Los Botnets - Los zombis: ¿Y eso es informática?

Cuando hace una temporada oí hablar de los "zombis" me sonaba a ese tipo de personas que nos cuentan que han sido manipuladas en ceremonias tipo vudú y que solo pensarlo da cierto repelús. Más tarde se piensa en esas películas en las que aparecen retornados a la vida de mala cara y peor aspecto, pero nada que ver con un PC, ni con una Tableta ni con un portátil, smartphone ni nada por el estilo.

¿Qué son los "botnets" - "zombis"?

Se conoce como zombi un ordenador o una PC como dicen los hispano hablantes (término más correcto que el de ordenador, dicho sea de paso) que está siendo manejado o manipulado a distancia por alguien sin que nosotros lo sepamos.

Es simple: han convertido nuestro ordenata en un servidor, en una máquina al servicio de otros mediante algún tipo de programilla que se ha instalado sin nosotros saberlo, bien sea "spyware" o Troyanos (ver el capitulillo de los "espías") y que usan nuestra máquina para enviar correo basura, programas indeseables e indeseados, spam o correo masivo no solicitado y todo tipo de operaciones "delictivas" de este estilo y como nuestro aparatillo es un "zombi" pues hace eso, lo que le manden, sin protestar además.

En **Wikipedia** se puede leer:

Botnet *es un término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota y normalmente lo hace a través del IRC. Las nuevas versiones de estas botnets se están enfocando hacia entornos de control mediante HTTP, con lo que el control de estas máquinas será mucho más simple.*

Y también:

Zombis*: Grupos organizados pueden llegar a controlar grupos de decenas de miles de computadores infectados, zombis, que pueden usar para generar grandes cantidades de tráfico proveniente de multitud de fuentes en Internet, dirigido a una sola red o servidor. Esto genera lo que se conoce como un Distributed Denial of Service o DDoS por sus siglas. Esto suele ser usado para chantajear a las víctimas, que deben pagar una suerte de peaje para mantener sus servicios en la red.*

Por lo general –aunque no sólo- suelen ser PCs que disponen de banda ancha (ADSL o similar), que no se han preocupado mucho de actualizar su software y sus antivirus y que no usan para nada medidas de protección, quizás porque no saben o quizás (y conozco a varias personas) por dejadez. He apuntado antes lo de la conexión de banda ancha porque el número de horas de conexión es mayor y el trasiego de información también.

Cómo será el problema que los gigantes informáticos ya hablan de serio problema,

http://www.seguridad.unam.mx/noticias/?noti=1652.
http://www.idg.es/pcworld/noticia.asp?idn=43956
http://www.vsantivirus.com/mydoom-zombie.htm
http://es.norton.com/botnet
http://www.eset-la.com/centro-amenazas/amenazas/2235-Botnets

Muchos de los virus más dañinos como el mydoom, en el fondo lo que hacían era convertir las redes de ordenadores o de PCs en zombis, las llamadas ***botnet*** que no es otra cosa que NET= red y BOT = robot, es decir, una red de robots.

Hoy día además, con eso de la computación en la nube (cloud computing) la amenaza es superior y la alarma está encendida y si a alguien puede interesarle basta bajarse y leer el pdf:
http://www.sophos.com/es-es/medialibrary/Gated%20Assets/white%20papers/sophosbotnetswpna.pdf

¿Por qué he hablado de Microsoft?

Microsoft hizo un experimento: dejó un ordenador sin protección, no quisiera pensar que como muchos de los de los lectores de este articulillo, y estudió lo que sucedía. El resultado fue que en menos de un mes desde el exterior habían accedido a él varios **millones** de… llamémosles "visitantes" que a su vez lo usaron para mandar entre 15 y 20 millones de mensajes de correo no deseado.

Pero no solo es Microsoft, hoy en día, las unidades de las policías de los diferentes países luchan contra el "spam" o correo no deseado, engañoso, o como se quiera llamar.

¿Y dónde van esos mensajes? A nuestros buzones de correo, naturalmente, muchos de los cuales acumulan tal cantidad de ellos que resultan inviables. En otras ocasiones nos presentan mensajes engañosos incluso diciéndonos que nuestro ordenador está infectado o que el mismo Bil Gates nos avisa de que hay que actualizar el sistema operativo o no sé qué programa para el correcto funcionamiento del mismo.

Tras el susto que se llevaron los responsables de la Seguridad en Internet de Microsoft analizaron y encontraron varios puntos de origen, contra los cuales, como aparece en una de las direcciones a visitar que aparecen anteriormente citadas, interpusieron demanda judicial y ahí siguen con denuncias y demás pleitos porque no se habla de uno ni de dos, se habla de muchos miles de PCs zombis, de muchas redes de botnets, de millones y millones de correo "spam" que sale y se distribuye a diario para vendernos las direcciones de correo actualizadas para venderles nuestro servicio hasta ropa, aparatos electrónicos o viagra, para el caso es lo mismo.

Hay que defenderse

Si en muchos casos la mejor defensa es un ataque, en este no sirve. Aunque respondiéramos a la dirección desde la que se nos vende la última novela o el barco de recreo, nos daríamos cuenta de que por lo general nadie contesta y eso cuando no te viene devuelto porque no existe o directamente te avisan de que No-reply (no responder). Al día siguiente recibimos lo mismo desde otra y así sucesivamente.

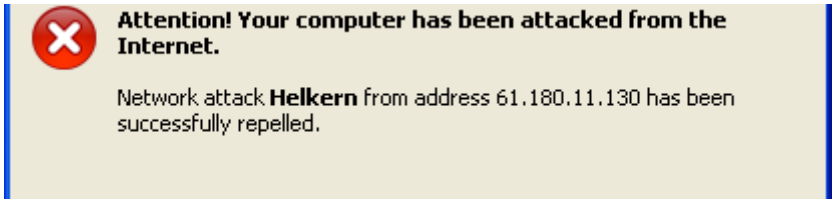
¿Qué hacer?

Pues es fácil:

1º.- Actualizar el antivirus, la mayoría de ellos ya trae algún sistema de protección añadido como un cortafuegos, anti malaware o similares.

2º.- Tener un cortafuegos: Son programillas que evitan que alguien que anda buscando agujeros por los que colarse no encuentren el nuestro. Los hay de uso doméstico, gratuitos y eficaces. Yo usaba el Zone Alarm y me fue bien. El Sistema operativo suele traerlo incorporado, pero también las soluciones antivirus.

Un ejemplo: en mi pantalla ha saltado una alarma que copio:



En mi caso, el cortafuegos ha funcionado. La traducción vendría a ser:

Atención! Su PC ha sido atacado desde Internet.
Ha sido atacado desde la dirección 61.180.11.130 y ha sido repelida con éxito.

Ese número que aparece ahí es como el carné de identidad de la máquina que intentó acceder a mi ordenador, es decir, que se puede saber de dónde viene, en este caso:

(**61.180.11.130**) está localizada en Milton, Australia

3º .- No abrir los adjuntos que me lleguen si no me avisan de que me los envían. Y pueden decirnos que han descubierto que nuestro sistema está infectado, que tenemos que actualizar el antivirus (hablo de que en el correo nos avisan de ello = desconfiar)

4º.- No ir a visitar aquellas direcciones que me llegan en los correos electrónicos. En ocasiones vienen en correo de personas conocidas. Aun así mejor preguntarle al remitente antes de abrirlo para evitar sorpresas desagradables..

5º .- Muchas personas mantienen este tipo de rutinas, pero se olvidan de ellas cuando están "chateando" en foros abiertos o cuando lo hacen con sus amigos a través de los sistemas de mensajería instantánea como MSN, Yahoo Messenger, AOL, y otros similares. No hacerlo puede evitarnos repetirnos el viejo refrán que dice que "de aquellos lodos estos barros".

6º.- Está de moda bajarse cosas de Internet: imágenes, archivos, presentaciones de PPT/PPS, archivos en flash que son "mu monos" o "mu grasiosos" que diría mi sobrina y que son "mu peligrosos" si no se mantienen las debidas protecciones. Cuantas veces tal o cual MP3, o programita que hemos bajado con los programas de P2P como Emule (la mula), Edonkey (el burro o la burra), Kazaa, Torrent y tantos otros, lejos de ser un programa, canción, mini video, PPS que esperamos, es un troyanito que se nos colará con nuestro permiso. Tal vez a más de uno se nos quede la cara un poco así, como de tonto, al no entender qué había allí. Le dimos, hizo como que empezaba a instalarse, incluso se nos abrió alguna ventana fugazmente y … ¡¡Y ya la hemos liado!!

Por tanto volver al primer punto: Pasarle el antivirus actualizado antes de cualquier acción. Aquí el refrán que más vale es el de "vale más prevenir que lamentar", desconfiar de correos, de mensajes, instalar solo lo que queremos instalar. Si algo nos dicen que es gratuito y cuando pretendo bajarlo me piden un número de móvil no es trigo limpio. Y así podría continuar con otros muchos de los mensajes que nos llegan a diario.

Jose Carlos. jcmontalban@gmail.com