compartidos de red.

2003: Zombis y suplantación de identidades

El gusano Sobig cedía el control de los ordenadores personales a los ciberdelincuentes para convertirlos en zombis y utilizarlos para enviar correo no deseado.

El gusano Mimail se hacía pasar por un mensaje de correo electrónico de Paypal en el que se pedía a los usuarios que confirmasen los datos de sus tarjetas de crédito.

2004: *Bots* para IRC

Se crearon los primeros *bots* maliciosos para IRC (Internet Relay Chat). Los troyanos podían colocar el *bot* en un ordenador, desde el que se conectaba a un canal de IRC sin el conocimiento del usuario para ceder el control del equipo a los ciberdelincuentes.

2005: *Rootkits*

El sistema de protección contra copias DRM de Sony, incluido en discos CD de música, instalaba un *rootkit* en los ordenadores de los usuarios que ocultaba los archivos para no poder duplicarlos. Los ciberdelincuentes crearon troyanos que aprovechaban este punto débil de la seguridad e instalaban puertas traseras ocultas.

2006: Timos sobre precios de acciones

Se hizo habitual el correo no deseado que promocionaba de forma exagerada las acciones de compañías pequeñas.

2006: *Ransomware*

Los troyanos Zippo y Archiveus, que cifraban los archivos de los usuarios y pedían un rescate a cambio de la contraseña, fueron los primeros ejemplos de *ransomware*.

2006: Primera amenaza avanzada recurrente detectada

Acuñadas por primera vez por el Ejército del Aire de los Estados Unidos en 2006 y definidas funcionalmente por la empresa de seguridad Mandiant (Virginia, EE. UU.) en 2008 como un grupo de ataques sofisticados, rotundos y coordinados. Este tipo de amenazas están equipadas con las funciones y el propósito de atacar de forma recurrente y eficaz entidades específicas. Entre los vectores de ataque identificados se incluyen medios infectados, manipulaciones de la cadena de suministro e ingeniería social.

2008: Programas antivirus falsos

Las tácticas alarmistas incitan a los usuarios a revelar información de tarjetas de crédito para adquirir antivirus falsos como AntiVirus 2008.

2008: Primer programa malicioso para iPhone

El Equipo de Respuesta Informática Urgente de los EE. UU. (US-CERT) publicó una advertencia sobre una actualización falsa para dispositivos iPhone, "iPhone firmware 1.1.3 prep", que se estaba difundiendo por Internet, para que los usuarios no cayeran en la trampa de instalarla. Al instalar el troyano, se modificaban otros componentes de las aplicaciones. Al desinstalarlo, también podían desinstalarse las aplicaciones afectadas.

2009: Conficker inunda los titulares

Conficker, un gusano que en un principio se propagaba por equipos en los que faltaban parches, revoluciona los medios de comunicación en todo el mundo.

2009: Los virus polimórficos vuelven a aumentar

Los virus complejos vuelven con más fuerza, incluido Scribble, un virus que cambia de aspecto en cada infección y utiliza múltiples vectores de ataque.

2009: Primer programa malicioso para Android

Android FakePlayerAndroid/FakePlayer.A es un troyano que envía mensajes SMS a números de teléfono de tarifas especiales. El troyano se introduce en los teléfonos inteligentes Android disfrazado de aplicación normal. Los usuarios reciben un aviso para instalar un archivo pequeño de alrededor de 13 KB con la extensión .APK habitual de Android. Sin embargo, una vez instalada la aplicación en el dispositivo, el troyano que contiene empieza a enviar mensajes de texto a números de teléfono de tarifas especiales (que cobran por recibir mensajes). Los delincuentes están al mando de dichos números, por lo que se benefician de los cargos realizados a las cuentas de las víctimas.

2010: Stuxnet

Descubierto en junio de 2010, el gusano Stuxnet se propagaba en un principio de forma indiscriminada, pero más tarde se descubrió que contenía un programa malicioso muy especializado dirigido solamente a los sistemas de adquisición de datos y vigilancia (SCADA) de Siemens, configurados para controlar determinados procesos industriales. Se cree que el principal objetivo de Stuxnet era una infraestructura de enriquecimiento de uranio iraní.

2012: Primer programa malicioso automático para Android

Se descubre el primer programa malicioso automático para Android, un troyano denominado NotCompatible, que se hace pasar por una actualización del sistema pero sirve para redirigir el servidor proxy. El sitio revisa la cadena usuario-agente del navegador de la víctima para comprobar que se trata de un dispositivo de Android y, a continuación, instala el troyano de forma automática. Los dispositivos infectados con NotCompatible pueden utilizarse para acceder a sistemas e información normalmente protegida como, por ejemplo, de empresas o instituciones gubernamentales.

2013: El retorno del *ransomware*

El *ransomware* reaparece como una de las principales amenazas de programas maliciosos. Algunas variedades utilizan técnicas avanzadas de cifrado que hacen que la recuperación de los archivos bloqueados resulte prácticamente imposible y sustituyen a los antivirus falsos como la amenaza favorita de los ciberdelincuentes para solicitar dinero.

Oxford (Reino Unido) | Boston (EE. UU.) | www.sophos.com/es-es/

SOPHOS

1090-10DD.es.simple