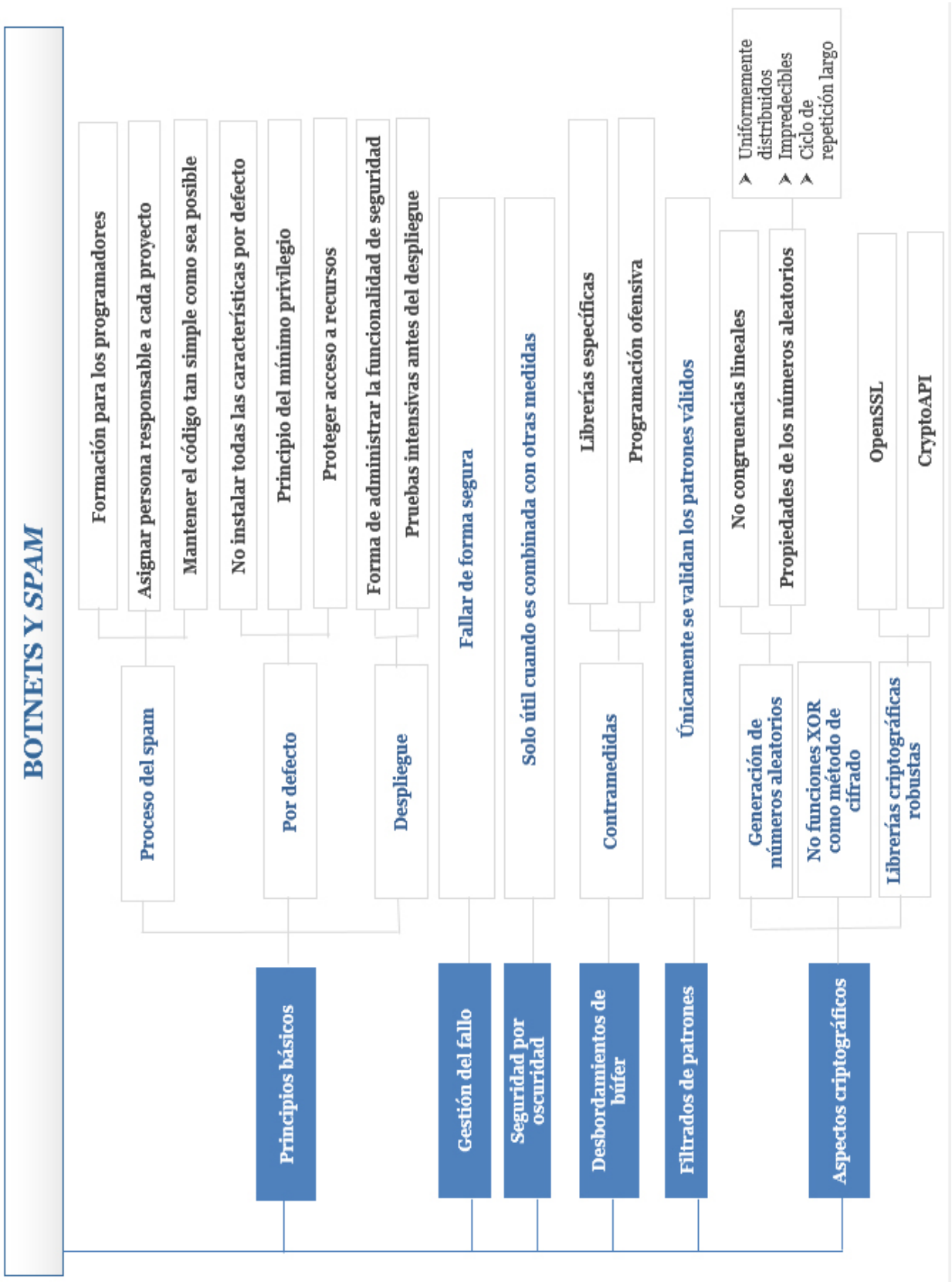
Botnets y *spam*

TEMA 9

Esquema


BOTNETS Y SPAM
Principios básicos
Proceso del spam
Formación para los programadores
Asignar persona responsable a cada proyecto
Mantener el código tan simple como sea posible
Por defecto
No instalar todas las características por defecto
Principio del mínimo privilegio
Proteger acceso a recursos
Despliegue
Forma de administrar la funcionalidad de seguridad
Pruebas intensivas antes del despliegue
Gestión del fallo
Fallar de forma segura
Seguridad por oscuridad
Solo útil cuando es combinada con otras medidas
Desbordamientos de búfer
Contramedidas
Librerías específicas
Programación ofensiva
Filtrados de patrones
Únicamente se validan los patrones válidos
Aspectos criptográficos
Generación de números aleatorios
No congruencias lineales
Propiedades de los números aleatorios
Uniformemente distribuidos
Impredecibles
Ciclo de repetición largo
No funciones XOR como método de cifrado
OpenSSL
Librerías criptográficas robustas
CryptoAPI

Ideas clave

9.1. ¿Cómo estudiar este tema?

El estudio de este tema se realiza a través de los contenidos desarrollados en las **Ideas clave** expuestas a continuación.

Sin un conocimiento profundo del actual panorama de la seguridad informática, podría creerse erróneamente que el ***spam*** es un problema superado. Los grandes proveedores de correo electrónico han mejorado sustancialmente sus detectores y el **nivel de SPAM** ciertamente ha descendido respecto al de hace sólo unos pocos años.

Sin embargo, como suele ocurrir en el mundo del cibercrimen y al igual que ha pasado con los viejos troyanos, ahora reconvertidos en troyanos especializados en robar credenciales bancarias, el *spam* ha resurgido de la mano de los ciberdelincuentes y de una nueva tecnología: **las botnets**.

9.2. Introducción: origen del problema

Ubicando al alumno en la problemática actual, existen múltiples tipos de malware en la actualidad. Botnet, Spam, Bug, Ransomware, Rootkit, Worm, Troyano, Spyware, Adwre... pero podemos decir que los dos primeros son desgraciadamete, los *campeones*.

Bot es una abreviación de robot. Son programas «inteligentes», se ejecutan automáticamente, no requieren de intervención humana y pueden realizar diversas funciones según se les ordene. Una Botnet (también llamada «red zombie»), es una red de «bots», controlada por el «BotnetMaster» de forma remota, y puede utilizar este ejército de «zombies» con diversos fines.

Al margen de las causas económicas, que también se analizarán más adelante en este tema, la **principal razón de la existencia del *spam*** es que resulta técnicamente **fácil y sencillo** de llevar a cabo. Básicamente esto es debido a la **falta de autenticación en los protocolos de envío de correo electrónico**.

Como ya sabemos, **la autenticación** es un proceso que permite asegurar las identidades de las partes involucradas en una comunicación. Junto a la privacidad e integridad, es uno de los aspectos imprescindibles para que podamos hablar de seguridad en el tratamiento de la información.

Como se ha comentado, **los protocolos de envío de correo son no autenticados**. Esto se traduce en que cualquier individuo u organización puede poner en marcha un servidor de correo y ser capaz de enviar y recibir un número ilimitado de correos electrónicos.
Por esta razón, algunas de las contramedidas planteadas para paliar el problema del *spam*, que analizaremos en el **apartado 9.6**, están específicamente dirigidas a tratar de contrarrestar esta falta de autenticación

9.3. Proceso del *spam*

A continuación analizaremos las fases más habituales de todo **proceso de envío de spam**, que se resumen en la **Figura 1**.

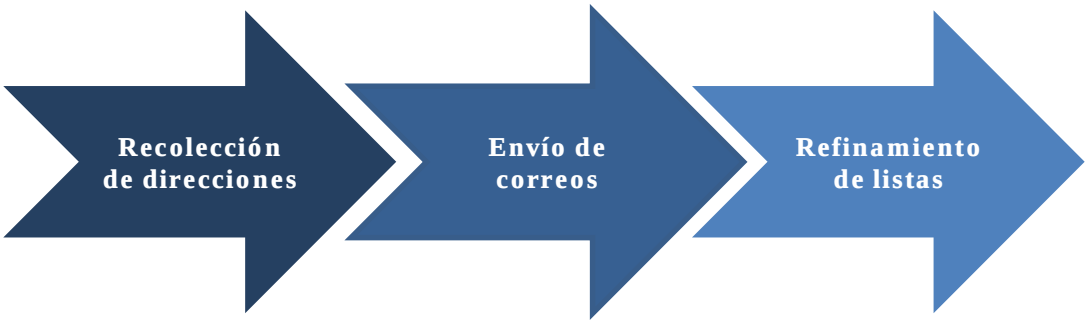


Figura 1. Fases habituales del proceso de *spam*

1. Recolección de direcciones

El **proceso del *spam*** debe comenzar, forzosamente, por la **obtención de una lista de direcciones electrónicas**, cuando más amplia mejor, a las que enviar el correo no solicitado.

Las estrategias utilizadas por los ***spammers*** para este propósito son muy variadas, pero podemos establecer la siguiente **clasificación** básica:

- **Recolección de direcciones electrónicas accesibles en Internet:** esta es, sin duda, una de las técnicas más utilizadas. Los expertos estiman que alrededor de un 70% de las direcciones recolectadas por los *spammers* provienen de esta fuente. A su vez, estas direcciones pueden encontrarse en multitud de servicios, como páginas Web, foros de discusión o listas de correo.
- **Generación automática:** esta técnica consiste en la generación automática de direcciones de correo, a través del uso de programas específicamente diseñados para ese propósito. Claramente un alto porcentaje de las direcciones generadas no existen, pero esto no es algo que preocupe especialmente a los *spammers*. Además, estas listas pueden ser refinadas posteriormente con técnicas que analizaremos más adelante.
- **Venta no autorizada de terceras partes:** en ocasiones, entidades supuestamente respetuosas con las políticas de protección de datos, hacen caso omiso de sus compromisos y utilizan las direcciones de correo proporcionadas para usos no autorizados. Se han descrito casos en que estas direcciones han sido, incluso, vendidas o cedidas por estas entidades.

2. Direcciones electrónicas accesibles en Internet

Direcciones accesibles en páginas Web

Una simple búsqueda en Internet, utilizando cualquier buscador puede revelar muchos millones de direcciones de correo. Tarde o temprano, la inmensa mayoría de estas direcciones recibirán correo no solicitado.

Para recolectar esta gran cantidad de direcciones, los *spammers* utilizan herramientas automáticas, denominadas ***arañas.*** Estos programas barren todas las páginas Web accesibles, analizándolas en busca de patrones que encajen con direcciones de correo electrónicas. Acto seguido, estas direcciones serán incorporadas a las listas masivas y comenzarán a recibir *spam* de inmediato.

Para evitar este problema, es práctica común tratar de ocultar la dirección real sustituyendo ciertos símbolos de la misma, como '@' y '.', propios de toda dirección de correo, por palabras que los simbolicen. Así, una dirección como «*prueba@dominio.com*», suele escribirse en una página Web como ***«prueba(AT)dominio(DOT)com»***.

Sin embargo, a pesar de ser una práctica común, esta técnica no es efectiva. Las razones son que los *spammers* aprenden rápido y han adaptado sus métodos de búsqueda a esta contramedida. De hecho, una simple búsqueda de la cadena **«AT * DOT *»** en un buscador proporciona casi 45.000.000 de resultados. Acto seguido, estos pueden ser fácilmente filtrados utilizando programas automáticos, de forma que las direcciones así obtenidas puedan ser directamente incluidas en las listas habitualmente utilizadas por los *spammers*. La ventaja además, radica en el hecho de que la mayoría de ellas son direcciones válidas, pues han sido especificadas por sus propios dueños.

Otra técnica común de protección frente a la búsqueda automática de direcciones en la Web es **especificar la misma utilizando un gráfico**, **en lugar de texto**. Para sobrepasar esta medida, los *spammers* tendrían que utilizar **software de reconocimiento automático de caracteres** lo que, aunque técnicamente posible, resultaría demasiado costoso, en tiempo e infraestructura, para sus propósitos. Esta es por tanto, la medida de protección más apropiada frente a esta amenaza.

Foros de discusión

Otra de las grandes fuentes de direcciones públicas para *spammers* son los **foros de discusión**, cada vez más comunes. Uno de los datos que suelen exigirse a los usuarios de estos servicios es, entre otros, su dirección de correo electrónico. Posteriormente, en ocasiones, esta dirección puede encontrarse en cada uno de los comentarios que el usuario haga en el foro. El siguiente gráfico ilustra el problema en un foro típico:

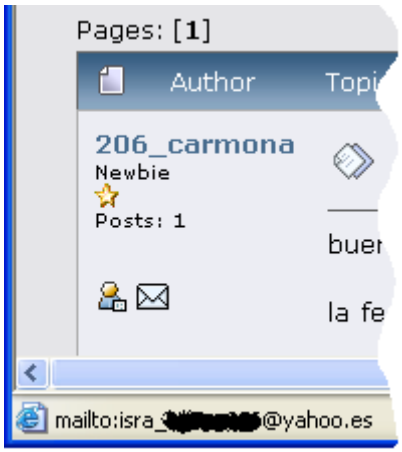


Figura 2. Un foro de discusión con direcciones de correo públicamente accesibles

Afortunadamente, este problema está remitiendo de forma gradual, aunque lenta, conforme los programadores toman conciencia de este problema e incluyen mecanismos para proteger la exposición pública de las direcciones de correo. Sin embargo, todavía es fácil encontrar literalmente millones de foros donde se publican, sin previo aviso, las direcciones de los usuarios.

A continuación se resumen las ventajas e inconvenientes de estas técnicas para los *spammers*, así como algunas contramedidas.

Ventajas
Una de las ventajas para los *spammers* de esta técnica es que pueden utilizar las mismas herramientas que en el método anterior, con mínimas modificaciones.
Inconvenientes
La efectividad de esta técnica está decreciendo rápidamente, por lo que cada vez resulta menos útil para los *spammers*.

Medidas de protección

Para mitigar este problema, pueden seguirse **una serie de medidas** sencillas:

- Elegir con cuidado los foros en los que se participa, comprobando de antemano si la dirección de correo se expondrá en cada comentario realizado.
- Si es así, no es aconsejable utilizar una dirección personal, que se desee mantener libre de spam.
- En este sentido sería recomendable disponer de varias cuentas de correo, cada una de ellas destinada a un uso específico. Así, una de ellas, podría utilizarse a la hora de participar en un foro de discusión, o registrarse en cualquier página Web.

3. Generación automática

El último gran grupo de provisión de direcciones de correo para los *spammers* lo constituye la generación automática de las mismas. De hecho, según los expertos, esta técnica ha crecido en popularidad en los últimos años, hasta el punto de que se estima que los *spammers* obtienen de esta forma alrededor del 70% de direcciones incluidas en sus listas masivas.

La **generación automática** consiste en tratar de adivinar, utilizando programas específicamente diseñados al efecto, las direcciones de correo, en lugar de tratar de recolectarlas de otras fuentes, como las que hemos visto en los puntos anteriores.

Para este propósito, los *spammers* utilizan, básicamente, dos tipos de técnicas:

- **Técnicas de fuerza bruta**, consistentes en generar todas las posibles combinaciones de letras, números y algunos símbolos, que podrían corresponder, o no, a una dirección de correo real. Habitualmente esta técnica se utiliza contra los servicios de correo de grandes proveedores, como *Microsoft*, *Yahoo!* o *Google*. La **Figura 3** ilustra cómo funcionaría el proceso.

- **Técnicas mixtas**, que consisten en un refinamiento de la técnica anterior. Además de generar parte de la dirección de forma sistemática, se añaden determinados prefijos o sufijos de uso común, en diferentes idiomas, con el objetivo de tratar de aumentar el número de cuentas válidas. Por ejemplo, a la dirección generada sistemáticamente '*abc@hotmail.com*' puede añadirse el sufijo '*1977*', que corresponderá a la fecha de nacimiento de muchísimas personas, y que es una técnica habitual utilizada por los usuarios ante la escasez de direcciones disponibles en los grandes proveedores. De esta forma, la dirección de correo generada por esta técnica quedaría finalmente '*abc1977@hotmail.com*' o '*abc_1977@hotmail.com*'. Como pueden observarse, las posibles combinaciones son altísimas.

Figura 3. Generación de direcciones de correo por fuerza bruta

Ventajas

Las ventajas de este tipo de técnicas para los *spammers* son claras. En primer lugar, es un método sencillo y rápido. No es necesario dedicar tiempo ni esfuerzos a escribir software específico que explore la Web en busca de direcciones, sino que en pocas horas pueden obtenerse millones de posibles direcciones.

Por supuesto, son sólo eso, *posibles* direcciones, pues no hay ninguna garantía de que correspondan a direcciones válidas. Sin embargo, esta técnica parece ser más efectiva de que podría parecer a priori. La razón radica fundamentalmente en que se estima que un servicio de coreo como Hotmail tiene un número aproximado de usuarios de alrededor de 380 millones en todo el mundo. Los usuarios, por supuesto, tienden a elegir direcciones de correo fáciles de recordar, lo más cortas posibles, siempre que éstas estén disponibles y no hayan sido elegidas ya por otro usuario.

Por tanto, el alto número de usuarios y su tendencia natural a elegir direcciones lo más cortas posibles provoca que éstas sean más fácilmente adivinables utilizando la técnica de búsqueda por fuerza bruta o mixta.

Inconvenientes
A pesar del fenómeno que se acaba de describir, esta técnica tiene sin duda una eficacia menor que la recolección de direcciones existentes. Sin embargo, como ya se ha comentado, se ha convertido en la más utilizada por los *spammers*. Esta baja eficacia, que en otros entornos o propósitos sería inaceptable, puede permitirse debido al coste prácticamente nulo que tiene el envío de *spam*. Así, cuesta lo mismo enviar 1 millón de correos no solicitados que 100, por lo que la baja eficacia no supone un problema real.

Medidas de protección

Según algunos estudios, parece existir una **relación directa entre la longitud de las direcciones de correo y el volumen de *spam* que reciben**. A pesar de que estas son, sin duda, mucho más cómodas para recordar y manejar, una dirección de pocos caracteres recibirá un alto volumen de *spam*, sin necesidad, siquiera, de que haya sido utilizada en ninguna ocasión.

4. Venta no autorizada de terceras partes

Esta **es una de las técnicas más conocidas y de más repercusión mediática**, aunque, sin embargo, no es de las más utilizadas.
Existen empresas que, con toda impunidad, anuncian la venta de listas de correo, bajo el eufemismo de *marketing directo*. Son listas larguísimas, de centenares de millones de direcciones, pero de baja calidad, con muchas direcciones inactivas, inexactas o, directamente, inexistentes. Por tanto el precio correspondiente no es muy elevado, alrededor de unos pocos centenares de dólares.

Por supuesto, los *spammers* también en ocasiones recurren al soborno, para hacerse con listas de altísima calidad, directamente proporcionadas por algún empleado de un ISP. Recientemente se ha conocido la noticia de un empleado de AOL, detenido por vender una lista con más de 92 millones de direcciones de usuarios de este ISP por unos 52.000 dólares.

Ventajas
Las ventajas de este método son claras. Aún cuando sean listas baratas, de baja calidad, esta técnica permite introducirse en el negocio del *spam* a personas con bajos o nulos conocimientos técnicos, a los que el uso de otras técnicas le resultaría más difícil. Y en el caso de que se tenga acceso a lista de alta calidad, más caras, serán rápidamente amortizadas, pues tienen una eficacia mucho más alta.
Inconvenientes
Como hemos comentado, las listas baratas, fácilmente localizables y adquiribles en Internet, implican una baja eficacia, por lo que es necesario dedicar una mayor número de recursos, tanto en tiempo como en ancho de banda, para obtener los mismos resultados que con listas de mayor calidad.

Medidas de protección

Desgraciadamente, esta es una técnica contra la que el usuario tiene poco o nada que hacer. Si un empleado corrupto de un ISP decide aceptar la oferta de un spammer y vender una lista de direcciones, sólo queda hacer uso de las medidas de filtrado que analizaremos en los siguientes apartados de este informe.

5. Recolección pasiva

En esta categoría se engloban una serie de técnicas menores, menos utilizadas por los *spammers*, principalmente por su baja efectividad.

Se tratan, por ejemplos, de **sitios Web operados por los propios *spammers***, que se anuncian como lugares donde es posible darse de baja de, precisamente, listas de *spam*. Por supuesto, la oferta es falsa y el propósito es, realmente, el contrario: incluir las direcciones proporcionadas en las listas correspondientes.

Otras páginas de este tipo ofertan toda clase de productos gratuitos, ofertas completamente desproporcionadas o servicios relacionados con sexo. Nuevamente, cada dirección de correo registrada en la página es automáticamente incorporada en las listas de correo correspondientes.

Ventajas
Este método resulta, claramente, muy sencillo y barato de llevar a cabo. Sólo hay que poner en marcha un sitio Web, y esperar que los usuarios que caen en el engaño vayan proporcionando sus direcciones de correo. Además, la calidad de las listas así generadas es alta, pues son los propios usuarios quienes especifican sus direcciones, por lo que, en un altísimo porcentaje, serán correctas y actuales.
Inconvenientes
Aunque es muy difícil poder hablar de unas cifras concretas, aunque sean aproximadas, el volumen de direcciones que esta técnica es capaz de recolectar es bajo comparado con otras, con la recolección activa o la generación automática.

Medidas de protección

Por más que las medidas de protección frente a esta técnica resulten obvias, es necesario insistir en ellas: **no debe proporcionarse nunca ningún tipo de dato en este tipo de páginas** que, por otro lado, resultan fácilmente detectables.

6. Coste económico, material, humano, etc.... de cada técnica

Cada una de las técnicas que hemos analizado tiene una serie de costes para el spammer. Aunque, como hemos visto, el **coste económico es muy bajo en casi todos los casos**, son necesarios también otros recursos, como los siguientes:

- **Recursos materiales:** ordenadores y ancho de banda, principalmente, con el coste asociado de cada uno de ellos.
- **Recursos humanos:** para las técnicas de recolección activa y generación automática son necesarios una serie de programas. No son técnicamente muy complejos, pero son necesarios ciertos conocimientos de redes y programación. Sin embargo, estos programas no se reescriben continuamente, sino que existen en forma de kit y se pueden encontrar fácilmente en Internet. Es un fenómeno similar al de *phishing*, en el que kits similares alcanzan altos grados de sofisticación, con características avanzadas de parametrización, paneles de control gráficos, etc....

7. Resumen de técnicas de recolección de direcciones

A continuación presentamos una tabla que resume los grandes grupos de técnicas para la obtención de direcciones que hemos analizado. Se especifica la dificultad técnica que implica llevarlas a cabo, su eficacia, en términos de usuarios reales obtenidos, junto con los recursos necesarios, tanto económicos, materiales y humanos.

Métodos de obtención de direcciones (%)					
Técnica	**Dificultad técnica**	**Eficacia**	**Recursos necesarios**		
			Económicos	Materiales	Humanos
Obtención direcciones expuestas	Media	Alta	Bajos	Bajos	Medios
Generación automática	Baja	Baja	Bajos	Bajos	Bajos
Compra de lista	Alta/Baja	Media	Altos/Bajos	N/A	Medios
Recolección pasiva	Baja	Baja	Bajos	Medios	Medios

En el siguiente gráfico se ilustran los **porcentajes de uso aproximado**, de acuerdo a algunos estudios, de las diversas técnicas que se están analizando. Hay que tener en cuenta que este porcentaje puede variar rápidamente, en función de las contramedidas que se van desarrollando y el impacto de éstas sobre las técnicas utilizadas por los *spammers*.

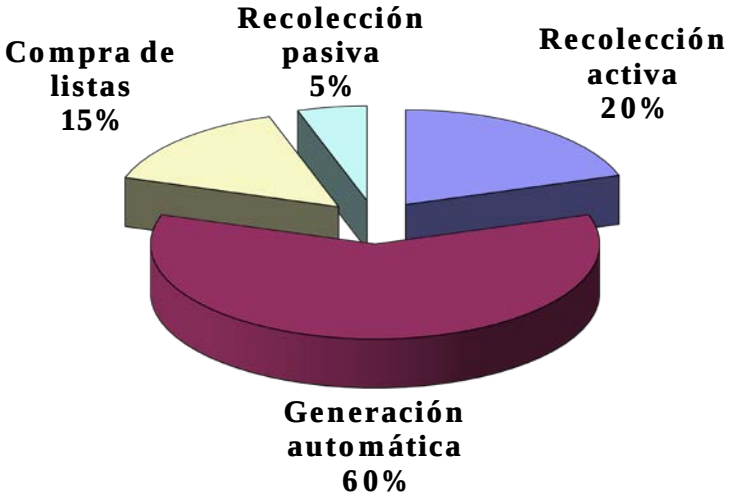


Figura 4. Porcentajes de uso de los métodos habituales de obtención de direcciones de correo. Fuente: INTECO

9.4. Envío del *spam*

El *spam*, como otras actividades delictivas como el phishing, se ha profesionalizado mucho en los últimos años. Así, han entrado en el negocio del *spam* parte de las mafias tradicionales, que ven en Internet y en esta actividad nuevas posibilidades de movimiento y blanqueo de capitales.

Por supuesto, los integrantes de estas mafias rara vez cuentan con los conocimientos técnicos suficientes para poner en marcha toda la infraestructura necesaria para la generación de *spam*. Tienen, por tanto, que subcontratar servicios, como si de una actividad comercial legal se tratase. Por tanto, el proceso de generación de *spam* se ha convertido en una cadena, siendo cada eslabón de la misma gestionado por grupos de personas distintas, muy especializadas y que no se dedican a otras actividades.

Así, algunos hackers son contratados por estas mafias para que escriban software específico o proporcionen su ayuda en cuestiones técnicas concretas. Existen foros especializados en Internet donde es posible, y fácil, que ambas partes se pongan en contacto.

Proceso de envío

Una vez que el *spammer* cuenta con suficiente número de direcciones, e independientemente del modo en que éstas han sido obtenidas, comienza el proceso de envío de correos.

La primera decisión a tomar es: **qué plataforma se utilizará para el envío**. La plataforma es la infraestructura necesaria formada, a su vez, por un conjunto de hardware y software. Las opciones con las que cuenta el spammer son, básicamente, las siguientes:

- **Ordenadores comprometidos o *botnets*:** que constituye, sin duda, la opción más utilizada. Consiste en comprometer, o tomar el control de ordenadores, bien de usuarios normales de Internet, bien de Universidades, empresas u otras instituciones, para instalar en ellos un software específicamente diseñado para utilizar estos ordenadores como plataforma de envío de *spam*. Por supuesto, todo esto sin el consentimiento ni conocimiento del dueño o dueños de los ordenadores.

- **ISP's dedicados**: es público y notorio que existen gran cantidad de proveedores de servicio, ISP's por sus siglas en inglés, que no sólo son permisivos con el uso de sus instalaciones para el envío de *spam*, sino que lo aprueban y cobran por ello como por cualquier otro servicio. Hace unos años estos ISP estaban localizados principalmente en países del Este, como Rusia, o del sudeste asiático, como China. Sin embargo, hoy día esta tendencia no es tan clara y, de hecho, la mayoría de los ISP's corruptos están situados físicamente en EEUU.

- **Realizado por terceras partes:** como se ha comentado en el punto anterior, el negocio del *spam* ha sufrido un proceso de profesionalización. Y, por tanto, existen individuos que ofertan servicios de envío de *spam*, con diversas opciones y precios en función de los métodos concretos que se utilicen para el envío. Estos servicios pueden ser utilizados por mafias u otros individuos que quieran iniciarse en este negocio, pero que todavía no cuenten con la infraestructura técnica o conocimientos necesarios para empezar a operar.

Cada una de las técnicas anteriores tiene unos costes asociados, en forma de recursos necesarios para su realización. Estos **recursos** pueden, a su vez, ser de diversos tipos:

- **Recursos temporales**, puesto que el envío puede durar unos minutos, prolongarse durante horas o días, o ser continuo.
- **Recursos materiales**, que constituyen la plataforma de envío de mensajes, constituida principalmente por ordenadores. Por supuesto, también ancho de banda, que suele ser el factor limitante que determina la tasa máxima de envío de correos.
- **Recursos humanos**, como hackers, capaces de programar y gestionar las máquinas comprometidas que se utilizarán como plataforma de envío de correos.

Nueva generación de malware para *spam*

Los *spammers* han encontrado en los tradicionales **troyanos**, utilizados habitualmente hasta hace unos años con fines no lucrativos, la herramienta perfecta para sus actividades.

En lugar de utilizar **relays públicos de correo o ISP's** poco escrupulosos con la legalidad, l**os *spammers* utilizan estos troyanos para infectar y tomar el control de miles de máquinas en Internet**, que a partir de ese momento, podrán ser utilizadas como plataforma de distribución de *spam*.

Esta nueva generación de troyanos ha llevado el envío de spam a un nuevo nivel. Además de sus funcionalidades habituales, este tipo de malware tiene una serie de funcionalidades «profesionales», mucho más allá del mero envío de correos electrónicos, como el alojamiento de páginas web o cambios periódicos de las direcciones IP de las víctimas para evitar se incluidas en listas negras.

Se sabe, de hecho, que una parte importante de los últimos ataques masivos de gusanos en Internet fueron lanzados específicamente para encontrar víctimas en las que instalar este tipo de troyanos y poder **utilizar así estas máquinas como plataformas de envío de correos**.

Botnets

Las **botnets** son **redes de ordenadores comprometidos**, **en las que los spammers han instalado estos troyanos** descritos en el punto anterior, cuyo fin es controlarlas y utilizarlas de forma remota de forma coordinada. Los ordenadores que componen estas redes suelen conocerse con el nombre de máquina zombie.

Para gestionar un número muy alto de máquinas de forma sencilla los diseñadores de este tipo de software han utilizado tradicionalmente una idea ingeniosa: **utilizar el protocolo *IRC*** (el protocolo IRC, *Internet Relay Chat*, es uno de los primeros protocolos de mensajería instantánea) existente desde hace años. De esta forma, cada máquina, tras ser infectad, inicia una comunicación IRC, se registra en un servidor y canal concretos, cuyo acceso suele estar protegido por contraseña, y queda a la espera de instrucciones.

Este enfoque tiene una serie de ventajas: evita la necesidad de diseñar e implementar un protocolo propio de comunicaciones y que se camufla la comunicación dentro de tráfico IRC, que podría parecer inocuo a primera vista, sin un análisis detallado.

Sin embargo, al tratarse de un esquema centralizado, **si el servidor IRC falla o es desactivado por las autoridades, la comunicación con las máquinas zombies se pierde**.

Como los atacantes nunca descansan, los spammers ya utilizan otro tipo de esquema, que incluye características de las **redes P2P**, descentralizadas por naturaleza, lo que hace su desactivación más difícil.

La importancia de este tipo de redes se ha hecho tan importante que, en la actualidad, se estima que más del 80% del *spam* se envía de esta forma.

Proceso de infección

Los distintos métodos utilizados por los spammers se hacen con el control de nuevas máquinas, que pasan a formar parte de su *botnet*, se conocen con el nombre de **vectores de infección**, y son muy similares, por no decir idénticas, a las que estudiaremos con mayor detalle en el tema 11, dedicado al ***malware*.**

Los más importantes y utilizados para este propósito son la **navegación Web**, aprovechando vulnerabilidades en los navegadores y que es, probablemente, la vía de infección más común, las **redes P2P**, donde se estima que casi el 50% de los programas ejecutables están infectados con alguna clase de malware o el eterno **correo electrónico**.

Infección Web

Aprovechando ciertas vulnerabilidades en los navegadores los atacantes pueden conseguir que un usuario, por el mero hecho de visitar un sitio Web malicioso, quede infectado. El proceso comienza con el compromiso de sitios web existentes, tanto mejor cuando más conocidos y visitados sean éstos.

Para ello suelen utilizar herramientas automáticas, que explotan vulnerabilidades concretas, y que en poco tiempo, pueden reunir una colección de cientos de máquinas comprometidas. Acto seguido, se instala en cada una de ellas un pequeño código, de unos pocos kilobytes, que suele conocerse con el nombre de ***dropper***.

A continuación se modifica el código fuente de la página web, a menudo sin alterar el comportamiento ni el aspecto de la misma, de forma que, cuando el usuario la visite, se explote la vulnerabilidad del navegador y se provoque la descarga y ejecución del *dropper* al ordenador de la víctima. A partir de ese momento, dicho *dropper* toma el control y comienza su misión, consistente en descargar el verdadero troyano. Para ello cuenta con una lista de direcciones donde, previamente, los creadores del troyano han colocado copias del mismo. Comenzará probando con la primera de ellas y, en el caso de que falle, seguirá avanzando por la lista hasta agotarla.

De esta forma, los delincuentes consiguen **aumentar la resistencia del sistema** y que este **siga funcionando aunque las autoridades cierren uno o varios de los sitios de descarga**. Sirve, incluso, para generar distintas versiones de los troyanos, con mejoras o personalizaciones, de forma que no es necesario modificar el código del sitio web comprometido para que se descarguen las nuevas versiones. Dado el nuevo modelo de negocio del cibercrimen, esta característica resulta muy deseable para vender copias personalizadas a distintos compradores.

Todo este proceso se lleva a cabo, por supuesto, sin que el usuario note que algo extraño está sucediendo. En el **Figura 5** puede verse ilustrado el proceso completo.

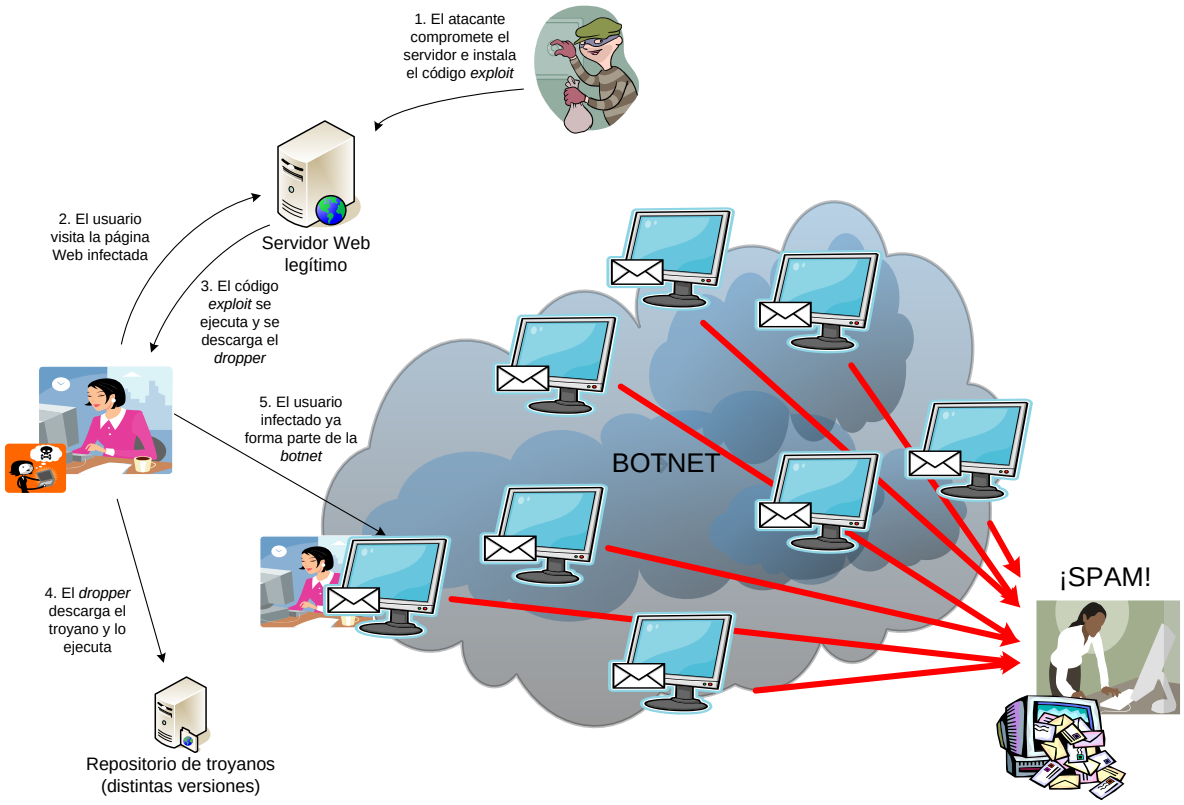


Figura 5. Infección vía Web e inclusión de una máquina en una *botnet*

Resumen

Ténicas para el envío de *spam*					
Técnica	**Tasa de envío**	**Tiempo de envío**	**Recursos necesarios**		
			Económicos	Materiales	Humanos
Botnets	Máxima	Continuo	Bajos	Bajos	Medios
ISP's dedicados	Contratada	Contratado	Bajos	Bajos	Bajos
Realizado por terceros	Por volumen	El necesario	Altos/Bajos	N/A	Medios

9.5. Refinamiento de las listas de direcciones de correo

Como último paso en el proceso del *spam*, los *spammers* dedican tiempo continuamente a refinar sus listas, con el objetivo de eliminar direcciones «muertas» o inexactas y aumentar el número de direcciones válidas.

Las **técnicas** que se utilizan para este propósito son muy variadas, pero a continuación resumimos las más representativas:

- **Pruebas de lectura**
- **Enlaces o páginas de baja de direcciones**
- **Correos de confirmación**
- **Pruebas de lectura**

Las ***pruebas de lectura*** es una de las técnicas que suelen utilizarse **para comprobar quién, cuándo y desde qué ordenador un usuario está visitando una página Web o leyendo un correo electrónico**.

Aunque existen varias implementaciones, el más común y uno de los más sencillos es incluir una enlace a una pequeña imagen, normalmente 1 pixel de tamaño y de color transparente, por lo que resulta invisible, en el correo enviado a la dirección que el spammer desea verificar.

Cuando el usuario abra el correo, la imagen será descargada desde un servidor preparado por el atacante. De esta forma, en los registros del servidor quedan datos que permiten determinar al atacante qué direcciones de correo son válidas, siempre que el usuario abra el correo, por supuesto.

Contramedidas

Afortunadamente los grandes proveedores de correo gratuito están empezando a **restringir la carga de imágenes y en general, código HTML en los correos recibidos**. De esta forma sencilla, la gran mayoría de variantes de la técnica anterior se vuelven inútiles.

- **Páginas de baja de direcciones**

En muchas ocasiones, parte del *spam* recibido contiene enlaces para en teoría, solicitar la baja en supuestas listas de suscripción. Por supuesto, como resulta previsible, este correo es falso, la lista de distribución no existe, y lo único que pretende es **detectar nuevas direcciones de correo a las que seguir enviando más spam**.

Por tanto, si se responde, habitualmente se detectará un aumento del volumen de *spam* recibido en esas direcciones. La razón es que, al solicitar la baja, en realidad se está confirmando que la dirección es válida y, automáticamente, está es incluida en nuevas listas y utilizada por más *spammers*.

Contramedidas

Afortunadamente, existe una contramedida sencilla y eficaz para este problema: **no responder nunca a este tipo de correos, ni seguir ningún enlace incluido en un correo de *spam***. Sólo cuando la entidad que envía el correo no solicitado ofrezca las suficientes garantías puede utilizarse el servicio de tramitación de baja.

9.6. Técnicas de protección frente al *spam*

La lucha contra el *spam* es, sin duda, uno de los grandes frentes que deben resolverse en el futuro próximo de Internet. Por tanto, es una de las áreas de investigación más activas y una gran oportunidad de negocio para las compañías de seguridad.

En la actualidad se utilizan muchas medidas defensivas que, si bien no resultan definitivas, sí suponen un gran alivio en la carga económica y de recursos humanos y temporales que supone el *spam*.

Las **técnicas de protección básicas** en uso más importantes hoy en día incluyen las siguientes:

1. **Listas negras y blancas de orígenes**
2. **Listas negras de documentos**
3. **Uso de palabras claves**
4. **Filtros bayesianos**

1. Listas negras

Las **listas negras anti-*spam*** son **listas de servidores, redes o dominios de Internet de los que se tiene la certeza, o una sospecha muy fundada, de que son utilizados por *spammers*.** Estas listas son incluidas en los servidores de correo o software anti-*spam* para bloquear el correo procedentes de las entradas incluidas en las listas.

Estas listas son mantenidas por multitud de organizaciones independientes, como *Spamhaus* o *Spews*.

Criterios de inclusión

Cada organización utiliza diferentes criterios para incluir a ciertos servidores o redes en estas listas. Algunas de ellas tienen en cuenta los informes generados por los usuarios o por profesionales de los diferentes ISP's.

Otras organizaciones realizan una **monitorización automática de redes y servidores** en busca de potenciales factores de riesgo, como proxies abiertos o servidores de correo inseguros, por ejemplo con versiones anticuadas del software.

Modo de funcionamiento

Las listas negras funcionan normalmente **utilizando el soporte de los servidores de traducción de nombres, o DNS's.** Así, para comprobar si una dirección IP está incluida en una lista negra, se realizaría u**na consulta a los servidores DNS de la organización que gestiona la lista**. En su respuesta se incluirían datos para determinar si la dirección está en la lista, junto con otra información de interés.

Inconvenientes

Las listas negras tienen una serie de inconvenientes siendo el principal el hecho de que **necesitan una constante actualización**. Si no son exactas o están desactualizadas, las listas pierden toda su eficacia.

Además, **pueden suponer incluso un problema legal, al incluir por error a una institución u organización en una lista**. En este sentido, pueden darse situaciones paradójicas, como una reciente sentencia en EEUU que condenaba a Spamhaus a pagar una gran suma de dinero, más de 11 millones de dólares, a e360insight, una compañía radicada en Gran Bretaña, por incluirla en una de sus listas. Se da la circunstancia de que el director de esta compañía, David Linhardt, es un conocido spammer (!).

Resumen

Las listas negras ayudan a mitigar el problema, pero están lejos de ser una solución al mismo. Por esta razón, **habitualmente se utilizan en combinación con algún otro de los métodos** que vamos a analizar a continuación.

2. Listas negras de documentos

En este caso, la aproximación cambia el enfoque: **en lugar de generar listas con los dominios o servidores problemáticos, se utilizan valores *hash*** (una función *hash* genera un valor de longitud fija, normalmente de 64 o 128 bits, único para cada documento. Algunas de las funciones *hash* más conocidas son MD5 y SHA1) **de los correos electrónicos**, evitando así tener que almacenar el documento completo.

Sin embargo, esta no puede considerarse una técnica de detección de *spam*, pues no tiene ninguna capacidad para hacerlo. Es más bien un método auxiliar, que puede ayudar a reducir el enorme volumen de almacenamiento necesario para tratar todo el tráfico de *spam* de una gran corporación.

Además este método adolece de un serio inconveniente: el valor hash cambia a la mínima modificación del texto de entrada, por lo que cualquier ligero cambio en el correo electrónico, como la adición de una tilde o el cambio de cualquier signo de puntuación, provoca que se generen valores hash completamente diferentes y, por tanto, sean clasificados como dos correos distintos.

3. Uso de palabras clave

Las herramientas que utilizan esta técnica **marcan como *spam* aquellos mensajes que contengan alguna palabra denominada *clave*, de una lista de palabras previamente especificada**.

Esta lista contendrá palabras que aparecen típicamente en los correos de *spam*, como «viagra o sexo». Obviamente no es una solución completa, pues marcará como *spam* multitud de correo legítimo que haga uso de alguna de las palabras clave.

Además este sistema es fácilmente evitable: basta con insertar separadores, cometer algún error ortográfico, etc.... para que la búsqueda de palabras clave falle. Así para evitar que la palabra *Viagra* sea detectada, basta con escribirla como «Via-gra». De hecho, es una técnica muy común, utilizada habitualmente por los *spammers*.

Listas blancas

Como su nombre indica, este método **utiliza el enfoque contrario al de las listas negras**: una lista blanca **es una relación de contactos que el usuario en los que confía y cuyos envíos no deberían ser considerados *spam***. Es decir, se asume que todo correo es *spam* a no ser que sea enviado por alguien perteneciente a la lista blanca.

Estas listas pueden ser excluyentes o no. Si lo es, significa que sólo el correo proveniente de una entrada autorizada de la lista llegará finalmente a la bandeja de entrada del usuario. Si, por el contario, no es excluyente el correo se marcará como *spam* y será el usuario quien decida si se visualiza o no.

Por otra parte, esta es una medida que, habitualmente, sólo resultará de interés para usuarios finales o corporaciones, pero no para proveedores de servicio, o ISP's, que deben atender multitud de correos electrónicos en principio "desconocidos" y a los que sería imposible aplicar una lista blanca.

Inconvenientes

Las listas blancas surgieron de la idea que la mayoría del correo legítimo se recibe de un conjunto relativamente pequeño y más o menos fijo de remitentes. Sin embargo, estas listas tienen inconveniente de que pu**eden llegar a bloquear, o al menos marcar como *spam*, todo aquellos correos que sean remitidos por un nuevo contacto**.

Para tratar de minimizar este inconveniente, esta técnica se utiliza normalmente en combinación con otras, como las listas negras y búsqueda de palabras claves.

Listas blancas comerciales

Las listas blancas comerciales utilizan un enfoque distinto a las analizadas en el punto anterior, más apropiadas para usuarios finales. En este caso se trata de **un sistema dirigido a proveedores de servicio**, que **permiten a ciertas entidades evitar sus filtros anti-*spam* a cambio de una cuota, bien fija o bien dependiente del volumen de correo enviado**.

Así, las compañías que legítimamente envían correo, típicamente publicitario, a sus clientes pueden tener la seguridad de que éste no será interceptado por los filtros anti-*spam*. Ahora bien, para evitar el abuso del sistema por parte de los propios *spammers*, las tasas que las compañías deben pagar se incrementan notablemente con cada queja recibida por los usuarios finales. Si el número de queja alcanza un umbral definido suficientemente alto, el contrato se rescinde.

4. Técnicas de Inteligencia Artificial: Redes Bayesianas

Las técnicas de inteligencia artificial empezaron a aplicarse por primera vez al problema del *spam* a finales de 1990. Desde entonces se ha convertido en **uno de los enfoques más utilizados y eficaces**.

A su vez, de las técnicas de aprendizaje utilizadas, la más común ha sido el uso de *clasificadores bayesianos*, que son redes bayesianas aplicadas a tareas de clasificación. Estas técnicas tienen la gran ventaja de que cuentan con capacidad de **aprendizaje**, y permiten adaptarse a los cambios y ser personalizadas por los usuarios.

Su fundamento matemático es sencillo y hace uso del ***Teorema de Bayes***. Este teorema, aplicado al problema del *spam*, permite deducir que la probabilidad de que un correo sea *spam*, dado que contiene ciertas palabras, es igual a la probabilidad de encontrar esas palabras en los correos de *spam* en general multiplicada por la probabilidad de que cualquier correo sea *spam*, y dividido por la probabilidad de encontrar dichas palabras en cualquier correo (sea o no *spam*). Matemáticamente puede formularse así:

$$\mathbf{Pr(}\mathit{spam}\mathbf{/palabras)=}\frac{\Pr(\text{palabras}/\mathit{spam})\cdot\Pr(\mathit{spam})}{\Pr(\text{palabras})}$$

Modo de funcionamiento

Los **filtros bayesianos** necesitan ser entrenados antes de su puesta en marcha definitiva. Es necesaria, por tanto, una fase inicial en la que el propio usuario marca al sistema qué mensajes considera como *spam* y cuáles no. El filtro va aprendiendo las características de cada tipo de mensaje, *spam* y legítimo, y va mejorando sus tasas de clasificaciones correctas.

Es importante señalar que este entrenamiento debería llevarse a cabo por cada usuario individual. De esta forma se permite que el sistema «capte» las distintas necesidades de cada usuario. Existirán, por ejemplo, usuarios para los que las palabras «Viagra» o «sexo» aparezcan habitualmente en sus correos legítimos.

Sin embargo, es perfectamente posible que existan filtros bayesianos a nivel de toda la corporación, que habitualmente serán entrenados por los administradores del sistema.

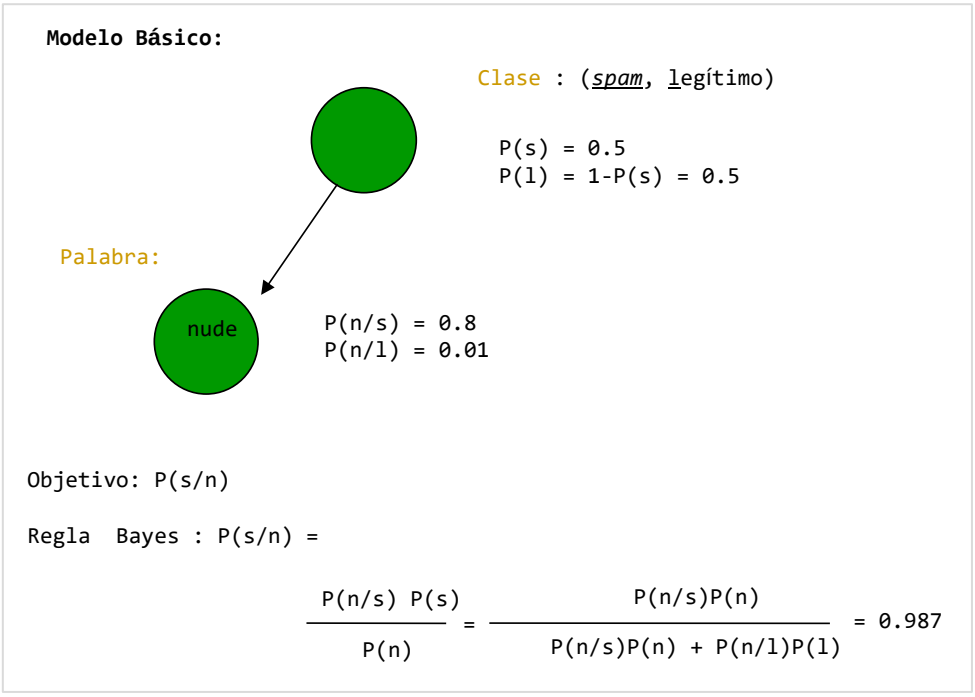


Figura 6. Modelo bayesiano de ejemplo de un filtro de *spam*

Inconvenientes

Uno de los inconvenientes de esta técnica es que, como otras, es susceptible de ciertos ataques por parte de los *spammers*. En este caso, el ataque se conoce con el nombre de ***envenenamiento bayesiano*** y aprovecha el modo en el que funcionan estos filtros.

Para llevar a cabo este ataque, un spammer incluirá grandes cantidades de texto legítimo, por ejemplo tomado de cualquier diario en línea, para tratar de confundir al filtro bayesiano que, al detectar palabras que normalmente no aparecen asociadas a correos *spam*, puede terminar clasificando el correo como legítimo.

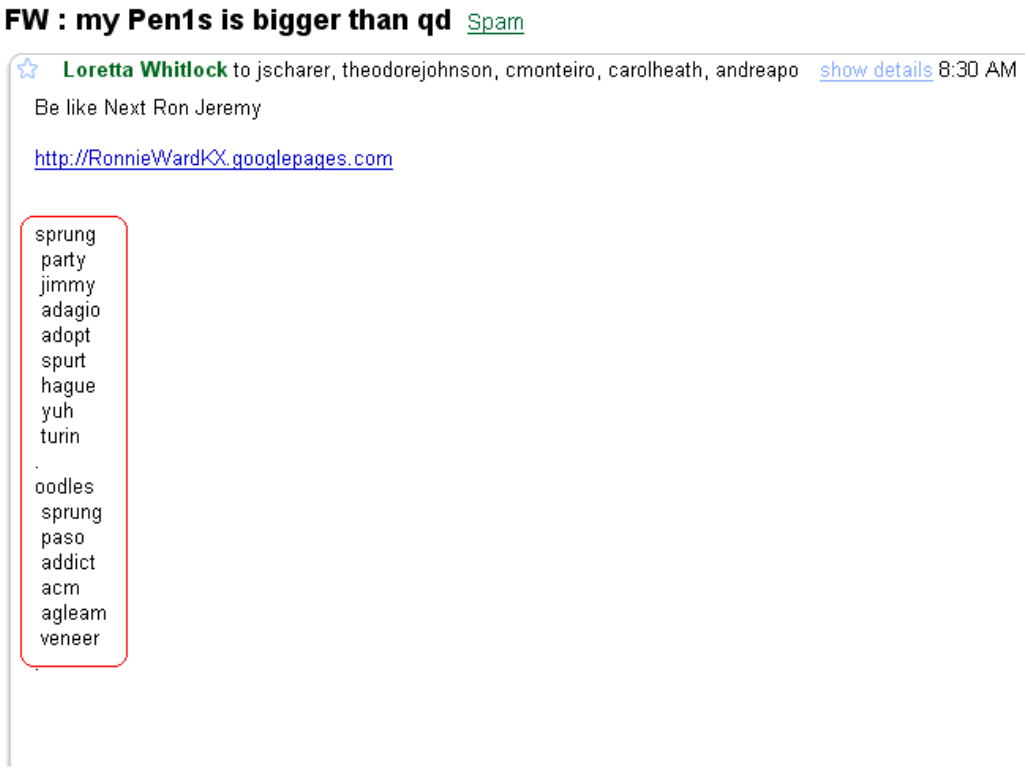


Figura 7. Intento de envenenamiento bayesiano

Filtros bayesianos en clientes de correo

Existe, por otro lado, una serie de **software que implementan filtros bayesianos como medidas anti-*spam***. Para los administradores de sistemas destacan *BogoFilter*, *DSPAM* o *SpamAssasin*. Y, entre los clientes de correo para clientes finales, *Mozilla Thunderbird* y varios filtros escritos para *Microsoft Outlook*, como *SpamBayes*.

Resumen

Los filtros bayesianos se han convertido en la **técnica anti-*spam* más utilizada y eficaz desde su planteamiento en 1998**, alcanzando eficacias cercanas al 95% de clasificaciones correctas.

Como inconvenientes de este enfoque podríamos citar que necesitan de una **fase de entrenamiento adecuada para alcanzar esas tasas de detección** lo que, en determinados entornos, puede resultar problemático.

9.7. Servicios anti-*spam* ofrecidos por terceros

No cabe duda que el *spam* es un gran negocio, por supuesto para los *spammers*. Pero también para muchas compañías de seguridad, que han encontrado en la lucha contra el *spam* una gran oportunidad de negocio. Parte de este negocio consiste en **ofrecer servicios anti-*spam* de forma remota o gestionada**. A continuación analizamos las iniciativas más destacables.

Direcciones de correo desechables

Estos servicios **ofrecen direcciones de correo únicas**, **normalmente de un solo uso**, diferentes para cada contacto.

Para utilizar esta técnica normalmente es necesario consultar el correo desde una página Web concreta, utilizando un navegador. Esta característica puede ser incómoda o inadmisible en ciertos entornos, por lo que ciertos proveedores de este tipo de servicios están empezando a ofrecer la posibilidad de que el correo sea reenviado a una cuenta POP3, accesible por el cliente de correo habitual del usuario.

Si alguna de las direcciones desechables comienza a recibir *spam*, esta puede ser desactivada y generada una nueva.

Servicios de reto/respuesta

Esta técnica funciona **utilizando un servicio de verificación del remitente del correo basado en el método conocido como reto/respuesta**. Cuando un correo llega por primera vez de un remitente desconocido, se responde al mismo con un nuevo correo que pide al remitente resolver algún tipo de reto para verificar su identidad.

Este reto puede consistir en algo tan sencillo como pulsar en un enlace, resolver un ***CAPTCHA***, típicamente teclear el texto incluido en una imagen distorsionada para que sólo un humano sea capaz de leerlo, teclear una frase incluida en un fichero de audio, etc....

Servicios anti-spam gestionados

Por último, existe otra categoría de servicios ofrecidos por terceros que **consiste en delegar la gestión del correo entrante y saliente de una corporación a otra que se encarga de su filtrado**.

Para ello, es necesario redirigir el registro MX, que designa la máquina servidora de correo, a la red del proveedor del servicio. A partir de ese momento, el proveedor se encarga de la detección y filtrado del correo recibido, reenviando la salida al cliente.

Los inconvenientes son, sin embargo, claros para clientes corporativos: **existen grandes problemas de privacidad y confianza en esta solución**, pues el correo electrónico es, cada vez más, la vía más importante de comunicación.

9.8. Casos de estudio

A continuación analizaremos algunas de las iniciativas llevadas a cabo por algunos de los grandes fabricantes de la industria, como *Microsoft*, a **través de su plataforma de correo *MSN/Hotmail* y *Yahoo!***.

1. Microsoft: SenderID

La *plataforma SenderID* es una **tecnología de autenticación de correo que ayuda a mitigar el problema del *spam*, así como de otros fraudes**, como el *phishing*, **verificando el dominio desde el que los correos electrónicos son enviados**.

Esta verificación consiste en la comprobación de que la dirección IP asociada al dominio que envía el correo aparece en una lista de servidores autorizados por el dueño del dominio. Una vez que el remitente ha sido correctamente autenticado, el servidor de correo puede aplicar los filtros de contenidos habituales.

Para poder utilizar esta plataforma, los dueños de cada dominio con capacidad para enviar correo deben declarar todas las direcciones IP de sus servidores de correo, o de las máquinas que pueden hacerlo en su nombre, e incluirlas en registros especiales, llamados SPF, de sus servidores de nombres, o DNS.

Modo de funcionamiento

El proceso completo de esta medida de protección puede resumirse en los siguientes **pasos**:

1. Un usuario envía un correo electrónico a través de su cliente de correo habitual. No es necesario ningún cambio en este cliente.
2. El servidor de correo de destino recibe el mensaje. A continuación, realiza una consulta a su DNS para pedir el registro SPF correspondiente al dominio que envía el correo.
3. Tras recibir la respuesta, comprueba que la dirección IP de la máquina que envía el correo corresponde con la autorizada en la respuesta SPF.
4. Si la comprobación es satisfactoria, se aumenta la reputación de ese dominio y se hace llegar el correo al usuario correspondiente.
5. Si la comprobación falla, se disminuye la reputación del dominio remitente y el correo se marca como *spam*. En ese momento, según la política que se haya definido, el correo puede descartarse directamente.

Ventajas e inconvenientes

Dado que el *spam* es debido, básicamente, a una falta de autenticación en el protocolo de envío de correo, esta solución parece a priori, muy adecuada. Sin embargo, exige un gran esfuerzo a muchos administradores, que deben generar listas con todas las máquinas autorizadas para enviar correo.

Sin tener en cuenta los recursos necesarios para crear estas listas, tanto humanos como temporales, en determinados escenarios, como grandes corporaciones, altamente dinámicas, este proceso puede resultar, sencillamente, muy difícil de llevar a cabo.
Por otra parte, cualquier cambio en el direccionamiento de los servidores de correo, así como la adición de un nuevo servidor o la baja de uno de ellos, deben ser notificados.

2. Yahoo!: DomainKeys

DomainKeys, al igual que *SenderID*, es un e**squema de autenticación de correo electrónico**. Fue diseñado en 2004 por Mark Delany, *de Yahoo*, y, en la actualidad, es aplicado en todos los correos enviados y recibidos por esta compañía. Google también ha comenzado a utilizarlo recientemente para su servicio de correo Gmail.

Modo de funcionamiento

DomainKeys es, en cierta manera, superior a SenderID pues **utiliza criptografía de clave pública para autenticar el remitente y receptor del correo, así como su integridad**, es decir, que no ha sido modificado en tránsito desde su envío.

Al igual que *SenderID*, necesita que los dueños de cada dominio añadan un campo especial, que contiene su clave pública, en los registros DNS de estos dominios. Esta clave se utilizará más adelante, como veremos a continuación, para verificar la procedencia de los correos.

El proceso puede resumirse en los siguientes **pasos:**

1. El cliente de correo saliente añade una cabecera llamada «DomainKey-Signature» que contiene una firma digital de los contenidos del mensaje.
2. El servidor de correo receptor realiza una petición DNS especial. En la respuesta, entre otra información, recibe una copia de la clave pública del dominio remitente.

3. El receptor puede ahora comprobar la firma del correo recién recibido. Si la firma se verifica, puede tener la seguridad de que el correo fue enviado desde el dominio correcto y que éste no ha sido modificado desde su envío.

Ventajas e inconvenientes

A pesar de *DomainKeys*, al igual que *SenderID*, exige de los administradores un cierto trabajo para su puesta en marcha, es un esquema mucho más robusto. Si un dominio cambia la dirección IP de su servidor de correo, circunstancia que puede resultar muy habitual, añade un nuevo servidor o da de baja uno de ellos, DomainKeys no necesita que se realicen modificaciones en su infraestructura. SenderID, por el contrario, necesitaría que se actualizaran los registros SPF de los servidores de nombres correspondientes.

Esta ventaja puede resultar decisiva a la hora de que una solución u otra sea adoptada por la mayoría de los responsables de sistemas.

Comparativa de *SenderID* y *DomainKeys*			
Técnica	**Tipo de defensa**	**Autenticación**	**Flexibilidad/ Escalabilidad**
SenderID	Autenticación origen	Por dirección IP	Baja
Au	Autotenticación origen	Clave pública	Alta

Resumen de técnicas

En la práctica, ninguna de las medidas de protección que hemos analizado en los puntos anteriores es definitiva ni se utiliza en solitario.

Es muy común recurrir a una **solución combinada**, que utiliza varias de las técnicas anteriores. **Un escenario típico podría incluir listas negras y blancas, junto con un filtro bayesiano adecuadamente entrenado.**

Sin embargo, aunque tampoco son la solución definitiva, l**os filtros bayesianos destacan en efectividad** del resto de contramedidas analizadas. En la actualidad pueden alcanzar tasas de detección superiores al 95%, eso sí, con un entrenamiento adecuado.

Teniendo en cuenta que, además, las técnicas utilizadas por los *spammers* para tratar de eludir estos filtros cambian continuamente, la efectividad del mismo bajará con el tiempo si no sigue siendo entrenado periódicamente. De hecho, se estima que en un mes aparecen 3 nuevas técnicas de ocultación u ofuscación de contenidos por parte de los *spammers*, con el fin de eludir la técnicas anti-*spam* actuales.

9.9. Spam exótico

Lo cierto es que la imaginación de los spammers por evitar los filtros no tiene límites. En esta sección veremos algunos ejemplos de «casos exóticos» de spam, que rozan límites casi humorísticos.

Codificación del mensaje en archivos adjuntos

Como hemos visto, ya se utilizan habitualmente por los *spammers* técnicas para codificar el contenido de los mensajes en imágenes, archivos PDF u otros formatos, como hojas de cálculo y archivos de texto.

La siguiente ilustración muestra un **mensaje *spam* codificado en un archivo de** texto y, a su vez, **incluido en un archivo ZIP**, con el fin de tratar de evitar el filtro anti-*spam*:

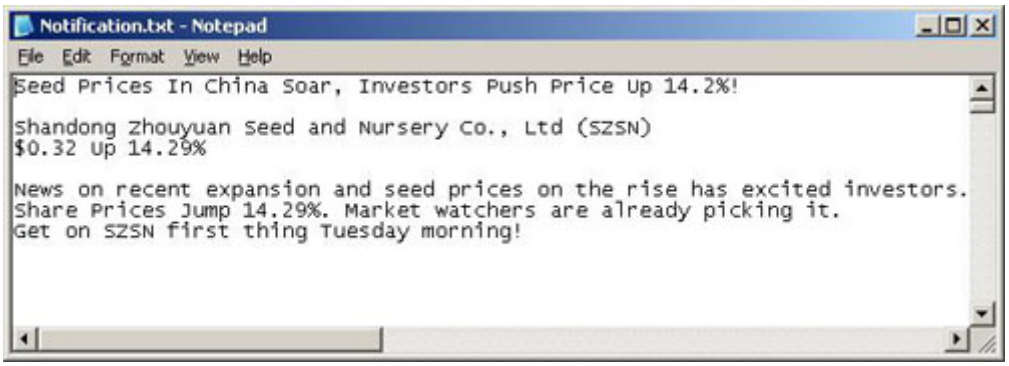
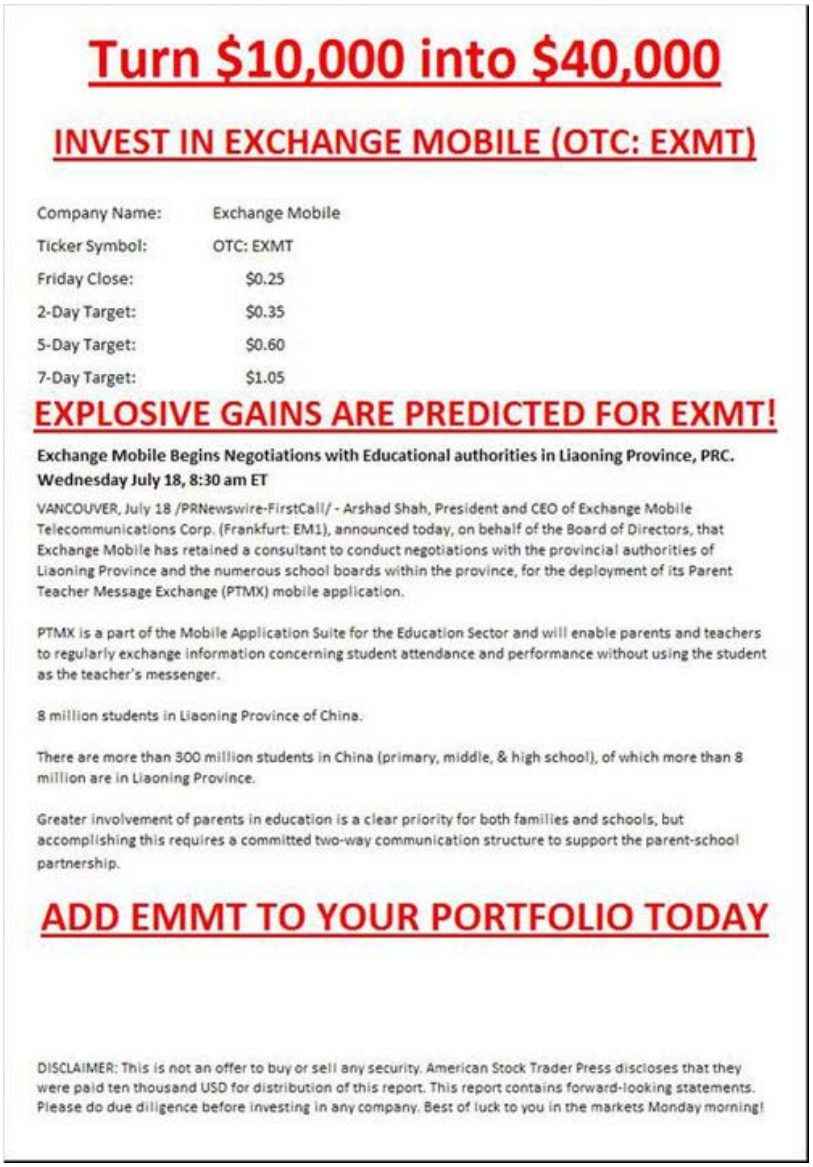


Figura 8. Mensaje de *spam* en un adjunto de texto y comprimido en un archivo ZIP

Por supuesto, los *spammers* no se limitan a un tipo de archivo adjunto. El siguiente ejemplo ilustra el mensaje escrito en una hoja de cálculo:



Turn $10,000 into $40,000

INVEST IN EXCHANGE MOBILE (OTC: EXMT)

Company Name:	Exchange Mobile
Ticker Symbol:	OTC: EXMT
Friday Close:	$0.25
2-Day Target:	$0.35
5-Day Target:	$0.60
7-Day Target:	$1.05

EXPLOSIVE GAINS ARE PREDICTED FOR EXMT!

Exchange Mobile Begins Negotiations with Educational authorities in Liaoning Province, PRC. Wednesday July 18, 8:30 am ET

VANCOUVER, July 18 /PRNewswire-FirstCall/ - Arshad Shah, President and CEO of Exchange Mobile Telecommunications Corp. (Frankfurt: EM1), announced today, on behalf of the Board of Directors, that Exchange Mobile has retained a consultant to conduct negotiations with the provincial authorities of Liaoning Province and the numerous school boards within the province, for the deployment of its Parent Teacher Message Exchange (PTMX) mobile application.

PTMX is a part of the Mobile Application Suite for the Education Sector and will enable parents and teachers to regularly exchange information concerning student attendance and performance without using the student as the teacher's messenger.

8 million students in Liaoning Province of China.

There are more than 300 million students in China (primary, middle, & high school), of which more than 8 million are in Liaoning Province.

Greater involvement of parents in education is a clear priority for both families and schools, but accomplishing this requires a committed two-way communication structure to support the parent-school partnership.

ADD EMMT TO YOUR PORTFOLIO TODAY

DISCLAIMER: This is not an offer to buy or sell any security. American Stock Trader Press discloses that they were paid ten thousand USD for distribution of this report. This report contains forward-looking statements. Please do due diligence before investing in any company. Best of luck to you in the markets Monday morning!

Figura 9. *Spam* con el formato de una hoja de cálculo

Cabe esperar que estos métodos sigan siendo activamente explotados por los *spammers*, incluyendo modificaciones, como distorsiones en las imágenes, para dificultar su detección.

Codificación en archivos de audio

Uno de los casos más curiosos consiste en **mandar mensajes codificados en archivos de audio MP3 adjuntos**. Estos mensajes están compuestos de un fichero MP3 de 30 segundos, grabado a un bajo nivel de bits y con una voz femenina sintética que se dedica a promocionar un determinado producto. Dicha voz llega a los usuarios de forma muy distorsionada para evitar así su detección por medio de sistemas anti- spam basados en firmas.

Lo + recomendado

No dejes de leer...

A survey of machine learning techniques for spam filtering

Saad, O., Darwish, A., & Faraj, R. (2012). A survey of machine learning techniques for spam filtering. *IJCSNS International Journal of Computer Science and Network Security*, *12*(2), 66-73.

Desarrollo de distintos enfoques científicos creados para detener el spam con el filtrado como la parte más importante y popular.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
http://paper.ijcsns.org/07_book/201202/20120211.pdf

Mapa en tiempo real del envío de spam

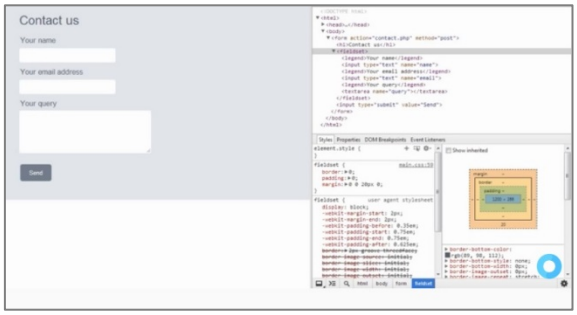
En los enlaces que encontrarás abajo podrás observa un curioso mapa en el que se muestra en tiempo real (o casi, es actualizado cada 60 minutos), cuál es el origen de spam en el mundo. Obviamente, sólo se muestran las grandes remesas capturadas por cada una de las empresas.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
http://www.spamshield.org/maps/spamworld.html
http://www.google.es/intl/en/insidesearch/howsearchworks/fighting-spam.html

No dejes de ver...

Prevent automated form spam

En este vídeo se explica cómo evitar de forma automática el spam.



Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=rYBomZIzrS4

La lucha de Google contra el spam

En este video podremos conocer de primera mano, a través de Matt Cutts, director del departamento de spam de *Google*, cómo esta empresa lucha contra este problema. Matt cuenta cómo es el día a día en la vida de un técnico anti-spam en el buscador, y responde a la pregunta sobre cómo actuan exactamente para clasificar un correo como spam o no.

Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=yPZwpGWc7L0

+ Información

A fondo

SpamAssasin

SpamAssasin es quizás la herramienta más utilizada y conocida por los administradores de sistemas para luchar contra el *spam*. Se trata de una herramienta libre y gratuita que se utiliza en combinación con el servidor de correo corporativo. En la siguiente URL podrás encontrar un breve tutorial sobre su funcionamiento e instalación.

Accede al documento a través del aula virtual o desde la siguiente dirección web: http://www.solvetic.com/tutorials/article/218-instalando-y-configurando-spamassassin-en-un-servidor/

Test

1. Uno de los métodos utilizados por los *spammers* para generar direcciones de correo es la generación automática por fuerza bruta. En este sentido, ¿te parece que una dirección de correo corta es más probable que reciba spam?

A. Sí, de acuerdo a algunos estudios
B. No, existen estudios que demuestran que no hay relación
C. Sólo si la cuenta de correo ha sido utilizada alguna vez
D. Sólo si la cuenta ha sido publicada en Internet o utilizada en algún foro

2. Una de las técnicas más sencillas y utilizada para publicar una dirección de correo en Internet y que no sea víctima del spam es:

A. Elegir con cuidado en qué lugar publicamos la dirección
B. Generar un gráfico con la dirección en lugar de texto plano
C. Utilizar una cuenta que no sea personal, para mantenerla libre de spam
D. Utilizar direcciones desechables, que pueden cambiarse fácilmente

3. El proceso de envío de los correos comienza cuando ya se tienen una lista grande de direcciones. ¿Cuál es la técnica más utilizada para este envío?

A. Externalizar el envío a terceras partes, que cobran por el mismo
B. ISP dedicados
C. El uso de botnets
D. Servidor de correo propio

4. Algunas de las contramedidas aconsejadas para evitar que nuestro ordenador se convierta en parte de una botnet son:

A. Utilizar software antivirus actualizado
B. Mantener los equipos actualizados y correctamente parcheados
C. Bloquear el tráfico de salida del puerto 25, utilizado por SMTP
D. Todas las respuestas anteriores son ciertas

5. Una de las siguientes técnicas **no** es utilizada por los spammers para refinar sus listas de direcciones de correo. ¿Puedes identificar cuál?

A. Pruebas de lectura
B. Páginas de baja de direcciones
C. Instalación de malware
D. Correos de confirmación

6. Una de las técnicas de protección contra el spam masivo es el uso de listas negras de orígenes. ¿En qué consiste esta contramedida?

A. Es una lista de máquinas que alguna vez han recibido spam
B. Es una lista de máquinas que pertenecen a una botnet
C. Es una lista de máquinas de las que se tiene la certeza, o sospecha muy fundada, que están siendo utilizadas por spammers
D. Es una lista de máquinas que contienen los filtros anti-spam

7. Los filtros bayesianos son otra de las grandes herramientas en la lucha contra el spam. ¿Cómo funcionan?

A. Calculan la probabilidad de que un correo haya sido remitido por un servidor de correo conocido por enviar spam habitualmente
B. Calculan la probabilidad de que un correo sea spam o no haciendo uso del Teorema de Bayes
C. Calculan la probabilidad de que un correo contenga palabras de una lista clasificada como spam, haciendo uso del Teorema de Bayes
D. Es una técnica que mezcla el enfoque de lista negra y blanca de los orígenes

8. ¿Cuál es uno de los principales inconvenientes de los filtros bayesianos?

A. Que necesitan de una fase de entrenamiento, lo que, en determinados entornos, puede ser problemático
B. Pueden ser atacados como otras contramedidas (envenenamiento bayesiano)
C. Pierden eficacia con el tiempo, aunque hayan sido bien entrenados en su instalación
D. Tienen una tasa de eficacia bastante baja, no muy superior a otras técnicas

9. Al margen de las motivaciones económicas, técnicamente el envío de spam es posible debido básicamente a:

A. La existencia de las botnets, que es el método más utilizado para el envío de spam

B. La falta de seguridad de los servidores de correo, que hace que sean fácilmente comprometidos

C. La falta de autenticación del protocolo de envío de correo electrónico, STMP

D. Algunos errores de implementación en los protocolos de envío de correo electrónico

10. Algunas de las técnicas más exóticas utilizadas por los spammers incluyen:

A. El envío de imágenes en lugar de texto para tratar de evitar los filtros

B. El envío de correos con archivos adjuntos

C. Las dos respuestas anteriores

D. El envío de correos sólo a direcciones verificadas como auténticas