EL RECORRIDO DE UN CLICK:
Análisis total de la cadena de valor del "spam".

Fuente: Universidad de California

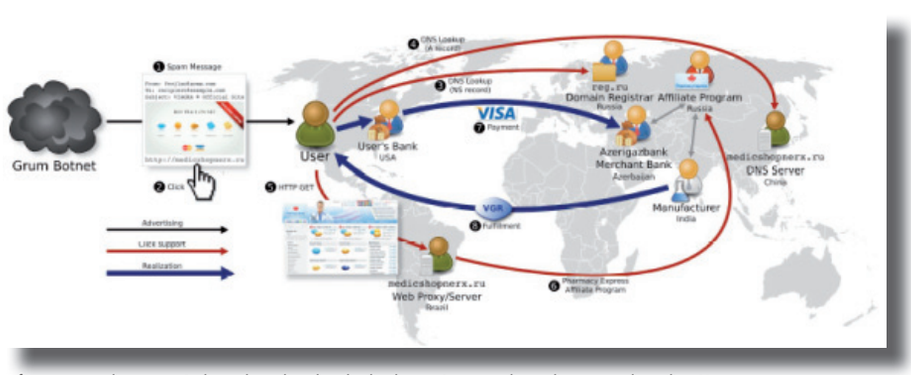
Un grupo liderado por analistas informáticos de las Universidades de California, han realizado recientemente un estudio en profundidad sobre un fenómeno presente de forma continua en el universo de mensajería electrónica: los conocidos como "*spam*", mensajes basura o no deseados.

Los anuncios o propuestas difundidas a través del "*spam*" son un negocio, que ha generado aparte de una gran irritación, una industria "*anti-spam*" multimillonaria, que no consigue más que seguir auto-alimentándose. Falta, en general, un conocimiento sólido de las estructuras de este fenómeno y, por eso, la mayor parte de las intervenciones "*anti-spam*" se dirigen a una sola faceta de su cadena de valor, por ejemplo, al filtrado de mensajes, a crear listas negras de URLs, a eliminar sitios de internet, etc.).

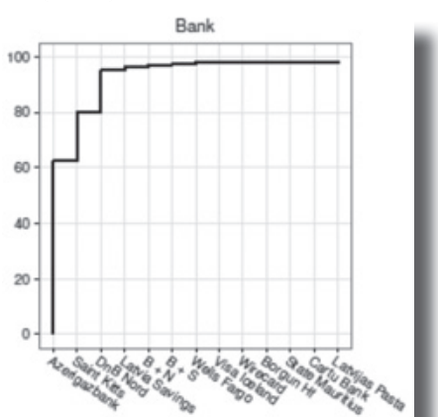
El estudio en cuestión ha realizado un análisis holístico que cuantifica el completo abanico de recursos empleados para monetizar los correos "*spam*" (nombres, alojamientos, pagos y cumplimiento), utilizando datos referentes a tres meses sobre diferentes "*spam*", amplio seguimiento a las infraestructuras de nombres y alojamientos y más de 100 compras en sitios anunciados a través de "*spam*". Se han pasado estos datos a las organizaciones que se ocupan de estas materias y utilizado para caracterizar las correspondientes propuestas de intervención defensiva en cada eslabón de su cadena de valor. Sobre todo, se ha hecho evidente que existe una concentración importante en esta cadena de valor: el 95% de los anuncios "*spam*" para venta de productos farmacéuticos, reproducciones y software, se monetizan a través de los servicios mercantiles de solo un puñado de bancos.

A título de ejemplo concreto, esquematizado en la imagen, se presenta el ciclo de compra de un producto farmacéutico a través de uno de esos medios. Un 27 de octubre, desde un emisor de "*spam*" se recibió y estudió un correo titulado *VIAGRAR Official Site*. El mensaje incluía una imagen de productos farmacéuticos para aumentar la potencialidad masculina y sus precios correspondientes, así como la posibilidad de conexión. Cuando se pulsaba dirigía directamente al usuario al dominio asociado (medicshopnerx.ru), registrado por REGRU-REG-RIPN (a.k.a.reg.ru) ese mismo mes de octubre. El servidor que facilitaba el nombre del servicio residía en **China**, mientras que el alojamiento se hallaba en un servidor de **Brasil**. Si el usuario continúa el ciclo, recibe un contenido de la tienda *Pharmacy Express*, asociada al programa farmacéutico basado en **Rusia**.

Después de seleccionar un producto y pulsar "*checkout*", la tienda redirige al usuario al portal de pago payquickonline.com, esta vez en un servidor con dirección en **Turquía**, que acepta el envío, el email de contacto y la información de pago, facilitando un número de confirmación de pedido. A continuación remite un correo confirmando el pedido, número de seguimiento y una dirección de contacto para preguntas del cliente. El banco que emitió la tarjeta de crédito del usuario transfirió el importe al banco que lo ingresa, en este caso el *Azerigazbank Joint-Stock Investment Bank* de Baku (**Azerbaijan**). Diez días más tarde, el producto llegó en un sobre acolchado, con indicación postal de haber sido remitido por un proveedor llamado PPW con dirección en Chennai (**India**).



Infraestructura de una particular cadena de valor, desde el anuncio, pasando por las etapas de realización.



Bancos involucrados en cobro de compras hechas en anuncios "spam"

Los autores estiman que los datos obtenidos por su estudio pueden facilitar el diseño de las intervenciones necesarias y ofrecen la evidencia de que la etapa de pagos es, con mucho, la más concentrada del sistema y sobre la que sería de actuación más efectiva para la intervención pública en los países occidentales. ■

NOTA: Se puede acceder al estudio completo en el vínculo:
http://www.revistadyna.com/dyna/documentos/noticiasweb/20110831_spam.pdf