El correo basura, las *botnet* y las redes sociales

Hace 40 años, en 1971, el programador Ray Tomlinson creó un sistema para enviar mensajes entre máquinas en el que se indicaba el nombre del usuario seguido de la arroba @ y el nombre del equipo. Tomlinson decidió utilizar la arroba porque en inglés se pronuncia como «at» (en) y de esta forma señalaba el nombre del usuario y el del equipo en el que se encontraba ese usuario. Y así se sigue usando. De aquel primer correo electrónico a los billones de hoy. Algunos datos sobre los correos electrónicos enviados por Internet en el año pasado:

- A lo largo del año se enviaron en el mundo 107 billones de correos electrónicos, más de 3.000.000 cada segundo.
- De todos los enviados, el 89% fueron basura (*spam*), unos 262.000 millones cada día.
- El año se cerró con más de 1.000 millones de usuarios de correo electrónico, con una media de 3 cuentas por usuario.
- A cada usuario le corresponden 293 correos de media al día. De ellos, 261 son basura.

Si esta ingente cantidad de correo basura no llega a nuestros buzones es gracias a la excelente calidad del *software* específico de filtrado del correo electrónico. Para inundar las redes de correo basura son necesarios cientos de miles de ordenadores infectados con troyanos que los secuestran y los convierten en zombis para ser controlados remotamente. Las posibles vías de infección de ordenadores con estos troyanos llegan a través páginas web maliciosas, correos electrónicos con archivos adjuntos especialmente manipulados o con enlaces a páginas web maliciosas, programas obtenidos a través de sistemas de intercambio de archivos, enlaces en redes sociales, o virus propagados con el uso de las memorias USB.

Los secuestradores de estas máquinas comprometidas normalmente las agrupan de miles en miles para controlarlas, creando así redes de ordenadores denominadas *botnets*. Una *botnet* (robot+net) es una colección de máquinas zombis controladas por cibercriminales.

- El 77% del correo basura se envía usando las *botnets*.
- Puede haber en el mundo unos 5 millones de ordenadores zombis, agrupados en *botnet* de decenas de miles o cientos de miles de ordenadores cada una.
- Cada máquina zombi suele llegar a enviar entre 70 y 150 correos por minuto.
- La *botnet* llamada Rustock, desmantelada en marzo de 2011, constaba de más de 1.100.000 máquinas zombis. Cada una podía enviar unos 150 correos por minuto.

¿Quienes y para que usan los servicios de las *botnets* enviando *spam*? Es decir, ¿quienes son los *spammers*? Aunque varía de un año al siguiente, durante 2010 su distribución fue:

- 64,2% productos farmacéuticos. Sugieren hacer clic en un enlace a una web.
- 9,3% envío de información no solicitada.
- 7,0% casinos y juegos de azar.
- 6,5% artículos de diseño falsos, especialmente a final del año.
- El resto incluye ofertas de empleo, sobre todo muleros, sexo y contactos, *software*, diplomas y títulos, *phising*, etc.

Pero, como indica Sergio de los Santos de Hispasec, Facebook, con 600 millones de miembros en mayo del 2011 y Twitter, con más de 200 millones, se están convirtiendo en la plataforma preferida para difundir ataques, por encima del correo tradicional. El *spam* tradicional pierde efectividad porque cada vez hay mejores filtros de correo y porque el internauta se ha concienciado e ignora los mensajes de publicidad que puedan llegar a su buzón. Si es que no han sido previamente filtrados. Facebook y Twitter son el nuevo objetivo de los *spammers*. En Facebook más del 15% de los mensajes con enlaces que circulan son *spam*. En las redes sociales un gran porcentaje de la gente visita los enlaces (en teoría se fían más), mientras que por correo electrónico apenas consiguen ratios del 0,00001% de incautos. Así que para conseguir unos beneficios similares en las redes sociales los atacantes necesitan enviar mucha menos cantidad de mensajes. En realidad la basura se desplaza, no desaparece.

Jesús Sanz

http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers
http://www.symanteccloud.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf
http://www.m86security.com/labs/spam_statistics.asp
http://en.wikipedia.org/wiki/Rustock_botnet
http://www.hispasec.com/unaaldia