



INFORME REALIZADO POR LA BUSINESS SOFTWARE ALLIANCE (BSA)
OCTUBRE DE 2008



Software ilegal en internet Una amenaza a su seguridad



Contenidos

Introducción	3
Diferentes formas de piratería de software en internet.....	5
Los riesgos para los consumidores	7
Una mirada más cercana a la piratería en sitios de remate	9
Investigaciones sobre piratería en P2P, sitios web y sitios web de remates	12
Acciones de cumplimiento.....	13
Alianzas de la BSA y su alcance educativo.....	16
Los sitios web de remates deben hacer más para proteger a los consumidores.....	17
¿Qué pueden hacer los consumidores para protegerse?.....	19
¿Cómo reportar software sospechoso de piratería y fraude?	20
Conclusiones	23

Gráficas e ilustraciones

Sitios web de software pirata que también difunden Malware.....	8
Top diez de empresas desarrolladoras de software con productos disponibles en eBay.....	9
eBay: evaluaciones de compra de software.....	10
Top diez de países con mayor número de solicitudes de retiro por piratería en sitios web de remates, primera mitad de 2008	11
Número de sitios de remate en línea dados de baja debido a solicitudes de la BSA.....	11

Introducción

Un empleado de Wagner Resource Group en McLean, Virginia, usó el computador de su oficina para bajar archivos de música y de video de internet mediante LimeWire, el famoso programa P2P.

Desafortunadamente, LimeWire es uno de tantos programas que se usa para intercambiar copias piratas de música, videos y software; y esos archivos contaminados por virus informáticos sirven de ayuda a los delincuentes cibernéticos para llevar a cabo sus fechorías.

En este caso, esta acción del empleado de Wagner inició una terrible reacción en cadena, abriendo las computadoras de la empresa a extraños y exponiendo los nombres, fechas de nacimiento y números de seguro social de aproximadamente dos mil clientes de la empresa, incluyendo a Stephen Breyer, miembro de la Corte Suprema de Justicia de los Estados Unidos. La compañía que Wagner contrató para ayudarlos a contener la fuga de información dijo que entraron más de 12 usuarios de LimeWire en lugares tan lejanos, como Sri Lanka y Colombia, que habían bajado la lista de información personal desde la red de Wagner. " Esto explica por qué hace dos semanas me llegó la cuenta de celular, con AT&T por U\$9000", dijo uno de los clientes de Wagner.¹

Un consumidor en Texas compró en línea software a un

precio considerablemente rebajado. Pero al recibir el producto por correo se dio cuenta de que había un problema. "Para obtener el número de serie y activar el producto, tuve que usar el archivo keygen.exe, que venía incluido en el disco", dijo. El consumidor hizo su propia investigación en internet y descubrió que la aplicación keygen.exe se usa para generar claves o números de serie que se requieren para la activación de software. Estos están disponibles en internet y, a menudo, diversos grupos de piratas los incluyen en paquetes de software. El uso de estos keygens para generar números de serie sin comprar el producto original es ilegal.²

En un día cualquiera, cerca de 1.5 millones de personas alrededor del mundo - 1 de cada 4 seres humanos- se conectarán a internet para comunicarse con amigos, familia y socios comerciales, comprar una buena oferta, investigar para el colegio o la universidad o simplemente buscar entretenimiento. La cifra global de los usuarios de internet creció más de un 300% entre 2000 y 2008.³

Sin embargo, internet tiene un lado oscuro cuando se hace referencia al tema de las estafas en línea que suelen atraer a los consumidores con productos a bajos precios.

AUNQUE EL CONSUMIDOR PIENSE QUE ESTÁ OBTENIENDO UN BUEN PRECIO CUANDO COMPRA SOFTWARE A BAJO COSTO DE UNA FIRMA EN LÍNEA DESCONOCIDA, LO MÁS POSIBLE ES QUE RECIBA UN PRODUCTO DE BAJA CALIDAD Y CON AMENAZAS OCULTAS QUE LO EXPONDRÁ A UN ROBO DE IDENTIDAD Y A LA PÉRDIDA DE MILES DE DÓLARES.

Una de las estafas más comunes involucra programas robados o sin licencia, por ejemplo: software pirata ofrecido a precios con descuento. Aunque el consumidor piense que está haciendo un buen negocio cuando compra software a un buen precio proveniente de una firma en línea desconocida, lo más probable es que reciba un producto de baja calidad y con amenazas ocultas que lo expondrán a un robo de identidad y la pérdida de miles de dólares. Como se describe más adelante, la piratería de software se realiza a través de diversos canales en el mundo en línea; sin embargo la piratería a través de sitios de remate, como e-bay, se torna cada día más desafiante.

El software pirata puede llegar también a implicar al consumidor inconsciente en futuras actividades criminales, a medida que la computadora del consumidor se convierte en un "robot" y es explotada remotamente por el delincuente cibernético. El delito cibernético es perpetrado en escala creciente por el crimen organizado alrededor del mundo. "El delito cibernético ya no tiene que ver con simples cretinos frente a una computadora divirtiéndose a expensas de otros", dice Rob Clyde, Vicepresidente de Tecnología en Symantec. "Son criminales reales, que hacen dinero real gracias a víctimas reales. Y se torna más serio con el transcurso de los días".⁴

El robo y la distribución extendida de software falso muestran que el valor de la Propiedad Intelectual (PI) es atacada alrededor del mundo. Demasiadas personas no tienen conciencia de la forma en la que manejan el software y computadoras al no respetar el valor y el esfuerzo invertido en el desarrollo de los programas o los peligros que puede traer su abuso. Algunas personas actúan como si la copia o el robo de la PI fuera un crimen que no deja víctimas o como si los creadores de trabajos como software, música,

películas y libros pueden ser robados indiscriminadamente y sin consecuencias. Personas que ni siquiera soñarían con robar un disco de música o un paquete de software, van a una tienda en línea a buscar copias o, simplemente, software ilegal.

En el mundo, más de un tercio de todo el software instalado en computadoras personales ha sido obtenido ilegalmente y sus ingresos dejan de ser percibidos por la industria de software, ingresos que están cerca de los U\$40 mil millones de dólares anuales, dinero que podría ser invertido en la creación de nuevos puestos de trabajo o soluciones a las necesidades de las generaciones venideras. El efecto de estas pérdidas también incluye impuestos a ganancias no declarados, que son destinados a la fuerza policial y protección de la sociedad y la construcción de nuevos colegios. Un estudio realizado en el 2008 descubrió que, de reducirse la piratería en el mundo tan sólo en un 10%, en los próximos cuatro años podría generar 600.000 nuevos empleos, U\$141 mil millones de dólares en crecimiento económico y U\$24 mil millones de dólares en recaudación impositiva por encima de las proyecciones actuales.⁵

La BSA ha invertido más de 20 años defendiendo el valor de la PI y persiguiendo a los piratas de software. En la década pasada, esta misión se extendió para incluir en la lista a aquellos que ofrecen software vía ilegal P2P, sitios de remate y toda clase de canales de internet. El siguiente informe describe el alcance y la naturaleza del problema de la piratería en internet y además los pasos que se deben tomar para reducirlo, con un énfasis especial en las estafas que se realizan en los sitios de remates.

Diferentes formas de piratería de software en internet

Antes del surgimiento de internet la copia sin autorización de software requería, por lo general, un intercambio físico de discos u otra plataforma a través del correo o en las calles. Pero a medida que las conexiones de alta velocidad han ido expandiéndose alrededor del mundo, la piratería de software se trasladó de las calles a internet.

Generalmente, la piratería en internet hacen referencia al uso de internet para:

- Proveer acceso a copias de software piratas que se pueden bajar de la red;
- Publicitar y comerciar software pirata que se puede enviar a través del correo u
- Ofrecer o transmitir códigos u otras tecnologías para burlar dispositivos de seguridad anti-copiado.

El proceso puede tener tantos pasos como cualquier otra actividad ilegal. Los compradores pueden ser dirigidos a un sitio web donde eligen y pagan un programa de software y luego recibir instrucciones para ir a otro sitio web y bajar el producto. Este proceso menos directo hace que el pirata sea menos vulnerable a ser detectado.

Las estafas en internet pueden llevarse a cabo a través de diversos canales:

SITIOS WEB DE REMATES: Los sitios de remate en línea se encuentran entre los más populares en la web con millones de personas que se registran diariamente para comprar y vender una amplia gama de productos. Los sitios de remates más conocidos son: e-bay, Ubid, Mercadolibre en Latinoamérica; TaoBao en China y QXL en Europa. Yahoo! opera fuertemente en Hong Kong, Singapur y Taiwán. A la vez que muchos productos se venden en sitios de remates también son objeto de abusos, especialmente cuando se trata de venta de software (más detalles abajo).

PEER-TO-PEER (P2P): La tecnología Peer-to-Peer conecta individualmente usuarios desde una computadora con

otros, sin un punto central de manejo o administración. Para acceder a una red P2P, los usuarios bajan e instalan una aplicación P2P. Millones de individuos tienen programas P2P instalados en sus computadoras, que permiten la búsqueda de archivos en las computadoras de unos y otros y bajar todos los documentos que quieran incluyendo software, música, películas y programas de televisión.

Las redes P2P más populares son: BitTorrent, eDonkey, Gnutella y FastTrack. Aplicaciones P2P pueden ser: BitTorrent, eMule, KaZaa, BearShare y Limewire. En Europa, Medio Oriente Medio y Australia, el tráfico P2P consume entre el 49% y el 89% de todo el tráfico de internet durante el día. De noche puede elevarse a un impresionante 95%.⁶

OTROS SITIOS WEB: Algunas estafas de software en internet pueden ser realizadas a través de sitios web que ofrecen publicidad, como Craigslist, Google o Yahoo!. iOffer.com se describe a sí mismo como una "comunidad de intercambio" en línea, sin remates o tarifas de entrada. Otras estafas ocurren a través de sitios "file-hosting" (alojamiento de archivos) como RapidShare, donde los usuarios pueden subir su contenido, reciben un link y luego proveen ese link a otros usuarios a través de correos electrónicos o avisos en otros sitios web. Encontrar y frenar la piratería de software en dichos sitios web se torna cada vez más difícil en la medida en que el número de dominios de internet y sitios web con base en países extranjeros prolifera. Algunos observadores avanzados de internet proponen que el hecho de permitir bloquear la información de los registros en los nombres de los dominios sobre quien controla el sitio web hace más difícil proteger al consumidor del fraude al que se puede ver expuesto.

LA TECNOLOGÍA P2P SE USA PRIMORDIALMENTE PARA LA PIRATERÍA DE LA PROPIEDAD INTELECTUAL. EN ALGUNAS PARTES DEL MUNDO, EL TRÁFICO DE REDES P2P CONSUME ENTRE EL 49% Y EL 89% DEL TRÁFICO EN INTERNET DURANTE EL DÍA, Y SUBE HASTA UN 95% DURANTE LA NOCHE.

BOTNETS: Las Botnets ilustran la manera como la piratería de software y el delito cibernético está creciendo alrededor del mundo. Estas redes contribuyen a la piratería de software y además a uno de sus más alarmantes efectos colaterales. En términos simples, "bot" es la abreviación de robot, una parte del software programada por un código para realizar tareas repetitivas. En el contexto de un delito cibernético, los delincuentes cibernéticos y/o sus cómplices envían "bots" a través de varias técnicas, que incluyen spam en el correo electrónico y códigos malignos (malware) agregado a software pirata. Los bots y malware infectan la computadora del usuario que ahora se vuelve un "zombi" controlado remotamente. Los zombis afectados pueden ser organizados en una "Botnet" y explotados remotamente por delincuentes cibernéticos para llevar a cabo una variedad de actividades ilegales, que incluyen, albergar archivos para piratería. De acuerdo al FBI, más de un millón de computadoras han sido

agrupadas en botnets,⁷ y los dueños no tienen ni idea de lo que está pasando", dice Dave Marcus, Director de Comunicaciones e Investigaciones de McAfee Avert Labs.

ANTIGUAS FORMAS DE PIRATERÍA EN INTERNET: Todavía se pueden ver varias formas antiguas de piratería en internet, pero están siendo reemplazadas por las técnicas descritas anteriormente. Estas técnicas incluyen el Internet Relay Chat (IRC), que son locaciones en internet para conversaciones multiusuarios, en tiempo real e interactivas; el protocolo de transferencia de archivo (FTP), un lenguaje estándar de computadoras que permite el intercambio y almacenamiento de archivos en forma rápida y fácil; y los Newsgroups, grupos de discusión establecidos en internet que operan como una casilla de correo de acceso público.

Los Riesgos para los consumidores

El comercio en internet es esencialmente ilimitado, auto regulado y anónimo. Los consumidores deben proceder con precaución cuando compran y usan software proveniente de un vendedor desconocido. Usar software ilegal puede poner en riesgo la información, reputación y seguridad financiera del usuario. En el mejor de los casos puede llevar a incompatibilidades de software y virus, generar costos de mantenimiento y dejar al usuario sin soporte técnico ni actualizaciones de seguridad. En el peor de los casos puede costarle al usuario común y corriente cientos y miles de dólares, pérdidas de tiempo y robo de identidad poniendo al descubierto su información personal.

“CUANDO ALGUIEN VIENE A NUESTRO SITIO WEB, HACE SU COMPRA EN LÍNEA, YA SEA CON UNA TARJETA DE CRÉDITO O DÉBITO, SIGNIFICA QUE AHORA, LA PERSONA A LA QUE LE ESTÁS COMPRANDO SOFTWARE PIRATA, TIENE LA INFORMACIÓN DE TU TARJETA DE CRÉDITO O DÉBITO.”

DANNY FERRER, UN PIRATA DE SOFTWARE CONVICTO, QUIEN SE ENCUENTRA ACTUALMENTE CONDENADO A UNA SENTENCIA DE SEIS AÑOS DE CÁRCEL.

Las estadísticas de los riesgos para los consumidores no presagian nada bueno. De acuerdo con una encuesta realizada por Forrester Research en nombre de la BSA, uno de cada cinco consumidores en los Estados Unidos que compró software en línea en el 2006 tuvo problemas. Entre los que tuvieron problemas:

- El 53% recibió software que no correspondía con el que ordenó;
- El 36% reportó que el software no funcionó;
- El 14% de inmediato se dio cuenta de que el software era pirata; y
- El 12% nunca recibió el producto.⁸

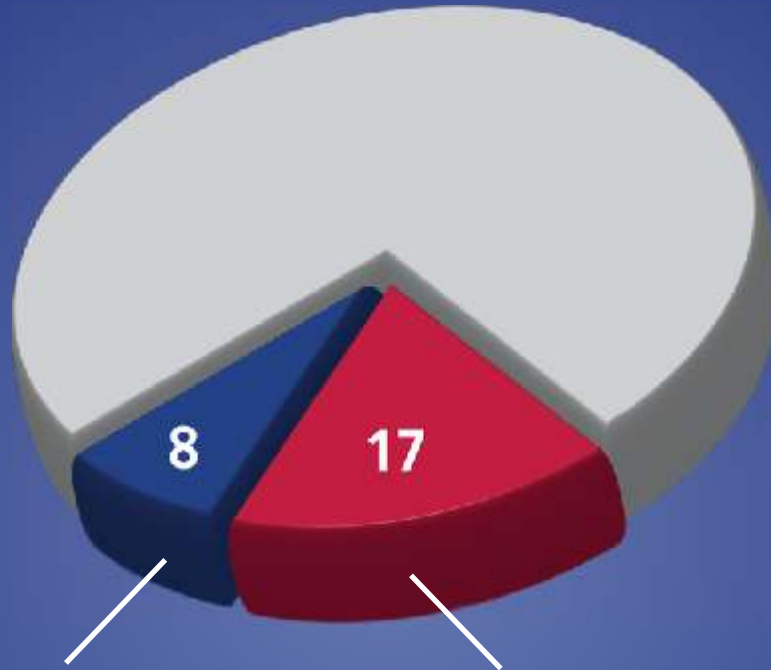
Entre los riesgos que pueden correr los consumidores también se incluyen:

- No recibir actualizaciones, soporte técnico, manuales o documentación;
- Recibir una versión incompleta, alterada o de prueba del software;
- Permitir el acceso de criminales a información personal y financiera; e
- Infectar la computadora del consumidor con virus o herramientas para el delito cibernético controlado de manera remota.

Un reporte hecho en el 2006 por la IDC revela que el 25% de los sitios web que ofrecen acceso a software pirata y herramientas relacionadas con la piratería estaban distribuyendo códigos malignos que pueden poner en riesgo la seguridad de los equipos y su adecuado funcionamiento. En algunos casos los sitios web explotaban las vulnerabilidades en las computadoras de los usuarios para instalar automáticamente software indeseado.⁹

SITIOS WEB DE PIRATERÍA DE SOFTWARE QUE TAMBIÉN DIFUNDEN MALWARE

MUESTRA DE 98 SITIOS WEB



Sitios web con software maligno o potencialmente indeseado.

Sitios web con instancias múltiples de software maligno o potencialmente indeseado.

*SITIOS QUE OFRECEN SOFTWARE PIRATA Y HERRAMIENTAS RELACIONADAS CON LA PIRATERÍA

FUENTE: ESTUDIO DE IDC, RIESGOS POR OBTENER Y USAR SOFTWARE PIRATA, 2006

Una mirada más cercana a la piratería en sitios de remate

Entre las diversas clases de piratería en internet, la piratería en sitios de remate es la más tortuosa porque involucra ventas reales de software a consumidores, en oposición a los otros tipos de piratería, que distribuye copias gratuitas de software a personas lo suficientemente experimentadas como para navegar a través de programas P2P y otros canales de internet.

Ningún programa de software está exento de la amenaza de la piratería en los sitios web de remates. Una búsqueda en los sitios de remates más populares de los programas más vendidos arroja miles de resultados, muchos de ellos con la opción de "cómpralo ahora".

Mientras que nadie ha cuantificado el verdadero alcance de la piratería en sitios de remate con altos niveles de confianza, los estimados se han calculado en el rango comprendido entre el 50% y el 90%. Por ejemplo, en un estudio de 2005 que involucra pruebas de compra de más de 115 copias de software adquiridas en e-bay, el 39% era falsa y el 12% venía con software oculto adicional, que resultó ser falsificado o alterado a partir de software original. Esta información indica que existe menos de una en dos posibilidades de comprar software genuino, en software con licencia de e-bay que no ha sido alterado.¹⁰

Algunos sitios de remates proveen medidas de seguridad limitadas, tales como consejos a los consumidores, comentarios hechos por vendedores, publicados por usuarios, y/o protección contra sitios web indeseados, que consisten en una barra de herramientas que alerta al usuario cuando se encuentra en un sitio web fraudulento. Pero en general los dueños de sitios de remate niegan tener relación alguna con la legitimidad de cualquier producto vendido o transacción realizada en el sitio web.



Al no haber ninguna acción correctiva efectuada por los sitios web de remates para frenar la piratería, lo más seguro es asumir que esta práctica continuará expandiéndose a medida que más y más personas alrededor del mundo se conectan todos los días y aprenden cómo comprar y vender artículos en los sitios web de remates.

Resumiendo, la piratería en sitios web de remates no está en vías de desaparecer y, por el contrario, tiene más posibilidades de emular al popular juego "Whack 'a mole" donde el topo desaparece por un hueco pero reaparece en otro, en la medida en que los piratas continúen trabajando para evadir los sistemas de control.

ESTUDIO DE CASO DE ESTUDIO: eBay

En su posición de líder mundial del mercado en línea, eBay mantiene un alto interés en asegurar que su plataforma de mercado en línea es confiable. En el 2007, eBay registró aproximadamente 84 millones de usuarios activos alrededor del mundo, que comercializaron más de U\$60 billones de dólares en diferentes artículos. Desafortunadamente el sitio es objeto de diversos abusos como lo hizo notar el New York Times, quien se refirió a eBay como el "centro de un nuevo universo de falsificaciones, virtualmente sin vigilancias"

La BSA ha estado trabajando en conjunto con eBay para combatir la piratería de software por aproximadamente diez años, y de hecho, eBay ha tomado una serie de medidas para combatir la piratería. Por ejemplo, eBay prohíbe la venta de "Original Equipment Manufacturer" (OEM) o "regalos" de copias de software que se obtiene como parte de la compra de una nueva computadora- a menos que el vendedor la venda con el hardware

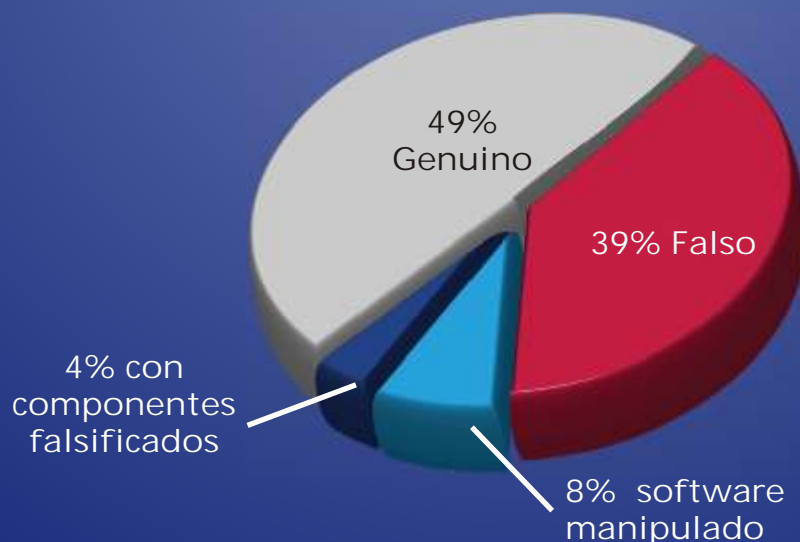
original. Pero eBay no vigila actualmente los listados de productos ofertados en su sitio web y además niega tener la responsabilidad de hacerlo.

Como otra medida, eBay creó el programa "Verified Rights Owner" (VeRO), dando un beneficio a los dueños de derechos de propiedad intelectual que reporten productos en los listados de eBay que se encuentren infringiendo sus derechos. Basados en información brindada por dueños titulares de derechos, eBay investiga pistas sobre posible piratería y remueve de sus listados a posibles violadores de las políticas de VeRO.

Sin embargo, el sistema deja la carga principal del problema -vigilar los listados- a los dueños titulares de los derechos. El programa no está diseñado para proteger al consumidor y los beneficios que le puede brindar a éste son limitados.

1.-" Seeing Fakes, Angry Trades Confront eBay," Katie Hafner, New York Times, Enero 29 de 2006.

eBAY: EVALUACIONES DE COMPRA DE SOFTWARE MUESTRA DE 115



FUENTE: EQUIPO LEGAL DE MICROSOFT, 2006, CITADO EN "LOS RIESGOS DE OBTENER Y USAR SOFTWARE PIRATA" IDC, OCTUBRE DE 2006. MANIPULADO INCLUYE PARTES TANTO GENUINAS COMO FALSAS Y SOFTWARE GENUINO QUE HA SIDO UTILIZADO PARA MANIPULAR.

ESTUDIO DE CASO DE ESTUDIO: iOffer

iOffer se lanzó en 2001 como alternativa a eBay y otros sitios web de remates altamente competitivos. Desafortunadamente tampoco ha sido inmune ante las actividades de los piratas de software y tampoco asume ninguna responsabilidad por la legitimidad de las transacciones en línea efectuadas en su plataforma.

Como respuesta a las preocupaciones sobre piratería, iOffer lanzó C.O.P.S. (Counter Online Piracy System), que permite a los dueños titulares de los derechos de autor remover y/o desactivar el acceso a productos que puedan infringir sus derechos.

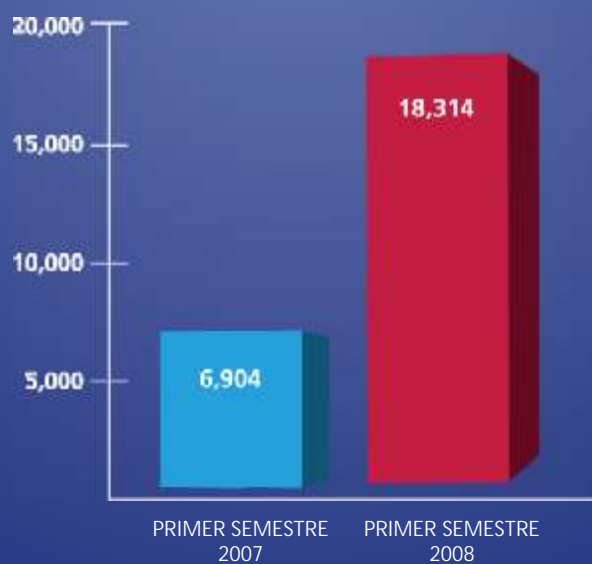
La BSA añadió recientemente a iOffer a la lista de sitios web que son monitoreados contra transacciones ilegales de software y posibles avisos de retiro de la web.

TOP DIEZ DE PAÍSES CON MAYOR NÚMERO SE SOLICITUDES DE RETIRO POR PIRATERÍA EN SITIOS WEB DE REMATES, PRIMERA MITAD DE 2008



FUENTE: BSA

NÚMERO DE SITIOS DE REMATE EN LÍNEA DADOS DE BAJA A SOLICITUDES DE LA BSA



La BSA ha expandido sus esfuerzos para solicitar bajas en remates en línea de software que resulten sospechosas. Las cancelaciones aumentaron un 265% del 2007 al 2008.

FUENTE: INFORMACIÓN DE LA BSA

Investigaciones sobre piratería en P2P, sitios web y sitios web de remates

La industria del software ha trabajado para combatir las estafas en internet por más de una década. La pieza central de los esfuerzos de la BSA es la Online Auction Tracking System (OATS), una herramienta que monitorea permanentemente sitios web de remates y Bit-Torrents (descritos anteriormente) mientras que otra herramienta monitorea la actividad en redes P2P. Estos sistemas identifican a diario miles de casos de actividades sospechosas a diario, en países donde este monitoreo esté permitido por la Ley. La BSA analiza cada caso para determinar si merece o no tomar medidas en el futuro.

Una vez que la BSA identifica la oferta de software ilegal a través de varios sitios web y redes P2P, puede emitir un aviso de "retiro" a los ISPs (Internet Service Providers) pidiéndoles que retiren el software pirata. En la primera mitad de 2007, la BSA envió 471.694 avisos de retiro a diversos ISPs. En la primera mitad de 2008 la BSA aumentó sus esfuerzos y envió 782.832 avisos de retiro.

En el 2007, la BSA lanzó un programa propio que inspecciona las páginas web de manera metódica y automatizada (crawler) para aumentar el impacto en la cadena de intercambio masivo de archivos, además de los avisos enviados ya a nivel de "exigencia" donde sea permitido por la Ley. En la primera mitad de 2008, la BSA envió más de 48.000 avisos relacionados con

archivos de intercambio masivo que estaban siendo usados por 633.000 personas que habían bajado software de miembros de la BSA evaluados en un estimado de U\$525 millones.

Cuando la BSA encuentra que se está ofreciendo software sospechoso en sitios web de remates, envía solicitudes de retiro al sitio para que estos productos sean retirados de sus listados. En el 2007 la BSA solicitó que los proveedores de sitios web de remates cancelen más de 13.800 remates en línea que se encontraban ofreciendo más de 50.500 productos con un valor total de venta al público de más de U\$13.3 millones. Casi dos tercios de los remates que se cancelaron se estaban realizando en sitios web de remates de los Estados Unidos. Durante la primera mitad de 2008, la BSA aumentó sus esfuerzos y solicitó a los proveedores de sitios web de remates que cancelen 18.314 remates que ofrecían 45.000 productos por un valor total de U\$22 millones.

Como lo indica la gráfica de la página 11, el número de remates cancelados en la primera mitad de 2008 se incrementó en casi tres veces en comparación al mismo período de 2007, reflejando el incremento en aumento de los esfuerzos de la BSA por combatir la piratería en sitios web de remates.

Acciones de cumplimiento

Cuando es necesario y apropiado, la BSA entabla demandas civiles para tratar de frenar la piratería en internet, y en algunos casos deriva la acción al Departamento de Justicia de los Estados Unidos (DOJ) para su proceso criminal. Algunos casos pueden acarrear consecuencias muy serias. Los casos por infringir los derechos de autor son procesados federalmente y pueden resultar en multas de hasta U\$250.000 y, en algunos casos, prisión.

Durante la década pasada, la BSA, sus compañías asociadas y otras empresas han brindado una significativa ayuda al DOJ en cientos de juicios abiertos a criminales que estaban operando en estafas en línea de software, en ocasiones con ánimo de lucro y en otros casos sin ánimo de lucro. Varios de estos casos resultaron en sentencias de prisión entre 6 y 9 años y millones de dólares en compensaciones.

Los siguientes son varios casos notables de acciones en contra de la piratería en internet.

Estados Unidos:

GEORGIA: En Julio de 2008, en Savannah, Georgia, una mujer fue detenida vendiendo copias falsificadas de software de Corel en eBay. Una investigación de la BSA demostró que la mujer había vendido más de U\$212.000 en software sin licencia a cientos de consumidores entre Enero y Mayo de 2008. Se le entabló un juicio civil en su contra por U\$250.000.

PENNSYLVANIA: Jon Crain, de Caraopolis, Pennsylvania, operaba cerca de 20 sitios web, distribuyendo en línea copias sin licencia de software sin licencia de Adobe, McAfee, Microsoft y Symantec. Fue ubicado por la BSA en Marzo de 2007 como parte de una acción legal

internacional en contra de cinco piratas de software. Los otros criminales fueron ubicados en el Reino Unido, Austria y Alemania, en muchos de estos casos la BSA fue alertada de la actividad ilegal mediante reportes o quejas de clientes insatisfechos quienes se vieron atraídos inicialmente por los bajos precios a los que se ofrecían los productos.

La BSA demandó a Crain y se entabló un juicio civil en su contra, el cual incluía un pago en calidad de resarcimiento y una solicitud de eliminar todo el software ilegal de sus sitios web.

OREGON: En Julio de 2008, Jeremiah Mondello, un hombre de 23 años nacido en Oregon, fue sentenciado a 4 años de cárcel en una prisión federal por vender más de un millón de dólares en software pirata y distribuir malware por medio de redes de mensajería instantánea para robar información financiera a decenas de consumidores. Luego usó la información de cuentas bancarias robadas para abrir más de 40 cuentas de remates en línea con el nombre de las víctimas y retirar dinero de sus cuentas débito. Además de su sentencia a prisión, los investigadores federales confiscaron sus computadoras y U\$220.000 en efectivo. El Gobierno está autorizado para confiscar su casa y terrenos aledaños.

CALIFORNIA: Nathan Peterson operaba un sitio web con fines de lucro basado en Los Angeles, California, llamado www.backups.net, desde donde vendía copias ilegales de software de Adobe, MacroMedia, Microsoft, Symantec y otros. Una investigación del FBI apoyada por la BSA determinó que Peterson vendió más de U\$20 millones en copias ilegales de software que le generaron una ganancia neta de más de U\$ 5.4 millones.

El DOJ cree que Peterson es el “distribuidor más prolífico de comercio en línea de software pirata que jamás haya sido encarcelado en los Estados Unidos”. Peterson fue sentenciado a 87 meses de prisión y se le ordenó pagar U\$5.4 millones como restitución.

Asia Occidental:

TAIWÁN: En Octubre de 2007, la policía Taiwanesa llevó a cabo una redada a un gran pirata de internet denominado el Taller de Información XYZ, en Kaohsiung, y arrestó a un padre y su hijo, ambos involucrados en piratería. Las autoridades confiscaron 27 quemadores de discos compactos que contenían software de negocios, juegos, música y películas. El valor al público estimado de los bienes era de más de U\$30 millones y los ingresos diarios de los piratas se estimaron en tres mil dólares. La BSA colaboró activamente con la policía en este caso.

TAILANDIA: En Abril de 2008, la policía de Bangkok hizo un allanamiento en las oficinas de www.idsoft.org, un sitio web que ofrecía software falsificado por correo. En la redada la policía arrestó a un pirata de 28 años que operaba el sitio web y confiscó una cantidad significativa de evidencia que incluía grandes cantidades de insumos necesarios para hacer y enviar copias de software, además de 134 discos compactos con software de Adobe, Autodesk y Microsoft.

INDIA: En el 2007, la BSA llevó a cabo acciones civiles en Hyderabad, en contra de SM Technologies, que llevaron a confiscar software pirata valorado en U\$475.000 aproximadamente. Se recuperaron un total de 1.843 discos compactos. Esta fue la segunda vez en

tres años que la compañía fue allanada. En septiembre de 2004 la BSA entabló una demanda criminal en contra de la empresa, que desencadenó en tres allanamientos a tres diferentes lugares de Hyderabad. SM Technologies estaba fabricando “CDs de compilaciones piratas” con productos de Adobe, Autodesk, Microsoft y Symantec y comercializaba el software pirata a través de diversos canales, incluyendo internet, revendedores y venta directa a consumidores.

Europa, Oriente Medio y África:

UCRANIA: En Mayo de 2006, un hombre ucraniano, Maksym Vysochansky, fue sentenciado a 35 meses de prisión por su participación en la venta de copias de software pirata de Adobe, Autodesk, Borland y Microsoft a través de sitios web que el mismo operaba y de eBay. El caso fue uno de los primeros que supuso la extradición en un juicio relacionado a violaciones de la propiedad intelectual. Autoridades de Canadá, Lituania y Ucrania formaron parte de la investigación y la Real Policía Tailandesa colaboró directamente en la captura de Vysochansky, ya que este se encontraba de viaje en Tailandia.

RUSIA: En Abril de 2008, la corte del distrito de Izhevsk impuso un veredicto criminal a un hombre ruso que había creado un FTP en su computadora personal para vender copias piratas de programas de Adobe y Microsoft valorados en más de U\$15.000. La policía local realizó varias compras de prueba desde Titov y coincidieron con las de la computadora del pirata.

ESTUDIO DE CASO DE ESTUDIO: Danny Ferrer

Se pueden ver extractos del video de la entrevista con Danny Ferrer en www.bsacybersafety.com/video

Luego de recibir una pista por parte de la BSA, una investigación del FBI iniciada desde fines del 2002, dio con Danny Ferrer, oriundo de Lakeland, Florida, quien operaba sitios web que vendían software ilegal de Adobe y Autodesk. Ferrer vendió aproximadamente U\$20 millones en productos con derechos de autor en www.BuysUSA.com a precios considerablemente más bajos que los sugeridos para su venta al público. Por ejemplo, software con un valor comercial de más de U\$600 era comercializado por Ferrer a U\$57. Los productos estaban grabados en cd's regrabables y distribuidos por correo. En los discos regrabados,

Ferrer incluía etiquetas con marcas registradas de software legítimo y un número de serie que permitía al comprador activar y usar el producto.

Ferrer ganó más de U\$4.1 millones con su operación, que fueron destinados a comprar vehículos de lujo, aviones, un helicóptero y barcos. Todos estos bienes fueron confiscados por el FBI y Ferrer fue sentenciado a seis años de cárcel en una prisión federal. También se le ordenó pagar más de U\$4.1 millones en restituciones.

ESTUDIO DE CASO DE ESTUDIO: Los Hermanos Robberson

A principios de 2002, la BSA, luego de recibir quejas de diversas compañías de software, inició una investigación a Maurice A. Robberson y su hermano, Thomas Robberson. Luego de revisar los cuatro sitios web reportados como sospechosos, la BSA realizó compras de prueba y llegó a la conclusión que el software que se vendía era pirata. La BSA refirió el caso a la oficina del FBI en Washington del FBI, que condujo la investigación hasta octubre de 2005, cuando se dio por finalizada.

La investigación del FBI determinó que desde fines de 2002, los hermanos Robberson vendieron más de U\$5 millones de productos falsificados. Además de operar cuatro sitios web con fines de lucro, los hermanos Robberson estaban asociados con Danny Ferrer en el manejo de www.buysUSA.com.

Durante el tiempo que manejó los sitios web, Thomas Robberson ganó más de U\$150.000 vendiendo software con un valor de venta al público de casi un millón de dólares. Maurice Robberson, por su parte, ganó más de U\$855.000 vendiendo software con un valor comercial de casi U\$5.6 millones.

En marzo de 2008, Maurice Robberson fue sentenciado a 36 meses de prisión, mientras que su hermano Thomas fue sentenciado a 30 meses. Además se ordenó que ambos fueran sujetos a una libertad condicional de 3 años luego de su liberación y a pagar una suma de restitución.

Alianzas de la BSA y alcance educativo

Más allá de las acciones de cumplimiento, la BSA trabaja en conjunto con varias organizaciones para asegurar un mejor entendimiento de lo que significa la piratería en internet y para educar al público sobre los riesgos de comprar software a fuentes poco confiables en internet.

NATIONAL COMPUTER FORENSICS TRAINING ALLIANCE (NCFTA): En Febrero de 2005, la BSA comenzó a patrocinar analistas forenses del NCFTA. Dicha institución proporciona un sitio de acción colaborativo neutro donde la información crítica y confidencial sobre el delito cibernético -incluyendo la piratería de software- puede compartirse de manera discreta. Es también el ambiente propicio para compartir los recursos entre la industria, la academia y la autoridad competente. Esta sociedad le ha proporcionado a la BSA información vital sobre seguridad cibernética y piratería de software.

NATIONAL INTELLECTUAL PROPERTY LAW ENFORCEMENT COORDINATION COUNCIL (NIPLECC): La NIPLECC es un grupo interdisciplinario responsable de coordinar las actividades domésticas e internacionales de cumplimiento de las leyes de propiedad intelectual en los Estados Unidos. Entre sus miembros están el director de la Oficina de Patentes y Marcas Registradas; el Asistente del Fiscal General de la División Criminal; el Subsecretario de Estado para Asuntos de Economía, Negocios y Agricultura; el Diputado Representante de Comercio de los Estados Unidos; el Comisionado de Aduana, y el Subsecretario de Comercio Internacional. La BSA se encuentra entre las asociaciones de la industria que ha fijado lazos entre sus miembros y los miembros del Departamento de Comercio de los Estados Unidos.

US IPR TRAINING COORDINATION GROUP: La BSA trabaja estrechamente con el US State Department Bureau of International Narcotics y con el Law Enforcement Affairs (INL) y el Bureau of Economic, Energy and Business Affairs (EEB), que dirige el Intellectual Property Rights Training Coordination Group (IPRTCG). El IPRTCG, fundado en 1998, está comprometido con agencias del Gobierno de los Estados Unidos y asociaciones industriales que proporcionan educación, entrenamiento y asistencia técnica a políticos y oficiales extranjeros.

El Departamento de Justicia y Comercio, el Representante de Comercio, el FBI, La Aduana y Protección de Fronteras de los Estados Unidos, la Oficina de Patentes y Marcas Registradas, la Agencia para el desarrollo Internacional y la Oficina de Derechos de Autor, participan en la IPRTCG.

Entre los socios del sector privado se incluyen la Alianza Internacional de Propiedad Intelectual, la Cámara de Comercio de los Estados Unidos, la Coalición Internacional en contra de la Falsificación y otras organizaciones industriales.

BETTER BUSINESS BUREAU: En el 2003, la BSA unió sus fuerzas con el Council of Better Business Bureaus (CBBB) con el fin de educar a los consumidores acerca de los riesgos que corren al comprar software en sitios web de remates. Juntas, las dos organizaciones han llegado a un estimado de 6 millones de consumidores a través de recorridos por los medios, correo directo, publicidad en radio y televisión e iniciativas en línea.

“DON'T GET DUPED”: El sitio web de la BSA “No se deje engañar” ofrece a los consumidores un lugar para contar sus historias de cómo fueron engañados al comprar en línea software ilegal. En los últimos años, más de 400 consumidores escribieron en el sitio web compartiendo sus experiencias. Más de 150 quejas tienen que ver con eBay.

Por ejemplo, muchos consumidores se quejaron de recibir software claramente pirata, a menudo en discos compactos regrabables comprados en tiendas con los títulos escritos a mano, sin códigos de registro ni manuales. En un caso en particular, un consumidor en Texas compró el Adobe Photoshop CS por U\$155 en eBay un programa que tiene un costo al público de U\$650- se dio cuenta que el vendedor canceló su cuenta pocos días después. Luego de varias quejas vía correo electrónico, que no fueron respondidas, eBay le recomendó esperar diez días pasado el cierre del remate para elevar su queja a través de Pay-Pal, la plataforma de pagos. Pay-Pal pudo contactar al vendedor, quien al poco tiempo envió el software por correo. Pero la historia no acaba allí: “Era muy fácil saber que era un programa pirata,” dijo el usuario, “venía en un empaque delgado solamente con un CD grabado adentro y una nota escrita a mano en el disco explicando lo que era. Cuando abrí el paquete y vi su contenido, de inmediato le mandé un correo electrónico solicitándole que me devolviera el dinero”. El hombre nunca recibió su dinero.

Más historias sobre consumidores que fueron engañados se encuentran en el sitio web de la BSA sobre seguridad cibernética: www.bsacybersafety.com

PIENSA ANTES DE COPIAR: En América Latina, la BSA maneja una campaña sobre seguridad cibernética y ética dirigida a los jóvenes entre 8 y 18 años. La pieza central de esta iniciativa es un sitio web “Piensa antes de copiar” (www.piensaantesdecopiar.com) que contiene recursos para los educadores, los jóvenes y sus padres. Por ejemplo, el sitio web contiene lecciones y consejos de profesores acerca de cómo mostrar el valor de la Propiedad Intelectual en los alumnos. Con el tiempo, la BSA espera alentar a los encargados de la educación a incorporar unidades de ética y seguridad enfocadas a internet en los planes educativos de varios países. A la fecha, la campaña se ha presentado en Argentina, Brasil, Colombia, Chile, Ecuador, México, Paraguay, Perú y Uruguay.

VIDEO EDUCATIVO: Para evitar que la gente compre software fraudulento, la BSA desarrolló un video educativo, “El Software Pirata Expuesto: Un Negocio Peligroso Para Compradores y Vendedores.” El video pretende educar a los consumidores sobre la compra segura en línea a la vez que advierte a los vendedores sobre las consecuencias legales que trae la piratería. El video incluye entrevistas con Danny Ferrer, un pirata de software condenado a seis años de prisión (ver caso de estudio); una víctima de fraude de remates en línea; un alto oficial del Departamento de Justicia; un vocero de la BSA; y consejos útiles para prevenir el fraude en contra del consumidor. El video está disponible en www.bsacybersafety.com

BASTA DE PIRATERIA: El portal de denuncias de BSA www.bastadepirateria.com busca promover la legalidad y la conciencia sobre el delito, invitando a los usuarios de América Latina a que denuncien de manera confidencial situaciones de uso ilegal de software. Luego de haber sido lanzada oficialmente al público, la página ha tenido gran acogida en toda la región con más de 5.800 visitas en las primeras semanas.

El gran rompecabezas del crimen en internet

Las estafas en línea de software forman una pieza más en el gran rompecabezas del crimen en internet. En los Estados Unidos, el Centro de Quejas de Crimen en Internet (IC3), una sociedad entre el FBI y el Centro Nacional Contra con el Crimen de Cuello Blanco (NW3C), recibe quejas relacionadas a crimen en internet y deriva los casos a la agencia local, estatal, federal o nacional que corresponda para una posible investigación y acusación.

En el 2007, la IC3 procesó más de 219.553 quejas que abarcan el espectro de crímenes en internet, fraude en sitios web de remates, fraude en tarjetas débito y crédito, correo electrónico no pedido solicitado (spam) y pornografía infantil. Desde las propuestas, la IC3 derivó 90.008 quejas hacia la debida agencia de la ley. La pérdida total, en dólares, de todos los casos referidos a fraude fue de U\$239.09 millones, con un promedio de pérdida de U\$680 por queja. Lo que significa un incremento de U\$198.44 millones en pérdidas totales reportadas en el 2006.

Para más información visite www.ic3.gov

Los sitios web de remates deben hacer más para proteger a los consumidores

Debido al creciente protagonismo que tienen los sitios web de remates en la piratería de software y especialmente a los obstáculos para identificar y combatir dicha piratería, la BSA considera que los sitios web de remates deberían seguir los siguientes pasos para proteger al consumidor:

ASUMIR LA RESPONSABILIDAD: Hasta hoy los sitios web de remates insisten en que la piratería en sus sitios está más allá de su posibilidad de vigilancia. Aunque el desafío es ciertamente profundo y complicado, los sitios web podrán hacer mucho más para proteger al consumidor si trabajaran más de cerca con la industria de software compartiendo información y colaborando para lograr mejores usos.

ADVERTENCIAS: Actualmente las advertencias a los vendedores y compradores de software - si es que siquiera existen- tienden a estar ocultas en áreas difíciles de encontrar de los sitios web. Para lograr un mayor impacto, los sitios web de remates deberían mostrar las advertencias al vendedor en el momento de publicar su producto y al comprador en el momento de ofertar. Estas advertencias podrían aparecer en forma de ventanas emergentes reiterando los riesgos y penalidades que acarrea negociar software pirata.

CALMA AL MOMENTO DE COMPRAR: Varios de los sitios web ofrecen al consumidor la opción de "compre ahora" acortando el proceso de remate favoreciendo la venta rápida a precios bajos. Sin embargo, la velocidad a la que se realizan dichas transacciones hace imposible atrapar a los estafadores. Al reconocer que entre el 50% y el 90% del software en sus sitios web es ilegítimo, los sitios web de remates deberían eliminar la opción de "compre ahora" para venta de software.

¿Qué pueden hacer los consumidores para protegerse?

Como se describe a lo largo de este informe, los consumidores afrontan un serio riesgo de robo de identidad, que sus computadoras se vean involucradas en delitos cibernéticos y muchas otras molestias cuando compran software en línea procedente de dudosas fuentes dudosas. Sin embargo, si los consumidores se arman con la información adecuada pueden evitar las estafas de software pirata y proteger su propio bienestar. A continuación, una lista de consejos para los consumidores:

Actualice su software.

Tome ventaja de las actualizaciones gratuitas que le ofrece la empresa productora del software original, que a menudo contienen “parches” para arreglar problemas o fallas de seguridad que ellos mismos han descubierto en sus productos.

Confíe en sus instintos.

Cuando usted compra software a productores originales, fuentes de marcas reconocidas u otras fuentes en línea que ofrecen condiciones de seguridad, es más probable obtener un producto seguro y legítimo que si lo compra a fuentes anónimas y poco profesionales. Además compare el precio ofrecido por el vendedor en línea con el precio sugerido al público del software. Ya sea que el producto se venda nuevo o usado, si el precio por el software es “demasiado bueno para ser cierto”, probablemente así lo sea.

Busque una “marca de confianza.”

Busque una “marca de confianza” proveniente de alguna organización reconocida para asegurarse que el vendedor en línea sea confiable y posea una clientela satisfecha. Si tiene dudas, busque rasgos que le permitan comprobar la legitimidad del sitio web. Si lo desea, revise un informe del Better Business Bureau en www.bbb.org.

Haga su tarea.

En sitios web de remates, revise la calificación del vendedor o comentarios de otros usuarios. La mayoría de los vendedores legítimos tendrán respuesta de otros usuarios y si son legítimos, casi todos estos comentarios deben ser positivos.

Asegúrese de que es auténtico.

Sospeche de los productos que no incluyan una prueba de autenticidad, como discos originales, manuales, licencias, cláusulas de servicio y garantías. Tenga cuidado con los productos que no se vean genuinos, como aquellos con etiquetas escritas a mano.

Tenga cuidado con las copias de respaldo.

Evite a los vendedores que le ofrecen realizar “copias de respaldo”. Esto indica claramente que el software es ilegal. También asegúrese de chequear la versión del software. Mucha gente recibe versiones educativas o promocionales del software cuando se les asegura que están comprando la versión completa o estándar del producto.

Manténgase alejado de los compilados.

Sea cauto con los compilados de títulos de diferentes empresas productoras de software en un mismo disco. Esta es una clara señal de que el software ha sido pirateado y posiblemente alterado. Cuando compre más de un programa, asegúrese de que cada programa venga en un disco separado.

De ser posible, obtenga la dirección del vendedor.

Recuerde que si no puede contactarse con el vendedor luego de la transacción, no tendrá ningún recurso si el producto resulta ser pirata o no funciona. La BSA recibe numerosas quejas sobre vendedores que resultan imposibles de ubicar tan pronto como se realiza el pago.

Conserve su recibo.

Conserve toda la información que pueda sobre la transacción y el vendedor. Imprima una copia de la orden con el número de confirmación y guárdela con sus registros. Esta información le será de utilidad si el producto resulta ser pirata y se requieren tomar medidas con el sitio web de remates o el sitio web del ente recaudador.

Comprenda las condiciones de la transacción.

Asegúrese de obtener una explicación clara de las cláusulas de la mercancía concernientes al reembolso del dinero o devoluciones, costos de envío y seguridad y privacidad antes de que complete la transacción. Revise las cláusulas de privacidad del sitio web para entender qué tipo de información personal requerirán, así como también cómo se usará y se protegerá su información.

Garantice una forma de pago segura.

Antes de brindar su forma de pago, asegúrese que la conexión de internet que usted use sea segura. La mayoría de los sitios web muestran la imagen de un candado cuando usted se encuentra en un sitio seguro o puede chequear la dirección del sitio web en la barra de direcciones. Si la conexión es segura, la dirección del sitio web estará precedida por https:// en lugar de http://. Preste atención a cualquier ventana emergente que le avise sobre cualquier “certificado de seguridad” inválido.

Sea cauteloso cuando trate con vendedores de software en otros países.

Muchos anillos de delito cibernético tienen base en países del extranjero. Es más, la distancia física, diferencias en el sistema legal, y otros factores pueden complicar las cosas si la transacción no resulta de la manera esperada.

Reconozca y evite el e-mail spam.

Indicadores de que un e-mail pueda ser spam pueden ser que los envía alguien que usted no reconoce, tipografías y/o frases raras en la línea de asunto, y precios que son demasiado buenos para ser verdad. Borre esos e-mails sin siquiera abrirlos y borre con frecuencia su folder de “spam” .

Cómo reportar software sospechoso de piratería y fraude

Los consumidores tienen un rol clave como centinelas ante un posible fraude por internet. Las personas que crean tener información sobre piratería de software o quienes se hayan convertido en víctimas de dicho fraude- se les invita a enviar un reporte confidencial a través de la página www.bsa.org o www.bastadepirateria.com

Conclusiones

La piratería de software puede ser tentadora para aquellos que no están familiarizados con los riesgos. Pero lejos está de ser un crimen inocente y sin víctimas, la piratería expone a los usuarios a niveles inaceptables de riesgos de seguridad cibernética, incluyendo el robo de identidad. También atenta contra el valor de la propiedad intelectual, la cual constituye un valor fundamental para la innovación y la manera en que millones de personas se ganan la vida.

En la economía actual, crecientemente interconectada globalmente, internet ha abierto increíbles nuevas fronteras para comunicarse, comprar, aprender o simplemente divertirse. Al mismo tiempo, el alcance global de internet, su anonimato y velocidad pueden usarse tanto para propósitos perjudiciales como para buenos también. Mientras que internet se mantenga como el frente central en la guerra contra la piratería de software y crímenes relacionados, la BSA continuará elevando el conocimiento del problema y orientará todos sus recursos para empujar hacia atrás el derrotar al enemigo.

Para más información sobre la BSA acerca de la piratería de software en línea, u otro asunto importante relacionado con las tecnologías de la información (TI), visite www.bsa.org.

Notas finales

1. Justice Breyer is Among Victims in Data Breach by File Sharing," Brian Krebs, The Washington Post, 9 de Julio 9 de 2008.
2. Fuentes de la BSA.
3. Cifras estimadas a Mayo 31 de 2008. Estadísticas mundiales en Internet por Miniwatts Marketing Group, <http://www.internetworldstats.com/>.
4. "The fight for Cyber Space:High Tech and Law Enforcement Experts on Defeating Today's Cyber Criminals," BSA, 2007.
5. "2007 Global Software Piracy Study," IDC, Mayo de 2008; "2007 State Piracy Study," IDC Julio de 2008; "Piracy Reduction Impact Study," IDC, 2008, todos disponibles en www.bsa.org.
6. Basado en un estudio del tráfico en internet en Europa, Medio Oriente Medio y Australia entre Agosto y Septiembre de 2007. "Majority of Internet bandwidth consumed by P2P services," Paul Mah, IT News Digest en Tech Republic.com.com/tech-news/?p=1651.
7. "Over 1 Million Potential Victims of Botnet Cyber Crime," Comunicado de prensa del FBI, 13 de Junio 13 de 2007.
8. "National Survey Reveals Consumers Concerned About Safety and Security of Online Shopping," Comunicado de prensa de la BSA, 15 de Noviembre 15 de 2006.
9. "The Risks of Obtaining and Using Pirated Software," IDC, Octubre de 2006.
- 10."The Risks of Obtaining and Using Pirated Software," IDC, Octubre de 2006.



BUSINESS SOFTWARE ALLIANCE
1150 18th Street, NW
Suite 700
Washington, DC 20036
T. +1 202 872 5500
F. +1 202 872 5501

BSA ASIA-PACIFIC
300 Beach Road
#25-08 The Concourse
Singapore 199555
T +65 6292 2072
F +65 6292 6369

BSA EUROPE-MIDDLE EAST-AFRICA
2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom
T +44 [0] 20 7340 6080
F +44 [0] 20 7340 6090

WWW.BSA.ORG

