Los Botnets

Radamés Toro Martínez

Resumen

Un problema que afecta la seguridad de millones de computadoras alrededor del mundo es la proliferación de los botnets. Un ***botnet*** es una red compuesta por computadoras cuya seguridad ha sido comprometida y cuyo control ha pasado a manos de una persona ajena a esta (conocida como "botherder" o "botmaster"). Esta persona puede enviar comandos de forma remota a las computadoras que forman parte del botnet y utilizarlas para llevar a cabo funciones ilegales que pueden variar desde el envío masivo de correo no solicitado ("spam") hasta ataques DDoS.

Según The Atlantic (2010), "más de un billón de computadoras están en uso alrededor del mundo y según algunos estimados, una cuarta parte de éstas ha sido enlazada a un botnet". Las estadísticas de Daily Botnet Statistics (2011) hasta marzo estiman en 4922 las direcciones IP que se sospecha corresponden a botnets. Estamos hablando de una amenaza real y muy seria, que se ha convertido incluso en un lucrativo negocio. La revista electrónica eWeek Europe (2010) reporta que por "entre $50.00 hasta varios miles de dólares se puede alquilar un botnet para llevar a cabo un ataque DDosS por 24 horas". Lo peor es que la mayoría de los usuarios cuyas computadoras forman parte de un botnet, no están apercibidos de que, sin querer, contribuyen a la realización de algún acto ilícito.

¿Cómo puede una computadoraser víctima de un botnet? Hay diferentes medios que utilizan los "botherders":

1. gusanos, como el caso de Conficker, según reportado en The Atlantic (2010),
2. troyanos ocultos en aplicaciones,
3. páginas de Internet que parecen legítimas,
4. páginas de Internet con "scripts" que descargan el malware necesario para controlar a distancia una computadora.

Dada la magnitud del problema se hace necesario:

1. Exponer en detalle el problema, estudiar los síntomas que puede presentar una computadora que ha sido comprometida, conocidas como "zombies" según Bradley (2006).

2. Plantear las medidas que se pueden adoptar para prevenir ser víctima de un botnet, y qué hacer si se sospecha que un equipo ya forma parte de una de estas redes.

Según la página de Microsoft Online Safety (2010), un botnet "es una red usada para infectar un alto número de computadoras". Dado que la infección ocurre de forma discreta, mediante un gusano o troyano, o simplemente al visitar una página infectada, un usuario con poco conocimiento de computación no se percatará de que su computadora ha sido convertida en un "zombie" haciendo del problema uno más agudo.

Con la sofisticación de los sistemas e información, también se han sofisticado y mejorado las técnicas de los cibercriminales para el diseño y uso de los botnets. De redes centralizadas se han movido a las redes "peer-to-peer" que hacen más difícil identificar al "botherder" y poder desarticular el botnet en cuestión. Además el asunto se ha convertido en uno de carácter económico, donde el propósito del botnet es lucrase de forma ilícita, al punto de que existe la venta y alquiler de estas redes. Un caso reseñado por CNET News (2009) es el de "Golden Cash Network", grupo dedicado a la venta de acceso a botnets, lo que pone de manifiesto la seriedad del asunto. Ya no se trata de adolescentes compitiendo por ver quién violenta primero la seguridad de un sistema, se trata de generar dinero de forma ilícita a través del fraude y el robo de información.

En un principio, los botnets comenzaron como una herramienta que no tenía fines criminales. Originalmente se desarrollaron como instrumentos virtuales usados en los IRC ("Internet Relay Chat") para realizar ciertas tareas cuando el usuario no podía estar presente. Según el documento History of IRC (2008), el IRC es desarrollado por Jarkko Oikarinenen Finlandia para 1988 y se considera a GM como el primer botnet, desarrollado el 1989. Estos primeros botnets en realidad eran robots percibidos por los usuarios del IRC como humanos. Su función era ayudar al usuario del IRC a manejar sus conexiones. Otros programadores observaron que los robots podían ser utilizados para hacer las tareas que hacían los humanos, como por ejemplo, los operadores del IRC. Los bots comenzaron a ser usados para mantener un canal abierto y evitar que usuarios con propósitos maliciosos se apoderaran del canal cuando el operador estuviera ocupado.

Los bots evolucionaron de un código que ayudaba a un usuario, a uno que puede ejecutar y administrar un canal de IRC. Más tarde, algunos bots comenzaron a incluir la capacidad de hacer disponible a los usuarios cuentas del "shell" del sistema operativo, lo que permitía a los

usuarios ejecutar comandos en el "host" del IRC. El estudio de Mahathi, Botnets: Overview and Case Study (2008), nos provee los pasos que se siguen en el desarrollo de un botnet, lo que se conoce como el Ciclo de Vida del botnet:

1. Explotación del potencial cliente del botnet: El ciclo comienza cuando se aprovecha alguna vulnerabilidad de seguridad en la víctima para insertar el código necesario para controlar la computadora y hacerla parte del botnet. Esto se puede lograr aprovechando sistemas operativos o aplicaciones con vulnerabilidades al descubierto, utilizando troyanos con "backdoors" y /o gusanos.
2. El nuevo bot se comunica ("rallying") con el "botherder" al servidor C&C ("Command and Control") para que este sepa que ya es parte del botnet.
3. Se instala un módulo "anti anti-antivirus" en el bot. Esto se logra cuando el código malicioso logra obtener la contraseña de administrador y ejecuta un "batch fie" con instrucciones para desactivar el antivirus, además de utilizar un archivo tipo "dynamic link library" que engañe al usuario haciéndole creer que el antivirus está funcionando, cuando en realidad no está escaneando ni detectando nada. Mahathi en su estudio Bots: An Overview and Study (2008) muestra un ejemplo del "batch file" usado por el gusano Rbot para desactivar el antivirus Norton de Symantec:

```
net start >>starts
net stop "Symantec antivirus client"
net stop "Symantec AntiVirus"
net stop "Trend NT Realtime Service"
net stop "Symantec AntiVirus"
net stop "Norton antivirus client"
net stop "Norton antivirus"
net stop "etrust antivirus"syngress.com
net stop "network associate mcshields" net stop "surveyor"
```

5. El nuevo bot espera recibir comandos desde el servidor C&C. Los comandos varían de acuerdo al botnet.
6. Una vez recibido los comandos, éstos son ejecutados.
7. El bot reporta al servidor C&C los resultados de la ejecución de los comandos.
8. De ser necesario, se ejecuta un comando que borra la evidencia y se abandona el bot.

Hay diferentes medios que un "botherder" puede utilizar para instalar el código necesario para controlar de forma remota una computadora. La importancia de conocer estos medios está en que, conociéndolos, el usuario puede tomar medidas preventivas para no ser víctima de un botnet.

1. Phishing: Correos electrónicos con aparentes mensajes de empresas legítimas, especialmente de la banca, que mediante un enlace llevan al usuario a revelar nombres de usuario y contraseñas que pueden ayudar al "botherder" a obtener víctimas de una misma categoría. Las más recientes estadísticas de phishing publicadas por la empresa de seguridad Avira (2011) indican que el primer lugar en incidencias de phishing lo ocupa Amércica del norte con un 57.14%.
2. Páginas de Internet con troyanos: Al pulsar en un enlace, se descarga un troyano con el código necesario para reclutar un nuevo bot.
3. Correos electrónicos con anejos o enlaces que al ser ejecutados activan código malicioso.
4. Vulnerabilidades sin corregir: Tanto en el sistema operativo, como en aplicaciones, pueden existir vulnerabilidades. Los miembros del botnet utilizan herramientas que escanean otras computadoras para verificar la existencia de vulnerabilidades y aprovecharlas para añadir nuevos miembros al botnet.
5. Una práctica es desarrollar "exploits", definidos por Segu-Info (2009) como "un programa o código que "explota" una vulnerabilidad del sistema o de parte de él para aprovechar esta deficiencia en beneficio del creador del mismo". Los hackers esperan aprovecharse de los usuarios que nunca descargan y aplican los "parchos" y dejan sus computadoras vulnerables para ser accedidas. Mahathi en su estudio Botnet: An Overview and Study (2008) ofrece algunos ejemplos de vulnerabilidades comúnmente explotadas:
    a. NetBIOS en el puerto 139.
    b. LSASS.exe y Crypt32.dll en los puertos 135, 139 y 445.
    c. WebDav en el puerto 80.
    d. Vulnerabilidad de Microsoft Plug and Play (MS 05-039)

6. Puertas traseras dejadas por troyanos o gusanos: Accesos abiertos por malware que permiten el control remoto sin el conocimiento del usuario. Ejemplos: Optix Backdoor, Bagle Backdoor y MyDoom Backdoor.

7. Revelación de contraseñas o uso de programas de fuerza bruta: Usados para lograr acceso a servidores y computadoras en general.

Algunos ejemplos de botnets que se pueden señalar son:.

1. SDBot: Este botnet existe desde aproximadamente hace 5 años y tiene cientos de variantes. La Enciclopedia de Virus de Panda Security (2011) señala que está dirigido específicamente a sistemas Windows. Una de las razones para su popularidad y duración es que fue creado como un malware de código abierto, además de que su autor original proveía apoyo al incluir su información de contacto. Otra razón para su éxito es que SDBot utiliza la ausencia de contraseñas y la pobre seguridad para seguir extendiéndose, así que la mejor defensa contra éste es un sistema con una seguridad adecuada. Una vez infectada la computadora con SDBot, un troyano se conectará con un servidor IRC esperando instrucciones, además de recoger información de la víctima, como el sistema operativo que utiliza y su dirección IP. SDBot coloca una copia de su código en C:\Windows\System32, but SDBot uses the %System% y hace cambios en el registry de Windows.

2. RBot: Es uno de los botnets más complejos y peligrosos. Fue creado en el 2003 y ha ido evolucionando hasta convertirse en uno de los botnets más complejos y peligrosos. Existe con diferentes nombres y funciones, incluyendo acciones aleatorias que hacen más difícil su identificación y es uno de los primeros botnets en utilizar encriptación. Una vez infectada una computadora, el "botherder" puede controlarla de varias formas:

a. Ejecutando archivos a través del Internet.

b. Utilizando claves de videojuegos.

c. Por medio de ataques DDoS ("Distributed Denial of Service").

d. Enviando correos electrónicos.

e. Por medio de una webcam.

La página VSAntivirus (2005) provee una lista con algunos de los nombres por los que se conoce a Rbot:

a. W32/SDbot.worm.gen.g

b. W32.Spybot.worm

c. Worm_RBot

d. Win32/RBot.

RBot aprovecha contraseñas débiles, así como seguridad deficiente. Adicional, aprovecha vulnerabilidades conocidas de los sistemas Windows y de algunas aplicaciones. Una vez instalado, Rbot se copia a sí mismo en el directorio C:\Windows\System32 con los atributos "hidden" y "Read Only" y se comunicará con el "botherder" vía IRC.

3. Agobot: Conocido también como Gaobot y Phatbot, introdujo el concepto de modularidad en el malware, infectando por fases:

Fase 1: Infecta la computadora con el bot y mediante un "backdoor" permite al "botherder" controlar la computadora.

Fase 2: Intenta desactivar procesos del antivirus y otras aplicaciones de seguridad.

Fase 3: Finalmente, bloquea el acceso de la computadora infectada a páginas de Internet relacionadas a seguridad y antivirus.

La página de Trend Micro (2003) menciona algunos nombres con los que se conoce a Agobot:

a. W32/Gaobot.worm

b. Worm_Agobot.Gen

c. W32/Agobot-Fam.

Este botnet se puede propagar utilizando redes P2P como Kazaa, Grokser y Bearshare utilizando nombres que atraen la atención de los usuarios.

4. Spybot: Usman en su presentación Botnets (2006) indica que este evolucionó de SDBot, añadiendo características de spyware. Se propaga aprovechando la pobre seguridad y a través de redes P2P. Una vez instalado, abre un "backdoor" para que el "botherder" pueda enviar comandos, pero también permite enviar spam utilizando IM (SPIM). Impide la instalación del Windows XP SP 2 y desactiva el Security Center de Windows. Algunos nombres por los que se conoce son:

a. Win32.Spybot.gen

b. W32.Spybot.Worm

c. Worm.P2P.SpyBot.Gen.

Algunas medidas que la empresa y los usuarios pueden tomar para prevenir que sus sistemas sean infectados por un botnet son:

1. Monitoreo constante: En el caso de computadoras individuales, es imprescindible utilizar un "firewall" y mantenerlo actualizado. Se deben observar las bitácoras que genera el "firewall" cada dos o tres días para detectar intentos de acceder o acciones sospechosas, además de no ignorar actividades que no sean las normales. Los antivirus y aplicaciones antispyware también ayudan en la prevención y detección temprana de actividades relacionadas a botnets. En el caso de servidores, Xombra Team (2005) recomienda el uso de "honeypots" y proxys, así como estar atentos a las actualizaciones del sistema operativo y aplicaciones de seguridad.
2. Análisis de los puertos, tanto en servidores, como en los clientes. Es importante asegurarse de que los puertos abiertos que no se necesiten se cierren y de que aquellos que deben permanecer abiertos seas monitoreados.
3. Implementación de actualizaciones (los llamados"parchos" del sistema operativo) y corregir vulnerabilidades en aplicaciones.
4. Ajustar la configuración del "firewall" según sea necesario.
5. Revisión general, como por ejemplo:
    a. asegurarse de que las actualizaciones se hayan instalado correctamente,
    b. que el antivirus esté actualizado,
    c. verificar entradas sospechosas en el "registry" de Windows,
    d. atender cualquier otro detalle que pueda levantar una bandera roja indicando que algo no anda bien.
6. Educar a los usuarios en el uso correcto de los recursos y en la seguridad general del sistema y luego reforzar esa educación con políticas claras y concisas de seguridad. Esto incluye:
    a. No acceder a páginas de contenido cuestionable o de software pirateado.
    b. No pulsar en banners, anuncios o "pop-ups".
    c. No instalar aplicaciones sin autorización del administrador del sistema.
    d. Notificar de cualquier irregularidad en el sistema a los técnicos.

e. Asegurarse de que se está utilizando la versión más reciente del navegador (Internet Explorer, Firefox, Google Chrome, Opera).

f. Hacer copias de respaldo frecuentemente.

Conclusión

Los botnets son un problema real y muy serio, que afecta no solamente la banca y las corporaciones, sino también a los usuarios de todo tipo, que utilizan sus computadoras como cómplices en el logro de sus delitos. La academia es un excelente lugar para el desarrollo de investigaciones y soluciones relacionadas con este problema, puesto que cuentan con en la mayoría de los casos con los recursos de hardware. Hay software disponible libre de costo, provisto por organizaciones como GNU, foros y páginas dedicadas al tema de seguridad que presentan recursos e ideas. A los estudiantes de programación, por ejemplo, se les puede asignar la descomposición del malware en su código original con el propósito de estudiarlo para luego desarrollar soluciones para la detección y remoción de malware como parte de sus proyectos de cursos. Los desarrolladores de malware en general son muy diligentes en mejorar sus productos, de la misma forma debemos nosotros ser ágiles en mejorar las soluciones y plantear nuevas alternativas para la prevención de infecciones y en caso de que ya existan, poder removerlas. Por otra parte, la educación sobre el tema a los usuarios es imperativa puesto que la mayoría de los usuarios desconocen el tema de la seguridad en los sistemas. Todas las medidas de seguridad que se desarrollen serán fútiles si el usuario no utiliza las prácticas básicas de seguridad.

Referencias

"Botnet Statistics [2011-03-08]." *Daily Botnet Statistics*. Web. 09 Mar. 2011. <http://botnet-tracker.blogspot.com/2011/03/botnet-statistics-2011-03-08.html>.

Bowden, Mark. "The Enemy Within - Magazine - The Atlantic." *The Atlantic — News and Analysis on Politics, Business, Culture, Technology, National, International, and Food – TheAtlantic.com*.Web. 09 Mar. 2011.

"Cómo es el Sdbot.ftp. – Información De Virus - Panda Security." *ANTIVIRUS - Download - CLOUD - SOFTWARE 2011 - Buy - Protection - News - PANDA SECURITY*.Web. 09 Mar. 2011. <http://www.pandasecurity.com/spain/homeusers/security-info/56244/information/Sdbot.ftp>.

<http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/>.

"'Golden Cash' Network - Rent a Botnet - ZDNet." *Technology News, Analysis, Comments and Product Reviews for IT Professionals | ZDNet*.Web. 09 Mar. 2011. <http://www.zdnet.com/news/golden-cash-network-rent-a-botnet/312957>.

"History of IRC (Internet Relay Chat)." *Daniel.haxx.se -- Daniel Stenberg*.Web.09 Mar. 2011. <http://daniel.haxx.se/irchistory.html>.

"Honeypots (Servidores Trampa) ::." *XombraWebsite * Seguridad Informatica *.* Web. 09 Mar. 2011. <http://www.xombra.com/go_articulo.php?articulo=56>.

Kiran.Kola, Mahathi. "Botnets: Overview and Case Study." *Mercy.edu*. 2008.Web. 2011. <https://www.mercy.edu/ias/kola.pdf>.

"Phishing Statistics - World Phishing." *Avira*. 2011. Web. 2011. <http://row.avira.com/es/threats/section/worldphishing/top/7/index.html>.

"Rbot. Descripción Genérica Del Gusano "Rbot"" *VSAntivirus*. Web. 09 Mar. 2011. <http://www.vsantivirus.com/rbot.htm>.

"Seguridad Informática / Exploit." *Www.segu-info.com.ar / Seguridad Informática / Seguridad De La Información*. Web. 09 Mar. 2011. <http://www.segu-info.com.ar/malware/exploit.htm>.

Usman, Jafarey. "Botnets." *Ucf*.Web. 2011.<http://www.cs.ucf.edu/~czou/CDA6938/Jared1.ppt>.

"What Is A Bot (or Zombie)?" *Internet / Network Security - Tips, Advice and Tutorials About Internet Security and Network Security*. Web. 09 Mar. 2011. <http://netsecurity.about.com/od/frequentlyaskedquestions/qt/pr_bot.htm>.

"What Is a Botnet?" Web. 09 Mar. 2011. <http://www.microsoft.com/protect/terms/botnet.aspx>.

"Worm Agobot." *Trend Micro Threat Encyclopedia | Latest Information on Malware, Spam, Malicious URLs, Vulnerabilities*. Web. 09 Mar. 2011. <http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=WORM_AGOBOT.GEN>."

Zombie Bot - Computer Definition." *Computer, Hacker, Telecom Dictionary Definitions*.Web. 09 Mar. 2011. <http://computer.yourdictionary.com/zombie-bot>.

Radamés Toro Martínez, rtoro@ponce.inter.edu Instructor de Ciencias de Cómputos de la Universidad Interamericana de Puerto Rico –Recinto de Ponce. M.B.A Pontificia Universidad Católica de Puerto Rico.