Diez tecnologías que explotan los delincuentes cibernéticos

Autor: Debra Littlejohn Shinder (10 de julio de 2008)

http://blogs.techrepublic.com.com/10things/?p=380

Traducción para Segu-Info: Raul Batista

Revisión: Lic. Cristian Borghello, CISSP

Fecha Publicación: 20 de julio de 2008

Introducción

Los delincuentes cibernéticos pueden perseguir a sus usuarios de muchas formas, y los resultados pueden ser devastadores. Comparta esta lista con ellos para ayudarlos a que se mantengan alertas en este mundo en línea cada vez más riesgoso.

Las nuevas tecnologías hacen más fácil para todos nosotros hacer nuestro trabajo en línea, comunicarse con otros, y aprovechar las ventajas de todo el entretenimiento basado en Internet que hoy está disponible. Pero muchas de esas mismas tecnologías han hecho más fácil a los delincuentes cibernéticos -los chicos malos que usan la red para propósitos ilegales- poder hacer sus malas acciones. Estamos hablando de hackers, atacantes, spammers, scammers, phishers y otros tipos de criminales.

En este artículo, daremos un vistazo a las 10 tecnologías principales que ellos adoran explotar y veremos cómo se puede proteger, tanto en casa como en su empresa, cuando usa estas tecnologías.

#1: Conectividad de banda ancha

La banda ancha ha llegado a la mayor parte de los Estados Unidos, con cerca de 73 millones de abonados hacia fines de 2007. Esto es más del 50% de los hogares y más del 70% de todos los abonados de Internet. Los expertos predicen que para 2012, más del 70% de los hogares tendrán acceso de banda ancha.

La banda ancha presenta muchas ventajas a los usuarios, incluyendo la alta velocidad y la característica de "siempre en línea" que elimina la necesidad de comenzar sesión en el PSI cada vez que uno quiere acceder a Internet. Pero esas mismas características las hacen también la tecnología perfecta para ser explotada por hackers y atacantes. Teniendo su computadora conectada a la Red 7 x 24 significa que los delincuentes cibernéticos tienen una ventana más amplia de oportunidad para conseguir acceso y robar sus datos, colgar su computadora, u otra cosa que le haga daño. Y la alta velocidad de las nuevas tecnologías de acceso (por ejemplo Verizon ofrece ahora planes de 50Mbps y predicen velocidades de 100Mbps o más en el futuro cercano) implican que programas auto-descargados podrían ser un gran archivo malicioso y entrar en su máquina en apenas unos segundos.

#2: Redes inalámbricas

Otra tecnología que se ha vuelto increíblemente popular es el Wi-Fi, o redes inalámbricas 802.11. Con frecuencia creciente, tanto en el hogar como en las empresas las redes se conectan mediante tecnologías inalámbricas en lugar de cables Ethernet, y los puntos de acceso Wi-Fi proliferan en lugares públicos tales como cafés, aeropuertos, hoteles, y parques públicos. El Wi-Fi ofrece máxima comodidad porque uno puede andar por allí y permanece conectado, pero también lo hace más conveniente al criminal para meterse en su red y dentro de su sistema sin que Ud. siquiera lo sepa, ya que cualquiera con una Notebook inalámbrica dentro del rango de alcance puede interceptar las señales.

A diferencia de sus antiguos homólogos, los nuevos dispositivos inalámbricos usan por defecto el cifrado – pero Ud. debe verificar y asegurarse que el suyo use el cifrado más segura, como la WPA/WPA2/802.11i en lugar de WEP que es fácil de quebrar. También debería usar cifrado fuerte para las aplicaciones que corren en una red inalámbrica (por ejemplo, SSH y TLS/HTTPS). Puede usar una VPN (red privada virtual) o IPSec para cifrar el tráfico que va por la LAN inalámbrica, y debería crear un segmento de red separado para sus comunicaciones inalámbricas si también tiene una LAN por cable. Para mayor información vea http://www.wardrive.net/

#3: Medios removibles

Los disquetes han sido casi completamente reemplazados por lectoras/grabadoras de CD/DVD, lectores de tarjetas flash, y discos USB, pero cualquiera sea, los delincuentes cibernéticos adoran los medios removibles. Si pueden conseguir acceso físico a una computadora, pueden rápida y fácilmente copiar archivos y borrarlos, a menudo sin darse cuenta. Los medios removibles también plantean un riesgo de seguridad porque es fácil perder un disco, un pen-drive, una tarjeta flash o similares.

Puede usar las Políticas de Grupo de Vista o editar el registro en XP para deshabilitar los dispositivos USB. También puede usar programas de terceros para bloquear el uso de cualquier dispositivo E/S mediante puertos USB e IEEE1394 o que usen conexiones inalámbricas BlueTooth. Por ejemplo vea http://www.lumension.com/usb_security.jsp

Si está preocupado por que los dispositivos de almacenamiento removibles o tarjetas se pierdan o sean robadas y con ello accedidos los datos, puede cifrar los datos en memorias flash, CDs y DVDs de forma que uno pueda seguir trabajando con ellos en distintas computadoras pero no un ladrón. Vea por ejemplo http://www.dekart.com/howto/howto_disk_encryption/encrypt_flash_drive_cd_dvd/.

#4: La Web

La Web difícilmente sea ahora una tecnología “nueva”, pero aun es favorita de los delincuentes cibernéticos porque casi todos los que se conectan a Internet usan un navegador Web. Antes cuando la Web era solo texto, navegar era una actividad bastante segura, pero hoy en día se espera que una página Web haga

mucho más, y muchas de ellas ejecutan programas -como Javascripts y controles Active-X- para darle a los usuarios una experiencia multimedia mucho más rica. El problema es que los atacantes pueden usar esas capacidades del navegador para ejecutar programas maliciosos en su computadora.

No se engañe pensando que porque usando un navegador web en particular usted está seguro. Todos los navegadores tienen vulnerabilidades que pueden ser explotadas. Es más importante la configuración del navegador. Si deshabilita Javascript y Active-X para la mayoría de los sitios, le hará más difícil a los atacantes el ingresar a su computadora mediante su navegador (pero probablemente usted no podrá ver apropiadamente algunos sitios). También es importante instalar las actualizaciones de seguridad de su navegador cuando estas sean publicadas.

#5: Correo electrónico y mensajería instantánea

El correo electrónico se está volviendo ubicuo. Prácticamente todos tienen una o más direcciones de correo, y es una de las formas más convenientes de comunicarse. Tiene casi la misma inmediatez que una llamada telefónica o un mensaje instantáneo sin la presión de responder en tiempo real a menos que uno lo desee hacer.

Desafortunadamente el correo electrónico tiene algunas características que los hace atractivo para los delincuentes. Ellos pueden enviar mensajes con direcciones remitente falsas de forma de que sea difícil o imposible conocer el verdadero origen de los mensajes. Así, pueden eludir el haber enviado spam, mensajes phishing, amenazas, pornografía infantil, y otros tipos de correspondencia ilegal.

Los programas de mensajería instantánea también pueden representar una amenaza. Tal como el correo electrónico, los IMers pueden pretender ser otra persona, y la mayor parte de los programas de IM ahora permiten transferencia de archivos, lo que les provee a los delincuentes una forma de descargar programas maliciosos en su máquina.

Las tecnologías para autentificar la identidad de los remitentes de correo electrónico, tales como el Sender ID de Microsoft y el más genérico SPF, pueden resolver el problema de la falsificación -pero solo si todos los propietarios de dominios de correo lo usan. Mientras tanto, puede protegerse con programas de filtrado de spam que le permiten crear una lista blanca o lista de remitentes seguros y siguiendo las mejores prácticas tales como no clickear en los hipervínculos de los correos, ver los mensajes en formatos de solo texto (no correo HTML), no entablar conversaciones por IM o intercambio de archivos con gente que Ud. no conoce.

#6: Comunicaciones Unificadas

Las Comunicaciones Unificadas (UC) son una tendencia popular en el ámbito empresarial, y las compañías están encontrando muchas ventajas en combinar su correo electrónico, telefonía, mensajería Instantánea (IM) y aplicaciones de conferencias de forma que esos programas puedan interactuar unos con otros. Con

la voz sobre IP (VoIP) reemplazando lentamente a los servicios de telefonía tradicional, todas estas tecnologías de comunicaciones pueden correr sobre la misma red.

Sin embargo, esto también significa que ahora sus llamadas telefónicas están sujetas a las mismas amenazas a las que siempre han sido vulnerables sus datos: los paquetes de VoIP pueden ser interceptados o incluso modificados en tránsito tal como cualquier otro dato. Para saber más sobre las amenazas en UC vea http://blogs.techrepublic.com.com/security/?p=406.

Para protegerse en un mundo unificado, use cifrado para proteger la información confidencial importante ya sea texto, voz u otra. También asegúrese que el software de UC se actualice regularmente (junto con el sistema operativo subyacente) y use la autentificación para verificar el origen de los mensajes para asegurarse que no han sido interferidos.

#7: Programas P2P (par a par)

El medio más popular de intercambiar archivos grandes rápidamente a través de Internet es usando programas P2P y redes, tales como BitTorrent, KaZaA, Gnutella, y Napster. La gente los usa para compartir música y películas violando las leyes de derecho de autor, pero también con propósitos legítimos tales como distribuir sus propias fotos y películas caseras. El número de canciones intercambiadas mediante redes P2P es estimado en miles de millones por año.

Los criminales adoran las redes P2P porque pueden falsear el nombre de archivos que comparten y provocar que uno descargue malware (tal como programas que permitirán que el delincuente tome control de su computadora) cuando cree que está descargando una canción. Ya que todas estas redes luchan por proteger el anonimato de los usuarios, los chicos malos tienen poco riesgo de ser capturados.

La mejor forma de protegerse de los peligros del uso de aplicaciones P2P es no usarlos en absoluto.

#8: Comercio electrónico y banca en línea

Más y más de nosotros llevamos cada vez más nuestros negocios por Internet. Es conveniente comprar los que necesitamos desde nuestra casa y que nos sea entregado en la puerta y pagar nuestras cuentas y transferir dinero entre cuentas si siquiera ir al banco. Los delincuentes aman esta tendencia, porque les da más oportunidades de hacerse de nuestro dinero. Pueden interceptar la información que viaja por la red, irrumpir en bases de datos de negocios en línea o instituciones financieras para robar información, o establecer sus propios sitios falsos de comercio electrónico y atraerlo a dar su número de tarjeta de crédito y otra información bajo el pretexto de venderle algo.

Para protegerse cuando compre o haga banca en línea, haga negocios solo con sitios reconocidos y asegúrese que su tráfico Web esté encriptado (su navegador le indicará cuando un sitio es seguro). Navegue a esos sitios en forma directa. (No haga clic en un vínculo de un correo electrónico para entrar allí) No grabe su información de tarjeta de crédito en los sitios Web, en su lugar ingrésela

cada vez. Mantenga vigilada su resumen bancario y de tarjeta de crédito e informe inmediatamente cualquier movimiento sospechoso o no autorizado.

#9: Computación Móvil

La computación se ha vuelto cada vez más móvil y dispositivos que van desde el pequeño teléfono PDA hasta las laptop están siendo usados para almacenar datos importantes y conectarse a la casa y a las redes de las empresas. Debido a su movilidad, sin embargo, estos dispositivos se pueden perder o ser robados fácilmente – y con ello los datos que contienen. Si el dispositivo contiene su información personal, podría Ud. ser objeto de un robo de identidad. Si contiene información de clientes de su empresa, puede poner en riesgo a esos clientes y posiblemente poner en violación de los requerimientos regulatorios a su empresa. Afortunadamente hay una cantidad de formas de protegerse de estas amenazas.

Muchas computadoras portátiles actuales viene con TPMs (Módulos de Plataforma Confiable), que son chips de criptografía basada en hardware que funcionan con tecnologías de software como BitLocker de Microsoft (incluido en algunas ediciones de Windows Vista y Server 2008) para cifrar el disco y prevenir que un ladrón pueda ingresar o acceder a cualquier archivo. Más y más laptops también incluyen software de reconocimiento dactilar y otras medidas de seguridad extra. También se puede instalar software de rastreo que hará que la laptop llame a casa cuando se conecte a Internet si uno falla al ingresar la contraseña correcta.

Muchos teléfonos celulares inteligentes permiten protección por contraseña y se pueden comprar programas de terceros para cifrar los datos en el teléfono. La última versión de Windows Mobile le permite cifrar la información en la tarjeta de memoria sin necesidad de programas de terceros, y uno puede borrar el dispositivo y la tarjeta en forma remota.

#10: Conectividad Universal

Íntimamente relacionado con la movilidad está la conectividad universal. Estamos poniendo no solo nuestras computadoras sino nuestras vidas enteras en línea. Ahora hay aparatos de cocina y maquinas de lavar que pueden conectarse a Internet, equipo de piletas y spa que puede ser accedido en linea y más. Muchos de nosotros tenemos cámaras de vigilancia con servidores Web incorporados, que podemos monitorear desde cualquier parte del mundo en tanto tengamos acceso a una conexión Internet. Toda esta conectividad es maravillosa, pero abre avenidas por las que los delincuentes pueden invadir nuestros hogares si poner nunca un pie adentro.

También nos ponemos en línea a nosotros mismos de otra forma. Tenemos sitios Web personales, cuentas MySpace o Facebook, Second Life, y otros lugares donde revelamos mucho más sobre nosotros de lo que nos damos cuenta. Los delincuentes adoran estas herramientas de redes sociales porque les hace más fácil elegir a sus víctimas y saber sobre ellas, sin verlas.

Precauciones razonables

Entonces. ¿cuál es la solución?. ¿Debemos desconectarnos de la red global, borrar nuestras presencias de la Web, y escondernos en nuestra habitación? Aún si eso fuera posible (y no lo es), la cura podría ser peor que la enfermedad. En el mundo de hoy, funcionar sin la tecnología se hace cada vez más difícil, y una vez que uno se zambulló en la tecnología, la información está "allá afuera" - no hay vuelta atrás.

La clave es un aumento de conciencia y vigilancia constante. Use el sentido común, tal como lo hace en el mundo real. No confíe automáticamente en extraños. No deambule en lugares (físicos o virtuales) donde no conoce el terreno. No divulgue información sensible, como los números de tarjeta de crédito o de cuenta bancaria, números de seguro social fecha de nacimiento, que puedan ser usados para robar su identidad.

La mayoría de los delincuentes cibernéticos son como la mayoría de los predadores: van tras de las marcas fáciles. Tomando algunas precauciones, ud. puede usar las tecnologías que ellos explotan – en tanto las use sabiamente – sin convertirse en una víctima.

Más sobre el ciber-crimen

Puede querer ver este capítulo completo (http://downloads.techrepublic.com.com/abstract.aspx?docid=375520) de Scene of the Cybercrime, 2nd Edition. En él, Deb Shinder y el coautor Michael Cross discuten definiciones de ciber-crimen y categorías, asuntos de jurisdicción, priorizar la aplicación del ciber-crimen, educar a los profesionales de la justicia y a la comunidad de IT, y estrategias para combatir el ciber-crimen.