Botnets: la amenaza invisible

JAVIER LÓPEZ DE TURISO Y SÁNCHEZ
Teniente Coronel de Aviación

Quién no se acuerda de aquellos virus informáticos de antaño que nos 'derretían' la pantalla, nos mostraban una calavera o, en el peor de los casos, nos formateaban el ordenador? ¡Qué virus aquellos, tan evidentes, tan notorios, tan predecibles y, a veces, tan inocentes!

Los tiempos en los que el *malware*[1] era codificado por diversión, para hacer gracias (o maldades) o para obtener fama o notoriedad han pasado a la historia.

Hoy día, aquel romanticismo ideológico ha derivado a vil materialismo. La mayoría del "malware" que se codifica en la actualidad busca una misma cosa: dinero, dinero y más dinero y todo lo que pueda llevar a éste (p.ej. robo de información). La codificación y el mercado de *malware* han pasado al mundo de las mafias y bandas organizadas porque son altamente rentables y producen cuantiosos beneficios. Caso aparte es el *malware* creado por los Estados para sus propios intereses, ciberespionaje o ciberguerra; pero eso es otra historia de la que hablaremos en otro momento.

En este artículo se va a exponer qué es lo que mueve a los actuales creadores y gestores de *malware*, cómo lo hacen y en qué nos afecta a los usuarios de medios de comunicación digitales, así como uno de los métodos más empleados para extender sus actividades criminales y conseguir mayores beneficios: las *botnets*.

FINES DEL *MALWARE*

Como hemos dicho, prácticamente la totalidad del *malware* desarrollado en la actualidad es para la obtención de algún tipo de beneficio económico:

- Robo de información personal del usuario (nº de cuentas corrientes, tarjetas de crédito, direcciones de correo

electrónico, etc.), que posteriormente será vendida a otras empresas u organizaciones (legales o ilegales).

• El uso de recursos de forma remota para conseguir mayor capacidad de proceso o transmisión: utilización de nuestros equipos como plataforma para hacer operaciones ilícitas (distribución de *spam*, ataques de denegación de servicio distribuido, expansión de otro *malware*, etc).

• Alteración del sistema operativo del equipo infectado para que facilite la entrada de nuevo *malware*, de manera que consiga que nuestro equipo entre en alguno de los dos grupos anteriores.

Para más inri, la cadena de creación de *malware* lleva asociado, en cada uno de sus eslabones, un sustancioso beneficio. Así, hay gente especializada en buscar y descubrir vulnerabilidades en sistemas operativos y aplicaciones. Éstos venden su hallazgo a programadores especializados que desarrollan el código de explotación o *exploit*[2] para aprovechar este fallo de seguridad. A su vez, éstos venden el *exploit* a otros desarrolladores que confeccionan el *malware* adecuado (virus, troyano, gusano, etc.) añadiendo al *exploit* las características del código dañino (replicación, ocultación, cifrado, etc.) y todo lo que sea necesario para que el nuevo producto tenga éxito. Esta gente vende su producto a los distribuidores de *malware*, quienes, a su vez, lo venden a los que expanden el virus y extraen la información y éstos, por su lado, venden esta información a las organizaciones y mafias encargadas de explotar esa información. Lo lucrativo de este negocio y la gran cantidad de grupos y organizaciones 'beneficiados' por su comercialización hacen extremadamente difícil no sólo su eliminación, sino también su persecución.

QUÉ SON LAS BOTNETS

Hemos visto someramente cuál es actualmente la finalidad principal del *malware*. Ahora vamos a ver uno de los métodos más extendidos para expandirlo y explotarlo: las *botnets*.

Una *botnet* es una red de ordenadores infectados con un determinado tipo de *malware*, que hace que las máquinas queden controladas a distancia por un atacante sin el conocimiento del propietario. Esta red puede llegar a estar compuesta por decenas, cientos o miles de ordenadores. La palabra *botnet* tiene su origen en los términos ingleses *software ro**bot net**work*, o red robot. Se denomina *bot* (apócope de *software robot*) al código o pieza de "software" (el *malware*) que, una vez introducido en los equipos infectados, se ejecuta silenciosamente en su interior y pone a la máquina afectada a las órdenes del atacante; esto hace que las máquinas actúen como robots o zombis. Por extensión, también se le denomina *bot* a la máquina afectada.

Hoy día, las *botnets* son consideradas como la mayor amenaza a la seguridad en Internet.

Pero ¿por qué son realmente una amenaza?

1) Por el enorme poder computacional que proporcionan miles de ordenadores trabajando simultáneamente.

2) Porque este poder computacional es susceptible de ser vendido, alquilado y comercializado como si de un servicio más de Internet se tratara.

3) Porque pueden ser (y son) utilizados para realizar ataques a gran escala.

4) Porque su utilización se está extendiendo enormemente gracias a las ganancias económicas que pueden reportar.

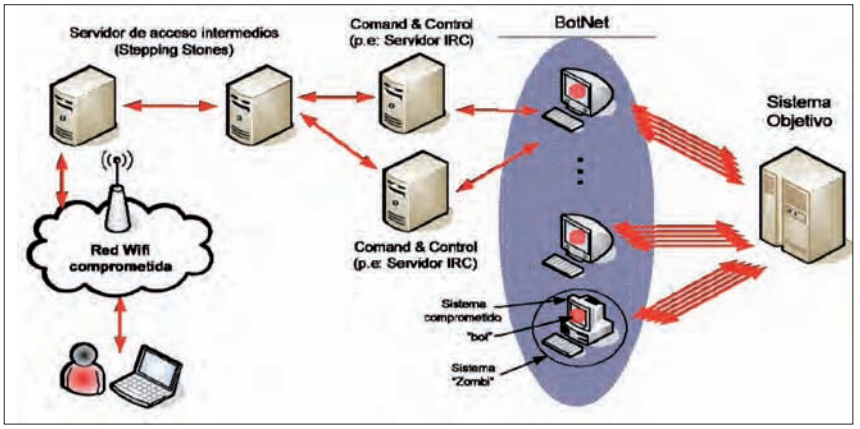
5) Porque son tremendamente dinámicas y muy difíciles de detectar, localizar y eliminar.

6) Porque se adaptan muy rápidamente a los nuevos sistemas de detección.

7) Por su bajo coste de producción y la gran variedad de formas de explotación.

FORMA DE ACTUACIÓN

El proceso de creación de una *botnet*, por el cual nuestro ordenador puede verse integrado en ella, es el siguiente:



Estructura de una botnet.

1) El atacante idea y planifica la creación de una *botnet* para alguna finalidad maliciosa determinada.

2) Para ello buscará algún tipo de *malware* (normalmente un troyano o gusano) que sea capaz de infectar el mayor número de equipos posible explotando alguna de las vulnerabilidades conocidas o desconocidas[3], recientes o no, pero de la que está seguro que habrá muchos equipos sin defensa.

3) Para obtener este *malware*, lo desarrollará por sí mismo, con su equipo o lo adquirirá en el mercado negro.

4) A continuación difundirá o contratará la difusión del *malware* de manera dirigida contra unos cuantos servidores[4] conocidos o desconocidos para el atacante, pero de los que sabe o cree que tienen alguna vulnerabilidad explotable.

5) La explotación de la vulnerabilidad de los servidores hace que el atacante los tenga bajo su control. Conseguido esto, los utilizará para propagar[5] el *malware* a miles de ordenadores mediante la explotación de las mismas u otras vulnerabilidades.

6) Dentro de la carga del *malware*, existirá un código que haga que el equipo atacado se conecte a un canal de comunicaciones. Anteriormente se trataba de canales de "chat", pero en la actualidad utilizan enlaces de todo tipo[6], por el cual el equipo atacado recibirá las órdenes en forma de comandos que le dicte el atacante. A partir de este momento el equipo infectado se encontrará a merced del atacante y podrá hacer todo lo que éste le pida, sin que la víctima se dé cuenta de ello.

Teniendo en cuenta que aproximadamente el 95% de los ordenadores del mundo utilizan Windows y que el 99,2% del *malware* creado[7] lo es para este entorno, es fácil suponer que los usuarios de este sistema operativo serán los principales objetivos de los atacantes.

Los *bots* se introducen sigilosamente en el equipo de una persona de muchas maneras. Suelen propagarse por Internet en busca de equipos vulnerables y desprotegidos a los que poder controlar. Cuando encuentran un equipo sin protección, lo infectan e informan a su creador. Su objetivo es permanecer ocultos hasta que se les indique, mediante un comando determinado, que realicen una tarea concreta.

VENTAJAS DEL ATAQUE CON *BOTNETS*

Lo que hace interesante a estas redes para el atacante frente a otros medios más tradicionales, es su infraestructura distribuida, esto es, multitud de ordenadores controlados por una misma persona u organización. Las *botnets* ofrecen claras ventajas a la hora de cometer actividades delictivas:

1. **Anonimato**: la actividad se produce desde muchos ordenadores a la vez. Localizar cualquiera de ellos puede ser muy complicado, tanto técnica, como judicialmente, ya que se pueden utilizar ordenadores de varios países, en los que la legislación puede ser absolutamente dispar, o incluso no haberla en absoluto. Llegar a descubrir al atacante puede resultar extraordinariamente complicado.

2. **Coste**: la inversión requerida comprende tan sólo el desarrollo del

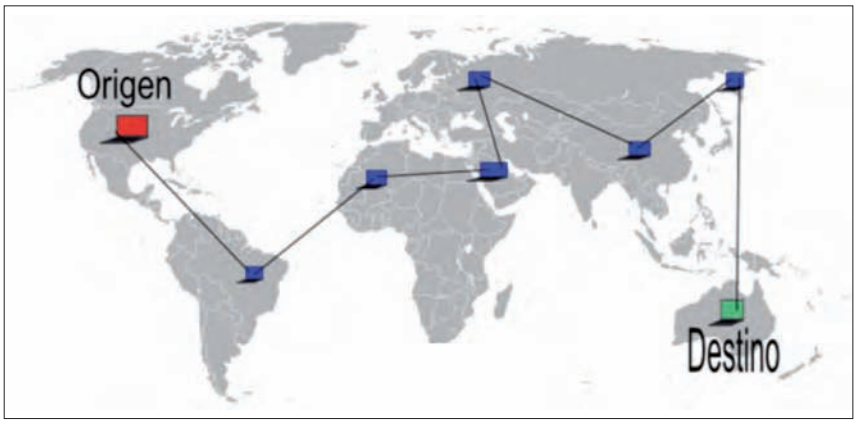
"software" malicioso, el ordenador y la línea de comunicaciones del atacante: irrisorio en comparación con los beneficios que aporta. El resto de la infraestructura necesaria para la *botnet* es puesta por los propietarios de los equipos zombis infectados.

3. **Computación distribuida**: al igual que este modelo se utiliza para proyectos legítimos con el consentimiento del usuario (SETI, Globos, etc.), en este caso se utiliza la potencia de miles de máquinas para procesos con una finalidad ilícita, como por ejemplo forzar contraseñas.

4. **Impunidad**: porque explotan y aprovechan las lagunas legales y la ausencia de jurisprudencia de gran parte de los países, lo que permite en muchos casos la impunidad de estos actos criminales.

5. **Beneficios económicos**: estas redes, que reportan un beneficio a las personas que las controlan, actualmente se aprovechan económicamente de tres modos:

– Explotación propia. El aprovechamiento económico, viene por la explotación directa de la misma por parte del propietario.



– Alquiler a terceros. El beneficio se obtiene de vender los servicios de la red a clientes siendo el propietario quién la controla.

– Venta de entornos de control: Se trata de la última tendencia en este tipo de servicios. Los promotores de la red, venden a cualquier usuario el programa de control de los zombis.

USO DE LAS *BOTNETS*

Debido a estas ventajas para el atacante, las *botnets* son ampliamente utilizadas para todo tipo de actividades delictivas[8]. Las principales son:

Ataques DDoS (Distributed Denial-of-Service)

Este, junto con el beneficio económico, son los dos usos más importantes de las *botnets*. Su misión consiste en bloquear un servidor enviando muchas peticiones en muy poco tiempo desde cada uno de los ordenadores infectados de la red zombi, de forma que logran saturarlo ralentizándolo y, en el peor de los casos, provocando su caída.

Envío de *spam*

Mediante las *botnets*, el atacante puede enviar masivas cantidades de correo basura (*spam*[9]), así como recolectar las direcciones de correo de las libretas electrónicas de sus atacados para enviar el *spam* a nuevas víctimas. El envío de spam también se puede utilizar para hacer *phishing*[10].

Capturar tráfico de red

Los *bots* pueden también capturar el tráfico de red[11] con el objeto de buscar datos en texto claro que pueda pasar a través del ordenador infectado. Estas capturas se suelen utilizar normalmente para obtener información sensible, como nombres de usuario y contraseñas. Una vez capturadas, el atacante tendrá control total sobre la máquina infectada o podrá suplantar su identidad.

Captura de teclado o pantalla

También se utilizan las *botnets* para introducir en los ordenadores atacados los capturadores de teclado (*keyloggers*) o pantalla (*screen loggers*), con los que el atacante podría obtener en un momento dado, tanto las pulsaciones del teclado de la víctima como capturas de pantalla, con el fin de obtener las contraseñas del usuario, aparte de otra información sensible, como cuentas de crédito, etc.

Instalación de anuncios en falsas páginas web

Existe una forma de publicidad en Internet en la que el anunciante paga al propietario de una página web por cada clic que los navegantes hagan sobre ese anuncio. Aquí, el atacante crea una falsa página web y la pone a disposición de anunciantes, para que pongan anuncios sobre ella. Posteriormente, se utilizará la *botnet* sobre la que tenga dominio para mandar a miles de los equipos zombis hacer clic sobre estos anuncios, lo que le proporcionará sustanciosos beneficios económicos.

Fraudes

Se utilizan las *botnets* para manipular negocios legítimos.

– Manipulación de encuestas: miles de ordenadores controlados pue-

den hacer que las encuestas se vuelquen en un sentido o en otro.

– Juegos en línea: se paga para que los equipos infectados actúen como jugadores o bien para beneficiar directa o indirectamente a otros jugadores.

Secuestro de ficheros y chantaje

Un atacante, una vez controlada la *botnet* puede:

– Robar ficheros y pedir dinero por ellos.

– Cifrarlos en el disco duro de la víctima y chantajear por descifrarlos.

– Colocar documentos o archivos comprometidos en el ordenador de la víctima (ej. documentos clasificados o pornografía infantil) y efectuar una denuncia anónima contra la víctima.

– Descargar grandes archivos que consumen mucho ancho de banda y que generalmente son ilícitos o ilegales.

Evasión de rastros y trazas de las actividades delictivas

Los delincuentes informáticos emplean las redes *botnet* también para ocultar su actividad criminal haciendo que sus circuitos de comunicación sean tan complejos e intrincados que sea en la práctica imposible de realizar un seguimiento policial de sus trazas.

EJEMPLOS DE ATAQUES REALES CON *BOTNETS*

Estonia

En la primavera de 2007, aparentemente debido al traslado de un monumento en honor de los soldados del Ejército Rojo en Tallín, Estonia recibió decenas de ataques DDoS contra decenas de sitios web del país, en concreto:

- La Presidencia estonia y su Parlamento.
- Casi todos los ministerios del Gobierno.
- Partidos políticos.
- Los tres medios de comunicación más importantes del país.
- Los dos mayores bancos.
- Empresas especializadas en comunicaciones.

Los ataques producidos durante varios días produjeron el colapso de los sistemas informáticos de unos de los países con mayor número de usuarios de Internet del mundo (más del 50% de su población usa habitualmente Internet). En total se identificaron 128 ataques DDOS sobre las webs de Estonia.

Kirguistán

Mucho más recientemente, a mediados de enero de 2009, dos de los principales proveedores de servicio de Internet de Kirguistán, una de las antiguas Repúblicas Socialistas Soviéticas situada entre China y Kazajistán, sufrieron una serie de ataques masivos DDoS efectuado por entre 150 y 180 millones de ordenadores zombis ubicados en todas partes del mundo, el mayor de este tipo producido hasta la fecha. Este ataque produjo la caída de cerca del 80 % de la conectividad de Internet del país. Se sospecha que el ataque pudo ser producido por cibermilicias rusas con el objeto, bien de desbaratar las acciones de la oposición política del país, cuya organización depende en gran

parte de Internet, o bien para presionar al actual gobierno que actualmente permite la presencia de la base estadounidense de Manás, cerca de la capital Bishkek.

DEFENSAS CONTRA LAS *BOTNETS*

Aunque uno de los objetivos de los controladores de las *botnets* es que pase desapercibida y duren el mayor tiempo que sea factible, para lo cual inoculan un código dañino lo más silencioso, transparente e inocuo posible para el funcionamiento del equipo víctima, un ordenador que está siendo víctima de una botnet suele presentar los siguientes síntomas:

– Ralentización de las comunicaciones o del sistema.

– Aparición de extraños mensajes (fallos en archivos, fallos de lectura/escritura en memoria, etc.).

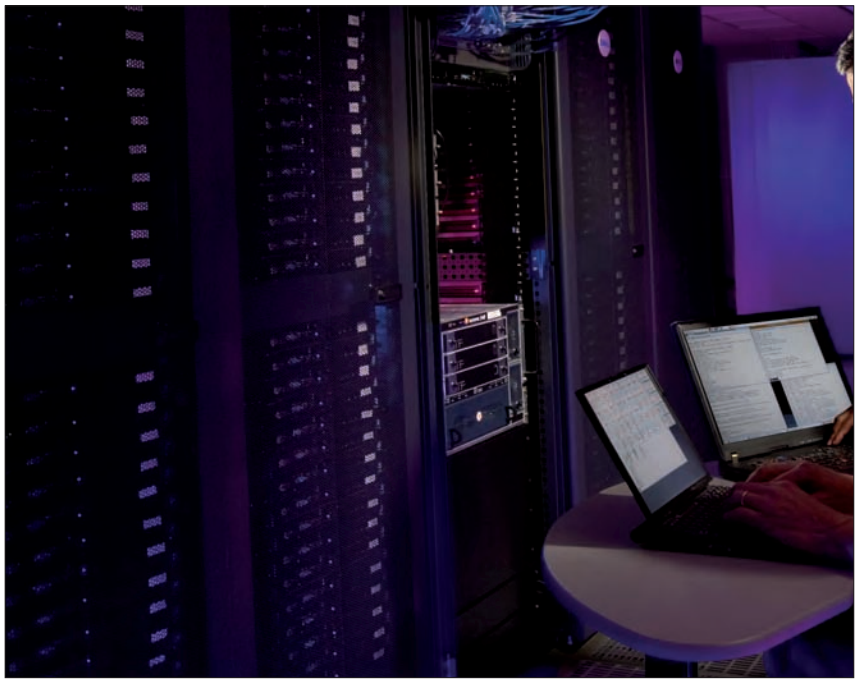
– Funcionamiento de manera inesperada (cierres repentinos de aplicaciones, aparición continua de funcionamiento en segundo plano –reloj de arena–, etc.).

Las medidas que se pueden adoptar para evitar caer en las redes de una botnet son:

1) Reducir el factor virus: en primer lugar, evitar las intrusiones. Si se consiguen mantener el sistema operativo, aplicaciones y los programas antivirus actualizados, el sistema tendrá más probabilidades de mantenerse a salvo.

2) Configurar el "software" para que se actualice de manera automática.

3) Aumentar las configuraciones de seguridad del navegador.



4) Limitar los derechos de usuario cuando está conectado, esto es, no utilizar habitualmente un usuario con privilegios de administrador.

5) Utilizar una contraseña fuerte para TODOS los usuarios.

6) Nunca abrir los archivos adjuntos, a menos que se tenga certeza de su origen y contenido.

7) Estar pendientes de las señales: los ordenadores van demasiado lentos o lanza demasiadas ventanas emergentes.

8) Siempre que sea posible monitorizar el sistema: los programas de detección de intrusiones buscan cualquier conducta que pueda parecerse a una actividad de *malware*, incluídas actividades de *botnet*. Estas intrusiones están fuera de la capacidad de detección de un cortafuegos normal.

9) Conseguir el control de los "puertos" de nuestro equipo: el uso que la mayoría de la gente hace de Internet requiere sólo unos pocos "puertos" abiertos, por lo que cerrar todos salvo los necesarios incrementará algo la seguridad del sistema.

CONCLUSIONES

El término *botnet* hace referencia a una red de ordenadores infectados por *malware* que pueden ser controlados en remoto para ejecutar órdenes de manera autónoma mediante cualquiera de los medios de comunicación existentes en Internet.

Una *botnet* puede, entre otras cosas:

– Hacer que infecte a los visitantes de una página web.

– Generar un ataque de denegación de servicio o participar en uno.

– Hacer que las máquinas alojen *malware, phishing* (fraude informático) o pornografía infantil.

– Utilizar las máquinas para cometer delitos.

– Utilizar las máquinas para enviar *spam*.

– Cifrar archivos y pedir dinero por descifrarlos.

– Hacer que nuestros equipos enriquezcan a un tercero.

– Formatear cualquier equipo.

– Infectar a otros equipos.

Las mejores protecciones son:

– Tener los sistemas operativos, aplicaciones y antivirus permanentemente actualizados.

– No utilizar habitualmente usuarios con privilegios de administración.

– Utilizar siempre contraseñas fuertes en todos los usuarios.

– Vigilar el comportamiento habitual de nuestro sistema.

– Sentido común.

NOTAS

[1]Software que se programa con intención de penetrar o dañar la información de los equipos en los que se aloja sin el conocimiento ni la autorización de su gestor o propietario.

[2]Código o secuencia de comandos que aprovecha un error, fallo o vulnerabilidad para obtener unos privilegios en el software o un comportamiento imprevisto del mismo.

[3]Desconocidas por la comunidad internacional y por el fabricante del software, pero no por los atacantes. Son las más peligrosas; las llamadas vulnerabilidades de día cero (Zero-day), contra las que hasta entonces no existe solución.

[4]Un servidor no tiene por qué ser una gran máquina muy protegida. Puede ser cualquier PC que esté directamente conectado a Internet prestando algún servicio (web, correo, etc.).

[5]Para entender la forma de difusión de una *botnet* hay que comprender cómo se propagan los gusanos y troyanos. Los gusanos tienen la capacidad de autorreplicarse y autopropagarse, no suelen infectar archivosm sino que residen en memoria y utilizan para expandirse los protocolos de comunicaciones permanentes que hay entre los ordenadores en red o las direcciones de correo-e de las libretas de los usuarios, enviándose a éstas y repitiendo el proceso sucesivamente en todos los equipos vulnerables que alcance. Los troyanos suelen hacerse pasar por archivos legítimos anexados en mensajes de correo electrónico procedentes de amigos existentes en la libreta de direcciones del usuario, que el incauto abrirá confiando en el origen del remitente. La simple acción de hacer doble clic sobre un archivo puede hacer que si nuestro equipo presenta alguna vulnerabilidad de sistema operativo o de aplicación (*Word, Adobe Reader*, etc.) no corregida, el equipo quede contaminado.

[6]Navegación web -http-, correo electrónico, redes sociales y redes P2P.

[7]Según la empresa alemana G DATA.

[8]Como ya se ha indicado, una vez que un equipo está bajo el control de una botnet, el atacante puede hacer lo que quiera con él: instalarle *software*, más *malware*, utilizarlo como un equipo remoto para atacar otros lugares, etc.

[9]Correo electrónico no deseado, normalmente utilizado para el envío de publicidad, lo que proporciona pingües beneficios al atacante o un tercero.

[10]Tipo de estafa informática por la que se obtienen datos confidenciales de los usuarios, facilitados por ellos mismos, mediante engaños o trucos, normalmente de ingeniería social y utilizando páginas web simuladas, correos electrónicos fraudulentos o llamadas telefónicas falsas.

[11]Los datos que nuestro ordenador transmite o recibe.