

¿De qué lado está? La defensa contra los zombis

Monográfico de Sophos

Noviembre de 2005

Ordenadores secuestrados, o zombis, se ocultan en el seno de redes, desde donde se usan para enviar spam, robar datos confidenciales de empresas y cometer otros delitos graves. Este monográfico describe cómo las empresas se hallan constantemente expuestas a los ataques de esta amenaza en rápida evolución, y cómo los zombis pueden aparecer incluso en redes dotadas de una sólida protección de gateway y de punto final.

También destaca la necesidad de protegerse con una herramienta de detección de zombis y describe cómo el Servicio ZombieAlert™ de Sophos ofrece a los clientes ese nivel adicional de seguridad.

Una amenaza para las empresas

Un zombi es un ordenador que de forma oculta ha sido infectado con un virus y que puede ser controlado por un usuario no autorizado o remoto. Una vez que un equipo ha sido convertido en zombi, el pirata informático o hacker lo conecta a una red de miles de ordenadores infectados y lo utiliza para cometer una gran variedad de delitos. Los piratas informáticos usan las redes de ordenadores zombi para enviar spam, virus, mensajes de pesca de información y pornografía de parte de una organización sin su conocimiento. Sophos estima que hasta un 60% del spam se envía desde equipos secuestrados. Se han hallado equipos zombis en todo tipo de organizaciones, desde empresas financieras hasta universidades pasando por centros hospitalarios. Alteran la actividad empresarial, dañan la red, roban datos confidenciales y perjudican la reputación de la empresa.

- **Alteraciones en la actividad empresarial:** A menudo, los administradores no son conscientes de que hay un zombi en su red hasta que la empresa aparece como fuente de spam en lista negras (DNSBL). Esto puede causar el bloqueo del sistema de correo de la empresa y paralizar así el conjunto de sus actividades habituales.
- **Carga en la red:** Los zombis lanzan ataques para infectar otros ordenadores en una empresa y ralentizan así las redes internas. También se usan para almacenar programas y películas piratas, y para introducirse en otras organizaciones, lo que supone un consumo de recursos de red todavía mayor.
- **Robo de datos:** Datos confidenciales como las bases de datos de clientes y las contraseñas de cuentas bancarias pueden peligrar ante equipos zombis. Ni siquiera las técnicas de encriptación pueden proteger tal información, puesto que un zombi puede instalar programas espía, como los capturadores de teclado, para almacenar las teclas pulsadas antes de enviar los datos a los hackers.
- **Perjuicio de la reputación:** Las acciones ilegales realizadas por los zombis perjudican la reputación,

imagen y valor de la marca de una empresa si es considerada como emisora de spam o como cómplice de otros delitos. Por ejemplo, las redes zombi se usan a menudo para lanzar ataques de denegación de servicio (DDoS), cuando miles de ordenadores acceden a un sitio Web de forma simultánea, lo que sobrecarga los servidores y provoca el bloqueo del mismo.

Rápidos e invisibles

Generalmente, los zombis operan sin el conocimiento del usuario y la magnitud de los daños que causan en una organización pasa de manera desapercibida. Con frecuencia los zombis están programados para mantenerse ocultos, activándose durante breves períodos de tiempo para enviar spam.

Si un equipo no protegido se conecta a Internet, existe un 50% de probabilidades de que se convierta en zombi en 12 minutos.

Además de su carácter oculto, nuevos zombis aparecen con suma rapidez. Según los análisis de Sophos, si un equipo sin protección antivirus o sin cortafuegos se conecta a Internet, existe un 50% de probabilidades de convertirse en zombi en 12 minutos. La velocidad de estos ataques se ilustra en la figura 1. El gráfico muestra cómo aumenta la probabilidad de una infección vírica con el tiempo de conexión a Internet en un equipo no protegido con Windows XP.

Una amenaza en expansión

La velocidad con la que se crean los ordenadores zombi y su capacidad de camuflaje los convierte en una herramienta comercial muy eficaz para los criminales. Los zombis pueden generar considerables beneficios mediante la instalación de adware o robando información confidencial a través de programas espía y de pesca de información. Los zombis

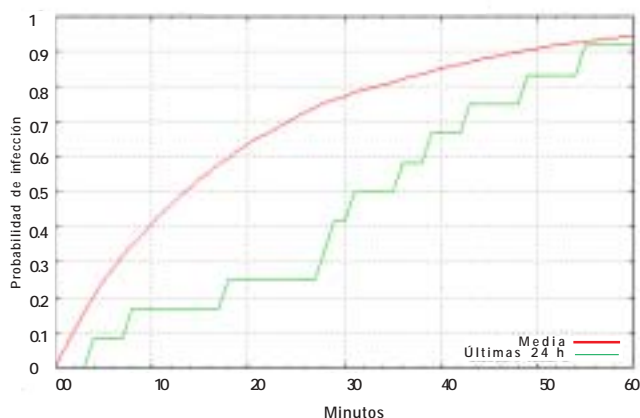


Figura 1: Probabilidad de infección de un ordenador no protegido conectado a Internet

también pueden instalar marcadores telefónicos que conllevarán elevadas facturas telefónicas, o bien pueden utilizarse para extorsionar a empresas con la amenaza de lanzar ataques DDoS. Las redes zombi pueden venderse: en un foro de spammers se ofrecían 20.000 ordenadores por entre 2.000 y 3.000 dólares.¹

Sin embargo, el método más habitual de generación de beneficios gracias a ordenadores zombi es el envío de spam. Las medidas anti-spam son cada vez más eficaces al bloquear mensajes de spam basándose en la reputación del remitente, gracias al uso de listas DNSBL. Las redes zombi responden al uso de estas listas negras enviando spam desde ordenadores secuestrados con una "buena" reputación. Para facilitar el envío de spam, es necesario un abastecimiento continuo de zombis para sustituir aquellos que han sido identificados y desinfectados, o aquellos incluidos en una lista negra.

A medida que las técnicas anti-spam siguen perfeccionándose, los creadores de spam continuarán reclutando nuevos zombis. El reciente y rápido crecimiento del número de virus zombi ilustra este aspecto: de los 300 virus más recientes detectados por SophosLabs™, una red global de análisis de amenazas, más de un tercio incorporaba funciones propias de un zombi.

Cómo se convierte un equipo en zombi

Un ordenador se convierte en zombi cuando en él se instala un bot, o programa automatizado, que permite a un hacker controlar el equipo e introducirlo en una red zombi, o botnet. La instalación de un bot requiere que se abra un puerto de Internet en el ordenador. Las puertas traseras (puertos de Internet abiertos) son creadas mediante virus, gusanos o troyanos al infectar un equipo. Una vez abierta la puerta trasera, se instala el bot, a menudo por el mismo virus, y el equipo se convierte en un zombi. En algunos casos, son los propios hackers quienes, después de buscar puertos abiertos, instalan el bot.

Generalmente, los virus infectan ordenadores y los transforman en zombis aprovechándose de vulnerabilidades en

el sistema operativo. Los virus también se propagan mediante técnicas de ingeniería social, donde un email infectado incita al usuario a ejecutar el código vírico o a visitar ciertas páginas Web. Una vez creados, un método habitual de activación de zombis es programarlos para entrar en ciertos canales de chat IRC. Cuando los hackers teclean un comando específico en el chat, los zombis de "despiertan" y ejecutan sus instrucciones. Los zombis también pueden ejecutar instrucciones preprogramadas. Por ejemplo, en mayo de 2005, el troyano Sober-Q y el gusano Sober-N operaron de forma conjunta para infectar y secuestrar ordenadores en todo el mundo, programándolos para enviar mensajes nacionalistas alemanes en plena campaña electoral.²

Defensa contra un ataque zombi

La protección más eficaz para evitar que hackers obtengan el control de los ordenadores de una red consiste en integrar un sistema de detección de zombis rápido y eficaz en las soluciones de seguridad de punto final y de gateway. No obstante, la protección integrada de estaciones de trabajo, grupos de trabajo, gateway y sistemas remotos continúa siendo el requisito fundamental.

Defensa de la pasarela de correo

La pasarela de correo es la primera línea de defensa de redes contra virus de email, incluidos aquellos que crean zombis. Sophos PureMessage® ofrece una solución fiable de protección integrada del gateway gracias a la tecnología Genotype™, un método único de detección automática de variantes de familias de virus y de campañas de spam.

Proteger la pasarela de correo no es suficiente puesto que los virus la pueden sortear para atacar redes a través de numerosas vías.

Sin embargo, proteger la pasarela de correo no es suficiente puesto que los virus la pueden sortear para atacar una red a través de numerosas vías:

- Internet – algunos gusanos que contienen las funcionalidades de un zombi, como Sasser y Rbot, no se propagan a través del email, sino que se aprovechan de vulnerabilidades en los sistemas operativos o navegadores Web para propagarse directamente a través de Internet.
- Dispositivos móviles – los virus pueden introducirse en las estaciones de trabajo y, por consiguiente, en toda la red, a través de aparatos como unidades de memoria USB, CD-ROM y portátiles que son usados fuera de la empresa y después de nuevo en la red interna.

- Mensajería instantánea– las aplicaciones MI sortean la pasarela de correo y ofrecen así otra vía de acceso a los virus.
- Servidores SMTP ilegítimos – algunos virus se propagan a otras redes usando su propio servidor SMTP que les permite sortear la pasarela de correo. Bofra constituye un ejemplo. Asimismo, una vez que un zombi se ha creado en una red, también puede usar su propio servidor SMTP para enviar spam directamente desde el equipo infectado y evitar así la detección de los sistemas de filtrado en correo de salida.

Protección de punto final y políticas internas

Dado que los ordenadores pueden convertirse en zombis incluso dentro de un perímetro seguro, es esencial que la protección del gateway de redes se complemente con una protección antivirus de punto final como la que ofrece Sophos Anti-Virus®.

Del mismo modo, es vital reforzar esta protección de punto final y de gateway con sólidas políticas internas. Los ataques constantes a los sistemas significan que los zombis pueden originarse a raíz del más mínimo agujero de seguridad, incluso de carácter temporal. Aunque todos los puntos estén protegidos, cualquier descuido en la política de seguridad, como por ejemplo, no actualizar los sistemas operativos con los últimos parches de seguridad, puede permitir el secuestro de ordenadores. Este aspecto es especialmente importante en el caso de redes de gran tamaño y de carácter descentralizado. Los virus pueden introducirse en una organización por los empleados que acceden a la red vía VPN desde casa o por usuarios invitados que se conectan a la red con su propio equipo. En entornos de tal complejidad, no siempre es posible tener el control centralizado de todos los ordenadores, pero basta que un solo ordenador no esté bien protegido o no se actualice frecuentemente para que infecte la red con zombis.

Incluso si todos los puntos están protegidos, cualquier descuido en la política de seguridad puede conllevar el secuestro de un ordenador.

Las políticas internas, así como la concienciación de los usuarios en aspectos de seguridad, y la prohibición del acceso a redes de intercambio de archivos y sitios Web potencialmente infectados juegan un papel importante. Asimismo, el uso de un cortafuegos para bloquear los puertos de Internet entrantes y salientes que no son indispensables para la comunicación ayuda a prevenir que hackers accedan a los equipos. Incluso con una protección fiable y políticas internas estrictas, la velocidad a la que se produce una

infección combinada con la naturaleza heterogénea de las amenazas significa que el riesgo de albergar zombis en la propia red nunca puede descartarse por completo. La última línea de defensa debe ser un sistema de alerta que detecte zombis en la red y ayude a neutralizarlos lo antes posible.

Detección de zombis con el Servicio ZombieAlert

Sophos ZombieAlert es un servicio único que identifica ordenadores zombi emisores de spam en empresas. SophosLabs vigila las amenazas de spam y virus las 24 horas: examina millones de mensajes cada día mediante una red mundial de receptores de spam usados para evaluar, depurar y desarrollar soluciones anti-spam. La visión global de SophosLabs ante las nuevas amenazas permite a Sophos ofrecer una rápida notificación de cualquier equipo zombi detectado en la red de un cliente. El aviso puede llegar en cuestión de minutos después de que SophosLabs reciba un mensaje de spam procedente de su organización.

El servicio ZombieAlert ofrece información inmediata que permite a la empresa afectada identificar, desinfectar y proteger rápidamente sus ordenadores contra futuros ataques. Como se ilustra en la figura 2, las alertas incluyen información sobre la fuente IP, muestras de mensajes y otros datos sobre direcciones IP en la red de un cliente que figura en listas negras (DNSBL). Puesto que ZombieAlert es un servicio de email, el cliente no necesita ninguna infraestructura adicional para soportar el servicio. ZombieAlert incluye soporte técnico 24 horas por teléfono, email y a través del sitio Web.

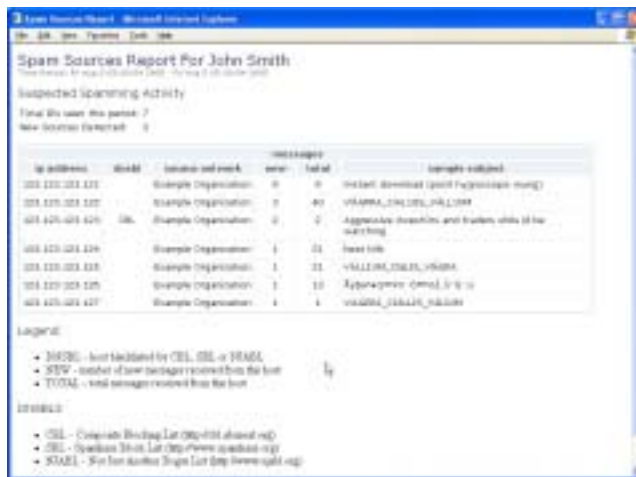


Figura 2: Ejemplo de una alerta del Servicio ZombieAlert de Sophos

Conclusión

Cada vez hay más casos de ordenadores secuestrados en empresas, y el uso de redes zombi tiene cada vez más adeptos entre los criminales. Los zombis son difíciles de

detectar y pueden acarrear daños considerables para las empresas. Las redes no cesan de ser objeto de ataques rápidos, procedentes de orígenes diferentes y que pueden producirse a través de todos los puntos de entrada de la red. El primer nivel de defensa contra los zombis debe ser una solución de seguridad integrada de punto final y de gateway. Sin embargo, la complejidad de algunas redes, combinada con la velocidad e intensidad de los ataques requiere una solución ante cualquier contingencia. El Servicio ZombieAlert de Sophos avisa rápidamente a las empresas de la presencia de ordenadores zombi en su red, lo que les permite integrar su protección con una solución fiable y eficaz en el caso de una infección de zombis.

Para obtener más información sobre Sophos y sobre cómo nuestros productos pueden proteger su empresa, visite www.esp.sophos.com.

Fuentes

- 1 Going price for network of zombie PCs: \$2,000 - \$3,000, Byron Acohido and Jon Swartz, USA Today, www.usatoday.com/tech/news/computersecurity/2004-09-08-zombieprice_x.htm
- 2 Troyano de spam Sober-Q no burla la tecnología Genotype de Sophos, Sophos, 16 de mayo de 2005, www.esp.sophos.com/pressoffice/news/articles/2005/05/va_soberq.html

Acerca de Sophos

Sophos es el líder mundial en soluciones integradas de control de amenazas para empresas, educación y gobiernos. Nuestros productos, caracterizados por su gran precisión y facilidad de uso, protegen a más de 35 millones de usuarios en más de 150 países. Con más de 20 años de experiencia, Sophos cuenta con dedicados técnicos antivirus y anti-spam, y con una red global de análisis de amenazas, para responder con rapidez ante cualquier nueva amenaza – por compleja que resulte – y garantizar así el más alto nivel de satisfacción del cliente.

Boston, EE.UU. • Mainz, Alemania • Milán, Italia • Oxford, BG • París, Francia
Singapur • Sydney, Australia • Vancouver, Canadá • Yokohama, Japón

© Copyright 2005. Sophos Plc.

*Todas las marcas registradas por Sophos.
Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sin la previa autorización escrita por parte del propietario.*

SOPHOS
WWW.SOPHOS.COM