

Derrotando a los Botnets del Futuro

El siguiente artículo es un extracto de Entendiendo y bloqueando los nuevos botnets, un white paper investigado y escrito por Scott Pinzon, CISSP y Corey Nachreiner, CISSP, del equipo WatchGuard® LiveSecurity®. Para ver una mirada fascinante sobre los botnets, cómo es su evolución y cómo operan hoy en día, descargue una copia gratuita del white paper en www.watchguard.com/whitepapers.asp.

Los botnets constituyen lo último en amenazas combinadas. El código de los botnets incluye casi todas las formas concebibles de software malicioso, desde spyware hasta downloaders, rootkits, generadores de spam, y más. Para responderles como es debido, quienes se defienden de ellos deben utilizar múltiples niveles de seguridad. La buena noticia es que las técnicas avaladas por el tiempo siguen siendo sorprendentemente efectivas contra los botnets. A continuación, sugerimos contramedidas que mitigan en gran manera la probabilidad de que una infección por bots opere desde su red.

1. Instale parches con puntualidad

Los bots pueden utilizar una amplia variedad de exploits para infectar a sus víctimas. Sin embargo, los bots más grandes y exitosos se basan en la explotación de vulnerabilidades que el vendor parcheó entre seis y dieciocho meses antes. En los casos más extremos, hemos visto bots tratando de explotar vulnerabilidades que fueron parcheadas incluso cuatro años antes. No podemos decir por qué las comunicaciones sobre bots y los sistemas de back end se renuevan a un ritmo tan acelerado, mientras que los bots utilizan exploits conocidos y viejos. Nuestra mejor presunción es que los dueños de los bots encuentran los exploits al esperar que los vendors hagan el parche para una vulnerabilidad y luego hacen ingeniería reversa para averiguar cuál era el flanco débil.

Es razonable esperar que explotar los flancos débiles más recientes sea una de las próximas áreas que los dueños de bots mejorarán. Pero, por ahora, hay una buena noticia para el administrador de red promedio. Si instala puntualmente los parches apenas los vendors lanzan las mejoras para el software que tiene en su red, usted se moverá más rápido que los creadores de los bots y resistirá los exploits.

2. Bloquee JavaScript

Cuando un bot de los que se aprovechan de exploits de la Web ataca una computadora víctima, invariablemente lo hace ejecutando JavaScript. Entonces, configurar los navegadores para avisar antes de ejecutar JavaScripts eliminará una gran franja de vectores de infección por bots. Recomendamos enfáticamente hacer que los usuarios utilicen Firefox como navegador primario, y usar el [NoScript plug-in](#) para avisar si un script intenta ejecutarse.

3. Vigile esos puertos

Esta es una recomendación con dos partes.

1) Aunque los últimos bots pueden comunicarse sobre puertos que todo administrador necesita dejar abiertos, la vasta mayoría aún se comunica mediante IRC (puerto 6667) y otros extraños puertos con números altos (como 31337 y 54321). Todos los puertos por encima del 1024 deberían bloquearse, tanto para paquetes entrantes como salientes, a menos que su organización tenga una aplicación en especial o alguna necesidad de abrir un puerto dado. Aún así, usted debe abrir cuidadosamente dicho puerto, e implementar políticas tales como “abrir solamente durante horas laborables” o “denegar todo, excepto el tráfico de la siguiente lista de direcciones IP confiables”. Esta simple medida previene los bots más corrientes y anticuados de alcanzar su Centro de Comandos y Control (C&C) para obtener instrucciones y actualizaciones, y logra esencialmente eliminar tales bots cuando llegan.

2) El tráfico de los botnets que viaja sobre puertos necesarios, como el 80 ó el 7, generalmente traiciona su presencia al generar tráfico donde no debería haberlo. Por lo común, los creadores de los bots actualizan sus zombis entre la 1:00 a.m. y las 5:00 a.m., cuando piensan que nadie los vigila. Habitúese a chequear los logs de los servidores todas las mañanas. Si usted ve actividad de navegadores cuando nadie estaba allí para navegar, es algo que debería investigar.

Los administradores que utilicen los modelos WatchGuard Firebox® estarán felices de saber que los proxies del Firebox detienen los intentos de todo tráfico no estándar de correr sobre puertos estándar. Por ejemplo, el botnet de spam Mega-D corre sobre el no estándar y casero puerto 80 HTTP. El proxy de HTTP del Firebox reconocería y bloquearía este tipo de tráfico instantáneamente, por defecto.

4. Redoble el entrenamiento para la toma de conciencia de los usuarios

Algunos bots hacen un escaneo masivo en Internet, encuentran máquinas vulnerables y las infectan. Esta práctica está actualmente disminuyendo. Hoy es más común que los bots hagan “ingeniería social” en su camino hacia su red, tentando a una víctima para hacer clic sobre un vínculo o a abrir un archivo. Estos bots tienen las mismas restricciones que ciertos vampiros legendarios: no pueden cruzar su umbral a menos que usted los invite a hacerlo.

Este enfoque “engatusador” gradualmente ha adoptado aún más restricciones. Los atacantes acostumbran enviar código malicioso ejecutable como adjunto en un mensaje de correo electrónico. Pero esta práctica también es minoritaria. La mayor parte de la acción hoy está basada en la Web. Los mensajes maliciosos que un par de años atrás hubiesen contenido un adjunto, hoy contienen un enlace hacia un sitio malicioso. Sitios web inocuos pueden ser infectados por Mpack u otro software malicioso subrepticio, para infectar a los visitantes que lleguen por haber hecho clic imprudentemente.

Es su deber explicar a los usuarios, en términos que puedan entender, por qué nunca deben invitar al vampiro a entrar. Dígales que no abran archivos adjuntos que lleguen en forma no solicitada ni esperada; por qué no deben hacer clics en vínculos que lleguen en un mensaje, y por qué deben pensar dos veces antes de clicar cualquier enlace inusual. Si necesita un punto de partida, haga circular un video nuestro que muestra cómo funcionan las descargas oportunistas, descrito para un público no técnico: <http://video.google.com/videoplay?docid=-4094518401580008932>. Si se aplican diligentemente controles como los que hemos citado, se tendrán redes libres de bots por años.

5. Permanezca vigilante

Esta recomendación parece muy obvia para ser mencionada, casi como “¡Trate de no infectarse!”. Sin embargo, siempre nos encontramos con administradores de IT que pasan demasiado tiempo apagando incendios y manteniendo una mesa de ayuda escasa de personal, así que nunca miran los logs de sus sistemas. Nunca monitorean el uso de ancho de banda. No pueden decir quién se está conectando a qué desde sus redes. Y tienen dispositivos conectados en sus redes que ni siquiera saben que están ahí.

Si esto lo describe a usted, todo lo que podemos decir es que está buscándose problemas. Usted podría tener bots en su red mientras lee esto. Si usted es un administrador que rara vez mira sus logs, debería empezar a leerlos. Hoy. Una vez que conozca como es el aspecto “normal” de su red, sólo necesitará 30 minutos al día para hacer el chequeo.

Si esto lo describe, lo más probable es que usted no sea negligente, sino que esté constreñido por la falta de personal y de recursos. Explique la amenaza a sus jefes y vea si ellos lo respaldan para reservar media hora cada mañana para chequear el estatus de su red. Este tiempo debe ser defendido contra pedidos de reuniones, llamadas y otras típicas interrupciones. Esta forma de asegurarse es muy barata en comparación con el costo de comprometer la red.

Creemos que los recientes y sin precedentes brotes de bots sólo preanuncian las innovaciones que están por venir. Como nunca antes en nuestros años en seguridad de Internet, cada mes parece traer nuevos exploits descubiertos que los investigadores no pueden explicar completamente.

Los botnets han sido amenazas combinadas, pero no han sido lo último en amenazas combinadas. Los creadores de los bots ahora suplementan con libertad la tradicional arquitectura de los botnets con componentes adicionales que mejoran la automatización, la administración y la evasión. Estas combinaciones de tecnologías son temiblemente sofisticadas y sorprendentemente pulidas. Cualquier observador puede predecir, sin temor a equivocarse, que esta tendencia no sólo continuará, sino que crecerá.

¿Están ganando los malos? Obviamente no, dado que nosotros estamos aún comprando y utilizando la banca en Internet. Pero el aluvión de actividad de los bots está creciendo, así que debemos revertir la tendencia, contenerlo y revelar las técnicas de sus amos. Una manera simple de minar el poder de un creador de bots es hacer difícil para el código del bot reclutar víctimas. Los dispositivos de seguridad de WatchGuard utilizan numerosas capas de seguridad, aplicadas inteligentemente a lo largo de muchos protocolos, con una poderosa tecnología de proxy que detiene tanto el tráfico entrante como el saliente, para mantener su red a salvo.

Para más información acerca de las soluciones de seguridad de WatchGuard y la protección que ofrecen contra botnets y otras amenazas a la red, visítenos en www.watchguard.com o contacte a su reseller.