Revista Digital Universitaria
10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

ARTICULO

EL MERCADO NEGRO DE INTERNET

Rubén Aquino Luna
Coordinador e instructor de la Línea de Especialización Análisis Forense e Implicaciones Legales, e instructor del Plan de Becarios de Seguridad en Cómputo en las materias de Unix/Linux

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Resumen

El uso de Internet como herramienta para facilitar el acceso a diversos servicios de la vida cotidiana conlleva importantes riesgos para proveedores y usuarios, por ejemplo: convertirlos en víctimas de toda una sofisticada y redituable estructura "subterránea" en Internet que opera para aprovechar ilegítimamente los recursos de los equipos de cómputo conectados a ella, y para cometer delitos que pueden afectar directamente a la economía de las personas u organizaciones.

Palabras Clave: bots, malware y exploits.

http://www.revista.unam.mx/vol.9/num4/art24/int24.htm

INICIO

Internet se ha convertido en un medio a través del cual se ofrecen diversos tipos de servicios entre organizaciones e individuos, distribuidos en distintos puntos geográficos del mundo, entre los que se encuentran el correo electrónico, portales web, comercio en línea, banca electrónica, pago de impuestos y servicios, trámites gubernamentales, etc. De esta forma, la red se ha convertido en una parte fundamental de la economía mundial y de la vida cotidiana de muchas personas. Pero en este medio también ocurren actividades y servicios clandestinos o ilegales, por medio de los cuales se obtienen beneficios económicos; se trata del mercado negro de Internet.

Los servicios de dicho mercado están orientados a actividades como el fraude, la venta de productos ilegales, la piratería, la extorsión, etc., que han existido desde hace mucho tiempo, pero ahora encuentran en la red un medio atractivo para ser desarrolladas, debido a la creciente cantidad de transacciones que se realizan en ella y al valor que éstas tienen.

En México, según estimaciones de la Asociación Mexicana de Internet (AMIPCI), el importe de las ventas por comercio electrónico en 2007 fue de alrededor de 765 millones de dólares.

El impacto que Internet tiene sobre las actividades habituales de las personas se puede percibir también en nuestro país, en donde a finales de 2007 había 23.7 millones de internautas[1]. Actualmente, éstos usan cada vez más la red para el comercio electrónico (compra/venta por Internet), pago de servicios y banca electrónica, lo que en muchos casos se ha vuelto indispensable en su vida cotidiana[2]. En México, el 15% de los usuarios de Internet utilizan la banca electrónica[3], es decir, aproximadamente 3 millones y medio de personas.

La red se ha convertido en un objetivo atractivo para personas que buscan afectar a los usuarios y obtener beneficios económicos, ya sea a través del uso de recursos de forma no autorizada o de la comisión de delitos que afectan directamente la economía de las víctimas, como fraudes.

El perfil de los intrusos

Hace algunos años, las historias de hackers parecían lejanas para los usuarios comunes de computadoras, […] estaban relacionadas, por ejemplo, con accesos ilegales y modificación de sitios web de grandes corporaciones o entidades, como la NASA, el FBI, etc., y muchas veces tenían que ver más con movimientos ideológicos como el Hacktivismo, que con un beneficio económico. Los riesgos a los que estaba expuesto el usuario común de computadoras y de Internet eran infecciones masivas de algún tipo de virus o gusano. Sin embargo, también se realizaban actividades ilegales en la red, como el espionaje o el robo de propiedad industrial […]; éstas eran hechas por personas con conocimientos técnicos especializados que prestaban sus servicios a cambio de alguna remuneración económica. Dichas maniobras también estaban dirigidas a grandes compañías. […]

Desde hace algunos años, la perspectiva de la especialización técnica para desarrollar estas actividades ha ido cambiando paulatinamente, debido al crecimiento y desarrollo de Internet. Actualmente, siguen existiendo las amenazas mencionadas […], pero se han desarrollado o reutilizado algunas otras con una perspectiva diferente, ya que no requieren de conocimientos técnicos avanzados y tienen como objetivo el usuario común, cualquiera que tenga un equipo de cómputo.

Hoy por hoy, no se requiere ninguna habilidad extraordinaria para utilizar herramientas que permitan realizar ataques informáticos hacia cualquier sistema en Internet.

1 "Estudio 2007, Usuarios de Internet en México y Uso de Nuevas Tecnologías", AMIPCI.
2 Estudio de hábitos de usuarios en Internet 2007, AMIPCI.
3 Estudio AMIPCI de Banca por Internet en México, 2007

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Como se mencionó, han aparecido nuevos objetivos y destinatarios de los ataques a redes informáticas. […] La capacidad de cómputo de las computadoras personales y el acceso masivo al servicio de Internet de banda ancha han hecho que los recursos de cualquier usuario de Internet se vuelvan valiosos para utilizarlos como herramientas para alojar o lanzar ataques que pueden venderse o rentarse al mejor postor para, potencialmente, realizar actividades clandestinas o ilegales.

Las TI y la economía en línea

La seguridad es fundamental para las transacciones comerciales en Internet, se debe proteger la información transmitida y almacenada en este tipo de operaciones. Algunos de los datos que pueden ser usados para usurpar la identidad o defraudar al usuario son: información de autenticación como usuario, contraseña, NIP, números de tarjetas de crédito. Existe un conjunto de elementos tecnológicos que se utilizan para conformar la infraestructura necesaria para el comercio electrónico y para implementar mecanismos de seguridad que garanticen sobre todo la confidencialidad e integridad de la información en las transacciones y de los usuarios. La seguridad debe estar presente en toda operación de los procesos utilizados para el comercio electrónico, desde la selección y asignación de datos para su validación, pasando por el medio empleado en la transferencia, hasta el almacenamiento de los datos. Igualmente importante resulta la seguridad en la acumulación de datos y el manejo de los mismos, es en éstos dos últimos aspectos donde se encuentran más puntos débiles que son utilizados por intrusos y defraudadores para comprometer recursos o información de la víctima.

Ataques informáticos y actividades clandestinas o ilícitas

Dentro de los principales tipos de ataques masivos que se observan actualmente hacia o en los equipos conectados a Internet, se encuentran: escaneos, infección por bots, envío de correo spam y Phishing Scam.

En los últimos años, la infección por bots es una de las principales actividades intrusivas en Internet. De acuerdo a PandaLabs, alrededor de medio millón de PCs son infectadas por este tipo de software malicioso todos los días. La importancia de los bots en el mercado negro de Internet, radica en que este tipo de software es código malicioso que puede ser utilizado para diferentes actividades por los intrusos. Los bots , llamados también zombies, se alojan en un sistema de cómputo y se conectan a un servidor de Comando y Control (C&C) para recibir instrucciones remotamente; establecen comunicación con el servidor de C&C a través de protocolos diversos como IRC (chat), http (web), mensajería instantánea o P2P (Limewire, Emule, etc.); se pueden alojar en cualquier equipo que esté conectado a la red, para propagar la infección de este tipo de malware, los intrusos hacen uso de la explotación de vulnerabilidades en los sistemas o de la ingeniería social.

La explotación de los sistemas vulnerables se realiza de dos formas principalmente. La primera alternativa es realizar barridos (escaneos) masivos en la red para ubicar sistemas vulnerables y explotarlos posteriormente para alojar el software malicioso (malware). La explotación puede darse utilizando desde herramientas para realizar ataques de fuerza bruta (adivinar contraseñas, por ejemplo), hasta la utilización de exploits de día cero. La segunda alternativa es conseguir que el usuario visite un sitio web malicioso, configurado por el intruso para intentar infectar el sistema del visitante y alojar el malware.

No es indispensable que exista un sistema vulnerable para que el intruso pueda alojar el código malicioso en un sistema de cómputo, ya que también es frecuente utilizar la ingeniería social para este fin: el intruso puede engañar al usuario a través de un sitio o un correo electrónico falsos para convencerlo de descargar un archivo que infectará su sistema. Es frecuente engañar a los usuarios mediante el correo spam, haciéndolo atractivo a través de una noticia amarillista o por el envío de supuestas tarjetas electrónicas. Esta técnica es muy efectiva para infectar equipos de cómputo, ya que muchas veces se puede incluso esquivar la protección antivirus con que cuentan los equipos.

En el caso de los bots, una vez que se alojan en el sistema, se comunican con el C&C, se unen a una botnet y quedan a la espera de instrucciones que pueden ser diversas:

Buscar datos específicos en el equipo infectado, como contraseñas, NIPs o números de tarjeta de crédito.
Espiar las actividades del usuario a través de keyloggers.
Buscar equipos vulnerables en la red local y/o en otras redes.
Realizar ataques a otros equipos (DoS).
Actualizarse a sí mismo para obtener nuevas características, etc.

Todos los equipos conectados a Internet son en alguna medida susceptibles a este tipo de infección.

Por otro lado, un equipo en la red puede también ser vulnerado para alojar los servicios que se rentan en Internet o que son utilizados para proporcionar algún servicio para la cadena de la economía ciber-subterránea. Los equipos conectados a Internet pueden ser vulnerados para, por ejemplo, alojar páginas falsas de entidades legítimas que buscan obtener información personal o de autenticación del usuario. También pueden ser utilizados para alojar datos ilegales que se venden en la red: música, películas, información de tarjetas de crédito, pornografía infantil, etc. Otro uso frecuente es para alojar los servicios de la propia infraestructura que requieren para sus actividades. Así, un sistema puede ser comprometido para alojar un servidor de C&C a través de servicios como IRC, http o P2P.

Elementos del mercado negro de Internet

A través de la observación de patrones de comportamiento de intrusos y defraudadores en línea, de varias partes del mundo, se han podido establecer actividades específicas que se llevan a cabo como parte de la cadena de operación estructural económica que opera "detrás" de Internet y los productos que se ponen a la venta.

Algunas personas desarrollan software para explotar vulnerabilidades en los sistemas y venderlo en el "mercado negro" de Internet al mejor postor. La particularidad es que, a diferencia de quiénes encuentran vulnerabilidades por investigación, éstos no publican sus hallazgos ni se ponen en contacto con el fabricante correspondiente para permitir que la vulnerabilidad sea reparada.

Existe una gran variedad de malware (código malicioso) que se puede utilizar en la red para las actividades que se han descrito, incluyendo: exploits para vulnerabilidades específicas, bots, caballos de Troya, mailers (programas para el envío de spam), etc.

Es posible encontrar software muy fáciles de utilizar y que, por lo tanto, no requieren de una gran habilidad técnica por parte del usuario. Algunos de estos programas son comerciales. Se puede obtener un programa para controlar una botnet a un costo de 400 USD, un caballo de Troya en 30 USD. Por supuesto, también se pueden conseguir crackeados en la red, pero la ventaja de adquirirlos de forma comercial es que incluyen soporte técnico.

Hay otro sector de ese mercado negro que se dedica a comprometer servidores de web para alojar malware, sitios para Phishing Scam o cualquier otra información que pueda ser utilizada dentro de las actividades del "mercado negro" en la red. En estos casos, lo que se "oferta" son las contraseñas de acceso a los servidores para poder instalar lo que el "cliente" requiera.

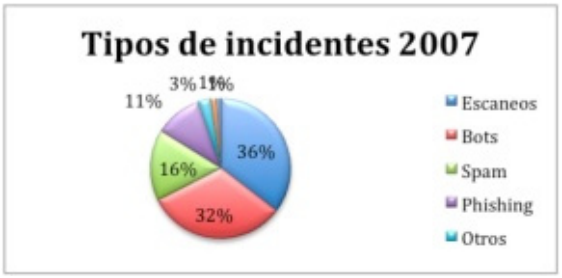
Los sitios web también pueden ser comprometidos para redirigir a los visitantes a sitios maliciosos que busquen infectar el equipo del usuario con bots o caballos de Troya, o bien robarle información específica, como números de tarjetas de crédito o datos de autenticación para banca electrónica. El servicio en este caso consiste en conseguir visitas a los sitios web maliciosos y el costo del mismo puede establecerse de acuerdo a la cantidad de visitas obtenidas.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Por otro lado, quienes comprometen equipos conectados a Internet para infectarlos con bots y unirlos en botnets, rentan la capacidad de cómputo y de control sobre todos los equipos conectados. Se calcula que el costo promedio de una botnet es de alrededor de 0.4 USD por cada equipo controlado. Sin embargo, existe evidencia de casos en que el costo puede llegar hasta los 7 USD. Si tomamos en cuenta que se pueden comprometer hasta medio millón de equipos diariamente, deducimos que el monto de las transacciones en el mercado negro es considerable.

La actividad en México

México no está exento del crecimiento en la actividad clandestina o ilegal relacionada con el mercado negro de Internet. Los problemas observados a nivel global también se presentan en nuestro país. La cantidad de actividad relacionada con fraudes en comercio y en banca electrónica ha crecido en los años recientes. La cantidad de reportes sobre infección de bots y sitios para realizar Phishing Scam, se ha incrementado. Una referencia en este sentido son las estadísticas del UNAM-CERT sobre reportes de incidentes de seguridad informática durante 2007, que están basadas en la actividad observada en RedUNAM y una parte del mercado de Internet en México, a través de la colaboración de UNAM-CERT con otras entidades.



Estadísticas de Incidentes de UNAM-CERT, 2007

Una tendencia observada en fechas recientes, es la regionalización de los ataques informáticos relacionados con fraudes electrónicos. Un ejemplo de ésto es el desarrollo y explotación de vulnerabilidades con el objetivo de afectar directamente a los usuarios de Internet de nuestro país. En diciembre de 2007, por ejemplo, UNAM-CERT identificó la actividad de un exploit para modificar la configuración de ruteadores 2wire[4]. Este tipo de modem ruteador es utilizado por una gran cantidad de usuarios en México. El exploit que se detectó, y que estaba siendo distribuido en la red a través de correos electrónicos con supuestas tarjetas de felicitación, aprovechaba una vulnerabilidad no publicada, lo que indica que se utilizó con fines económicos. De acuerdo con lo observado sobre este vector de ataque, la explotación ha sido manipulada teniendo como objetivo los usuarios de banca en línea de instituciones que operan en México. La modificación en los ruteadores 2wire permite al intruso alterar la configuración para redirigir al usuario a sitios falsos de banca en línea. Esta técnica se conoce como Pharming. Los sitios falsos en este tipo de ataques son en su mayoría de instituciones mexicanas y buscan obtener los datos de acceso de los usuarios para luego defraudarlos, realizando transferencias electrónicas en los sitios legítimos, usurpando la identidad de los usuarios que han sido víctimas.

En el caso de los ruteadores 2wire, se puede establecer la relación entre las diversas actividades clandestinas o ilegales que se desarrollan para realizar el fraude:

Desarrollo y uso de código malicioso (exploit para ruteadores 2Wire).
Intrusión a equipos para alojar sitios para Phishing Scam.
Intrusión a servidores web para alojar malware.

4 Nota de Seguridad UNAM-CERT-2007-001

Envío de correo spam que, a través de ingeniería social, convence al usuario de descargar un archivo que modifica su sistema o la configuración de su ruteador.

Todas estas actividades se realizan con el objetivo de obtener ganancias económicas. En cada una de las etapas hay personas involucradas que están recibiendo una parte de esas ganancias económicas.

Conclusiones

La creciente cantidad de transferencias de dinero de forma electrónica que se realizan en Internet, han convertido a la red y los equipos conectados a ella en un blanco fácil de personas que realizan actividades clandestinas o ilegales con el fin de obtener ganancias y que prestan sus servicios en lo puede denominarse el mercado negro de Internet.

En los últimos meses, se ha observado un crecimiento importante de la economía que gira en torno a la comisión de actividades ilegales o ilegítimas que utilizan las tecnologías de la información. Los delitos que se cometen no son nuevos (extorsión, fraude, etc.), pero ahora hacen uso de las TI como una herramienta para realizarlos. En varias partes del mundo se ha documentado que incluso bandas criminales "tradicionales" están migrando al uso de las TI como alternativa para llevar a cabo sus actividades y ven a los usuarios de las redes informáticas como sus víctimas potenciales, quienes muchas veces no están concientes del peligro que enfrentan al usar los recursos tecnológicos y que pueden caer con facilidad en trampas de defraudadores que hacen uso de algunas técnicas sofisticadas y novedosas, pero también de otras antiguas pero efectivas, como la ingeniería social.

El mercado negro de Internet es un reto para todos los actores involucrados en la operación y uso de las TI, así como para las autoridades encargadas de la procuración de justicia, ya que la proliferación de éste tipo de actividad pone en riesgo el uso de Internet como una herramienta para el desarrollo de la sociedad.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Referencias electrónicas.

Thomas, Rob; Martín, Jerry. "The underground economy: priceless". ;Login;, Diciembre 2006 [en línea]. Disponible en: http://www.usenix.com/publications/login/2006-12/openpdfs/cymru.pdf. [consulta: 24 marzo 2008].

Jianwei Zhuge, Thorsten Holz, Chengyu Song, Jinpeng Guo, Xinhui Han, Wei Zou. "Studying malicious Websites and the Underground Economy on the Chinese Web" [en línea]. Disponible en: http://honeyblog.org/junkyard/reports/www-china-TR.pdf. [Consulta: 24 marzo 2008]

Nota de Seguridad UNAM-CERT-2007-001 [En línea]. Disponible en: http://www.cert.org.mx/nota/?vulne=5534. [Consulta: 25 marzo 2008].

"UNAM-CERT. Distribución de correos electrónicos falsos" [En línea]. Disponible en: http://www.seguridad.unam.mx/pharming.dsc. [Consulta: 25 marzo 2008]

"Estudio de hábitos de usuarios en Internet", AMIPCI. http://www.amipci.org.mx/temp/pdf-031596700119342674OB.pdf

"Estudio 2007, Usuarios de Internet en México y Uso de Nuevas Tecnologías". http://www.amipci.org.mx/temp/Estudio__Amipci_2007_Usuarios_de_Internet_en_Mexico_y_Uso_de_Nuevas_Tecnologias-008216000117941824 1OB.pdf

Proyecto "Honeynet UNAM" [En línea]. Disponible en: http://www.honeynet.unam.mx/es/papers.pl. [Consulta: 25 marzo 2008]

Proyecto "Malware UNAM" [En línea]. Disponible en: http://www.malware.unam.mx. [Consulta: 25 marzo 2008]