Una amenaza creciente

NORMAN®

Una amenaza creciente

Nunca antes fue tan fácil comunicarse con la mayor parte de la población del mundo de forma casi instantánea. El correo electrónico se ha convertido en la principal forma de comunicación de negocios y empresas de todos los tamaños.

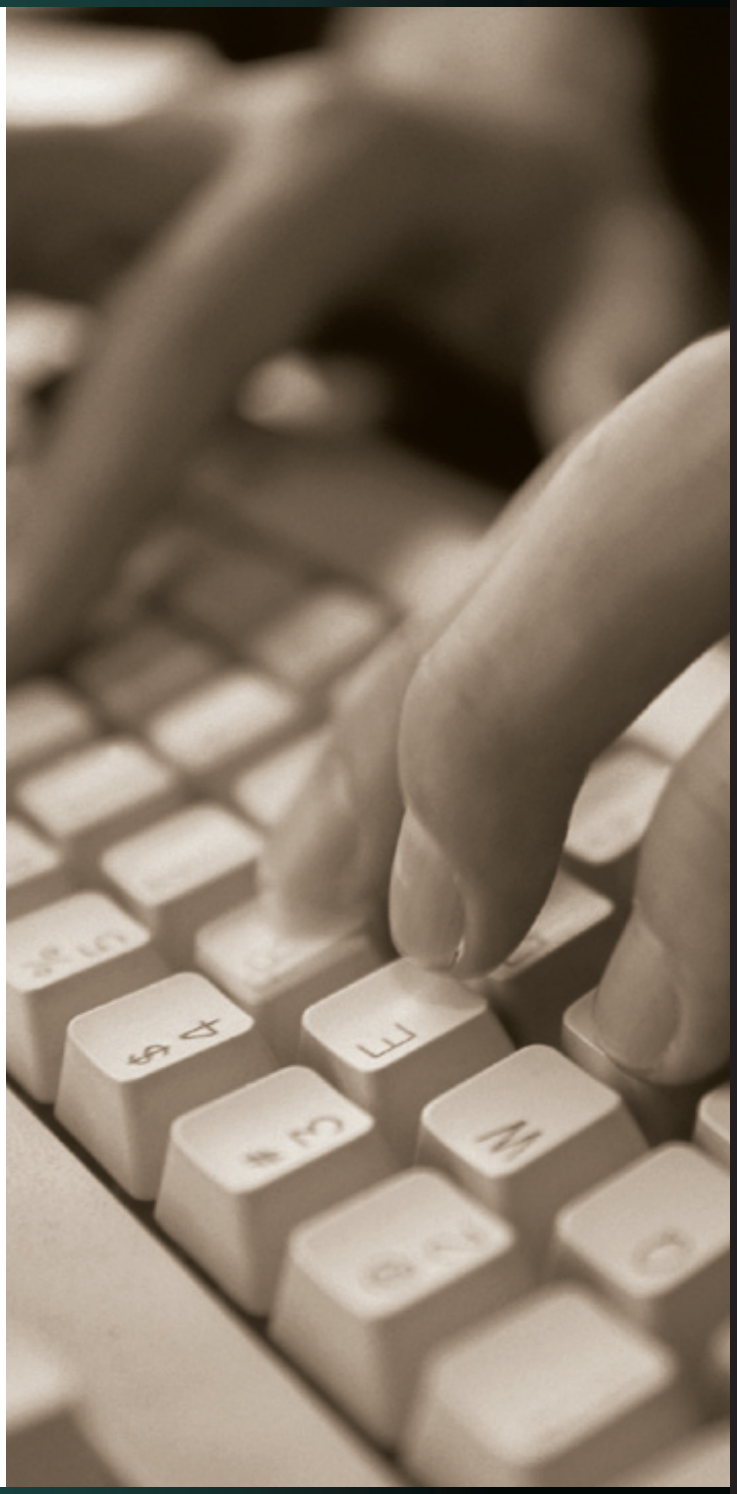
No obstante, todo lo bueno tiene su lado malo que, en el caso del correo electrónico, es el spam.

Como hemos observado, el spam representa más del 80% de todo el tráfico de correo electrónico y este número continúa creciendo. Una de las principales razones de este aumento espectacular es el spam basado en imágenes, una molestia cada vez más frecuente y sofisticada que supone más del 25% de todo el spam.

El spam de imágenes resulta difícil de bloquear, ya que los filtros del correo electrónico no pueden leer los mensajes con imágenes incrustadas. Por este motivo, los emisores de spam consiguen evitar los filtros con facilidad enviando una variación de la misma imagen para cada campaña de spam.

Los emisores de spam combinan esta técnica, denominada serialización de imágenes, con el uso de equipos o redes zombi (ordenadores infectados que controlan en secreto) para transmitir el spam. Mediante la combinación de estos dos métodos, los emisores de spam confunden a la mayoría de las tecnologías antispam existentes en el mercado.

Para las empresas, el spam ha dejado de ser una simple cuestión de productividad. El spam expone a los empleados a posibles fraudes y la empresa tiene la responsabilidad de proteger a sus empleados. Para los administradores de sistemas, la batalla contra el spam se libra en varios frentes:



❶ Resulta más difícil detectar el spam de imágenes
- El departamento técnico dedica más tiempo a afinar los filtros convencionales del correo electrónico

❷ Un mensaje de spam de imágenes suele ser bastante más grande que un mensaje de spam basado en texto.
- Un mensaje de spam basado en texto tiene un tamaño de unos 5 a 10 KB mientras que un mensaje de spam de imágenes suele estar entre 10 y 70 KB
- Por lo tanto, el departamento técnico debe asignar un ancho de banda y capacidad de almacenamiento muy superiores para su infraestructura de correo electrónico.

❸ Se tarda más en analizar los mensajes de spam de imágenes
- El departamento técnico puede necesitar actualizar o sustituir las plataformas existentes para obtener la capacidad de procesamiento necesaria.

Si no se administra y gestiona debidamente, el spam de imágenes puede saturar las redes, lo que reduce espectacularmente el tiempo de respuesta y afecta a otras aplicaciones críticas de la empresa.

El spam representa más del 80% de todo el tráfico de correo electrónico y este número continúa creciendo.

Una amenaza en evolución

El spam de imágenes es de aparición relativamente reciente. Cuando se introdujeron por primera vez, estos mensajes no contenían mensajes.

En vez de ello, las imágenes se cargaban desde internet mediante URL ocultas. Como la mayor parte de los filtros del correo electrónico buscaban palabras clave, estos mensajes de spam conseguían atravesarlos.

A medida que las soluciones de filtrado del correo electrónico empezaron a incorporan el uso de listas URL de bloqueo de spam en tiempo real (SURBL) o auténticas bases de datos de URL, los emisores de spam de imágenes se vieron obligados a mejorar sus métodos. Comenzaron a incrustar la imagen en el mensaje, evitando los enlaces URL para salvar los filtros.

Este último punto plantea una pregunta: ¿Por qué alguien que reciba este tipo de spam de imágenes copiaría o escribiría la URL indicada en su navegador web? Para responder esta pregunta, debemos analizar la naturaleza de los mensajes de spam de imágenes. Mientras que unos promocionan Viagra a bajo precio, por ejemplo, la mayoría de ellos son mensajes de especulación financiera donde los emisores del spam invierten primero en una acción y, después, envían spam para elevar (inflar) su precio. El objetivo consiste en aumentar el precio de la acción antes de vender (soltar) los valores al precio inflado. No hace falta ningún enlace, solo un gancho que insta a llamar a nuestro agente bursátil. Muchas víctimas caen en esta trampa de «dinero fácil». Para empeorar la situación, los especuladores se benefician del alza que rodea a la campaña de spam para obtener beneficios.

No todos los mensajes de especulación financiera utilizan spam de imágenes, pero se mueven en esta dirección, como explicamos en el informe técnico correspondiente. Los mensajes de especulación financiera están extendiéndose tanto que, el 8 de marzo de 2007, la SEC suspendió la cotización de 35 empresas que habían sido objeto de recientes y repetidas campañas de spam1.

Esto resalta los posibles beneficios de estos fraudes y explica por qué los emisores de spam son tan ingeniosos a la hora de pensar en la manera de evitar las técnicas de filtrado. Por ejemplo, para evitar la técnica del análisis de huellas (fingerprinting), los emisores de spam comenzaron a enviar una imagen única y ligeramente distinta cada vez modificando el formato de imagen, añadiendo píxeles, texturas, etc. Varios filtros de correo electrónico han probado a utilizar tecnología de reconocimiento óptico de caracteres (OCR) para identificar mensajes incluidos en los gráficos. Aunque este esfuerzo requiere una capacidad de procesamiento muy superior, los emisores de spam han aprendido a evitar la tecnología OCR variando las fuentes y fondos o utilizando patrones moteados para que el mensaje sea perfectamente legible para el ojo humano pero irreconocible para una máquina. En este interminable juego del ratón y el gato, el spam de imágenes disfraza ahora palabras o frases clave en una imagen o incluye texto que no se considera spam al final del mensaje. Esta parte de texto, que suele denominarse «ensalada de palabras», contiene palabras enlazadas entre sí pero sin significado alguno. Con frecuencia, los emisores de spam utilizan pasajes de obras literarias o copias de notas de prensa. Esta técnica engaña a la mayoría de los filtros antispam al reducir la probabilidad de que el mensaje se considere spam debido al gran número de palabras con sentido. Otro método cada vez más popular es el uso de archivos GIF animados y con capas que dividen los mensajes en varias imágenes que apilan una encima de otra. Los emisores de spam combinan estas tecnologías con el uso de equipos o, peor todavía, redes zombie (botnets) para realizar la serialización del spam de imágenes.

El spam basado en imágenes representa más del 25% de todo el spam.

1. Para obtener más información, consulte la nota de prensa de la SEC en http://www.sec.gov/news/press/2007/2007-34.htm

¿Una amenaza imbatible?

En un esfuerzo de mitigar el spam de imágenes, las empresas podrían bloquear todos los mensajes que contengan imágenes o archivos adjuntos para evitar que lleguen a la bandeja de entrada de los usuarios. No obstante, para la mayor parte de las empresas, esta medida resultaría demasiado drástica, ya que los empleados pueden enviar y/o recibir mensajes que contengan imágenes (como firmas con el logotipo de la empresa).

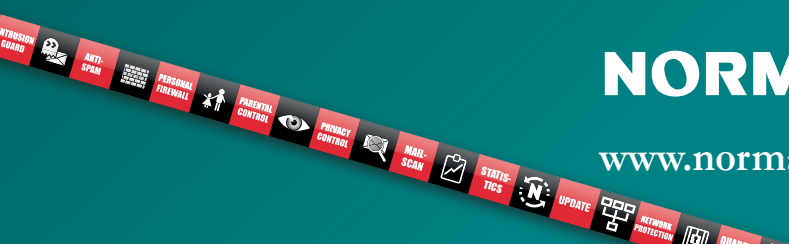
Con la variedad de técnicas que emplean los emisores de spam para evitar los filtros antispam, una solución satisfactoria sería combinar varios métodos, incluidas tanto medidas bien probadas como otras nuevas y adaptables dirigidas a amenazas específicas. Para luchar contra el spam de imágenes, son esenciales tres estrategias de filtrado:

1. **Defensa perimetral:** proporciona un solo punto de entrada para limitar las formas en las que el spam se introduce en la red e incluye una serie de funciones de análisis del emisor, como camas de autenticación, validación y acreditación del emisor.
2. **Análisis de mensajes:** Tbusca patrones de spam reconocidos (como URL incrustadas), analizando la forma en la que están construidos los mensajes y qué características de la red tomaron parte en su entrega.
3. **Análisis de imágenes:** examina el contenido y el formato de las imágenes, comparándolas con imágenes de spam conocidas o con imágenes de seguimiento para evitar nuevas oleadas de spam de imágenes. Aunque son esenciales, estas técnicas de filtrado no deben estar solas en la lucha contra el spam de imágenes. No deben pasarse por alto dos aspectos importantes:
1. **Análisis humano:** no es recomendable depender en exclusiva de la tecnología OCR para luchar contra el spam de imágenes, ya que las soluciones automáticas no suelen ser infalibles. El análisis humano es necesario para mejorar las tasas de detección o para corregir los inevitables errores debidos a las decisiones de máquinas.
2. **Tecnología preparada para el futuro:** el spam de imágenes es simplemente el último asalto del combate entre los emisores de spam y los usuarios del correo electrónico. A medida que los emisores de spam cambian continuamente sus tácticas y técnicas, las soluciones de filtrado del correo electrónico deben confiar en diseños flexibles para ofrecer las capacidades de ampliación necesarias para enfrentase a las amenazas modernas, así como la flexibilidad y capacidad de ampliación imprescindibles para luchar contra las amenazas futuras.

El análisis humano es necesario para mejorar las tasas de detección.

Norman ASA

Norman ASA, fundada en Oslo (Noruega) en 1984, es una empresa líder global y pionera en soluciones de seguridad proactiva del contenido y en herramientas de diagnóstico del malware. Norman ofrece analizadores de malware, soluciones de protección de terminales y seguridad de redes para satisfacer las necesidades de seguridad de los clientes. Las soluciones de Norman están disponibles a través de las filiales de Norman y de una red de socios en todo el mundo.



NORMAN®

www.norman.com