BOTNETS ¿QUÉ ES UNA RED DE ORDENADORES ZOMBIS?

Botnet o red de ordenadores zombis es el conjunto formado por ordenadores infectados por un tipo de software malicioso, que permite al atacante controlar dicha red de forma remota. Los equipos que integran la red se denominan "zombis", o también *drones*.

La ciberdelincuencia suele estar detrás de estas *botnets*, con manifestaciones tan comunes como el spam o el ataque combinado a sitios web (Ataque de Denegación de Servicio Distribuido, DDoS).

Este fenómeno ha experimentado un crecimiento continuado desde 2006, año en que los creadores de malware provocaron su proliferación y su influencia a la vista de la rentabilidad que proporcionan los negocios ilícitos en Internet, hasta llegar en la actualidad a las 6.000 botnets repartidas por todo el mundo[1]. Un ejemplo de la gran trascendencia que tienen las redes de ordenadores zombis es la detención en marzo de 2010 de la *botnet* "Mariposa"[2], cuya influencia abarcaba a trece millones de ordenadores en 190 países.

I Compartir recursos

Como se indica en la introducción, los fines ilícitos motivan el crecimiento de las *botnets*, a pesar de que el modelo utilizado, la **informática distribuida**, está creado para entornos empresariales e institucionales, con fines productivos. Este sistema utiliza en red una serie de equipos organizados por un administrador para realizar tareas complejas de una forma coordinada y sostenible.

En este sentido, el poder de cómputo de estas redes supera el de los superordenadores en la resolución de problemas complejos en un tiempo razonable. Además, puede utilizar sistemas heterogéneos (Windows, Linux, Mac, etc.), combinándolos de la forma más eficiente.

Las empresas y grandes compañías disponen de estas redes de ordenadores y el trabajo del administrador de la red, en estos casos, es controlar el resto de ordenadores de los usuarios para poder administrar, manipular, actualizar y gestionar la red.

Más aún, su potencial ha permitido la creación de iniciativas de repercusión global. A continuación se muestran varios ejemplos:

[1] Disponible en: http://www.imatica.org/bloges/2010/03/260358542010.html
[2] Disponible en: http://www.elpais.com/articulo/tecnologia/Cae/red/cibercriminal/Mariposa/controlaba/millones/ordenadores/zombis/190/paises/elpeputec/20100302elpeputec_8/Tes

- *Distributed.net* es un proyecto destinado a comprobar la seguridad de los algoritmos de cifrado más conocidos. Voluntarios prestan de forma altruista la potencia de sus máquinas para procesar datos del algoritmo de cifrado elegido. Esta acción se realiza mediante un sistema distribuido donde a cada voluntario se le asigna una tarea y es coordinada por un servidor.

- SETI, o la *Búsqueda de Inteligencia Extraterrestre*, es otro esfuerzo distribuido que trata de determinar si hay vida inteligente en el Universo. Su proyecto *SETI@Home*, al igual que el anterior, utiliza ordenadores personales de usuarios voluntarios que ceden los recursos de su ordenador (por ejemplo, Internet) mientras no lo están utilizando, para que el organismo aproveche estos recursos y pueda procesar los datos producidos en sus radiotelescopios internacionales.

- BOINC, *Programas de código abierto para computación voluntaria y computación en red*[3], es un proyecto científico para utilizar el potencial de ordenadores personales de todo el mundo para la investigación en múltiples campos (salud, clima, etc.).

La nota común en los diferentes ejemplos de infraestructuras distribuidas es el **conocimiento** por parte de los usuarios de su inclusión (la de su equipo) en una red para realizar determinadas tareas con **fines beneficiosos** para la sociedad.

Por el contrario, **en el caso de las redes de ordenadores zombis** estas características se invierten y se observa cómo un controlador utiliza una serie de equipos **sin su consentimiento** (ni conocimiento) **con un propósito fraudulento**. El ciberatacante instala un cliente en el equipo del usuario (como en el caso de SETI), asegurándose el uso remoto del mismo para alojar programas maliciosos de fraude online en la web, distribuir material pornográfico, o realizar ataques a empresas en base a sus contenidos en Internet, por ejemplo. La ciberdelincuencia, por tanto, ha aprovechado el poder de la informática distribuida para provocar una evolución en sus prácticas, aumentando la envergadura de sus redes y sus consecuencias.

II Formación de una *botnet* y funcionamiento

Aunque los métodos de creación y desarrollo del funcionamiento de una *botnet* son muy variados, se identifican una serie de **etapas comunes** en la vida útil de este tipo de redes:

1. El creador de la *botnet* diseña la red que va a crear, definiendo los objetivos y los medios necesarios que va a emplear, incluido el sistema de control de la red.

[3] Disponible en: http://boinc.berkeley.edu/

2. Además necesitará un malware que se aloje en los equipos y permita el control del mismo, denominado *bot*, que frecuentemente es un troyano. Este malware puede ser creado por él mismo (el creador de la red) o puede comprar este *bot* a un creador de malware.

3. El siguiente paso consiste en distribuir el malware o *bot* por cualquier método: correo basura, páginas con vulnerabilidades, ingeniería social, etc. El objetivo final es que las víctimas ejecuten el programa y se infecten. En la mayoría de las ocasiones el propio troyano se propaga por sí mismo, y es capaz (como los gusanos tradicionales, pero diseñados específicamente para formar parte de una red concreta una vez infectados) de llegar a otros sistemas desde un sistema infectado a su vez. Si tiene éxito, el número de zombis puede llegar a crecer exponencialmente.

4. Una vez que el atacante consigue una masa crítica suficiente de sistemas infectados, puede conseguir el propósito buscado al programar el sistema. Algunas de estas actuaciones pueden ser:

    - Robar información de los equipos infectados.
    - Enviar correo basura o spam.
    - Realizar ataques combinados a una página web o ataques de denegación de servicio distribuido.
    - Construir servidores web para alojar material ilícito (pornográfico y/o pedofílico), realizar ataques de fraude online (*phishing*), alojar software malicioso.
    - Distribuir o instalar nuevo malware.
    - Crear nuevas redes de equipos zombis.
    - Manipular juegos online.
    - Observar lo que la víctima hace si el programa ofrece la posibilidad de visionado de escritorio remoto.

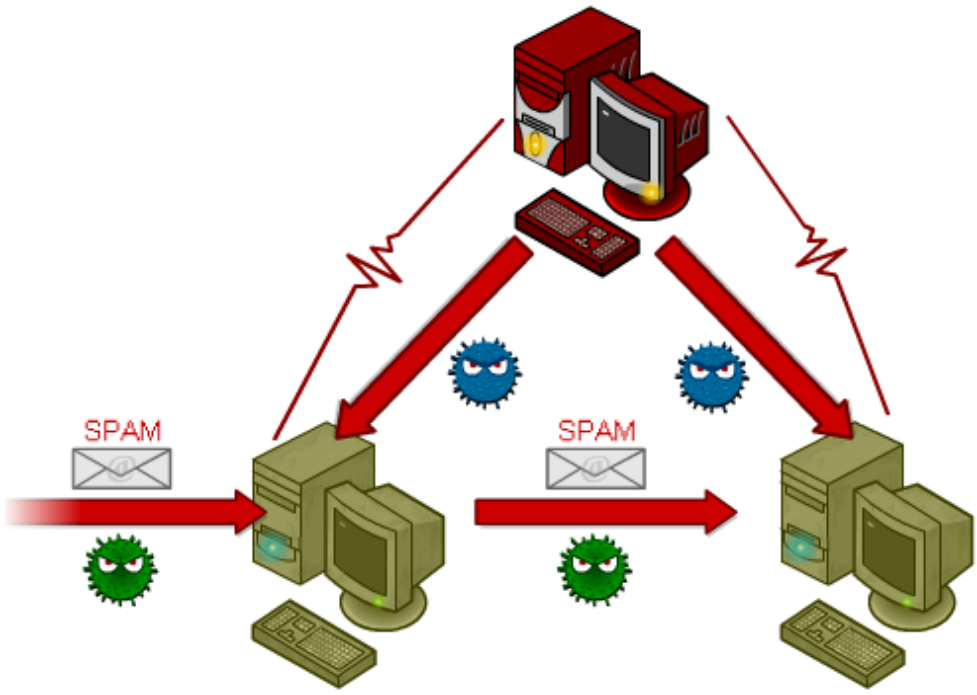
5. El creador de la *botnet* puede explotarla de diversas formas:

    - Utilizar la red directamente en su beneficio.
    - Alquilarla a terceros, de tal forma que el cliente recibe los servicios y el creador controla la red.

- Vender entornos de control, es decir, el creador vende el programa de control de zombis al cliente, para que este último lo explote.

6. La *botnet* permanecerá activa mientras se produzca la actualización del *bot* para dificultar su detección, añadir alguna funcionalidad o alguna otra mejora. El declive de la misma puede provocarse con la resolución de vulnerabilidades de sistemas operativos y aplicaciones tras la publicación por parte de los fabricantes de las actualizaciones, la mejora en el control de las redes, utilización de antivirus y antiespías, etc.

Ilustración 1: Esquema de actualización de infección de una *botnet*



Fuente: HISPASEC

III Métodos de control de las *botnets*

El método de control o protocolo de comunicación de la *botnet* es su núcleo y ofrece diferentes posibilidades al atacante, desde el control de forma segmentada (canales de IRC) al control por medio de sistemas de nombre de dominio (DNS) o control a través de la navegación web (HTTP), entre otros. La evolución de estos protocolos implica a su vez fórmulas más sofisticadas de protección del malware para evitar que la red zombi sea descubierta. La dificultad de realizar esta detección plantea problemas no solo técnicos, sino también judiciales, ya que estas redes suelen propagarse por varios países a la vez, afectando por tanto a varias legislaciones.

A continuación se muestra brevemente los tipos de protocolos de control de las *botnet*s.

Puertos fijos y puertas traseras

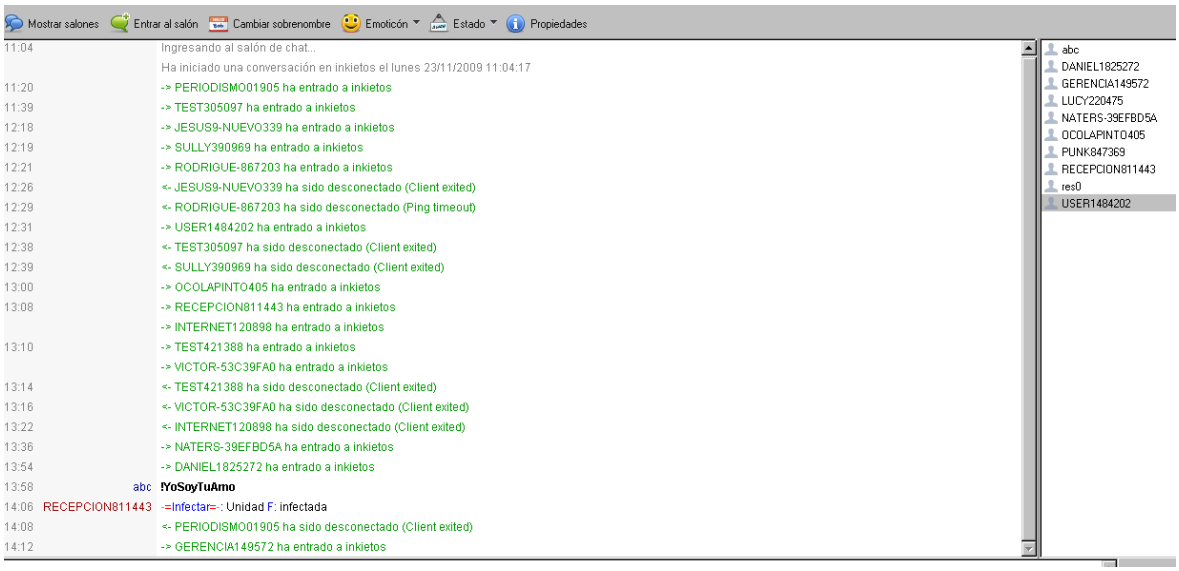
Los *bot* tradicionales abrían una puerta trasera en un ordenador (un puerto lógico o *socket*) que permitía al atacante conectarse directamente y controlar el sistema infectado. Aunque los programas ofrecían ventajas para gestionar a un gran número de sistemas con la puerta trasera "disponible", esto resultaba incómodo para el atacante, y no era una forma eficiente de controlar una *botnet*. Además, la aparición del cortafuegos activo por defecto con el *Service Pack 2* de Windows XP, limitó en gran medida la posibilidad de este tipo de conexión.

IRC (chat)

La forma tradicional de control que se ha venido empleando ha sido a través de un típico chat (protocolo IRC o *Internet Relay Chat*). Los sistemas zombi infectados pasan a formar parte de una sala privada, como las tradicionales salas de chat en las que los participantes pueden enviarse mensajes cruzados. En esta sala, su operador principal (denominado Comando y Control o *Command & Control*, C&C) en vez de "hablar" con los usuarios, les envía comandos. Estos comandos son interpretados como órdenes por los sistemas infectados que visitan la sala. El *bot* o troyano alojado en la víctima se encarga de procesar ese comando y ejecutarlo. El comando puede ser cualquier cosa para lo que esté diseñado, desde "infecta a otros sistemas" hasta "abre la bandeja de la unidad de CD/DVD".

Poco a poco el IRC ha perdido protagonismo, aunque todavía es usado. Posee la desventaja de que los comandos son enviados por la red sin cifrar, lo que supone un riesgo para que el atacante sea atrapado. Además, la evolución de otros programas que permiten una gestión de la *botnet* más cómoda ha desplazado a este método tradicional.

Ilustración 2: Panel de control de una *botnet* a través de IRC



Fuente: HISPASEC

HTTP (web)

Para eludir los cortafuegos, los atacantes idearon una nueva forma de comunicar los zombis con el controlador. Prácticamente todos los cortafuegos permitían (y permiten) conexión hacia una web, por tanto hicieron que los troyanos (*bots*) se comunicaran por este protocolo con el sistema central. Hoy es uno de los métodos más usados, debido a lo complejo que es para el usuario detectar tráfico HTTP (navegación) "anómalo" en su tráfico HTTP habitual. Además, HTTP permite cifrar de forma sencilla el tráfico, lo que hace que los atacantes puedan pasar desapercibidos en mayor medida.

Los creadores de *botnets* han conseguido también gestionarlas de forma que son dirigidas a una página web y, como un panel de control "tradicional", el controlador puede realizar cualquier acción sobre sus víctimas de forma cómoda, con todas las ventajas que ya ofrece la web 2.0 actualmente.

Otros

En los últimos años se observan métodos alternativos para controlar los sistemas zombis, destinados a eludir en lo posible que la red resulte detectada. En 2007 se informó el uso de redes P2P para el control de *botnets*, que prescindían de un controlador clásico y realizaban este control por medio de un sistema distribuido similar al que se usa para el intercambio de archivos multimedia (redes de pares o P2P) en populares programas como eMule.

Las redes sociales son actualmente uno de los focos de infección preferidos para alojar *botnets*. En agosto de 2009 se utilizó la infraestructura de Twitter como panel de control

de una *botnet*. Un usuario registrado (el atacante) cada vez que publicaba una nota estaba en realidad enviando mensajes a las máquinas comprometidas que formaban parte de la *botnet*. Los mensajes se hallaban codificados de forma que resultaban incomprensibles, pero el equipo de Seguridad de Twitter pudo descifrarlos y detectarlos, evitando así su propagación[4].

De nuevo en mayo de 2010 Twitter ha sido objeto de otro ciberataque de estas características[5], detectándose una aplicación que permite infectar usuarios registrados en la red social. El malware recibe los comandos a través del perfil del usuario, por lo que atacante puede controlar los equipos infectados a través de los contenidos que escriba en su perfil de Twitter. Entre los ataques que puede realizar el ciberatacante están la denegación de servicio distribuida (DDoS), apertura automática de páginas web o descarga de nuevos códigos maliciosos en el equipo de la víctima. Por último, el atacante puede realizar la eliminación automática de la *botnet* y el perfil Twitter si quiere pasar inadvertido.

IV Finalidad de una *botnet*

Como se indicaba en el apartado II.3, el creador de una *botnet* necesita reunir un número suficiente de equipos infectados para poder explotarla de la forma más rentable, desde utilizarla directamente a alquilarla o venderla.

Por tanto, los ciberataques que realiza el controlador pueden revestir diversas fórmulas, ilegítimas pero muy lucrativas en su mayoría. Se desarrollan las principales a continuación.

Fraudes de tipo “click”

Muchas de las *botnets* de hoy en día están destinadas a realizar fraudes de tipo publicitario. Los dueños de páginas web con publicidad pueden programar aplicaciones que simulen un “click” en el anuncio, o hacerlo ellos mismos repetidas veces y obtener así beneficios. Además, servicios como *Google AdSense* pagan una pequeña cantidad de dinero a las personas que incrustan publicidad en su web por cada visita recibida: cuantos más individuos visiten la página y pulsen sobre uno de estos anuncios, más dinero obtiene el dueño de la página que incrusta el *banner*.

Google AdSense ya controla estos tipos de estafas, y (a través de muy diferentes métodos) controla quién y cómo se pulsa en la publicidad. Por ejemplo, no permite que se visite la publicidad desde un mismo ordenador más de una vez al día.

[4] Disponible en: http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/
[5] Disponible en: http://blogs.eset-la.com/laboratorio/2010/05/14/botnet-a-traves-twitter/

Sin embargo, los controladores de una *botnet* son capaces de ordenar a sus zombis que visiten el banner o la publicidad una vez al día, de forma automática y ordenada, sin que las víctimas lo perciban. Dependiendo del número de equipos infectados que lo visiten, la cantidad que gana la persona que aloja la publicidad (también el dueño de la *botnet*) puede ser considerable. Esta práctica no levantará sospechas ni para el anunciante ni para sistemas como *Google AdSense* porque, realmente, las visitas provienen de diferentes máquinas repartidas por todo el planeta (la red de zombis).

Denegación de servicio distribuida (DDoS)

Hoy en día el ancho de banda de la conexión a Internet es un recurso que los atacantes tienen muy en cuenta. Los dueños de una *botnet* pueden usarla para realizar "denegaciones de servicio". Esto significa que pueden ordenar a los zombis que visiten de forma continua una página web a la que quieren atacar, y agotar sus recursos. Por ejemplo, pueden ordenar que una red de 100.000 zombis acceda al mismo tiempo a una página web de un servidor "enemigo" y comiencen a descargar archivos, realizar visitas, etc. Si el servidor no está preparado para recibir tanto tráfico, se colapsará y quedará fuera de servicio o, en el peor de los casos, implicará su fin definitivo. En suma, es difícil eliminar definitivamente la recepción de estos ataques, ya que no proceden de una sola fuente, sino de cada uno de los zombis.

En ocasiones estas *botnet* se sirven de ordenadores no infectados (o reflectores) en su ataque[6]. Así, el atacante ordena a sus zombis que soliciten conexión con los reflectores. Estos reflectores no perciben ninguna amenaza de los zombis, por lo que comienzan a enviar información a un tercero o víctima, cuyo sistema experimenta una cantidad de peticiones y respuestas tal, que finalmente cae. Los zombis en este proceso permanecen ocultos, ya que para la víctima el ataque proviene de los reflectores y para éstos, la víctima es quien ha requerido la información. Servicios como *eBay, CNN* o *Microsoft* han sufrido estos ataques, algunos de ellos tan relevantes que tienen su propia definición: *ping de la muerte*[7], *mailbomb*[8] o *teardrop*[9].

Con los DDoS, los ciberatacantes pueden extorsionar a la víctima, pidiéndole una suma de dinero para detener el ataque. Si no cede, continúan indefinidamente ordenando a los zombis que visiten la web y la colapsen. Si se trata de una tienda online, o negocios basados exclusivamente en la web, esto supone un perjuicio económico importante para el dueño del servidor. Para actividades como casinos online, o sitios de apuestas de dudosa reputación, es un riesgo habitual. La inversión en tecnología necesaria para detener este tipo de ataques puede ser mayor que la suma requerida por el atacante, por

[6] Disponible en: http://www.ordenadores-y-portatiles.com/ordenadores-zombie-2.html
[7] La víctima recibe paquetes de datos de gran tamaño hasta provocar un colapso.
[8] Los servidores de correo reciben tal cantidad de emails que acaban cayendo.
[9] La víctima recibe partes de un paquete ilegítimo, y al intentar recomponer el paquete, su sistema cae.

lo que las víctimas acceden a la extorsión: cada minuto offline de este tipo de páginas puede suponerle pérdidas sustanciosas.

Robo de información

La mayoría de las *botnets* actuales ya vienen preparadas para, una vez infectado el sistema, robar toda la información posible de su disco duro y de su tráfico en Internet. Esto significa que se escanea el disco duro buscando contraseñas almacenadas, certificados digitales y otras cuentas de correo a las que poder enviar correo basura o el propio malware para expandir la *botnet*.

También analizan el tráfico web que genera el sistema infectado, de forma que cada vez que se introduce una contraseña en una página, se envía al sistema de control que gestiona el atacante. Esto ocurre aunque la página esté cifrada, puesto que el troyano suele operar en un nivel en el sistema operativo (está incrustado en él) que actúa antes del cifrado de la información.

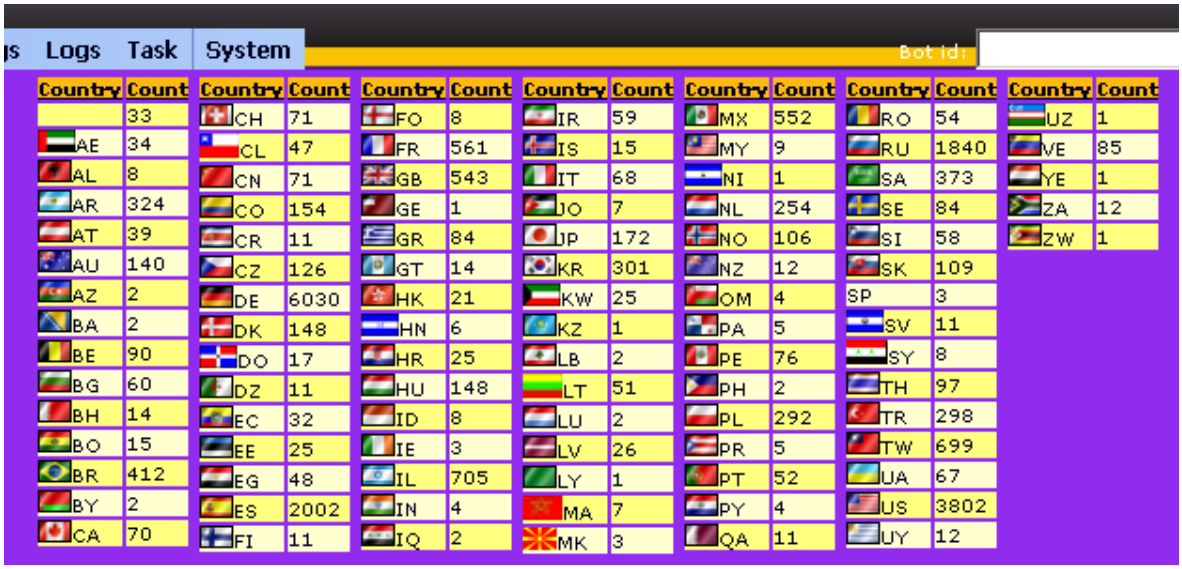
Los atacantes suelen recopilar así todo tipo de contraseñas de los usuarios infectados, la cuales quedan ordenadas en un panel de control en el que pueden realizar búsquedas por tipo de contraseña, por certificado, por país, etc.

También obtienen contraseñas y todo tipo de información si instalan un *keylogger* (capturador de pulsaciones de teclado) en el sistema infectado. Esto envía al atacante todo lo que se teclea en el ordenador.

En 2009, fue descubierta una red de zombis de robo de datos a partir del troyano *Clampi*, que infectó entre 100.000 y un millón de PC con Windows en todo el mundo, afectando a los nombres y contraseñas de usuarios de 4.500 páginas web[10]. No sólo se dirigía a páginas bancarias, sino a cualquier página en la que el usuario pudiera introducir información valiosa para obtener un lucro. La red de zombis recopilaba esta información, diluyendo el rastro, por lo que su depurada forma de trabajar lo diferenciaba de los troyanos bancarios habituales.

[10] Disponible en http://www.xombra.com/go_news.php?articulo=4286

Ilustración 3: Panel de control HTTP de una *botnet* ordenando los sistemas infectados por países



Country	Count	Country	Count	Country	Count	Country	Count	Country	Count	Country	Count	Country	Count
	33	CH	71	FO	8	IR	59	MX	552	RO	54	UZ	1
AE	34	CL	47	FR	561	IS	15	MY	9	RU	1840	VE	85
AL	8	CN	71	GB	543	IT	68	NI	1	SA	373	YE	1
AR	324	CO	154	GE	1	JO	7	NL	254	SE	84	ZA	12
AT	39	CR	11	GR	84	JP	172	NO	106	SI	58	ZW	1
AU	140	CZ	126	GT	14	KR	301	NZ	12	SK	109		
AZ	2	DE	6030	HK	21	KW	25	OM	4	SP	3		
BA	2	DK	148	HN	6	KZ	1	PA	5	SV	11		
BE	90	DO	17	HR	25	LB	2	PE	76	SY	8		
BG	60	DZ	11	HU	148	LT	51	PH	2	TH	97		
BH	14	EC	32	ID	8	LU	2	PL	292	TR	298		
BO	15	EE	25	IE	3	LV	26	PR	5	TW	699		
BR	412	EG	48	IL	705	LY	1	PT	52	UA	67		
BY	2	ES	2002	IN	4	MA	7	PY	4	US	3802		
CA	70	FI	11	IQ	2	MK	3	QA	11	UY	12		

Fuente: HISPASEC

Correo basura

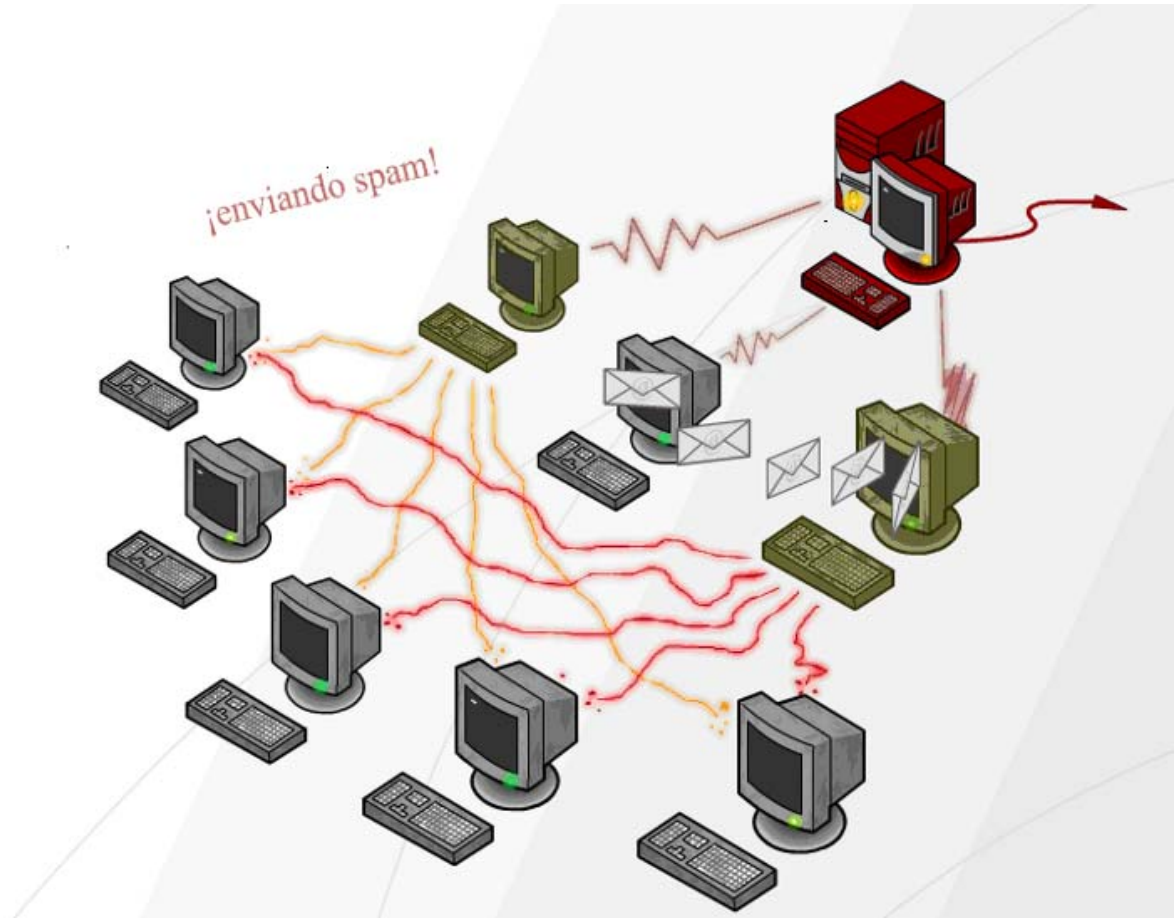
La mayor parte del correo basura (spam) que se recibe hoy en día en los buzones de todo el mundo proviene de otras máquinas de usuarios infectados, por lo que es uno de los códigos maliciosos con mayor presencia. Desde el servidor que actúa como controlador se prepara un mensaje y se da la orden de que todas las máquinas infectadas que pertenecen a la *botnet* lo reenvíen a otras cuentas de correo; bien las que el usuario tenga en su agenda, bien creadas al azar sobre la marcha por el propio *bot* o troyano.

Esta es la forma más económica para el atacante de enviar correo basura (que normalmente contiene otro tipo de estafas) puesto que no requiere invertir en ancho de banda y además, el origen del correo basura queda diluido entre la maraña de ordenadores de la red.

Pushdo, es uno de los ejemplos de estas redes. Este código malicioso, activo desde 2007, enviaba a mediados de 2009 unos 8 mil millones de correos no deseados por día. Entre las razones de su permanencia en el tiempo, puede esgrimirse que las actualizaciones de *Pushdo* pueden ser de diferentes ejecutables, como spam de sitios pornográficos o pedofílicos, de farmacias online, de artículos falsificados, etc[11].

[11] Disponible en: http://www.rompecadenas.com.ar/articulos/millones-diarios-botnet.php

Ilustración 4: Esquema de infección y envío de correo basura de una *botnet*



Fuente: HISPASEC

Aplicaciones Pirateadas (*Warez*)

Los atacantes también buscan en sus víctimas licencias de software legal, para poder así piratearlo y usar licencias ajenas, o para alojar los *cracks* (pequeños programas ilegales que eluden el sistema de licencias del software) o software pirata.

Las webs especializadas para cibercriminales ofrecen todas las herramientas que necesita el controlador de la *botnet*: desde manuales de pirateo y paquetes para la creación "casera" de virus, hasta sofisticadas herramientas para expertos informáticos. La creciente conexión entre piratas informáticos y cibercriminales profesionales proporciona el tándem perfecto entre habilidades criminales y know-how informático para la creación de un nuevo nivel de riesgo para los negocios a escala mundial. Además, estos expertos han sabido aprovecharse de la conectividad, la integración económica y el crecimiento de los servicios financieros a nivel mundial para globalizar sus ataques sin sufrir

repercusiones legales, ya que estos actos delictivos son realizados realmente por la red de víctimas de la *botnet*[12].

Por otro lado, en ocasiones el ataque se produce al intentar descargar una versión pirata de un programa legítimo. En 2009, un troyano en la versión de Windows 7 RC pirata descargado a través de los programas P2P, provocó una botnet de 25.000 ordenadores en todo el mundo[13].

Alquiler de *botnets*

La persona o mafia que ha creado la *botnet* no siempre le da utilidad directamente, ya que existe toda una industria de "alquiler" en la que los creadores permiten a un tercero el uso de estas redes para el fin que estimen oportuno, a cambio de una contraprestación económica.

Normalmente, la persona o equipo que ha creado la *botnet* accede a ella a través de un panel de control web protegido por usuario y contraseña. A cambio de una cantidad, ofrecen a un tercero un nuevo usuario y contraseña que será válido durante un tiempo determinado, previamente acordado, en función de la cantidad pagada. En el panel, el arrendatario tendrá a su disposición todas las posibilidades de la red de ordenadores zombis para realizar ciberataques.

Los creadores sólo se preocupan de mantener una cantidad suficiente de sistemas infectados para que resulten "atractivas" y puedan alquilarlas por una mayor cantidad de dinero. Actualmente, el alquiler diario de una botnet está en torno a los 60 euros, según concluye Verisign[14] tras una investigación online sobre 25 *botnets* realizada a principios de 2010.

V Recomendaciones de prevención y protección

Como se ha indicado anteriormente, los propios usuarios son los que fomentan el envío de spam, por ejemplo, sin percatarse de que han pasado a formar parte de una *botnet*. Las posibilidades de interconexión de usuarios que operan constantemente con otros sistemas crecen a ritmo exponencial, así como el potencial de infección. Con la adopción de unas medidas de prevención y protección adecuadas, se reduce la capacidad operativa de estas redes al eliminar las conexiones entre equipos, pudiendo conducir incluso a la inactividad.

[12] *McAfee Virtual Criminology Report (2005)*. Disponible en: http://www.inteco.es/studyCategory/Seguridad/Observatorio/Estudios_e_Informes/Biblioteca/Informe_de_Criminologia_Virtual_de_McAfee
[13] Diponible en: http://www.ethek.com/windows-7-rc-pirata-provoca-una-botnet-de-25-000-equipos/
[14] Disponible en. http://www.zdnet.co.uk/news/security-threats/2010/05/25/botnet-price-for-hourly-hire-on-par-with-cost-of-two-pints-40089028/

Para evitar que el ordenador se convierta en un zombi y pertenezca a una *botnet* no existen recomendaciones específicas, sino que pueden aplicarse las mismas que para mantener el sistema libre de malware, es decir, habituarse a realizar un comportamiento seguro en la Red y adoptar medidas técnicas de protección. Algunas de estos consejos son:

- El principal consejo para los usuarios de sistemas operativos en general (y los de Windows en particular) es no usar la cuenta de administrador. Se debe utilizar o crear la **cuenta de un usuario sin privilegios**, ya que como indica el Cuaderno de Notas del Observatorio "*Cuenta administrador vs. cuenta limitada*"[15], las acciones que pueden ser llevadas a cabo por otro usuario o por algún tipo de código malicioso en esta cuenta sin privilegios están acotadas.

- **Mantener actualizado** con los últimos parches de seguridad (modificaciones realizadas en un programa para solucionar problemas de usabilidad o funcionalidad) **tanto el sistema operativo como los programas** que el usuario tenga instalados en su ordenador. Esto es muy importante, pues una gran parte del malware hoy en día se aprovecha de vulnerabilidades conocidas que ya tienen parche. Los sistemas operativos mayoritarios contienen sistemas de auto-actualización, que corrigen las posibles vulnerabilidades y reducen las posibilidades de que el malware entre en nuestro equipo. El Centro de Repuesta a Incidentes de Seguridad (CERT) de INTECO ofrece servicios de información sobre parches y actualizaciones[16].

- Mantenerse informado sobre **tendencias de seguridad, malware y estado en general de la seguridad en la Red**. No se puede luchar contra lo que no se conoce. Para mantenerse actualizado respecto a virus y amenazas de seguridad, una recomendación es visitar con frecuencia web especializadas, o darse de alta en las suscripciones y/o boletines de seguridad que éstas proporcionan, como por ejemplo, los disponibles en el CERT [17] de INTECO.

- **No ejecutar programas ni abrir documentos que no hayan sido solicitados**, aunque provengan de una persona en la que se confíe.

- **Usar un antivirus actualizado**. La Oficina de Seguridad del Internauta (OSI) de INTECO, dispone de la sección *Protégete* que permite a los interesados estar informados y obtener herramientas gratuitas de protección frente a amenazas[18].

[15] Disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/cuenta_administrador_vs_limitada
[16] Disponible en: http://cert.inteco.es/Proteccion/Actualizaciones_SW/
[17] Disponible en: http://cert.inteco.es/Actualidad/Suscripciones/
[18] Disponible en: http://www.osi.es/Te_Ayudamos/

Más aún, el Observatorio de la Seguridad de la Información de INTECO[19] dispone de numerosos **documentos de consulta sobre seguridad y privacidad en la Red**, los cuales ofrecen consejos para prevenir y responder a estos ataques.

- *Estudio sobre la seguridad de la información y la e-confianza de los hogares* españoles *(informe anual 2009)*; *Estudio sobre el fraude a través de Internet*.

  http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/estudio_fraude_2009

- Artículos: *Ciberterrorismo: una amenaza real y creciente*; *¿Qué son y cómo* funcionan *los troyanos bancarios?*; *Cuenta administrador vs. cuenta limitada*; *Honeypots, monitorizando a los atacantes*; *Envenenamiento ARP*; etc.

  http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/

- Guía sobre la respuesta jurídica a los ataques contra la Seguridad de la Información

  http://www.inteco.es/Seguridad/Observatorio/manuales_es/GuiaManual_sobre_la_respuesta_juridica_a_ataque

- Sección multimedia: videos-píldoras que explican de forma amena diferentes conceptos de seguridad de la información:

  - Botnet, ¿qué es?

    http://www.inteco.es/Seguridad/Observatorio/Multimedia/botnet_multimedia

  - Troyanos, ¿qué son?

    http://www.inteco.es/Seguridad/Observatorio/Multimedia/troyanos_multimedia

[19] Disponible en: http://www.inteco.es/Seguridad/Observatorio/