SPAM: hoy, ahora y... ¿siempre?

SPAM: hoy, ahora y... ¿siempre?

Autor: Cristian Borghello, Technical & Educational Manager de ESET para Latinoamérica

Cuando se trata de persuadir a los usuarios para guiarlos de alguna manera a caer en la trampa, quienes están detrás de ello depositan mucha imaginación en la elaboración del engaño. Esto ocurre por una única razón: el dinero que potencialmente pueden ganar.

El caso del correo basura, correo electrónico no deseado o simplemente spam, es un muy buen ejemplo para describir cómo se actualizan constantemente las técnicas utilizadas por los delincuentes.

Ya no importa de qué manera se presente el mensaje ni que tan prolijo sea, ni la delicadeza de los detalles que tenga. Lo realmente importante es que el spam llegue a la bandeja de entrada. Una vez allí, existe cierta probabilidad de que el usuario haga clic en él e incluso intente comprar o invertir en algunas de las maravillas que se ofrecen.

Haciendo un repaso por las técnicas utilizadas por los spammers se pueden citar los siguientes hitos importantes:

1. El correo es enviado masivamente en formato texto. Es el primer tipo de spam que se empezó a sufrir y en su gran mayoría correspondía al texto plano con publicidades de diversos productos. El mayor desafío de los spammers era pasar los filtros de texto que comenzaron a perfeccionarse en esa época.

Imagen 1 – Spam

2. Al perfeccionarse los filtros antispam, se comienza a deformar el texto, de modo de engañar a los filtros, pero no al ojo humano que igualmente es capaz de leer el texto sin mayores complicaciones.

Imagen 2 – Spam con modificaciones. Notar “v1agra” y “c1al1s” así como el texto extraño al medio de la frase

3. La siguiente etapa estuvo (y está) dada por el perfeccionamiento de la técnica anterior en donde los textos se deforman al grado tal de ser difícilmente legibles. En esta etapa, también aparecen correos que incluyen publicidad con textos de conocidos libros y autores para confundir a los filtros.

Imagen 3 - Spam con texto confuso

- La siguiente y reciente etapa, corresponde a los correos masivos con imágenes adjuntas, preferentemente .GIF animados en donde se incorpora movimiento para llamar la atención del lector.

Imagen 4 – Spam en imágenes

Esta nueva etapa se caracteriza por dos situaciones:

- Los filtros no estaban preparados para este tipo de imágenes con texto y por ende, no eran filtrados hasta el momento en que se perfeccionaron dichos filtros mediante técnicas de

reconocimiento de caracteres (OCR).

- El usuario igualmente recibe un texto que es capaz de leer.

Este tipo de correos es enviado por spammers que trabajan con la bolsa (compra y venta de acciones). Esta técnica es conocida por pump-and-dump y consiste en que los atacantes adquieran un cierto número de acciones de bajo valor de alguna empresa conocida, o no. Luego, envían mensajes (spam) recomendando la compra de estas acciones. Quienes compren las acciones provocarán una suba del precio de las mismas. En este momento proceden a vender las acciones que compraron a bajo precio, asegurando su ganancia y el perjuicio de los inocentes debido a que la venta masiva produce una baja del precio de la acción.

- La etapa actual consiste en el envío de correos con otro tipo de adjuntos como pueden ser: archivos comprimidos (.zip, .rar, otros), documentos de ofimática (.doc, .xls, otros) o archivos portables (pdf, fpdf, otros). Si bien suele confundirse este tipo de adjuntos con el malware, lo que se envía es un archivo de texto con las mismas ofertas mencionadas anteriormente.

-

Imagen 5 – Spam en documentos

- Por último, el spam es el principal medio de propagación del malware (archivos comprimidos y/o ejecutables) y correos de phishing actual. Todos ellos tienen en común que poseen un archivo adjunto o un enlace en el cuerpo del correo.

Es importante remarcar que todas estas técnicas son actualmente utilizadas en forma conjunta para distintos fines:

- Publicidad de productos (farmacéuticos, placeres sexuales, artículos de colección, electrónicos, etc)
- Compra y venta de acciones
- Propagación de malware
- Realización de Phishing

- Estafas nigerianas (scam)

- Ingeniería Social para obtener información sensible

-

Cualquier otra forma de comunicación que involucre que el usuario deba realizar alguna acción

A continuación, puede verse un gráfico con las estadísticas de cada tipo:

Imagen 6 – Tipos de spam

Entonces, luego de lo analizado se puede concluir que el correo no deseado puede dividirse en los siguientes tipos:

- Correo con texto solamente
- Correo con imágenes adjuntas (publicidad, no dañino)
- Correo con documentos adjuntos (publicidad, no dañino)
- Correo con archivos dañinos adjuntos
- Correo con enlaces a publicidad en el cuerpo del correo
- Correo con enlaces a archivos dañinos
- Correo con enlaces a sitios de phishing

Como puede verse, el correo electrónico no deseado ya no es para nada novedoso, si bien actualiza sus técnicas constantemente. Sin embargo, se sigue recibiendo día a día más y más spam que llena la bandeja de entrada, al punto que en algunas estadísticas ya se estima que 9 de cada 10 correos son basura virtual, generando un costo elevado a quienes lo reciben (servidores involucrados, el ISP y el cliente).

Pero, ¿por qué existe el spam? Esta pregunta se traduce en un sencillo problema de oferta y demanda. Actualmente, si bien no se encuentran demasiadas estadísticas fiables, existen personas (clientes) que consumen los productos ofrecidos a través del

spam por necesidad, curiosidad o por el motivo que fuera. A modo de ejemplo:

En el estudio “[FONT='Tahoma','sans-serif']Profiting from fake pharma” [1][font], se afirma que sólo el comercio de medicamentos conocidos alcanza un importe aproximado a los 4.000 millones de dólares al año (y algunas empresas aseguran que sería mucho mayor). En el estudio realizado por MarkMonitor también se asegura que estos sitios tienen una media de 32.000 visitas diarias.

En otro estudio [2] se encuestó a 2.482 usuarios adultos resultando que un 17% había sido víctima de scam, un 81% abría mensajes de correo electrónico no solicitado y un 58% desconocía la existencia de este tipo de amenazas en la red.

Pero estos alarmantes números son sólo parte de la respuesta. La otra parte, corresponde al que realiza la oferta del producto. Muchas empresas prefieren realizar publicidad a través de correos masivos porque el precio de los mismos es irrisorio con respecto a cualquier otro tipo de publicidad existente en la actualidad. A continuación, se puede ver una tabla comparativa:

Imagen 7 – Estadísticas de publicidad

Otra de las causas de la gran cantidad de spam es que, al ser el correo electrónico un medio de comunicación rápido y eficiente, es el medio adecuado para propagar cualquier tipo de amenaza que tenga como objetivo sistemas informáticos.

El spam es sólo una de las piezas que conforman a todo un ciclo delictivo que por detrás encierra una verdadera organización de delincuentes informáticos. Este ciclo delictivo comienza al momento en que intentan, con alguna técnica de Ingeniería Social [3], convencer al usuario de hacer clic sobre algún enlace, abrir un archivo o instalar algún tipo de malware en el sistema.

Imagen 8 – Ciclo detrás del spam

A continuación se convence al usuario de la “buena oportunidad” para la compra de productos, se instala algún tipo de gusano o troyano en el sistema, o bien se lo

incita a entrar a un sitio para que ingrese sus datos privados (usuario, claves, documento, tarjeta, etc).

Actualmente todos nos encontramos en el medio de este círculo vicioso en donde la proliferación de spam con adjuntos dañinos tienen el objetivo de infectar a más usuarios para producir equipos zombies que pasan a formar parte de una red que, manipulada por delincuentes, produce más spam [4].

¿Por qué se sigue recibiendo este tipo de correos y qué se puede hacer para evitarlo o, por lo menos, ayudar a cortar la cadena?

Si bien la respuesta puede parecer obvia: cortando o eliminando una de las piezas que conforman el ciclo antes mencionado, la solución práctica es más difícil de concretar que de pensarla.

A continuación, se procede a desglosar el problema en etapas más pequeñas, de modo que cada una de ellas contribuya a una solución integral:

Responsabilidad del usuario

La recolección de correos es una de las principales necesidades de los spammers. Para ello se valen de diferentes técnicas [5].

La responsabilidad del usuario descansa en no “regalar” su dirección de correo para disminuir en forma notable la cantidad de spam que potencialmente podría llegarle. Debido a que las bases de datos de correos se comercializan, con ingresar a una sola lista es suficiente para figurar en cientos de bases de datos.

Es por ello que resulta necesario el uso correcto del correo electrónico para evitar que las direcciones de correo caigan en manos de delincuentes [6].

También es una buena práctica instalar un filtro antispam en el sistema que se utiliza a diario de modo de filtrar los correos que no haya filtrado el servidor.

Responsabilidad de las organizaciones

Aquí las responsabilidades cambian absolutamente con respecto a las del usuario, aunque las buenas prácticas en el uso del correo electrónico se deben mantener.

Para comenzar, las organizaciones que proveen correo electrónico a sus empleados, son responsables de este servicio y en consecuencia del aseguramiento de los servidores de correo electrónico. Lamentablemente, es común que las organizaciones no configuren adecuadamente sus servidores, generando que usuarios no autorizados (spammers) los encuentren y

los utilicen como servidores de correo basura.

El siguiente punto corresponde a los filtros antispam que deben aplicarse en los servidores de correo y gateways para que elimine gran parte del correo basura que llega a los buzones del usuario. Estos filtros actualmente se han convertido casi en una necesidad inevitable en cualquier organización que desee que sus empleados no pasen gran parte del día eliminando correo basura de sus buzones.

Responsabilidad del ISP (Internet Service Provider - Proveedor de Servicios de Internet)

En el caso de estas empresas, es fundamental que sigan las mismas buenas prácticas de cualquier organización, pero al ser proveedores del servicio de Internet, se torna fundamental que controlen el tráfico en sus cuentas de correo para detectar a posibles spammers dentro de su red o a aquellos usuarios particulares que puedan pensar que enviar publicidad de su producto es una buena idea.

Conclusiones

El correo basura vive entre nosotros desde hace tiempo y hasta que no se logre trabajar interdisciplinariamente -legislativa, judicial y técnicamente- será muy difícil lograr una solución que pueda considerarse definitiva.

Está en cada uno de los involucrados ser responsables tanto de no ser víctima ni participante activo (formando parte de una botnets) de la generación de spam como de la aplicación de correctos filtros y barreras anti-spam que ayuden a filtrar y disminuir, aunque sea en parte, este ataque del que es víctima día a día nuestro buzón y cuyo objetivo es violar nuestra privacidad y obtener nuestro dinero.