Glosario

Ancho de Banda. Es la cantidad de información o de datos que se pueden enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobits por segundo (kbps), o megabits por segundo (mps). A menudo se utiliza como sinónimo para la tasa de transferencia de datos - la cantidad de datos que se puedan llevar de un punto a otro en un período dado (generalmente un segundo).

Antispam. Aplicación o herramienta informática que se encarga de detectar y eliminar los correos no deseados. El principal objetivo de una herramienta antispam es lograr un buen porcentaje de filtrado de correo no deseado. Pero tampoco deben identificar al correo deseado como no deseado, pues eso traería peores consecuencias que "olvidar" filtrar algún spam.

Antivirus. Herramienta de seguridad encargada principalmente de detectar virus tanto en mensajes de correo electrónico como en internet en general, mediante un escaneo de archivos tiene como objetivo la detección, identificación y eliminación de malware. El software antivirus está formado por tres partes principales: Interfaz de usuario, motor de búsqueda y una base de datos de definición de virus.

Apache. Es un servidor web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP y la noción de sitio virtual.

Appliance. Suele ser un componente de hardware independiente y diseñado específicamente para proporcionar un recurso de cómputo específico, y que a menudo reside en una plataforma de hardware dedicado.

Arpanet. La red de computadoras ARPANET (Advanced Research ProjectsAgency Network) fue creada por encargo del Departamento de Defensa de los Estados Unidos ("DoD" por sus siglas en inglés) como medio de comunicación para los diferentes organismos del país. El primer nodo se creó en la Universidad de California, Los Ángeles y fue la espina dorsal de Internet hasta 1990, tras finalizar la transición al protocolo TCP/IP iniciada en 1983.

Black Hat. También conocidos como "crackers" muestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos hacking.

Código Malicioso. Es un término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tienen un fin malicioso. Esta definición incluye tanto programas malignos compilados, como macros y códigos que se ejecutan directamente, como los que suelen emplearse en las páginas web.

Pueden tener múltiples objetivos como:

- Extenderse a otra computadora en una red o por internet.
  Robar información y claves.
  Eliminar archivos e incluso formatear el disco duro.
- Mostrar publicidad invasiva.

Correo Electrónico. Es un servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet.

Daemon. Tipo especial de proceso que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario (es un proceso no interactivo). Este tipo de programas se ejecutan de forma continua (infinita), es decir, que aunque se intente cerrar o matar el proceso, este continuará en ejecución o se reiniciará automáticamente. Todo esto sin intervención de terceros y sin dependencia de consola alguna.

DNS. Significa Domain Name System que en español se puede nombrar como Sistema de Nombres de Dominio. Su función es proveer el mecanismo para el nombramiento de recursos y una manera en que los nombres son usables en diferentes equipos, redes, familias de protocolos, redes internas y organizaciones administrativas.

Filtrado Bayesiano. Se basa en el principio de que la mayoría de los sucesos están condicionados y que la probabilidad de que ocurra un suceso en el futuro puede ser deducido de las apariciones previas de ese suceso. Esta misma técnica se puede utilizar para clasificar spam. Si algún patrón de texto se encuentra a menudo en el spam pero no en el correo legítimo, entonces sería razonable asumir que este correo es probablemente spam. Es una técnica adaptativa basada en algoritmos de inteligencia artificial, los cuales están diseñados para soportar la gama más amplia de técnicas de envío de correo no deseado disponibles hoy en día

Gartner. Es un proyecto de investigación de tecnología de la información y de firma consultiva con sede en Stamford, Connecticut, Estados Unidos. Se conocían como el Grupo Gartner hasta 2001. Incluye como clientes algunas empresas grandes y agencias de gobierno así como empresas de tecnología y la comunidad de la inversión como BT, CV, Wall Street journal etc. La empresa consiste en la Investigación, Programas Ejecutivos, Consultas y eventos. Fue fundado en 1979,

Gartner tiene 4,000 socios, incluyendo a 1,200 analistas de investigación y consultores en 75 países por todo el mundo.

Hacker. Persona con conocimientos avanzados sobre redes de computadoras, sistemas operativos, técnicas de seguridad informática. Tiene la capacidad de vulnerar y explotar sistemas no con el fin de dañar, sino para encontrar sus fallas y poderlas corregir para hacer más seguros los sistemas de cómputo.

Lista Blanca. Es una lista de direcciones y dominios de correo de los cuales siempre desea recibir correo, es decir, el correo enviado desde estas direcciones o dominios nunca será marcado como spam. Además puede configurar palabras, que si se encuentran en el cuerpo o asunto, aprobará automáticamente el correo.

Lista Gris. Es una lista que se encarga del proceso por medio del cual el servidor de correo (a nivel del protocolo SMTP) rechaza el mensaje enviado y pide que éste sea reenviado. Esta técnica trata de aprovechar la existencia de "errores temporales" en el estándar SMTP. Un MTA que funcione conforme a dicho estándar reintentará el envío.

Lista Negra. Es una lista donde se registran las direcciones IPs que generan spam de forma voluntaria o involuntaria. Las blacklist son libres de tal forma que alguien de manera malintencionada puede añadir IPs inocentes e impedir que lleguen correos válidos.

Mensajería Instantánea. Es un punto intermedio entre los sistemas de chat y los mensajes de correo electrónico, las herramientas de mensajería instantánea, son programas regularmente gratuitos y versátiles, residen en el escritorio y, mientras hay una conexión a Internet, siempre están activos. El servicio de mensajería instantánea ofrece una ventana donde se escribe el mensaje, en texto plano o acompañado de iconos o "emoticons" (figuras que representan estados de ánimo), y se envían a uno o varios destinatarios quienes reciben los mensajes en tiempo real, el receptor lo lee y puede contestar en el acto.

MMS. Es un estándar de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video, fotos o cualquier otro contenido disponible en el futuro. La mensajería multimedia nos permite el envío de estos contenidos a cuentas de correo electrónico, ampliando las posibilidades de la comunicación móvil.

Perl. Es un lenguaje de programación interpretado y diseñado por Larry Wall en 1987. Toma características del lenguaje C, del lenguaje interpretado Shell, AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

Phishing. Del inglés "fishing" (pescando). Este término se utiliza para identificar la acción fraudulenta de conseguir información confidencial, vía correo electrónico o página web, con el propósito de que los usuarios de cuentas bancarias lo contesten, o entren a páginas aparentemente iguales a la del banco o de los portales con ingreso por contraseña.

Profeco. La Procuraduría Federal del Consumidor o la Oficina del Fiscal Federal para el Consumidor (PROFECO) es una organización del gobierno de México, a

cargo del Fiscal General, para proteger a los consumidores contra los abusos o fraudes por parte de las empresas que operan en México.

Programas Robot. Programas automáticos que recorren internet en busca de direcciones de correo electrónico como posibles víctimas de envío de spam.

Red de Computadoras. Es un conjunto de computadoras interconectadas entre sí mediante algún medio de transmisión con la finalidad de compartir información.

Scam. Es utilizado para referirse a correos relacionados con publicidad engañosa (enriquecimiento al instante, pornografía, premios, etc.) y cadenas (correos que incluyen textos en donde solicitan ser reenviados a otras personas con la promesa de cumplir deseos, traer buena suerte o ganar dinero)

SMS. Son las siglas de Servicio de Mensaje Corto. Disponible en redes digitales GSM permitiendo enviar y recibir mensajes de texto de hasta 160 caracteres a teléfonos móviles vía el centro de mensajes de un operador de red.

Spam. Correo comercial no solicitado generalmente enviado a las direcciones electrónicas de los consumidores sin la autorización y consentimiento del consumidor, comúnmente es enviado por empresas de mercadeo o telemercadeo, compañías legítimas o por individuos comisionados exclusivamente para dicho fin.

Spamassassin. Es un programa distribuido bajo la licencia Apache 2.0, se usa principalmente para el filtrado de correo electrónico en busca de mensajes con spam mediante el uso de reglas. Está escrito en perl.

Spammer. Son personas o empresas que envían mensajes Spam y lo realizan con diferentes técnicas para conseguir listas muy grandes de correos que son necesarias para realizar su actividad. La mayoría de los Spammers trabajan a través de programas automáticos, los cuales recorren la red buscando en sitios, foros, blogs, bases de datos, grupos de noticias entre otros. Cuando adquieren la información de los correos electrónicos se encargan de enviar los mensajes a los destinatarios, esto se utiliza, la mayoría de las veces con fines comerciales, pero también puede ser con la intención de causar un daño con algún virus o incurrir en fraudes a través del Phising.

Spim. Tipo de spam pero que en vez de atacar a través de los correos electrónicos, lo hace a través de la mensajería instantánea

Spit. Es una forma de hacer llegar publicidad a los usuarios de telefonía por Internet (Voz sobre IP)

Usenet. Es el acrónimo de Users Network (Red de usuarios), consistente en un sistema global de discusión en Internet, que evoluciona de las redes UUCP. Fue creado por Tom Truscott y Jim Ellis, estudiantes de la Universidad de Duke, en 1979. Los usuarios pueden leer o enviar mensajes (denominados artículos) a distintos grupos de noticias ordenados de forma jerárquica. El medio se sostiene gracias a un gran número de servidores distribuidos y actualizados mundialmente, que guardan y transmiten los mensajes.

Virus. Código malicioso que se propaga o infecta insertando una copia de sí mismo en otro programa para convertirse en parte de él. Un virus no puede ejecutarse por si mismo, requiere que el programa que lo aloja sea ejecutado para poder realizar sus operaciones.

White Hat. Un hacker de sombrero blanco, en jerga informática, se refiere a una ética hacker que se centra en asegurar y proteger los sistemas de Tecnologías de información y comunicación. Estas personas suelen trabajar para empresas de seguridad informática las cuales los denominan, en ocasiones, Tiger Team.