Alerta de la FTC para Consumidores

Comisión Federal de Comercio ■ Negociado de Protección del Consumidor ■ División de Educación del Consumidor y los Negocios

Robots, Piratas y Spam (¡Santo Cielo!)

Botnets and Hackers and Spam (Oh, My!)

Los piratas informáticos y quienes envían mensajes electrónicos masivos no solicitados o *spams* pueden estar utilizando su computadora en este mismo momento. Estos *hackers* y *spammers* invaden secretamente su computadora e instalan a escondidas un software que les permite acceder a su información, incluso a su programa de e-mail. Una vez que logran ingresar a su computadora pueden espiar sus sesiones de navegación en Internet, robar su información personal y utilizar su computadora para enviar *spam* — de contenido potencialmente ofensivo o ilegal — a otras computadoras sin que usted se entere.

A menudo, las computadoras intervenidas de este modo son incorporadas a una red robot, conocida por la abreviatura de "*botnet*". Usualmente, un *botnet*, también llamado "ejército de zombis" *(zombie army)* está compuesto de decenas o cientos de miles de computadoras hogareñas que envían millones de mensajes electrónicos. Los expertos en seguridad de computadoras estiman que la mayoría de los mensajes de tipo *spam* se envía desde computadoras hogareñas que están controladas remotamente y que millones de estas computadoras de usuarios particulares forman parte de las redes robot o *botnets*.

Los *spammers* pueden instalar un software oculto en su computadora de varias maneras. Primero escanean el Internet para encontrar computadoras sin protección y luego aprovechan esas "puertas abiertas" para instalar el software. Los *spammers* pueden enviarle un e-mail con algún documento adjunto, enlace electrónico o imágenes y si usted hace clic en el enlace o abre el documento o archivo adjunto le instalan un software oculto en su computadora. En ocasiones, el solo hecho de visitar un sitio Web o descargar archivos puede causar lo que se llama una descarga encubierta de archivos o *"drive-by download"* que le instala en su computadora un programa malicioso que podría convertirla en un *"bot"*. Las consecuencias pueden causarle más de un simple inconveniente, por ejemplo, su Proveedor de Servicio de Internet (ISP) puede cerrarle la cuenta.

Puede ser difícil determinar si un *spammer* instaló un software oculto en su computadora, pero hay algunos signos de advertencia. Tal vez reciba mensajes electrónicos acusándolo de enviar *spam*; es posible que encuentre mensajes electrónicos en su "bandeja de salida" que usted no envió; o quizás, de repente, su computadora comience a operar a menor velocidad o de manera desesperadamente lenta.

Convertirse en un integrante de un *botnet* no es algo inevitable. Usted puede reducir las probabilidades de convertirse en parte de un ejército de robots — y limitar el acceso a su computadora. Dejar su computadora encendida, conectada al Internet y sin protección es lo mismo que dejar abiertas las puertas de su casa de par en par. La FTC lo alienta a proteger su computadora tomando las siguientes medidas:

- **Use programas antivirus y *anti-spyware* y manténgalos actualizados.** Puede descargar estos programas del sitio Web de su Proveedor de Servicio de Internet o de compañías de software o puede comprarlos en tiendas minoristas. Busque programas antivirus y *anti-spyware* que eliminen los virus o que los coloquen en cuarentena y que se actualicen automáticamente todos los días.
- **Active el software del sistema operativo de su computadora configurándolo para que descargue y actualice automáticamente los parches de seguridad.** Las compañías que comercializan sistemas operativos ofrecen parches de seguridad para reparar las fallas de sus sistemas.

- **Tenga cuidado al abrir archivos electrónicos adjuntados o al descargar archivos de mensajes electrónicos recibidos.** No abra ningún archivo adjuntado a un e-mail — aunque aparente provenir de un amigo o colega de trabajo — a menos que lo esté esperando o conozca su contenido. Si usted envía un e-mail con un archivo adjunto, incluya un mensaje de texto explicando de qué se trata.
- **Utilice un *firewall* para proteger su computadora de los ataques de los *hackers* mientras está conectado al Internet.** El *firewall* es un software o hardware diseñado para bloquear el acceso de los *hackers* a su computadora. La protección ofrecida por el *firewall* es diferente a la de un programa antivirus: El software antivirus revisa los archivos y las comunicaciones entrantes a la búsqueda de virus problemáticos pero un programa *firewall* correctamente configurado lo ayudará a permanecer invisible en Internet y bloqueará todas las comunicaciones entrantes que provengan de fuentes no autorizadas. Es imprescindible que tenga instalado un *firewall* si tiene una conexión de banda ancha ya que la conexión está siempre abierta. La mayor parte de los sistemas operativos (incluso Windows XP y Vista) vienen con un programa *firewall* incorporado, pero es posible que usted tenga que activarlo.
- **Desconecte su computadora del Internet cuando no la use.** Aunque los programas antivirus y *anti-spyware* junto con un *firewall* son elementos cruciales de protección cuando está conectado al Internet, estos programas no son infalibles. Los *hackers* también podrían atacar su computadora cuando está desconectada del Internet.
- **Descargue programas gratuitos únicamente ofrecidos por sitios Web conocidos y confiables.** Puede resultar tentador descargar gratuitamente juegos, programas de archivos compartidos, barras de herramientas personalizadas o algunos otros programas de este tipo. Pero recuerde que muchas de las aplicaciones de estos programas gratuitos contienen otros programas, incluso *spyware*.
- **Controle la carpeta de mensajes enviados o la bandeja de salida de su programa de e-mail para detectar mensajes que no tuvo intención de enviar.** Si encuentra mensajes desconocidos en su bandeja de salida, esto puede significar que su computadora podría estar infectada con un programa espía o *spyware* y que puede formar parte de una red robot o *botnet*. Esto no es infalible ya que muchos *spammers* han aprendido a acceder sin autorización de manera encubierta.
- **Si su computadora se infecta, actúe inmediatamente.** Si su computadora es atacada o infectada por un virus, desconéctela de Internet inmediatamente. Luego haga un escáner completo con un programa antivirus y un *anti-spyware* totalmente actualizados. Reporte los incidentes de acceso no autorizado a su Proveedor de Servicio de Internet y al www.ic3.gov. Si sospecha que alguna de sus contraseñas está comprometida, llame inmediatamente a la compañía correspondiente para cambiarla.
- **Aprenda más sobre cómo proteger su computadora en www.AlertaenLinea.gov.** Este sitio Web frece recomendaciones prácticas brindadas por el gobierno federal y la industria tecnológica para ayudarlo a protegerse contra el fraude en el Internet, mantener su computadora segura y proteger su información personal.

La FTC trabaja en favor del consumidor para la prevención de prácticas comerciales fraudulentas, engañosas y desleales y para proveer información de utilidad al consumidor con el objetivo de identificar, detener y evitar dichas prácticas. Para presentar una queja o para obtener información gratuita sobre temas de interés del consumidor visite ftc.gov/espanol o llame sin cargo al 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. La FTC ingresa todas las quejas relacionadas a fraudes de Internet y sistema de telemercadeo, robo de identidad y otras quejas sobre prácticas fraudulentas a una base de datos segura llamada Centinela del Consumidor *(Consumer Sentinel)* que se encuentra a disposición de cientos de agencias de cumplimiento de las leyes civiles y penales en los Estados Unidos y en el extranjero.

Junio 2007