El desafío del spam

Informe de la Internet Society

También conocido como comunicaciones electrónicas no solicitadas, el spam representa para los usuarios de Internet una amenaza perjudicial, costosa y en permanente evolución. Los gobiernos pueden ayudar a reducir el impacto del spam, disuadiendo a quienes lo originan por medio de leyes y medidas de aplicación eficaces, esfuerzos antispam que involucren a múltiples partes interesadas, la adopción de mejores prácticas y la educación de los ciudadanos sobre los peligros del spam.

Introducción

El spam, esos mensajes de correo electrónico no solicitados que saturan nuestras bandejas de entrada, constituyen un desafío para los usuarios de Internet, para las empresas y también para los formuladores de políticas. Hay diferentes estimaciones, pero hay quienes sugieren que cada día se envían más de 100 mil millones de mensajes de spam, lo que representaría hasta un 85 por ciento del tráfico diario de correo electrónico a nivel mundial.[1]

El término *spam* generalmente se refiere a las comunicaciones electrónicas no solicitadas (típicamente mensajes de correo electrónico) o, en algunos casos, a las comunicaciones comerciales no solicitadas que se envían indiscriminadamente.[2] Algunos se refieren a este tipo de mensajes como *correo basura*. Si bien la actividad de spam toma mayormente la forma de mensajes de correo electrónico, el spam es una amenaza que evoluciona y se ha extendido a prácticamente todos los tipos de mensajes electrónicos, incluso a los mensajes SMS, a las publicaciones en los medios sociales, a los sistemas de mensajería instantánea y a los foros en línea .

Más allá de la molestia y el tiempo que se pierde a causa de los mensajes no deseados, el spam puede causar daños significativos, infectando las computadoras de los usuarios con software malicioso capaz de dañar los sistemas y robar información personal. También puede consumir recursos de la red.

Hoy en día, algunos de los tipos más comunes de spam perjudicial son los mensajes que buscan realizar alguna estafa financiera, los mensajes de correo electrónico con software de phishing[3], malware de botnets[4] y/o ransomware.[5] Los spammers son muy inventivos e incansables. Permanentemente se dedican a crear señuelos cada vez más atractivos para atraer a los usuarios y convencerlos de abrir mensajes que

---

[1] Cisco Systems, sistema de monitoreo de amenazas en tiempo real SenderBase, http://www.senderbase.org

[2] Artículo 7 del Reglamento *de Telecomunicaciones Internacionales, Conferencia Mundial de Telecomunicaciones Internacionales de la* UIT, http://www.itu.int/pub/S-CONF-WCIT-2012/en

[3] Por lo general, el phishing es un intento de adquirir información confidencial (nombres de usuario, contraseñas, detalles de tarjetas de crédito) haciéndose pasar por una entidad de confianza en una comunicación electrónica.

[4] *Malware* es un término que se utiliza para referirse a diferentes formas de software hostil o invasivo, entre ellas virus, gusanos, troyanos y otros programas maliciosos que infectan la computadora del usuario con diversas formas de código ejecutable, *scripts*, contenido activo y otros tipos de software invasivo.

[5] *Ransomware* es un tipo de malware que exige el pago de un rescate para eliminarlo de la computadora infectada.

contienen malware. Y continúan buscando nuevas listas de direcciones de correo electrónico y nuevos medios de comunicación para atacar.

Consideraciones clave

Los gobiernos de todo el mundo están tomando medidas legales para combatir el spam, aunque hasta ahora estos esfuerzos son más habituales entre los países occidentales y desarrollados. Esto podría deberse a que estos países debieron enfrentar antes la amenaza del spam. Los países que han adoptado legislación sobre el spam también han definido lo que consideran spam. Estos países han declarado el spam ilegal, ofrecido educación a los consumidores sobre cómo gestionar el spam y, en algunos casos, promulgado y utilizado medidas de aplicación para disuadir a los spammers. El resultado ha sido un descenso considerable del spam interno, como se confirmó en los Países Bajos en 2010. Luego de que el gobierno holandés promulgara una ley antispam, los usuarios de este país vieron una disminución del 85 por ciento en el spam doméstico.[6] Sin embargo, los spammers podrían haberse trasladado a países donde no existen leyes antispam. Además de la legislación nacional de los diferentes países, también existe una comunidad internacional conocida como Plan de Acción de Londres (LAP) que trabaja para promover la cooperación internacional en materia de spam y otros temas relacionados.[7]

Los operadores de redes y la comunidad técnica han desarrollado mejores prácticas para gestionar las amenazas a la seguridad de la red, entre ellas el spam. Por ejemplo, el M^{3}AAWG (*Messaging, Malware, and Mobile Anti-Abuse Working Group*)[8] produce documentos sobre los enfoques y herramientas disponibles para hacer frente a los problemas de seguridad, tales como la descripción de los pasos que se deben tomar para una mejor gestión del impacto del spam en una red.[9] El Proyecto Spamhaus[10] rastrea las operaciones y fuentes de spam para proveer a las redes de Internet protección en tiempo real y trabaja con las fuerzas de seguridad para combatir el spam. También existen organizaciones nacionales e internacionales que trabajan en diferentes formas de mejorar la gestión del spam, entre ellas la GSMA (Asociación *Groupe Speciale Mobile*), los Registros Regionales de Internet (RIR), la Unión Internacional de Telecomunicaciones (ITU) y la Internet Society.

Hay una gran variedad de herramientas para bloquear spam que pueden mejorar la forma en que los usuarios enfrentan el tema. Sin embargo, sin importar qué tan eficaz sea la tecnología de bloqueo de spam, los usuarios finales siempre tendrán que estar atentos a la posibilidad de recibir mensajes maliciosos, ya que ninguna herramienta es perfecta y los spammers están siempre inventando nuevas formas de enviar mensajes no deseados. También puede ser difícil para los usuarios reconocer si un mensaje es malicioso. El informe publicado por Verizon en 2015 titulado *Data Breach Investigations Report* indica que el 23 por ciento de quienes reciben mensajes de correo electrónico de phishing los abren y que el 11 por ciento hace clic en los archivos adjuntos, comprometiendo así sus equipos y sistemas en red.[11]

---

[6] Exitosa legislación antispam en los Países Bajos, https://www.spamexperts.com/about/news/dutch-anti-spam-law-has-success

[7] Plan de Acción de Londres, http://londonactionplan.org

[8] Información sobre el M^{3}AAWG (*Messaging, Malware, and Mobile Anti-Abuse Working Group*), https://www.maawg.org/published-documents

[9] En junio de 2015, el M^{3}AAWG y el Plan de Acción de Londres publicaron Operación red de seguridad: Mejores prácticas para abordar las amenazas en linea, móviles y en telefonía, https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf

[10] Información sobre el Proyecto Spamhaus: https://www.spamhaus.org/

[11] Verizon Corporation, *2015 Data Breach Investigations Report,* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015-insider_en_xg.pdf

Desafíos

Desde una perspectiva general, para muchos países el spam constituye un desafío técnico, económico y de seguridad en constante evolución. Como tal, se requiere un enfoque multifacético para hacer frente a los retos que plantea. Específicamente, el problema del spam presenta los siguientes desafíos:

- El spam es un problema costoso tanto para la infraestructura de Internet como para sus usuarios. Grandes volúmenes de spam consumen valiosos recursos de red y son una carga particularmente importante en países con acceso a Internet y ancho de banda limitados. Los proveedores de servicios de Internet (ISP) invierten grandes esfuerzos para gestionar este tráfico, mientras que los usuarios finales deben estar atentos y evitar abrir spam que contenga malware o estafas. En el caso de los abonados a servicios de datos móviles y quienes están suscritos a servicios medidos, el costo de recibir o enviar una gran cantidad de mensajes de spam sin saberlo puede ser significativo. Además, la reparación de los sistemas infectados y/o atacados por el malware entregado por mensajes de correo no deseados tiene un costo y también hay costos asociados con los datos robados a los usuarios.
- En general, la economía del spam se inclina fuertemente a favor de los spammers. Enviar mensajes no solicitados cuesta muy poco; de hecho, la mayoría de los costos son cubiertos por los destinatarios de los mensajes, los ISP, los usuarios infectados o los operadores de redes.
- La naturaleza del spam cambia a medida que se introducen nuevas aplicaciones y formas de intercambiar datos en Internet. Los spammers avanzan en su capacidad de utilizar estas plataformas para entregar mensajes más invasivos y perjudiciales con el fin de robar datos personales, dañar las redes e infectar los sistemas.
- El spam afecta a una amplia gama de usuarios de Internet. No existe ninguna organización que pueda resolver por sí sola las amenazas que presenta el correo no deseado, sino que lo que se necesita es una comunidad mundial de múltiples partes interesadas trabajando juntas para resolver el problema.
- Más allá del daño directo a los usuarios y la carga sobre los recursos de red, el correo no deseado también crea —de manera sutil— una falta de confianza entre los usuarios y hay quienes lo ven como un obstáculo que limita el uso de Internet y el comercio electrónico. También se debe considerar el impacto potencialmente negativo sobre la reputación de un usuario cuya identidad sea robada por los spammers y utilizada para enviar spam.
- Las comunidades que participan en la implementación de medidas antispam pueden ser objeto de represalias (por ejemplo, víctimas de ataques de denegación de servicio distribuidos (DDoS), hacking), por lo que es importante que los miembros de las comunidades globales antispam no solo ofrezcan asistencia para combatir el spam, sino que también proporcionen apoyo técnico y de otro tipo contra posibles represalias.

Principios rectores

La Internet Society cree que un enfoque de colaboración entre todas las partes interesadas pertinentes permitirá lograr las mejores soluciones para mitigar el spam y proteger la seguridad de los usuarios. Este enfoque general se enfatiza en los principios de Seguridad Colaborativa de la Internet Society, que hacen hincapié en la responsabilidad compartida y colectiva entre todas las partes interesadas para lograr los resultados deseados.[12]

[12] Internet Society's Collaborative Security Principles, http://www.internetsociety.org/collaborativesecurity

Los gobiernos pueden ayudar a combatir el spam de las siguientes maneras:

- **Comprendiendo el cambiante panorama del spam.** Los métodos que los spammers utilizan para diseminar mensajes de correo electrónico maliciosos está en constante evolución. Los gobiernos deben esforzarse por mantenerse al día con las técnicas, tendencias y amenazas del spam. Los gobiernos también pueden desempeñar un papel clave apoyando investigaciones sobre identificación, rastreo y mitigación del spam y otras amenazas en línea, además del desarrollo de mediciones pertinentes en las cuales se puedan apoyar los formuladores de políticas. Los gobiernos también pueden fomentar el uso de métodos que respeten la privacidad de los usuarios y permitan el intercambio de información sobre riesgos y amenazas entre las partes interesadas, en tiempo real.
- **Generando alianzas con otras partes interesadas para lograr el éxito.** El spam es un problema polifacético. Son varias las partes interesadas que desempeñan un papel y deben participar en el desarrollo de estrategias, buenas prácticas y enfoques para la aplicación de medidas antispam, incluido el desarrollo de herramientas para mitigar el spam y el malware. Se deben desarrollar iniciativas de coordinación y alianzas entre los actores del sector público y privado a fin de producir soluciones robustas para el problema del spam. Las entidades que a las que sería útil involucrar incluyen las coaliciones y los grupos de trabajo antispam (por ejemplo, el M^{3}AAWG), los equipos de respuesta a incidentes de seguridad informática, los operadores de redes, los proveedores de Internet y de servicios en línea, la comunidad técnica de Internet, los grupos empresariales y de defensa al consumidor, la sociedad civil y otros grupos que tengan interés en combatir el spam, el malware y otras actividades maliciosas en línea.
- **Promulgando legislación y medidas de aplicación apropiadas.** Como ya se ha señalado, la legislación antispam, fuertes leyes de protección al consumidor y fuertes medidas de aplicación pueden ayudar a disuadir a los infractores y reducir la cantidad de spam enviado y recibido en un país.[13] Las agencias gubernamentales encargadas de hacer cumplir las leyes y reglamentos antispam deben contar con recursos suficientes, dar a conocer los resultados de las medidas de aplicación y hacer que sea más fácil para los usuarios de Internet denunciar la distribución de spam y malware.
- **Colaborando con sus pares a nivel internacional.** El spam es un problema que atraviesa fronteras. Colaborar con otros gobiernos en la aplicación de esfuerzos antispam, entre ellos acciones de cumplimiento internacionales, es fundamental para abordar con éxito la proliferación mundial del spam.
- **Educando y empoderando a los ciudadanos.** Los gobiernos deben apoyar iniciativas de los sectores público y privado que eduquen a los usuarios de Internet sobre cómo reconocer y protegerse contra el spam y otras amenazas en línea. Los usuarios de Internet también deben ser conscientes de su derecho legal de reclamar compensación por las pérdidas o daños causados por el spam ilegal y otras actividades maliciosas en línea.

[13] En http://www.spamlaws.com el lector encontrará una exhaustiva fuente de información sobre legislación antispam. Entre las herramientas que ofrece la Internet Society para combatir el spam (http://www.internetsociety.org/spamtoolkit) también se incluyen enlaces a los enfoques legislativos adoptados por diferentes países.

Recursos adicionales

La Internet Society ha publicado una serie de documentos y contenido relacionado con este tema. Estos materiales se pueden descargar de forma gratuita de nuestro sitio web.

> Herramientas de la Internet Society para combatir el spam, www.internetsociety.org/spamtoolkit

> Internet Society, Spam y amenazas en línea (curso de e-learning), http://www.internetsociety.org/what-we-do/inforum-learn-online/inforum-course-spam-and-online-threats

> Una breve guía sobre spam, http://internetsociety.org/spam/short-guide-spam

> Historia del spam, http://www.internetsociety.org/doc/history-spam

> Cómo combatir el spam: Enfoques desde las políticas, enfoques técnicos y enfoques desde la industria, http://www.internetsociety.org/doc/combating-spam-policy-technical-and-industry-approaches

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva, Switzerland
Tel: +41 22 807 1444 • Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave., Suite 201
Reston, VA 20190 USA
Tel: +1 703 439 2120 • Fax: +1 703 326 9881
Correo electrónico: info@isoc.org

bp-spam-20151030-es